BLOCKCHAIN® IN HEALTHCARE TODAY
PLATFORM APPROACHES IN HEALTHCARE

REVISIONES NARRATIVAS/SISTEMÁTICAS/METAANÁLISIS

Ética de Blockchain by Design: Guiando un futuro responsable para la innovación sanitaria

Muthu Ramachandran, PhD[1,2]

[1]Forti5 Tech Ltd., Londres, Inglaterra; [2]Centre for Augmented Intelligence and Data Science (CAIDS), School of Computing, College of Science, Engineering and Technology, University of South Africa, Pretoria, Sudáfrica

Autor correspondiente: Dr. Muthu Ramachandran, Correo electrónico:

muthuram@ieee.org DOI: https://doi.org/10.30953/bhty.v7.362

Resumen

La rápida evolución de la tecnología de cadena de bloques (blockchain) en la atención sanitaria presenta oportunidades inigualables de avance, como la mejora de la seguridad de los datos de los pacientes, los sistemas descentralizados para operaciones fiables y la gestión transparente de la cadena de suministro. Sin embargo, a medida que blockchain reconfigura el panorama sanitario, exige un sólido marco ético que guíe su diseño e implantación. "La ética de Blockchain por diseño" hace hincapié en la incorporación de principios éticos en el corazón de la innovación de blockchain, fomentando la confianza pública, la equidad y los beneficios sociales a largo plazo. En este artículo, el autor propone un conjunto de directrices de buenas prácticas sobre la ética de blockchain by design.

Resumen en lenguaje sencillo

Este artículo explora los retos éticos y las oportunidades del uso de la tecnología blockchain en la sanidad, haciendo hincapié en la necesidad de un diseño responsable. Blockchain no sólo puede mejorar la seguridad de los datos, la transparencia y la confianza de los pacientes, sino que también plantea problemas de desigualdad, acceso y consecuencias imprevistas. El autor propone un marco ético para guiar el desarrollo y el uso de la cadena de bloques en la sanidad, garantizando que se ajuste a principios como la equidad, la inclusión y la responsabilidad. Al implicar a diversas partes interesadas y dar prioridad al diseño centrado en el ser humano, este estudio pretende fomentar una innovación que beneficie a la vez que minimiza el daño. Las conclusiones ponen de relieve la importancia de tener en cuenta la equidad y el impacto social en la tecnología sanitaria.

Este estudio es conceptual y no incluye datos empíricos ni aplicaciones de casos concretos. El marco ético propuesto se basa en una síntesis de la literatura existente y en un análisis teórico, que puede no captar toda la diversidad de perspectivas o complejidades del mundo real en la implementación de sistemas blockchain en diversos contextos sanitarios. El trabajo futuro debe considerar estudios específicos de campo, despliegues prácticos e investigación impulsada por las partes interesadas para validar y refinar el marco, asegurando su aplicabilidad en diversos entornos sanitarios.

Recibido: 12 de noviembre de 2024; Aceptado: 26 de noviembre de 2024; Publicado: 16 de diciembre de 2024

El imperativo ético en el desarrollo de Blockchain

Las aplicaciones de blockchain en la sanidad, desde registros de pacientes inmutables hasta la gestión eficiente de ensayos clínicos, ilustran su potencial transformador[1,2]. Sin embargo, este potencial plantea importantes retos éticos, como la privacidad de los datos, la autonomía del paciente, la gobernanza y la accesibilidad. Como destacan Zwitter y Boisse-Despiaux[3], los marcos éticos son esenciales para garantizar que las tecnologías emergentes no perjudiquen inadvertidamente a los pacientes.

Para desarrollar sistemas éticamente sólidos, blockchain debe dar prioridad a la protección de datos, el acceso equitativo y las estructuras de gobernanza transparentes. Shah y De Filippi[4] sostienen que la permanencia de los datos, un rasgo distintivo de la inmutabilidad de blockchain, genera preocupaciones éticas en torno al derecho de los pacientes a modificar o eliminar sus datos. Los mecanismos que respetan la autonomía individual al tiempo que mantienen el sistema

la transparencia y la seguridad son fundamentales. La figura 1 ilustra dimensiones éticas clave como la privacidad, la seguridad, la gobernanza, la soberanía de los datos y la inclusión, mostrando su naturaleza interconectada dentro de un sistema sanitario de cadena de bloques.

Las dimensiones éticas del diseño de la cadena de bloques (privacidad, seguridad, gobernanza, soberanía de los datos e inclusión) están profundamente interconectadas. Como se ilustra en la figura 1, la eficacia de los marcos éticos se basa en abordar estas dimensiones de forma holística y no de forma aislada. Cada componente influye en los demás y les da forma, lo que subraya la necesidad de un planteamiento global e integrado del diseño ético de la cadena de bloques.

La figura 1 ilustra el concepto de *cadena de bloques ética en la sanidad*, organizado en un modelo circular que enfatiza principios y resultados interconectados. En su centro está la idea principal: aprovechar la tecnología de cadena de bloques para abordar los retos éticos de la atención sanitaria. Alrededor de este núcleo están *las dimensiones éticas básicas* que sustentan su aplicación, incluyendo (acceso controlado por el paciente a sus datos), *Seguridad* (cifrado e identidades descentralizadas para la protección), *Gobernanza* (contratos inteligentes que permiten el consenso de las partes interesadas), *Inclusividad* (garantizar la accesibilidad multi-guía), y *Soberanía de Datos* (cumplimiento de las leyes de jurisdicción local para el almacenamiento de datos). Estas dimensiones éticas conducen a *resultados* tangibles, como una mayor *confianza del paciente* en el sistema, el *cumplimiento de la normativa* y una mayor *accesibilidad* para los usuarios. Este modelo proporciona un marco holístico para integrar blockchain en la atención sanitaria de forma ética y eficaz. Al integrar estos valores en el núcleo tecnológico, las partes interesadas pueden garantizar que las soluciones de cadena de bloques en la sanidad defiendan la transparencia, la equidad y los derechos humanos, fomentando la confianza pública y mejorando los resultados para los pacientes.

Privacidad, seguridad y descentralización

La privacidad y la seguridad siguen siendo primordiales en las aplicaciones sanitarias de cadenas de bloques. Dagher et al.[5]sostienen que la protección de los datos de los pacientes frente a violaciones y usos indebidos requiere métodos criptográficos sólidos y mecanismos descentralizados de control de acceso. Sin embargo, la descentralización plantea problemas de responsabilidad compartida y gobernanza entre los participantes en la red. Kumar et al.[6]proponen que los marcos éticos deben incorporar controles como claves cifradas, seudonimización y contratos inteligentes basados en el consentimiento.

Las arquitecturas descentralizadas capacitan a los pacientes mediante la transparencia y el control de los datos. Sin embargo, como señala Wer-bach[7], los sistemas descentralizados suelen plantear cuestiones éticas en relación con la gobernanza y la rendición de cuentas. Las organizaciones autónomas descentralizadas (DAO, por sus siglas en inglés) pueden ofrecer modelos de gobernanza democrática que hagan hincapié en la equidad, la responsabilidad y la aportación de diversas partes interesadas. La incorporación de principios de explicabilidad para los sistemas basados en blockchain, como se explora en Ramachandran,[8,9]es esencial para garantizar que las decisiones tomadas por los procesos autónomos puedan ser entendidas y evaluadas por las partes interesadas.

Alineación con la normativa internacional

Garantizar que los sistemas blockchain se ajustan a la normativa internacional es vital para su implantación ética y legal en la asistencia sanitaria. Marcos como el Reglamento General de Protección de Datos (RGPD) en Europa y la Ley de Portabilidad y Responsabilidad del Seguro Médico de 1996 (HIPAA)[10]en Estados Unidos proporcionan directrices estrictas para la protección de datos y la privacidad. Al cumplir estos requisitos normativos, los sistemas blockchain pueden defender principios éticos y fomentar la confianza entre las partes interesadas.

Cumplimiento del GDPR: Almacenamiento fuera de la cadena y consentimiento del paciente

El GDPR exige que los individuos tengan control sobre sus datos personales, incluido el "derecho al olvido", que entra en conflicto con la naturaleza inmutable de blockchain[11-13]. Para conciliar esto, los marcos éticos de blockchain pueden adoptar

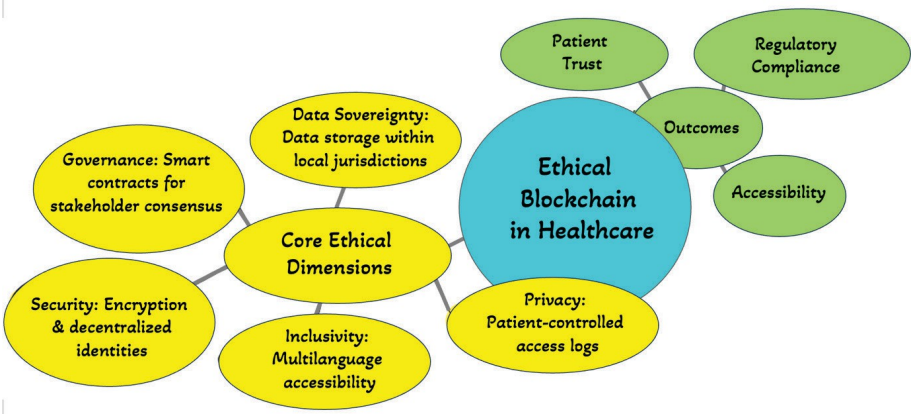

Fig. 1. Dimensiones éticas de blockchain por diseño en la sanidad.

Citación: Blockchain en la sanidad hoy 2024, **7**: 362 - https://doi.org/10.30953/bhty.v7.362

almacenamiento fuera de la cadena para los datos sensibles. En este modelo, sólo se almacenan referencias o hashes de los datos en la cadena de bloques, mientras que los datos reales residen en un almacenamiento seguro y modificable fuera de la cadena. Si los datos deben actualizarse o eliminarse, el hash queda obsoleto sin alterar la integridad de la cadena de bloques.

Los mecanismos de consentimiento de los pacientes son otra característica de la cadena de bloques que cumple el GDPR. Los pacientes pueden conceder o revocar el acceso a sus historiales a través de contratos inteligentes, lo que garantiza un consentimiento explícito e informado para cada transacción de datos. Por ejemplo, un paciente podría permitir el acceso a sus datos de salud para una duración o propósito específicos, alineando la funcionalidad de blockchain con los principios de transparencia y responsabilidad del GDPR.

Cumplimiento de la HIPAA: Cifrado y acceso autorizado

La HIPAA se centra en la protección de la información sanitaria protegida (PHI, [por]sus siglas en inglés), exigiendo salvaguardias como el cifrado y los controles de acceso basados en funciones[14].Los sistemas de cadena de bloques admiten intrínsecamente *el cifrado*, garantizando que la PHI solo sea accesible a las partes autorizadas. Las técnicas avanzadas, como *la encriptación homomórfica*, permiten a los proveedores sanitarios realizar cálculos sobre datos encriptados sin exponer información sensible, manteniendo el cumplimiento de las normas de seguridad de la HIPAA.

Además, *las redes de cadenas de bloques autorizadas* permiten un acceso basado en funciones. A diferencia de las cadenas de bloques públicas, los sistemas con permisos garantizan que sólo los interesados verificados, como proveedores de atención sanitaria, pacientes y aseguradoras, puedan interactuar con los datos. Los contratos inteligentes mejoran aún más el cumplimiento automatizando los permisos de acceso, garantizando el cumplimiento de la norma mínima necesaria de la HIPAA.

Estudio de caso: El sistema nacional de blockchain de Estonia

Estonia se ha convertido en un líder mundial en sistemas de salud impulsados por blockchain, proporcionando un ejemplo práctico de cumplimiento normativo en acción[15].El sistema de salud electrónica del país utiliza blockchain para asegurar más del 95% de los datos de salud de los ciudadanos. Al integrar *el almacenamiento fuera de la cadena* para los datos sensibles y el registro basado en blockchain para la transparencia del acceso, Estonia adapta su sistema al RGPD al tiempo que garantiza la confianza de los pacientes. Los ciudadanos pueden saber quién ha accedido a sus datos y con qué fin, lo que ejemplifica un enfoque de la implantación de blockchain centrado en el ser humano.

Soberanía de los datos, inclusión y rendición de cuentas

La soberanía de los datos es fundamental para las aplicaciones éticas de la cadena de bloques. Haque et al.[16]y Lindman et al.[17]afirman que los pacientes deben controlar sus datos y decidir su uso, fomentando la confianza y la autonomía. La inclusión también debe ser un principio rector, que garantice que la cadena de bloques beneficie a todas las poblaciones y no agrave las disparidades existentes en la atención sanitaria (por ejemplo, las desigualdades en el acceso a la atención sanitaria).

(por ejemplo, marcos como el Quality Framework for Explainable Artificial Intelli-gence (AI))[17,18]ofrecen herramientas para garantizar la accesibilidad y la participación equitativa.

La rendición de cuentas sigue siendo un reto crítico en los sistemas descentralizados, en los que la responsabilidad de las decisiones está dispersa. Raval[19]afirma que los marcos éticos por diseño deben incluir estructuras claras de rendición de cuentas para garantizar que los participantes de la red se adhieran a las normas establecidas.

Directrices de buenas prácticas para la ética de Blockchain By Design

Para apoyar el desarrollo ético de la cadena de bloques en la atención sanitaria, Ramachandran[8,9,18]propone las siguientes buenas prácticas, basadas en investigaciones y marcos establecidos, como el marco de ingeniería de software seguro y sostenible para aplicaciones de cadena de bloques de atención sanitaria (S^3EF-HBCA)[5]y los marcos de cadena de bloques de IA,[18]que incluyen los siguientes conceptos.

Principio de propiedad de los datos y consentimiento

Los pacientes deben mantener la propiedad de sus datos y conservar el control sobre su uso e intercambio. Los sistemas de gestión del consentimiento en tiempo real integrados en aplicaciones sanitarias basadas en blockchain ofrecen una forma de garantizar la autonomía del paciente.

Mecanismos de preservación de la privacidad

La incorporación de protocolos criptográficos y medidas de seguridad que preserven la privacidad garantiza que los datos de los pacientes sigan siendo confidenciales y seguros.[5]El marco S3EF-HBCA se centra en sistemas blockchain sanitarios sostenibles y seguros.[8]

Acceso equitativo e inclusión

Lindman et al.[17]afirman que los sistemas blockchain deben ser accesibles para todas las poblaciones, y que mitigar las disparidades en la atención sanitaria y garantizar la inclusividad es un valor fundamental. Esto concuerda con los principios éticos esbozados en los marcos de IA explicable para garantizar la interpretabilidad y la equidad en la toma de decisiones[9].

Gobernanza transparente y responsable

Los mecanismos de gobernanza deben ser transparentes y permitir la participación democrática de todas las partes interesadas[3,7].Los marcos éticos deben dar prioridad a los modelos de gobernanza descentralizados e inclusivos, como las DAO.

Interoperabilidad y diseño sostenible

Los sistemas deben integrarse perfectamente con la infraestructura sanitaria existente sin comprometer la seguridad o la sostenibilidad. Enfoques como los marcos integrados de IA y cadena de bloques pueden mejorar la interoperabilidad del sistema al tiempo que promueven el intercambio seguro de datos[18].La figura 2 ilustra las "Mejores

Fig. 2. Directrices de buenas prácticas para la ética de blockchain que ilustran el marco interconectado, destacando las dimensiones y prácticas éticas clave.

Fig. 2. "Directrices de buenas prácticas para la ética de blockchain" en la atención sanitaria, representadas como un marco interconectado que destaca dimensiones y prácticas éticas clave.

Las mejores prácticas propuestas para el desarrollo ético de blockchain en la atención sanitaria proporcionan un marco integral para guiar el diseño, la implementación y la gobernanza de los sistemas basados en blockchain. Al defender los principios de propiedad de los datos, privacidad, acceso equitativo, gobernanza transparente e in-teroperabilidad sostenible, estas directrices garantizan que la tecnología blockchain se aproveche de manera que empodere a los pacientes, proteja la información sensible y promueva servicios sanitarios inclusivos y responsables. A medida que crece la adopción de la cadena de bloques en el sector médico, el cumplimiento de estas consideraciones éticas será crucial para aprovechar todo el potencial transformador de esta tecnología, salvaguardando al mismo tiempo los derechos y el bienestar de los pacientes. La investigación en curso y la colaboración entre las partes interesadas de la sanidad, los tecnólogos y los especialistas en ética serán esenciales para seguir perfeccionando y operacionalizando estas mejores prácticas, dando forma en última instancia al desarrollo ético de blockchain en el ámbito de la sanidad.

Conclusión: Hacia un futuro ético de la cadena de bloques en la sanidad

"Ethics of Blockchain By Design" hace un llamamiento a desarrolladores, profesionales sanitarios, responsables políticos y partes interesadas para que colaboren en la innovación ética. Tsanidis[20]propone que integrando la ética en cada fase del diseño y la regulación del sistema blockchain, podemos proteger la autonomía del paciente, fomentar la confianza y maximizar el potencial de blockchain para el bien social.

La ética no es un obstáculo para la innovación, sino un cataclismo para el desarrollo responsable de la tecnología. Garantiza que los sistemas de blockchain estén en consonancia con la dignidad humana, defiendan la misión de "no hacer daño" y mejoren los resultados sanitarios en todo el mundo. A través de un diseño reflexivo, una gobernanza ética y una evaluación continua, podemos construir soluciones de cadena de bloques que sirvan realmente a las necesidades de los pacientes.

Futuras líneas de investigación

Aunque la cadena de bloques ofrece un potencial transformador para la atención sanitaria, la ampliación de las soluciones éticas a escala mundial presenta retos importantes. La investigación futura debe centrarse en varias áreas clave.

Citación: Blockchain en la sanidad hoy 2024, **7**: 362 - https://doi.org/10.30953/bhty.v7.362

Ampliación de las soluciones éticas a escala mundial

La implantación de la cadena de bloques en diversos sistemas sanitarios requiere la adaptación a distintos niveles de infraestructura, madurez tecnológica y marcos normativos. La investigación debe explorar marcos de blockchain modulares y adaptables que puedan adaptarse tanto a entornos de altos como de bajos recursos. Esto incluye la simplificación de los procesos de despliegue y la reducción de costes para garantizar la accesibilidad.

Integración de la cadena de bloques con la IA y el Internet de los objetos

La integración de blockchain con tecnologías emergentes como la IA y el Internet de las Cosas (IoT) promete mejorar la interoperabilidad y el análisis predictivo en la atención sanitaria. Sin embargo, deben abordarse consideraciones éticas, como la parcialidad de los modelos de IA o los riesgos para la privacidad de los datos de los dispositivos IoT. Los estudios futuros deben centrarse en el diseño de marcos de gobernanza que equilibren la innovación con las salvaguardias éticas. Por ejemplo, las herramientas de diagnóstico basadas en IA pueden utilizar blockchain para compartir datos de forma segura y garantizar la transparencia de los modelos.[18]

Abordar la equidad y la brecha digital

Las soluciones de blockchain corren el riesgo de exacerbar las desigualdades existentes si las poblaciones desatendidas carecen de acceso a la tecnología o la infraestructura necesarias. La investigación debe dar prioridad a diseños de blockchain inclusivos que aborden la *brecha* digital:

1. Redes con poco ancho de banda.
2. Diseñar interfaces fáciles de usar para poblaciones con escasos conocimientos digitales.
3. Asociarse con gobiernos y organizaciones no gubernamentales (ONG) para subvencionar el acceso a herramientas sanitarias basadas en cadenas de bloques.

Al abordar estas áreas, la comunidad sanitaria puede impulsar el potencial de blockchain y garantizar que sirva como herramienta ética y equitativa para la innovación sanitaria mundial.

Financiación

El autor no ha recibido apoyo de ninguna organización para el trabajo presentado.

Relaciones y actividades financieras y no financieras

Este artículo es una contribución individual del autor. No hay relaciones relevantes que comunicar.

Colaborador

El autor es responsable de todos los aspectos del artículo.

Aplicación de texto generado por IA o tecnología relacionada

Se utilizó ChatGPT4o para comprobar errores gramaticales, reescribir y corregir algunas secciones de este artículo.

Declaración de disponibilidad de datos (DAS), intercambio de datos, reproducibilidad y repositorios de datos

Los datos que respaldan las conclusiones de este estudio están disponibles abiertamente en la literatura publicada.

Referencias

1. Kuo T-T, Kim H-E, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applica-tions. J Am Med Inform Assoc. 2017;24(6):1211-20. https://doi.org/10.1093/jamia/ocx068
2. Engelhardt MA. Hitching healthcare to the blockchain: the prom-ise and the challenges. Blockchain Healthc Today. 2017;1:1-10.
3. Zwitter A, Boisse-Despiaux M. Blockchain para la acción humanitaria y la ayuda al desarrollo. J Int Hum Assist. 2018;3(1):16. https://doi.org/10.1186/s41018-018-0044-5
4. Shah S, De Filippi P. Blockchain y privacidad de datos: el papel de la confianza y la transparencia en el manejo ético de datos. J Inform Tech-nol Ethics. 2020;15(1):75-88.
5. Dagher GG, Mohler J, Milojkovic M, Marella PB. Ancile: pri-vacy-preserving framework for access control and interopera-bility of electronic health records using blockchain technology. Sustain Cities Soc. 2018;39:283-97. https://doi.org/10.1016/j.scs.2018.02.014
6. Kumar S, Smith R, Liao J. Privacy-preserving health informa-tion exchange with blockchain technology. Health Inform J. 2018;24(4):352-68.
7. Werbach K. La blockchain y la nueva arquitectura de la confianza. Cambridge, Massachusetts: MIT Press; 2018.
8. Ramachandran M. S3EF-HBCAs: secure and sustainable soft-ware engineering framework for healthcare blockchain applica-tions. Int J Blockchain Healthc Today. 2023;6:286. https://doi.org/10.30953/bhty.v6.286
9. FACTA UNIVERSITATIS. Series: Electronics and Energet-ics Vol. 37, No 1, March Wales: IET Press; 2024, pp. 169-193. Inglaterra y Escocia. Consultado el 10 de noviembre de 2024. https://doi.org/10.2298/FUEE2401169
10. Ley de Portabilidad y Responsabilidad de los Seguros Sanitarios de 1996. LEY PÚBLICA 104-191, 104º Congreso [Internet]. Assistant Secretary for Planning and Evaluation; 1996 [citado el 29 de noviembre de 2024]. Disponible en: https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996
11. Voigt P, Von dem Bussche A. The EU general data protec-tion regulation (GDPR): a practical guide. Cham: Springer International Publishing; 2017.
12. Zyskind G, Nathan O, Pentland A. Descentralización de la privacidad: uso de blockchain para proteger los datos personales. San José, CA: IEEE Security and Privacy Workshops; 2015, pp. 180-184. https://doi. org/10.1109/SPW.2015.27
13. Finck M. Blockchain y el reglamento general de protección de datos: ¿pueden cuadrar los ledgers distribuidos con la Ley de Protección de Datos de la UE? Eur Data Protect Law Rev. 2019;4(1):38-68.
14. McGhin T, Choo KKR, Liu CZ, He D. Blockchain en aplicaciones de atención médica: desafíos y oportunidades de investigación. J Netw Comput Appl. 2019;135:62-75. https://doi.org/10.1016/j.jnca.2019.02.027
15. Anthes G. Estonia: un modelo para el gobierno electrónico. Commun ACM. 2015;58(6):18–20. https://doi.org/10.1145/2754951
16. Haque A, Milstein A, Fei-Fei L. Iluminando los espacios oscuros de la asistencia sanitaria con IA y blockchain: ética y eficacia. J Health Ethics. 2021;17(2):45-61.

17. Lindman J, Rossi M, Tuunainen VK. Opportunities and risks of blockchain technologies in healthcare: a systematic review. Telemat Inform. 2017;34(2):199-207. Boston, MA. https://doi.org/10.24251/HICSS.2017.185
18. Ramachandran M. AI and blockchain framework for healthcare applications. Facta Univ Ser Electr Energ. 2024;37(1):169–93. https://doi.org/10.2298/FUEE2401169R
19. Raval S. Aplicaciones descentralizadas: Aprovechando la tecnología de cadena de bloques de Bitcoin. O'Reilly Media; 2016.
20. Tsanidis C. Marcos éticos para la gobernanza de blockchain. Technol Soc. 2019;21(3):49-63.