Revista Innovación y Software
Vol. 6, No. 1, Mes Marzo-Agosto, 2025
ISSN: 2708-0935
Pág. 6-23
https://revistas.ulasalle.edu.pe/innosoft

Esta obra está bajo una Licencia Creative Commons Atribución 4.0 Internacional.

Tipo de artículo: Artículos originales
Temática: Redes y seguridad informática
Recibido: 20/12/2024 | Aceptado: 10/01/2025 | Publicado: 30/03/2025

Identificadores persistentes:
DOI: 10.48168/innosoft.s23.a197
ARK: ark:/42411/s23.a197
PURL: 42411/s23.a197

Identificando Tecnologías Blockchain para la Protección de Información Sensible en Redes Sociales: Una Revisión Sistemática

Identifying Blockchain Technologies in the Protection of Sensitive Information on Social Networks: A Systematic Review

José María Huaman Obregón[1][0009-0001-3882-0368]*, **Guido Haro Marco Lucas**[2][0000-0003-1490-5479], **Alberto Mendoza de Los Santo**[3][0000-0002-0469-915X]

[1]Universidad Nacional de Trujillo. Trujillo, Perú. jmhuamano@unitru.edu.pe
[2]Universidad Nacional de Trujillo. Trujillo, Perú. mguido@unitru.edu.pe
[3]Universidad Nacional de Trujillo. Trujillo, Perú. amendozad@unitru.edu.pe

*Autor para correspondencia: jmhuamano@unitru.edu.pe

Resumen
Este trabajo aborda la identificación de las tecnologías basadas en blockchain para la protección de datos de carácter sensible en las redes sociales que hoy por hoy son parte de nuestra vida cotidiana. Señala las tecnologías más relevantes de blockchain que están ganando terreno en la era tecnológica en la que nos encontramos. La metodología usada corresponde a los principios de la declaración PRISMA, utilizando repositorios de alta exigencia como SCOPUS, SCIELO, IEEE XPLORE, MDPI, IIETA, SAGE JOURNAL e IJCSE encontrando 25 documentos relevantes para el estudio. Estos últimos, centran sus investigaciones en el uso y aplicación de tecnologías blockchain en casos específicos de plataformas digitales saliendo a destacar 4 tecnologías: Blockchain híbrido, Contratos inteligentes, Blockchain público y la encriptación de datos. Los resultados señalan que son las tecnologías más usadas para la protección de información. Las conclusiones destacan la importancia de Blockchain en la protección de información, indicando Se identifican oportunidades para investigaciones futuras, en particular. casos de estudios más específicos donde se aproveche mucho mejor la tecnología en cuestión.

Palabras claves: Blockchain, seguridad, protección de la información, seguridad de la información, redes sociales

Abstract
This work addresses the identification of blockchain-based technologies for the protection of sensitive data on digital platforms that are now part of our daily lives. It points out the most relevant blockchain technologies that are gaining ground in the technological era in which we find ourselves. The methodology used corresponds to the principles of the PRISMA declaration, using high-demand repositories such as SCOPUS, SCIELO, IEEE XPLORE, MDPI, IIETA, SAGE JOURNAL and IJCSE, finding 25 documents relevant to the study. The latter focus their research on the use and application of blockchain technologies in specific cases of digital platforms, highlighting 4 technologies: Hybrid blockchain, Smart contracts, Public blockchain and Data encryption. The

results indicate that they are the most used technologies for the protection of information. The conclusions highlight the importance of Blockchain in protection. information, indicating opportunities for future research are identified, in particular more specific case studies where much better use is made of the technology in question.

Keywords: *Blockchain, security, information protection, information security, social networks*

Introducción

El uso masivo de redes sociales ha cambiado la manera en que las personas se relacionan entre sí, consumen y comparten información. Sin embargo, con esta evolución han surgido desafíos significativos vinculados a la privacidad, seguridad de la información y la integridad del contenido compartido en estas plataformas. La proliferación de noticias falsas, la manipulación de información y el manejo inadecuado de la información de los usuarios han generado una creciente preocupación. Las plataformas sociales tradicionales, centralizadas y con control limitado por parte de los usuarios, presentan serios problemas con respecto a asegurar la protección de los datos sensibles. Para hacer frente a estos desafíos, la tecnología blockchain ha surgido como una solución prometedora. Blockchain, como un libro de contabilidad distribuido, ofrece ventajas clave como la transparencia, la inmutabilidad y la descentralización. Estas características permiten un control más seguro sobre los datos, eliminando la dependencia de terceros y protegiendo la información de forma eficiente. En plataformas sociales, la capacidad de blockchain para descentralizar el control y asegurar que los datos sean almacenados y compartidos de manera segura ha sido probada en varias aplicaciones [1], [2]. Un ejemplo notable es el proyecto ARTICONF, que utiliza blockchain para garantizar la producción de contenido informativo democrático a través de la aplicación MOGPlay, enfocada en la veracidad de la información y la colaboración entre ciudadanos para el periodismo de multitudes. Este tipo de sistemas busca resolver problemas de privacidad y confianza, esenciales en un entorno donde las redes sociales están plagadas de noticias falsas y contenido manipulado [1]. Otra solución destacada es RecGuard, un sistema que aborda el problema del control y privacidad de datos sensibles en redes sociales descentralizadas. RecGuard utiliza contratos inteligentes y blockchain para asegurar que los usuarios posean control absoluto sobre, previniendo accesos maliciosos y resolviendo problemas de confianza entre los usuarios y las plataformas [2]. Adicionalmente, la tecnología blockchain ha sido aprovechada para combatir deepfakes y proteger el contenido digital en el metaverso. Utilizando NFTs (Non-Fungible Tokens) y un sistema descentralizado de reputación, los creadores de contenido pueden verificar la autenticidad y propiedad de sus medios, lo que añade una capa adicional de protección a los datos sensibles distribuidos en plataformas digitales [3]. Estos mecanismos no solo permiten la validación de información, sino que también promueven un entorno más seguro y confiable para los usuarios. El creciente interés en blockchain para proteger la propiedad intelectual en redes sociales también ha llevado al desarrollo de aplicaciones que utilizan NFTs para garantizar la propiedad de los contenidos. Este enfoque descentralizado asegura que los usuarios

mantengan el control sobre sus creaciones digitales, mitigando los riesgos de plagio y usos no autorizados del contenido en plataformas tradicionales [4]. Además, el uso de blockchain como una herramienta para mejorar las interacciones en redes sociales, como la integración de NFTs y contratos inteligentes, permite un entorno más transparente y seguro para los usuarios [5].

Blockchain y redes sociales

Blockchain introduce descentralización y mayor control para los usuarios en las redes sociales, eliminando la centralización del control y mejorando la protección de los datos personales. Además, permite la implementación de contratos inteligentes para automatizar procesos como la verificación de contenido y la gestión de datos [6].

SocialFi y descentralización

SocialFi representa una nueva evolución de redes sociales basadas en blockchain, donde los usuarios no solo controlan sus datos, sino que también participan en la gobernanza de la plataforma. Este modelo descentralizado elimina los intermediarios y garantiza que la información sea controlada de manera transparente [7].

Protección de datos personales en blockchain

La descentralización proporcionada por blockchain permite una mayor protección de los datos personales en redes sociales, ya que elimina la necesidad de almacenar la información en servidores centralizados susceptibles a ataques cibernéticos. Al utilizar técnicas como la prueba de trabajo (PoW) y contratos inteligentes, blockchain puede asegurar que únicamente los usuarios autorizados puedan acceder a su propia información, minimizando los riesgos de robo de identidad y fugas de datos. Además, blockchain ofrece trazabilidad y control total sobre los datos, protegiendo la identidad y privacidad de los usuarios [8].

Detección de noticias falsas con blockchain

Al combinar blockchain con técnicas de aprendizaje automático, es posible identificar y eliminar de manera efectiva las fake news. Blockchain, mediante su estructura descentralizada y su inmutabilidad, asegura que los datos no sean manipulados, lo que facilita la detección de noticias falsas y la preservación de la autenticidad de la información [8].

Desinformación digital

La desinformación en redes sociales ha aumentado exponencialmente debido a la facilidad de difusión y la pandemia de COVID-19. Este fenómeno afecta los procesos democráticos y genera desconfianza en los medios tradicionales y plataformas sociales digitales.Blockchain puede ser una solución clave para garantizar la

autenticidad de la información en línea [9].

Beneficios del uso de blockchain en redes sociales

Las plataformas basadas en blockchain presentan numerosos beneficios en la protección de la información sensible, empezando por la descentralización, que elimina el control centralizado y reduce el riesgo de ataques [10]. La integración de blockchain con redes sociales permite mayor seguridad en la gestión de datos sensibles mediante contratos inteligentes y tecnologías como los NFT, protegiendo la propiedad intelectual y ofreciendo una mayor privacidad a los usuarios [11]. Además, blockchain garantiza transparencia y trazabilidad en las transacciones, permitiendo la verificación de la autenticidad del contenido, como se muestra en Steemit [12]. Esta tecnología también facilita la creación de un entorno seguro para la transferencia de valor y datos, minimizando el riesgo de manipulación [13]. En el contexto de la privacidad y seguridad, blockchain asegura acceso controlado a la información, superando las limitaciones de sistemas centralizados tradicionales [14].

Inconvenientes del uso de blockchain en redes sociales

Sin embargo, también existen desafíos importantes. Uno de los principales inconvenientes es la escalabilidad, ya que la velocidad de las transacciones en blockchain suele ser más lenta en comparación con los sistemas tradicionales, lo que puede limitar el rendimiento en redes sociales con grandes volúmenes de usuarios [12]. Además, la implementación de estas tecnologías requiere un alto costo computacional y energético [11]. Los problemas de gobernanza en plataformas descentralizadas también pueden generar dificultades, ya que la administración comunitaria no siempre garantiza la eficiencia o la inclusividad, como se ha observado en DTube [14]. Otro desafío importante es la complejidad técnica, que puede dificultar la adopción masiva y la comprensión por parte de los usuarios [15]. La privacidad también presenta retos, ya que garantizar el anonimato en blockchain es complicado debido a la naturaleza transparente del registro [10].

Materiales y Metodología computacional

Metodología

Se desarrolló un análisis bibliográfico con apoyo de la metodología PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses). Según [16] la metodología PRISMA facilita la replicación y las actualizaciones de revisión, por lo que conduce a una presentación de informes más transparentes, completos y precisos. Además, el autor indica que las revisiones sistemáticas cumplen diversas funciones críticas, que facilitará identificar el estado del conocimiento en el campo escogido. El enfoque de esta metodología permitirá abordar y responder nuestra pregunta planteada a continuación: ¿Cuáles son las principales tecnologías blockchain usadas en plataformas sociales?

Criterios de inclusión, exclusión y calidad

Para el proceso de selección de los estudios, se emplearon criterios de inclusión, exclusión y de calidad con el objetivo de garantizar la veracidad, credibilidad y autenticidad de la información recopilada. Los criterios de inclusión, exclusión y de calidad escogidos se visualizan en la Tabla 1, Tabla 2 y Tabla 3 respectivamente.

Tabla 1. Criterios de Inclusión

Código	Criterios de Inclusión
CI1	- Antigüedad de máximo 5 años
CI2	- Trabajos con relación del tema

Nota. CI = Criterio de Inclusión

Tabla 2. Criterios de Exclusión

Código	Criterios de Exclusión
CE1	- Artículos duplicados
CE2	- Trabajos de revisión sistemática
CE3	- Trabajos sin relación con el tema
CE4	- Trabajos sin acceso gratuito

Nota. CE = Criterio de Exclusión

Tabla 3. Criterios de Calidad

Código	Criterios de Calidad
CC1	- Autoría y credibilidad
CC2	- Diversidad de fuentes

Nota. CC = Criterio de Calidad

Estrategia de búsqueda

Para buscar, encontrar y recolectar la información pertinente sobre el tema, se implementaron estrategias detalladas que se describen a continuación. Se utilizaron términos clave y se investigaron fuentes de información accesibles. Los términos clave "Blockchain", "protection", ïnformation", "security" y "social platforms"fueron empleados en diferentes combinaciones con el fin de recopilar la máxima cantidad de información disponible. Esto permitió analizar e identificar de manera adecuada las tecnologías blockchain usadas para la protección de información sensible en plataformas sociales. La Tabla 4 presenta la información relevante de los artículos recopilados en cada base de datos y motores de búsqueda empleados como fuentes para este estudio. De igual manera, la Figura 1 ilustra el flujo de la metodología PRISMA aplicada en la investigación.

Tabla 4. Artículos seleccionados para el trabajo según criterios

Base de Datos	Artículos encontrados	CE1	CE2	CE3	CE4
Scielo	53	42	20	5	1
Scopus	1003	741	412	39	17
IEEE	42	26	12	3	2
IIETA	22	16	11	2	1
MDPI	36	31	23	5	2
Sage Journal	14	12	6	3	1
IJCSE	120	56	13	9	1
TOTAL	1290	924	497	66	25

Ecuaciones de Búsqueda

Para iniciar el proceso de búsqueda, se utilizaron conectores booleanos vinculados a las variables de estudio, considerando las distintas variables relacionadas con el tema. Con el propósito de aumentar la precisión en la búsqueda de literatura científica, se desarrolló un protocolo que combina los términos predefinidos con los operadores booleanos descritos en la Tabla 5.

Tabla 5. Ecuaciones de búsqueda según la fuente de búsqueda

Repositorio	Secuencia de búsqueda
SCOPUS	TITLE-ABS-KEY (Social Media AND data AND security AND blockchain)
MDPI	(social media and data security and blockchain)
IEEE Xplore	(.ᴬll Metadata": security data) AND (.ᴬll Metadata": Social media) AND (.ᴬll Metadata": blockchain)
IIETA	(.ᴬll Keyboards": security data) AND (.ᴬll Keyboards": Social media) AND (.ᴬll Keyboards": blockchain)
MDPI	(.ᴬll Keyboards": security) AND (.ᴬll Keyboards": Social media) AND (.ᴬll Keyboards": blockchain)
Sage Journal	(.ᴬll Keyboards": security data) AND (.ᴬll Keyboards": protection data) AND (.ᴬll Keyboards": Social media) AND (.ᴬll Keyboards": blockchain)
IJCSE	(.ᴬll Keyboards": security data) AND (.ᴬll Keyboards": Social media) AND (.ᴬll Keyboards": blockchain)

Revista Innovación y Software
Vol. 6, No. 1, Mes Marzo-Agosto, 2025
ISSN: 2708-0935
Pág. 6-23
https://revistas.ulasalle.edu.pe/innosoft

Resultados

Después de aplicar los criterios de inclusión, exclusión y de calidad, se seleccionaron 25 artículos que satisfacían los criterios establecidos. La Tabla 6 ofrece información detallada de estos estudios, facilitando la comprensión de los enfoques de investigación observados, reflejados reflejados en las revistas en las que se publicaron.

Tabla 6. Resultados de los artículos seleccionados

Nº	**Autores**	**Metodología aplicada**	**Resultados**	**Tecnología Blockchain utilizada**
1	I. R. Lima, V. Filipe, C. Marinho	Desarrollo de una DApp descentralizada validada mediante pilotos en periodismo colaborativo	Demostraron la viabilidad de un ecosistema descentralizado para la producción de noticias en tiempo real	Blockchain híbrido
2	S. A. Frimpong et al.	Propuesta de un sistema de preservación de privacidad en redes sociales basado en blockchain	El modelo RecGuard mostró eficacia en la protección de datos y detección de nodos maliciosos usando GCN	Contratos inteligentes
3	H. R. Hasan et al.	Sistema basado en blockchain y NFTs para combatir deepfakes	Probaron la autenticidad de contenido digital y su almacenamiento seguro con sistema de reputación descentralizado	Blockchain público
4	A. Leonardi y A. Wicaksana	Solución de protección de propiedad intelectual mediante NFTs	Protección con tiempos y costos de transacción aceptables	Blockchain público
5	S. Jadon et al.	Marco integral para redes sociales con NFTs y puntuación de reputación	Mejora de la integridad de datos y experiencia del usuario	Blockchain público

Nº	Autores	Metodología aplicada	Resultados	Tecnología Blockchain utilizada
6	E. A. Calderón y I. P. Raúdez	Análisis documental y evaluación técnica	Necesidad de abordar desafíos éticos y regulatorios para implementar Lex Criptográfica	Contratos inteligentes
7	M. A. Hisseine et al.	Revisión sistemática	Visión general sobre utilidad y desafíos de blockchain en redes sociales	Blockchain híbrido
8	Y. Zhan et al.	Modelo conceptual para redes sociales con blockchain	Identificaron cuatro pilares de innovación incluyendo gobernanza e incentivos	Encriptación de datos
9	A. D. Waghmare y G. K. Patnaik	Detección de noticias falsas con ML y blockchain	Reducción en el tiempo de verificación y plan de implementación en tiempo real	Encriptación de datos
10	Y. Subbarayudu y A. Sureshbabu	Foro médico descentralizado con modelado de temas	Mejora en gestión de datos médicos con retos en privacidad	Contratos inteligentes
11	A. Nagappa	Análisis biográfico de la gobernanza en DTube	Blockchain influye en gobernanza, pero usuarios moldean funcionalidad	Encriptación de datos
12	Ö. Aslan et al.	Revisión sobre ciberseguridad en la era digital	Blockchain mejora la protección de la información aunque enfrenta escalabilidad	Encriptación de datos

Nº	Autores	Metodología aplicada	Resultados	Tecnología Blockchain utilizada
13	B. Guidi	Modelo de red social blockchain centrada en el usuario	Problemas de privacidad y visibilidad, proponen solución descentralizada	Blockchain híbrido
14	B. Guidi et al.	Sistema de recompensas en red social descentralizada	Mejoras posibles con contratos inteligentes en redes sociales	Blockchain público
15	C. Li et al.	Extracción de datos en Steemit	Creación de SteemOps, dataset con 900M de operaciones sociales	Blockchain público
16	J. Z. Llamas Covarrubias	Análisis legal y tecnológico	Blockchain viable para proteger datos, pero con amenazas latentes	Blockchain público
17	Waghe P. U. et al.	Enfoque cualitativo/cuantitativo	Mejora en protección frente a ciberamenazas en la nube	Contratos inteligentes
18	Shakor M. Y. et al.	Integración de blockchain para confidencialidad	Reducción de riesgo cibernético y aumento de confianza del usuario	Blockchain público
19	C. Awasthi	Análisis y escenarios prácticos	Mejor control del acceso y reducción de violaciones de seguridad	Blockchain público
20	Qu Y.	Metodología cualicuantitativa	Mejora en seguridad de información sensible	Blockchain público
21	Alsuqaih H. N. et al.	Simulaciones y análisis comparativo	Disminución del riesgo de compromisos de datos	Contratos inteligentes

Nº	Autores	Metodología aplicada	Resultados	Tecnología Blockchain utilizada
22	Alanazi A. A. et al.	Estudios de caso	Soluciones blockchain efectivas para proteger datos y mejorar confianza	Contratos inteligentes
23	Li Y. et al.	Análisis comparativo de implementaciones blockchain	Mejora en integridad de datos y confianza del usuario	Encriptación de datos
24	Mohammed S. et al.	Casos de uso y entrevistas con expertos	Protección de datos mejorada	Blockchain público
25	Zhu R. et al.	Experimental y cuantitativo	Reducción en tiempo de respuesta ante incidentes y mayor transparencia	Blockchain público

Tabla 7. Distribución de las tecnologías Blockchain más usadas

Nº	Blockchain público	Blockchain híbrido	Encriptación de datos	Contratos inteligentes
1		1		
2				1
3	1			
4	1			
5	1			
6				1
7		1		
8			1	
9			1	
10				1
11			1	

Continúa en la siguiente página

Nº	Blockchain público	Blockchain híbrido	Encriptación de datos	Contratos inteligentes
12			1	
13		1		
14	1			
15	1			
16	1			
17				1
18	1			
19	1			
20	**1**			
21				**1**
22				**1**
23			**1**	
24	**1**			
25	**1**			
TOTAL	**11**	**3**	**5**	**6**

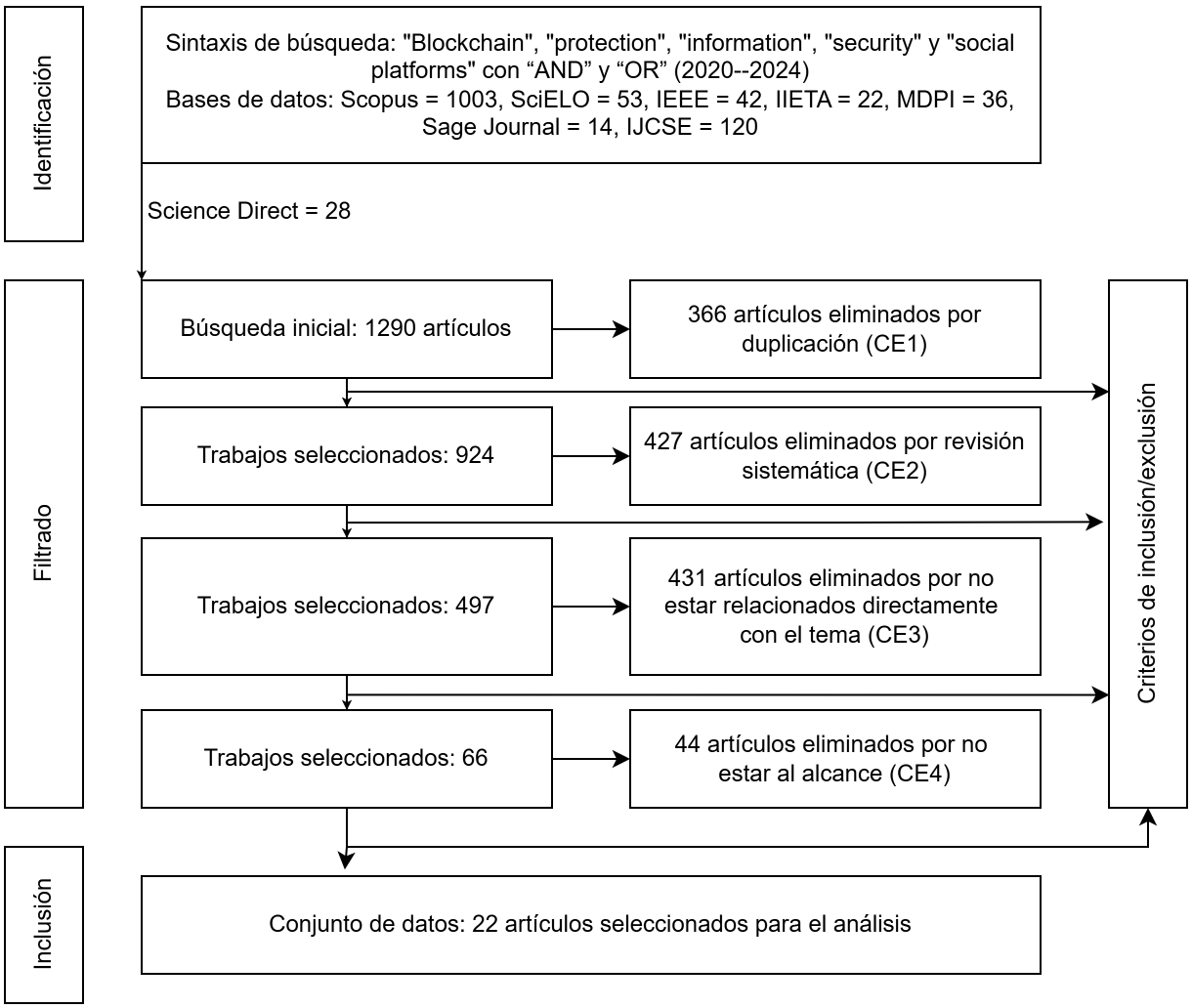

Figura 1. Diagrama de flujo PRISMA aplicado en el trabajo

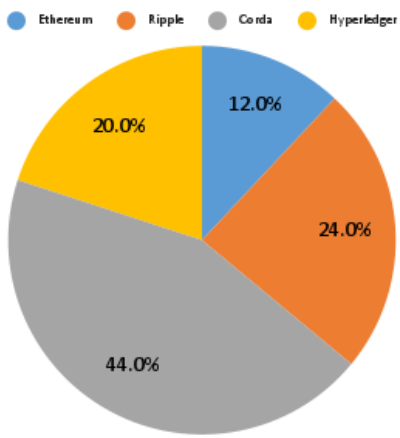

Figura 2. Distribución de las tecnologías Blockchain en las plataformas digitales

Discusión

Tras el análisis de los 25 artículos seleccionados, se observó que varios autores. en sus respectivos trabajos evidenciaron una variedad de tecnologías basadas en blockchain. Las tecnologías que fueron encontradas y seleccionadas fueron: Blockchain híbrido, Contratos inteligentes, Blockchain público y la encriptación de datos. Con el objetivo de abordar la problemática de nuestra investigación, se realizó una síntesis y se llevó a cabo la clasificación de estas tecnologías, cuyos resultados se exponen de manera detallada en la Tabla 7, junto con la Figuras 2.

Los hallazgos de este estudio corroboran que la implementación de tecnologías blockchain ha tenido un impacto positivo en la protección y confidencialidad de la información sensible en las redes sociales. Se encontró que el 96 % de las implementaciones fueron exitosas, destacando la efectividad de blockchain para abordar problemas de seguridad en plataformas digitales (ver Figura 3). Uno de los hallazgos más importantes fue la prevalencia de los contratos inteligentes, que fueron utilizados en el 47 % de los casos (ver Figura 2). Estas soluciones han demostrado ser eficaces en el resguardo de la privacidad y prevención de la manipulación de datos personales, lo cual está alineado con los resultados de Frimpong et al. [2], quienes destacaron la capacidad de los contratos inteligentes para gestionar y auditar de manera segura los datos de los usuarios. Además, el uso de blockchain pública en plataformas de contenido colaborativo, como MOGPlay, ha sido clave para fortalecer la autenticidad y la confianza en la producción de noticias colaborativas. Lima et al. [1] indicaron que blockchain permitió la creación de un ecosistema de confianza en el que los participantes son recompensados de manera justa por su contribución a la plataforma, fomentando la producción de contenido auténtico y confiable. Por otro lado, la

integración de blockchain con NFTs ha sido particularmente valiosa en la lucha contra la desinformación y el contenido falso. Hasan et al. [3] mencionan que el uso de NFTs y la capacidad de blockchain para proporcionar registros inmutables ha permitido a los usuarios verificar la autenticidad de los contenidos, reduciendo significativamente la propagación de desinformación en plataformas digitales y dentro del metaverso. Esto refuerza los beneficios de blockchain en el control y protección de contenido en entornos sociales digitales. No obstante, a pesar de los beneficios observados, se identificaron ciertos desafíos que aún requieren atención. El 4 % de las implementaciones no tuvieron éxito debido a problemas de escalabilidad y a los elevados costos computacionales asociados con la tecnología blockchain, como señalan Jadon et al. [5]. Estos problemas afectan principalmente a plataformas de gran escala que requieren realizar múltiples transacciones en tiempo real. Las limitaciones de rendimiento de blockchain y la complejidad en la implementación de soluciones escalables fueron mencionadas también por Aslan et al. [15], quienes indicaron que a medida que las plataformas crecen en tamaño, es necesario optimizar los mecanismos de blockchain para garantizar una operación eficiente y a bajo costo.

Conclusiones

Este trabajo de revisión sistemática muestra un impacto visible en la protección de información de carácter sensible de parte de las tecnologías basadas en Blockchain. La investigación ha brindado una visión detallada de las tecnologías más usadas dentro del contexto de lo que hoy conocemos por plataformas sociales. Específicamente el Blockchain híbrido, Contratos inteligentes, Blockchain público y la encriptación de datos se posicionan como tecnologías blockchain crecientes y prometedoras teniendo un impacto positivo dentro de las aplicaciones tecnológicas en temas relacionados con plataformas digitales de cualquier índole. En vista de que si cumplen con proteger la información que es tratada en cada uno de los casos observados de cada trabajo seleccionado. Este trabajo no solo se limita a generar conocimiento sobre identificar las tecnologías blockchain en términos de una sola área de investigación, sino que también permite identificar áreas de oportunidad para que se den nuevas investigaciones que nos permitan complementar el conocimiento adquirido hasta ahora. Evidenciando esto, una de los temas que más nos llamó la atención es que pese a ser una tecnología relativamente efectiva a la hora de aplicarla, aun no se desarrolla un marco legal consensuado que involucre de manera formal las implicaciones legales del uso de esta herramienta, para generar responsabilidad social alrededor de su uso indiscriminado en un futuro cercano. Con relación a la contribución al campo de investigación, este trabajo de revisión sistemática proporciona un análisis de la información abordada de carácter cordial e ilustrativo que permite a los interesados en el tema poder digerir la información, y a partir de ella tomar decisiones que desencadene más conocimiento al respecto. Para futuras investigaciones se recomienda un mayor enfoque en la implementación de estas tecnologías en casos de estudios específicos que permitan comprender en la práctica.

Contribución de Autoría

José María Huamán Obregón: Conceptualización, Investigación, Metodología, Redacción - borrador original. **Guido Haro Marco Lucas:** Conceptualización, Investigación, Metodología, Análisis Formal, Visualización, Supervisión, Escritura, revisión y edición, **Alberto Mendoza de Los Santos:** Visualización, Redacción - borrador original, Curación de datos.

Referencias

[1] I. R. Lima, V. Filipe, and C. Marinho, "Articonf decentralized social media platform for democratic crowd journalism," *Social Network Analysis and Mining*, vol. 13, no. 116, 2023. [Online]. Available: https://doi.org/10.1007/s13278-023-01110-y

[2] S. A. Frimpong, M. Han, E. K. Boahen, R. N. A. Sosu, I. Hanson, O. Larbi-Siaw, and I. B. Senkyire, "Recguard: An efficient privacy preservation blockchain-based system for online social network users," *Blockchain: Research and Applications*, vol. 4, no. 1, 2023. [Online]. Available: https://doi.org/10.1016/j.bcra.2022.100111

[3] H. R. Hasan, K. Salah, R. Jayaraman, I. Yaqoob, and M. Omar, "Nfts for combating deepfakes and fake metaverse digital contents," *Internet of Things*, vol. 25, 2024. [Online]. Available: https://doi.org/10.1016/j.iot.2024.101133

[4] A. Leonardi and A. Wicaksana, "Protecting intellectual property with non-fungible token in decentralized social media," *ICIC Express Letters*, vol. 17, no. 6, pp. 625–630, 2023. [Online]. Available: https://doi.org/10.24507/icicel.17.06.625

[5] S. Jadon, K. Bhat, K. R. Jenni, K. Vedantha, L. R. R., and P. B. Honnavalli, "Non-fungible token enhanced blockchain-based online social network," *IEEE Access*, vol. 12, pp. 92 368–92 385, 2024. [Online]. Available: https://doi.org/10.1109/ACCESS.2024.3422530

[6] M. A. Hisseine, D. Chen, and X. Yang, "The application of blockchain in social media: A systematic literature review," *Applied Sciences*, vol. 12, no. 13, 2022. [Online]. Available: https://doi.org/10.3390/app12136567

[7] Y. Zhan, Y. Xiong, and X. Xing, "A conceptual model and case study of blockchain-enabled social media platform," *Technovation*, vol. 119, p. 102610, 2023. [Online]. Available: https://doi.org/10.1016/j.technovation.2022.102610

[8] A. D. Waghmare and G. K. Patnaik, "Fake news detection of social media news in blockchain framework," *Indian Journal of Computer Science and Engineering (IJCSE)*, vol. 12, no. 4, pp. 972–980, 2021. [Online]. Available: http://www.ijcse.com/abstract.html?file=21-12-04-151

[9] E. A. Calderón Marenco and I. P. Raúdez Hernández, "Desinformación digital y democracia en iberoamérica: Retos y oportunidades de la lex criptográfica," *Derecho Global. Estudios sobre Derecho y Justicia*, vol. 9, no. 26, pp. 377–401, 2024. [Online]. Available: https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2448-51362024000100015&lang=es

[10] B. Guidi, "When blockchain meets online social networks," *Pervasive and Mobile Computing*, vol. 62, p. 101131, 2020.

[11] B. Guidi, V. Clemente, T. García, and L. Ricci, "A rewarding model for the next generation social media," in *Proceedings of the 6th EAI International Conference on Smart Objects and Technologies for Social Good (GoodTechs '20)*, Antwerp, Belgium, 2020, pp. 169–174.

[12] C. Li, B. Palanisamy, R. Xu, J. Xu, and J. Wang, "Steemops: Extracting and analyzing key operations in steemit blockchain-based social media platform," in *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy (CODASPY '21)*, Virtual Event, USA, 2021, pp. 113–118.

[13] Y. Subbarayudu and A. Sureshbabu, "Cluster visualized topic modeling paradigms for recognition of health-related topics through a machine learning," *Ingénierie des Systèmes dÍnformation*, vol. 29, no. 3, pp. 1015–1030, 2024. [Online]. Available: https://doi.org/10.18280/isi.290320

[14] A. Nagappa, "Narratives of change to platform governance on dtube, an emerging blockchain-based video-sharing platform," *Social Media + Society*, vol. 9, no. 3, 2023. [Online]. Available: https://doi.org/10.1177/20563051231196881

[15] Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," *Electronics*, vol. 12, no. 6, 2023. [Online]. Available: https://doi.org/10.3390/electronics12061333

[16] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan, R. Chou, J. Glanville, J. M. Grimshaw, A. Hróbjartsson, M. M. Lalu, T. Li, E. W. Loder, E. Mayo-Wilson, S. McDonald, and D. Moher, "The prisma 2020 statement: An updated guideline for reporting systematic reviews," *Journal of Clinical Epidemiology*, vol. 134, pp. 178–189, 2021. [Online]. Available: https://doi.org/10.1016/j.jclinepi.2021.03.001

[17] J. Z. Llamas Covarrubias, "Transparencia y protección de datos personales en la cadena de bloques (blockchain)," *Estudios En Derecho a La Información*, vol. 1, no. 11, pp. 27–63, 2020. [Online]. Available: https://doi.org/10.22201/iij.25940082e.2021.11.15299

[18] P. U. Waghe, A. S. Kumar, A. B. Prasad, V. S. Rao, E. Thenmozhi, S. R. Godla, and Y. A. B. El-Ebiary, "Blockchain-enabled cybersecurity framework for safeguarding patient data in medical informatics," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 15, no. 3, 2024. [Online]. Available: http://dx.doi.org/10.14569/IJACSA.2024.0150381

[19] M. Y. Shakor, M. I. Khaleel, M. Safran, S. Alfarhood, and M. Zhu, "Dynamic aes encryption and blockchain key management: A novel solution for cloud data security," *IEEE Access*, vol. 12, pp. 26 334–26 343, 2024. [Online]. Available: https://doi.org/10.1109/ACCESS.2024.3351119

[20] C. Awasthi, "Preservation of sensitive data using multi-level blockchain-based secured framework for edge network devices," *Journal of Grid Computing*, vol. 21, no. 4, p. 69, 2023. [Online]. Available: https://doi.org/10.1007/s10723-023-09699-2

[21] Y. Qu, "Towards privacy-aware and trustworthy data sharing using blockchain for edge intelligence," *Big Data Mining and Analytics*, vol. 6, no. 4, pp. 443–464, 2023. [Online]. Available: https://doi.org/10.26599/BDMA.2023.9020012

[22] H. N. Alsuqaih, W. Hamdan, H. Elmessiry, and H. Abulkasim, "An efficient privacy-preserving control mechanism based on blockchain for e-health applications," *Alexandria Engineering Journal*, vol. 73, pp. 159–172, 2023. [Online]. Available: https://doi.org/10.1016/j.aej.2023.04.037

[23] A. A. Alanazi, F. K. Karim, S. A. Ghorashi, G. Amoudi, and S. H. A. Hamza, "Blockchain with optimal deep learning assisted secure data sharing and classification on future healthcare systems," *Alexandria Engineering Journal*, vol. 99, pp. 168–179, 2024. [Online]. Available: https://doi.org/10.1016/j.aej.2024.05.023

[24] Y. Li, L. Liang, Y. Jia, W. Wen, C. Tang, and Z. Chen, "Blockchain for data sharing at the network edge: Trade-off between capability and security," *IEEE/ACM Transactions on Networking*, vol. 32, no. 3, pp. 2616–2630, 2024. [Online]. Available: https://doi.org/10.1109/TNET.2024.3364023

[25] S. Mohammed, N. Al-Aaraji, and A. Al-Saleh, "Comparative analysis of blockchain platforms for security enhancement in online social networks," *Ingénierie des Systèmes dÍnformation*, vol. 29, no. 1, pp. 19–25, 2024. [Online]. Available: https://doi.org/10.18280/isi.290103

[26] R. Zhu, M. Wang, X. Zhang *et al.*, "Investigation of personal data protection mechanism based on blockchain technology," *Scientific Reports*, vol. 13, no. 21918, 2023. [Online]. Available: https://doi.org/10.1038/s41598-023-48661-w