Artículo original

El *Blockchain*, propuesta de ciberseguridad para la infraestructura telemática de la salud cubana

Blockchain, a Cybersecurity Proposal for the Telematics Infrastructure of Cuban Healthcare

Inglis Pavón de la Tejera[1*] https://orcid.org/0000-0001-7464-4640

Nubia de la Tejera Chillón[2] https://orcid.org/0000-0002-1635-9304

Germán Del Rio Caballero[1] https://orcid.org/0000-0002-9857-9596

Sergio Daniel Cano Ortiz[3] https://orcid.org/0000-0003-0049-6256

Ariadna Velázquez Ricardo[1] https://orcid.org/0000-0001-6695-4251

[1]Universidad de Ciencias Médicas. Santiago de Cuba, Cuba.

[2]Universidad Latinoamericana de Medicina. La Habana, Cuba.

[3]Universidad de Oriente. Santiago de Cuba, Cuba.

[*]Autor para la correspondencia: iptcuba@infomed.sld.cu

RESUMEN

Introducción: En el año 2008 el criptógrafo Satoshi Nakamoto presentó el BITCOIN. En sus escritos Nakamot permite realizar un estudio del funcionamiento de esta tecnología.

Objetivos: Evaluar e implementar la tecnología *Blockchain* como una solución de ciberseguridad para la infraestructura telemática del Sistema Nacional de

Salud de Cuba, con el enfoque en la gestión eficaz de la seguridad de la información y la mitigación del ciberterrorismo.

Métodos: Se realizó un estudio analítico sobre la tecnología *Blockchain* y su aplicación en sistemas sanitarios telemáticos. Incluyó una revisión exhaustiva de sus políticas, protocolos y estructura, en relación con las legislaciones recientes en Cuba y las políticas de ciberseguridad. Además, se desarrolló un modelo estructurado para su implementación en los servicios de salud, a partir del seguimiento de los estándares HL7 y el respeto a la soberanía tecnológica.

Resultados: Se presentan dos alternativas de las muchas existentes según la prueba de consensos analizados sobre la capacidad de adaptarse a los procesos de desarrollo informático personalizados. Se propone un diseño estructural para el desarrollo sintáctico y operacional de la tecnología *Blockchain* y los factores decisores, en función de su posible implementación en los procesos informáticos del Sistema Nacional de Salud en Cuba.

Conclusiones: Se muestra una propuesta de un diseño estructurado y dos alternativas criptográficas para dar solución a las políticas de ciberseguridad y seguridad de la información en el sector de la salud, teniendo en cuenta el principio de soberanía tecnológica como estrategia gubernamental y la interoperabilidad con los estándares HL7.

Palabras clave: *Blockchain*; tecnología; estándares HL7; ciberseguridad; salud.

ABSTRACT

Introduction: In 2008, cryptographer Satoshi Nakamoto introduced BITCOIN. In his writings, Nakamoto allows for a study of the functioning of this technology.

Objective: To evaluate and implement Blockchain technology as a cybersecurity solution for the telematics infrastructure of the Cuban National Health System, focused on effective information security management and cyberterrorism mitigation.

Methods: An analytical study was conducted on Blockchain technology and its use in telematic healthcare systems. It included a comprehensive review of its policies, protocols, and structure, in relation to recent Cuban legislation and cybersecurity policies. In addition, a structured model was developed for its implementation in healthcare services, based on adherence to HL7 standards and respect for technological sovereignty.

Results: Two of the many existing alternatives are presented based on the analyzed consensus test regarding their adaptability to customized IT development processes. A structural design is proposed for the syntactic and operational development of Blockchain technology and the decision-making factors, based on its potential implementation in the IT processes of the Cuban National Health System.

Conclusions: A structured design and two cryptographic alternatives are proposed to address cybersecurity and information security policies in the healthcare sector, taking into account the principle of technological sovereignty as a government strategy and interoperability with HL7 standards.

Keywords: Blockchain; technology; HL7 standards; cybersecurity; health.

Recibido: 02/02/2024

Aceptado: 02/11/2024

Introducción

El alto nivel tecnológico que se muestra en la actualidad está condicionado por el desarrollo escalonado de las Tecnologías de la Información y las Comunicaciones (TIC). Este desarrollo se evidencia en la interoperabilidad multisectorial en todos los ámbitos. A inicios del presente siglo, se proyectó un

desarrollo exponencial de las tecnologías telemáticas, lo que propició que en la segunda década se proclamara la Cuarta Revolución Industrial (Revolución 4.0). Este fenómeno ha traído consigo nuevos conceptos que han permitido un salto cualitativo y cuantitativo en la tecnología y su aplicación en la sociedad.

En este contexto surge una línea de desarrollo criptográfico que predispone cambios significativos en los métodos de intercambio y procesamiento de la información en Internet. Entre estas innovaciones destaca la tecnología *Blockchain* (cadena de bloques), que se ha consolidado como un protocolo de desarrollo y seguridad. Esta característica es fundamental, ya que transforma los entornos digitales donde se aplica, y ofrece nuevas formas de interacción y confianza.

Pero, ¿qué es realmente el *Blockchain*? Según varios analistas y desarrolladores, como *Ibañez Jiménez*,[1] esta tecnología puede entenderse como una sintaxis de programación matricial que genera un árbol de códigos interrelacionados en varios ordenadores de forma idéntica y sincrónica. Este proceso permite la creación de un protocolo criptográfico robusto, lo cual asegura la integridad del contenido generado.

El mayor beneficio del uso de la tecnología *Blockchain* se experimenta en el sector económico, especialmente en el ámbito bancario, donde ha surgido y se ha adoptado el uso de criptomonedas o criptodivisas. Esta transformación en el sector económico marca un cambio significativo y establece nuevas dinámicas en el intercambio financiero global.[2]

Los objetivos de la investigación fueron evaluar e implementar la tecnología *Blockchain* como una solución de ciberseguridad para la infraestructura telemática del Sistema Nacional de Salud de Cuba, que se enfoque en la gestión eficaz de la seguridad de la información y la mitigación del ciberterrorismo.

Métodos

Se llevó a cabo una revisión bibliográfica exhaustiva sobre la tecnología *Blockchain*, se abarcaron sus políticas, protocolos y estructura, en relación con las recientes legislaciones en torno al uso de tecnologías en Cuba y las políticas de ciberseguridad. Además, se analizó el estudio de diferentes modelos estructurados y funcionales para su implementación en los servicios de salud, según los estándares HL7 y el respeto en los criterios de soberanía tecnológica. Este estudio también consideró las fortalezas, debilidades, limitaciones, beneficios y oportunidades del uso de este protocolo, así como la identificación de nuevas líneas de desarrollo para la infraestructura telemática de salud.

El *Blockchain*, modelo de seguridad y su uso en múltiples escenarios

Como se ha manifestado, el protocolo o tecnología *Blockchain* por sus grandes cualidades puede ser usado en cualquier entorno informático que se desee. Entre sus principales fortalezas se encuentran, según *Pava Díaz* y otros:[3]

- Su estructura de seguridad e inalterabilidad
- Sus algoritmos criptográficos robustos e inmutables
- Métodos de organización por bloques
- Su empleo en bases de datos distribuidas, abiertas y descentralizada
- Sus logaritmos de verificación de datos por varios usuarios y nodos
- Sus criterios de validan de la información
- La transparencia en sus procesos de información, entre otros

Desde la aparición de las plataformas *Blockchain*, estas han tenido varias actualizaciones en el proceso de perfeccionar su estructura sintáctica, las cuales se presentan en tres reajustes o generaciones, según lo plantea *Portmann* y otros.[4] El autor presenta las clasificaciones en el avance de esta tecnología, desde su primer enfoque en el uso de las criptodivisas, una segunda generación, la cual fue orientada a los contratos inteligentes (*Smart Contract*), y a las plataformas descentralizadas, lo que dio lugar a la tercera generación de *Blockchain* o *blockchain* 3.0, la que permite su utilización en diversos entornos, como el de la salud.

Al facilitar la sostenibilidad, la privacidad, la operatividad y el almacenamiento de registros en cadenas públicas, privadas e híbridas,[5] surgen numerosas opciones tecnológicas. A su vez, esto ha posibilita, junto con los sistemas de *Smart Contract*, el control y la verificación de la información propietaria. Además de permitir la interoperabilidad con otras plataformas, este proceso posiciona a estas tecnologías por encima de otras infraestructuras o plataformas telemáticas.

¿Cómo se desarrolla el *Blockchain*?

Esta tecnología presenta un cambio de paradigmas tradicionales y les da solución a problemas que antes del 2008 era comunes y afectaban diversas áreas sociales, comerciales y tecnológicas.

Esto generó un desafío para la tecnología, que en el caso financiero se resolvió con la eliminación de los bancos y la autenticación como una red por pares (P2P) o punto a punto (*peer to peer*) entre solo los activos actuantes. En este contexto, mediante complejos sistemas criptográficos y el uso de medios de cómputos, los usuarios participantes realizan las operaciones financieras y, cada vez que entra un nuevo usuario, se replica la información en sus activos informáticos para su autentificación en cadena, y el registro de todas las operaciones realizadas. A esto se le denomina minería de datos.

Su principal característica es que no presenta un servidor o nodo central; todos los usuarios activos o mineros reciben una copia del *Blockchain,* la cual deben validar para demostrar su originalidad y veracidad, lo que posibilita que cualquier modificación en el bloque o código, debe replicarse a todos los usuarios involucrados. Esto supone una fortaleza en la seguridad de la tecnología, ya que cualquier modificación no autorizada será detectada enseguida por los demás actuantes, lo que facilita tomar contramedidas inmediatamente por el acceso no autorizado.

De este análisis se deriva su principal fortaleza, al ser un sistema encriptado, condiciona que con la creación y cierre de un bloque la validación se garantiza por todos los usuarios o nodos de la red activa, lo que certifica la fiabilidad de la información y la gestión de su seguridad.

Sistemas criptográficos empleados

Entre los sistemas de seguridad criptográficas se presentan diversas funciones. Aunque existen diferentes algoritmos criptográficos de resumen de mensajes, no todos son usados. Esto se debe debido a su inseguridad, ya que la tecnología *Blockchain* exige niveles específicos criptográficos, razón por lo que se presenta como la solución más óptima y segura en la actualidad.

Otro aspecto de seguridad que se debe de analizar se relaciona con los protocolos de consenso distribuidos o los métodos de consenso, los cuales constituyen el soporte principal de la tecnología *Blockchain*, y se manifiestan en varios tipos de algoritmos que emplean. Según algunos autores[6,7] existen diversos métodos en su validación a través de la comparación de sus características, entre los que se encuentran:

- **Pruebas de trabajo (*Proof of Work*) o (PoW):** a criterios de algunos autores, este es uno de los consensos algorítmicos de mayor seguridad que existe y sirve de modelo a otras variantes propuestas, además de

brindar transparencia, estabilidad, facilidad en la verificación de patrones, descentralización, continuidad de procesos, al tener tolerancia a las fallas. Todas estas características son soportadas en su compleja estructura criptográfica de rompecabezas matemáticas, que lo hace difícil de calcular y fácil de verificar.[8,9]

- **Prueba de capacidad (*Proof of Capacity*) o (PoC):** tiene como base una concepción similar al PoW, pero emplea un mecanismo diferente en su algoritmo de consenso, el cual se orienta a utilizar las unidades de disco duro (HDD) de los ordenadores activos. Este método aprovecha el trazado del disco duro, evita la ralentización y el alto consumo energético del hardware. Se presenta así como una alternativa ecológica a la minería basada en PoW, ya que puede emplear cualquier tipo de HDD.[10]

- **Pruebas de participación (*Proof of Stake*) o (PoS):** es otro criterio que plantea el segundo método de consenso más frecuente en la tecnología *Blockchain*. Su arquitectura se realiza, definiendo un nodo central con una firma digital para validar su propiedad sobre la participación, en lugar de resolver un problema de *hash* complejo. De esta forma no necesita altos recursos computacionales y lo convierte en un método de consenso seguro.[11,12]

- **Prueba de participación delegada (*Delegated Proof of Stake*) o (DPoS**): es un método de consenso democrático representativo, donde todas las partes implicadas eligen, mediante votación, quienes serán los nodos testigos y delegados. De esta manera, se presentan las mejoras entre la DPoS, en relación con la PoS, en la evaluación del rendimiento, latencia y los niveles de seguridad, lo cual impacta en los bajos costos que manifiesta el protocolo.[13,14] Los nodos testigos son los responsables de crear nuevos bloques y son recompensados, mientras que los nodos delegados son los encargados de mantener la red y sugerir cambios tales como el tamaño de los bloques.

- **Prueba de importancia (*Proof of Importance*) o (PoI):** es un tipo de protocolo que utiliza el concepto de cuentas que validan y agregan

bloques a la red. Entre sus características se pueden apreciar que no demanda un uso desmedido de *hardware* para el proceso de minería, ya que utiliza los nodos conocidos para la actividad de recolección de datos. En el proceso se definen las características límites de los bloques o información procesada.[15,16]

– **Prueba de actividad (*Proof of Activity*) o (PoAc):** es un protocolo de consenso que es la combinación de PoW y PoS. Este proceso se centra en la producción de los bloques por parte de los mineros, utilizando el protocolo PoW. Posteriormente, pasan al protocolo PoS, que poseen la cabecera informativa del bloque creado y ubicación del nodo o minero. Por esta razón se considera una prueba de consenso híbrida, y su principal característica es la consolidación de seguridad contra ataques DDoS.[17,18]

El *Blockchain* en el sector de la salud

Uno de los criterios que deben considerarse para el diseño de cualquier infraestructura, plataforma o arquitectura telemática en la salud es la concepción tecnológica a utilizar. En este sentido, se presentan dos variantes informáticas:

– La informatización a medida: la cual se basa en el desarrollo de procesos independientes según necesidades y demandas (la más utilizada). Los sistemas de información se desarrollan de manera aisladas de los sanitarios. Estas soluciones son a corto plazo; su deficiencia está en las limitaciones de la infraestructura y de las plataformas tecnológicas sanitarias. No permite soberanía tecnología.
– La informatización soportada en estándares tecnológicos: esta se considera una estrategia a largo plazo en el desarrollo de una infraestructura y las plataformas tecnológicas que la acompañan en la integración de todas sus demandas y necesidades, además de los

requerimientos actuales y futuros, ajustados a políticas. Ello permite una cooperación global e institucional y favorece la libertad de acción e integración entre los proveedores, desarrolladores y la institución hospitalaria o el sector. Esta alternativa facilita los procesos de interoperabilidad y soberanía tecnológica.

La existencia de sistemas de registros médicos y el uso de las historias clínicas electrónicas o digitales proporciona que en sus bases de datos se recopile mucha información confidencial y sensible de los pacientes, trabajadores y de las instituciones de salud. Esta razón convierte a las instituciones sanitarias en el centro de diversas técnicas de ciberataques.

El uso de cortafuegos, sistemas cerrados de criptografía, antivirus, entre otros, no constituyen herramientas suficientes para evitar las violaciones desde afuera o desde adentro de las instituciones de salud. Hasta la fecha las soluciones no han sido muy efectivas, por lo que se hace necesario aplicar diferentes mecanismos de ciberseguridad. A esto se le suma la principal amenaza, riesgo y vulnerabilidad que tienen los sistemas telemáticos, los propios usuarios.

En el sector de la salud se presentan estándares informáticos propios ya predefinidos, estos están declarados para su utilización y uso por los sistemas y aplicaciones telemáticas. Entre ellos se encuentran los estándares HL7 (*Health Level Seven*), los estándares DICOM, entre otros estándares médicos tecnológicos, los cuales son utilizados en los procesos de mensajería y transmisión de imágenes médicas. Estos permiten la interoperabilidad de todas las plataformas y aplicaciones médicas, las cuales se conforman como infraestructuras telemáticas centralizadas, al unificar todas las informaciones gerenciales, sanitarias y económicas dentro del sector.

Con la presentación de dicha panorámica tecnológica en la salud y la existencia del *Blockchain* se propone una integración de estas dos tecnologías para el procesamiento, validación y movimiento de la información, que se debería condicionar en una red *Blockchain* privada para el sector de la salud. Esta última

tecnología serviría de algoritmo de empaquetamiento de los estándares médicos mencionados, los cuales se utilizarían en los diferentes nodos de las redes sanitarios, y se convertirían en los mineros de la información. En este aspecto los nodos centrales servirían como centros de datos primarios para el respaldo, verificación y validación de la información sanitaria.

Se crearían subunidades para el control de los sistemas de gestión y certificación documental, la trazabilidad de los recursos y activos, el intercambio entre los sistemas, según sus niveles jerárquicos y los roles establecidos; la protección y seguridad de la gestión de la información y barrera de ciberseguridad dinámica. Por último, los pacientes y los médicos o el personal de salud serían parte del sistema como máximos exponentes y generadores de toda la información que se produzca, y mineros de su propia información.

Interoperabilidad entre los estándares HL7 y la tecnología *Blockchain*

La estandarización de los sistemas telemáticos en el ámbito de la salud facilita su integración con la tecnología *Blockchain*. Existen varios estándares informáticos médicos ampliamente utilizados que contribuyen a este proceso:

- HL7-Salud nivel siete:[19] Estándar para facilitar el intercambio electrónico de información clínica; se presenta con diferentes subsistemas de comunicación.
- DICOM-Imagen digital y comunicación en medicina:[20,21] Estándar de transmisión de imágenes médicas entre *softwares* médico, por ejemplo, en la tomografía axial computarizada (TAC).
- CCR-Registro del cuidado continuado:[22] Estándar de los registros médicos.

- OpenEHR:[23] Estándar abierto que describe la administración y el almacenamiento de información sanitaria.
- PACS-Sistema de archivo y comunicación de imágenes:[23] más que un estándar se considera una arquitectura informática con el fundamento de capturar, almacenar, distribuir y mostrar archivos gráficos médicos.

Como se observa, estos sistemas se orientan en los procesos de mensajería de la información, el tratamiento de imágenes, la nomenclatura y el procesamiento de datos, entre otros procesos. Estos se agrupan en sistemas de gestores de base de datos que, por sus características de programación, facilitan la creación y ejecución de cadenas de bloques y su encapsulamiento en un registro matricial criptográfico predefinido. A la vez, posibilitan la introducción de datos, su procesamiento, resguardo y validación por las partes implicadas y los posibles actores, declarados por las instituciones médicas y los pacientes, acerca del uso de sus propias tecnologías sanitarias.

Resultados

Después de una búsqueda detallada y un análisis estructurado sobre el método *Blockchain*, se han determinado los diferentes modelos que pueden estructurarse para:

1. El diseño por parte de la Dirección Nacional de Informática del Ministerio de Salud Pública (MINSAP) de la arquitectura HL7, que se va a emplear en el Sistema Nacional de Salud (SNS), en correspondencia con criterios internacionales y directivas nacionales, siempre sobre el principio de la soberanía tecnología como estrategia del MINSAP y del gobierno cubano.

2. La presentación de la arquitectura HL7 al Ministerio de Comunicaciones y sus organismos reguladores para su revisión y validación.
3. Aprobación legislativa de esta arquitectura de programación por los órganos correspondientes del gobierno.
4. Constituir grupos de trabajo con las empresas creadoras de sistemas, las universidades, facultades y centros de investigación de desarrollo e investigaciones cibernéticas para el desarrollo e implementación de la arquitectura HL7 y la tecnología *Blockchain*.
5. Implementación en la infraestructura telemática de salud (INFOMED).

En este criterio los investigadores proponen la participación de varios usuarios, los cuales se determinarán por roles. La propuesta inicial es constituir una red *Blockchain* privada, con el propósito de ser una red híbrida en algún momento de su evolución. Entre los actuantes estarían: el MINSAP, con la red INFOMED y los nodos provinciales; las instituciones con nodos dedicados que prestarían servicio a la institución; y el médico y paciente.

Estos dos últimos serían los factores determinantes en la cadena, al cerrar el anillo de validación, según los procesos que se ejecutarían. De esta manera, ambos constituirían elementos vitales, según las actuales legislaciones sobre tecnología y ciberseguridad expuestas por el Parlamento cubano en las diferentes gacetas oficiales. Además de darle una participación activa al paciente sobre su información y su seguridad.

A partir de los criterios anteriores se presenta el protocolo de **prueba de consenso de participación** como uno de los métodos más factibles para el sector de la salud. Los participantes determinan la creación de un nuevo bloque y su validación con los niveles criptográficos definidos, en el que el encargado será la institución médica, y los demás participantes validarán la información, la cual tendrá niveles de almacenamiento y control.

Otra solución es la “Plataforma Hyperledger”; esta tecnología forma parte de un proyecto de la Fundación Linux y permite una relación dinámica entre el porteador y el propietario de la información (paciente). Esta considera la

seguridad como elemento primario.[25] Lo anterior permite, sobre las concepciones de soberanía tecnología, constituir un método factible de aplicar a los sistemas telemáticos de la salud cubana. Entre sus características se encuentran ser modular, contar excelentes procesos criptográficos y de seguridad; identidad conocida entre todos los participantes, confidencialidad de la información y compatibilidad con diferentes lenguajes de programación, protocolos y plataformas informáticas. Lo importante de esta plataforma es que existe una interface (*framework*) que permite su utilización en cualquier plataforma a la que se desee integrar con seguridad, escalable, altamente adaptable, y de gran flexibilidad de accesos y permisos.

Se consideran todas las variantes en las que se puede utilizar la tecnología *Blockchain* en el sector de la salud, en particular en su infraestructura telemática, en el respeto de la soberanía tecnológica, y la integración con los protocolos HL7. Se presentan dos alternativas de las muchas existentes, según la prueba de consensos analizados acerca de la capacidad de adaptarse a los procesos de desarrollo informático personalizados.

Esto no limita que sobre conceptos híbridos se puedan crear variantes de prueba, lo que permite la declaración de nuevos protocolos, principios criptográficos y de ciberseguridad en la gestión de la información sanitaria.

Discusión

La integración de la tecnología *Blockchain* en el Sistema Nacional de Salud de Cuba no resultará compleja con la infraestructura telemática de salud INFOMED. Para su diseño e implementación se propone contar con diferentes actores y decisores, ya declarados en la investigación "Transformación digital del Sistema Nacional de Salud en Cuba".[26]

Como se manifiesta, la tecnología *Blockchain* no solo tiene utilidad en el sector bancario-financiero, sino que con las herramientas correctas se puede utilizar

en cualquier entorno productivo y social. Entre sus principales características se exponen la participación activa y descentralizada de miembros, dígase mineros (usuarios) y nodos (ordenadores), en correspondencia con su arquitectura de consenso, la capacidad de soportar una gran cantidad de tráfico de datos, los cuales definen sus alcances y criterios criptográficos.

Se propone un diseño estructural para el desarrollo sintáctico y operacional para la tecnología *Blockchain*, así como los factores decisores para su posible implementación en los procesos informáticos del Sistema Nacional de Salud en Cuba.

El artículo presentó una propuesta de un diseño estructurado y dos alternativas criptográficas para dar solución a las políticas de ciberseguridad y seguridad de la información en el sector de la salud, sobre el principio de soberanía tecnológica como estrategia gubernamental y la interoperabilidad con los estándares HL7. Estas están definidas como estrategia para el desarrollo de los procesos tecnológicos sanitarios en Cuba. Se concluye que el análisis realizado de la tecnología *Blockchain* se orienta como una alternativa para minimizar los daños y perjuicios a los que está expuesto el sector de la salud.

Referencias bibliográficas

1. Ibáñez Jiménez JW. Blockchain, ¿el nuevo notario? 2016 [acceso 12//05/2023]. Disponible en: https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/14564/Blockchain_el_nuevo_notario.pdf?s

2. Grobys K, Ahmed S, Sapkota N. Technical trading rules in the cryptocurrency market. Finance Research Letters. 2019. DOI: https://doi.org/10.1016/j.frl.2019.101396

3. Pava Díaz RA, Pérez Castillo JN, Niño Vásquez LF. Perspectiva para el uso del modelo P6 de atención en salud bajo un escenario soportado en IoT y

blockchain. Tecnura. 2021;25(67):112-30. DOI: https://doi.org/10.14483/22487638.16159

4. Portmann E. Reseña: Blockchain: Plan para una nueva economía. HMD. 2018;55:1362-1364. DOI: https://doi.org/10.1365/s40702-018-00468-4

5. BSM Blockchain School for Management. Tipos de blockchain: pública, privada e híbrida. 2021 [acceso 15/01/2023]. Disponible en: https://www.bsmexecutive.com/diferencias-entre-blockchain-publica-privada-e-hibrida/

6. Campaña Iza XM, Zumba Sampedro WX. Métodos de consenso sobre plataformas blockchain: Un enfoque comparativo. [tesis de licenciatura en Internet]. Quito: Universidad Central del Ecuador; 2020 [acceso 17/01/2023]. Disponible en: http://www.dspace.uce.edu.ec/handle/25000/21832

7. Quesada Real FJ. Introducción a la tecnología Blockchain. Jaén: Universidad de Jaén; 2019. [acceso 15/01/2023]. Disponible en: https://hdl.handle.net/10953.1/11599

8. Nawari NO, Ravindran S. Blockchain and the built environment: Potentials and limitations. J Build Eng. 2019;25:100832. DOI: https://doi.org/10.1016/j.jobe.2019.100832

9. Viriyasitavat W, Hoonsopon D. Características de *blockchain* y consenso en los procesos de negocio modernos. 2019;13:32-39. DOI: https://doi.org/10.1016/j.jii.2018.07.004

10. Porta M. Prueba de capacidad (PoC): algoritmo de consenso que utiliza unidades de disco duro. 2019 [acceso 25/01/2023] Disponible en: https://en.cryptonomist.ch/2019/08/17/proof-of-capacity-poc-consensus-algorithm/

11. Lee JY. Una economía de fichas descentralizada: cómo la cadena de bloques y las criptomonedas pueden revolucionar los negocios. Business Horizons. 2019;62(6):773-84. DOI: https://doi.org/10.1016/j.bushor.2019.08.003

12. Debús J. Métodos de consenso en sistemas Blockchain. Escuela de Finanzas y Gestión de Frankfurt. 2017 [acceso 23/01/2023]. Disponible en: http://www.explore-ip.com/2017_Consensus-Methods-in-Blockchain-Systems.pdf

13. Campaña X, Zumba X, Morales M, Morales S. Análisis comparativo de Métodos de Consenso sobre plataformas Blockchain. Revista Tecnológica-Espol. 2021;33(2):25-42. DOI: https://doi.org/10.37815/rte.v33n2.828

14. Zhang S, Lee JH. Análisis de los principales protocolos de consenso de *blockchain*. 2020;6(2):93-97. DOI: https://doi.org/10.1016/j.icte.2019.08.001

15. Beltrán Triana CAF. Elaborar un protocolo de pruebas de seguridad para aplicaciones que hagan uso de la tecnología blockchain. Bogotá: Universidad El Bosque; 2022 [acceso 10/02/2023]. Disponible en: http://hdl.handle.net/20.500.12495/9506.

16. Abegg JP, Bramas Q, Noël T. Blockchain usando prueba de interacción. NETYS. 2021 [acceso 17/01/2023;129-43. Disponible en: https://link.springer.com/chapter/10.1007/978-3-030-91014-3_9

17. Boreiri Z, Azad AN. A Novel Consensus Protocol in Blockchain Network based on Proof of Activity Protocol and Game Theory. 8th International Conference on Web Research (ICWR). 2022:82-7. DOI: https://doi.org/10.1109/ICWR54782.2022.9786224

18. Rebello GAF, Camilo GF, Guimarães LCB, de Souza LAC, Thomaz GA, Duarte OCMB. Análisis de seguridad y rendimiento de protocolos de consenso basados en pruebas. Ann Telecommun. 2022;77:517-537. DOI: https://doi.org/10.1007/s12243-021-00896-2

19. Pardell. El estándar HL7. 2021 [acceso 12/02/2023]. Disponible en: https://www.pardell.es/el-estandar-hl7.html

20. Pardell. DICOM. 2021 [acceso 12/02/2023]. Disponible en: https://www.pardell.es/dicom-.html

21. D. McLean JM. DICOM. 2020. DOI: https://doi.org/10.1016/B978-0-323-08495-6.00002-6

22. Benson T, Grieve G. CDA-Arquitectura de documentos clínicos. Principios de Interoperabilidad en Salud. 2020:233-54. DOI: https://doi.org/10.1007/978-3-030-56883-2_13

23. Adler Milstein J, Adelman SJ, Tai Seale M, Patel VL, Dymek C. Registros de auditoría de EHR: ¿una nueva mina de oro para la investigación de servicios de salud? 2020. DOI: https://doi.org/10.1016/j.jbi.2019.103343

24. Marcillo Vera F, Palacios HR, Mora Zambrano ER, Shauri Romero JD, Torres Bastidas JP, Cobeña Cobeña SM. Hacia una arquitectura de software y hardware más fiable y escalable para los sistemas de salud. 2021:9(17):7-11. DOI: https://doi.org/10.29057/esh.v9i17.6570

25. Guisado Soriano J, Mora Serrano FJ, Zinggerling C, Priegue A. Desarrollo de una aplicación Blockchain con la tecnología Hyperledger Fabric orientado a IOT. 2022 [acceso 06/02/2023]. Disponible en: https://upcommons.upc.edu/bitstream/handle/2117/362748/memoria.pdf?sequence=1&isAllowed=y

26. Ramos Delgado A, Vidal Ledo M, Rodríguez Díaz A, Barthelemy Aguilar K, Torres Ávila D. Salud y transformación digital. Educación Médica Superior. 2022 [acceso 02/02/2024];36(2). Disponible en: https://ems.sld.cu/index.php/ems/article/view/3442

Conflicto de intereses

Los autores declaran que no tienen conflicto de intereses.

Contribución de los autores

Conceptualización: Inglis Pavón de la Tejera y Ariadna Velázquez Ricardo.

Curación de datos: Inglis Pavón de la Tejera y Ariadna Velázquez Ricardo.

Análisis formal: Inglis Pavón de la Tejera y Ariadna Velázquez Ricardo.

Supervisión:

Validación: Nubia de la Tejera Chillón, Germán Del Rio Caballero y Sergio Daniel Cano Ortiz.

Investigación: Inglis Pavón de la Tejera y Ariadna Velázquez Ricardo.

Metodología: Inglis Pavón de la Tejera, Ariadna Velázquez Ricardo, Nubia de la Tejera Chillón, Germán Del Rio Caballero y Sergio Daniel Cano Ortiz.

Administración del proyecto: Inglis Pavón de la Tejera y Ariadna Velázquez Ricardo.

Redacción – borrador original: Inglis Pavón de la Tejera, Ariadna Velázquez Ricardo, Nubia de la Tejera Chillón, Germán Del Rio Caballero y Sergio Daniel Cano Ortiz.

Redacción – revisión y edición: Inglis Pavón de la Tejera, Ariadna Velázquez Ricardo, Nubia de la Tejera Chillón, Germán Del Rio Caballero y Sergio Daniel Cano Ortiz.