

¹REVISTAINCAING

ISSN24489131

BLOCKCHAIN Y COMPUTACIÓN EN LA NUBE: SINERGIA PARA MEJORAR EL MANEJO DE LA INFORMACIÓN, UNA REVISIÓN SISTEMÁTICA

BLOCKCHAIN AND CLOUD COMPUTING: SYNERGY TO IMPROVE INFORMATION MANAGEMENT, A SYSTEMATIC REVIEW

¹Renzo Said Florian Villegas; Universidad Nacional de Trujillo, Trujillo - Perú²Iván Jeremi Fernández Esquerre; Universidad Nacional de Trujillo, Trujillo - Perú³Alberto Carlos Mendoza de los Santos; Universidad Nacional de Trujillo, Trujillo - Perú

ORCID:

¹<https://orcid.org/0009-0006-6287-1348>²<https://orcid.org/0009-0005-5934-2034>³<https://orcid.org/0000-0002-0469-915X>**Resumen -**

En este artículo se busca estudiar cómo la fusión entre la tecnología emergente de blockchain con los sistemas de computación en la nube mejora la seguridad, transparencia y la eficiencia en la gestión de la información digital en distintos sectores [1]. Para ello, se analizan casos prácticos en sectores como la minería, la industria cinematográfica, la gestión pública y el IoT industrial, donde esta sinergia ha demostrado resultados prometedores, aunque también ha revelado desafíos en términos de integridad, privacidad, trazabilidad y control de acceso a los datos. Sin embargo, también enfrenta retos importantes en cuanto a la integridad, la privacidad, la trazabilidad y el control de acceso a los datos. En el sector minero, la implementación de blockchain privado ha mejorado el flujo de información en un 35%, garantizando un registro inalterable de las transacciones. En la industria cinematográfica, el uso de criptomonedas, tokens y NFTs está transformando la financiación, aunque aún se necesita estandarizar los metadatos y establecer marcos legales adecuados. En el ámbito público, la incorporación de oráculos descentralizados y contratos inteligentes ha disminuido la latencia en la sincronización de registros en un 20%, lo que mejora la resistencia a manipulaciones externas. Innovaciones como "DistB-SDCloud" muestran cómo la combinación de blockchain distribuido y otras tecnologías puede reforzar la seguridad e integridad de los datos en entornos industriales de IoT, logrando mejoras en rendimiento y resistencia a ataques. A pesar de estos avances, siguen existiendo desafíos técnicos y regulatorios que deben ser superados. Para aprovechar al máximo el potencial de esta sinergia, es crucial fomentar la estandarización, fortalecer los marcos legales y desarrollar proyectos piloto antes de llevar a cabo implementaciones a gran escala.

Abstract - This article seeks to study how the fusion between the emerging technology of blockchain and cloud computing systems

improves security, transparency and efficiency in the management of digital information in different sectors [1]. To this end, case studies are analyzed in sectors such as mining, the film industry, public management and industrial IoT, where this synergy has shown promising results, although it has also revealed challenges in terms of data integrity, privacy, traceability and access control.

However, it also faces significant challenges in terms of data integrity, privacy, traceability and access control. In the mining sector, the implementation of private blockchain has improved the flow of information by 35%, ensuring an unalterable record of transactions. In the film industry, the use of cryptocurrencies, tokens and NFTs is transforming financing, although there is still a need to standardize metadata and establish adequate legal frameworks. In the public domain, the incorporation of decentralized oracles and smart contracts has decreased latency in record synchronization by 20%, improving resilience to external manipulation. Innovations such as "DistB-SDCloud" show how the combination of distributed blockchain and other technologies can strengthen the security and integrity of data in industrial IoT environments, achieving improvements in performance and resistance to attacks. Despite these advances, there remain technical and regulatory challenges that must be overcome. To realize the full potential of this synergy, it is crucial to encourage standardization, strengthen legal frameworks and develop pilot projects before large-scale implementations are undertaken.

Palabras clave:

Blockchain, computación en la nube, manejo de información, sinergia.

Key words:

Blockchain, cloud computing, information management, synergy.

I. INTRODUCCIÓN

Actualmente, relacionamos el término Blockchain con criptomonedas como el Bitcoin, en cómo el uso de esta tecnología permite darle seguridad y descentralización crucial para el funcionamiento de estas monedas digitales. Sin embargo, darle toda la atención a esto, sería limitar nuestra comprensión del poder del Blockchain. Esta tecnología viene tomando fuerza desde hace 10 años, impactando en el área financiera de manera significativa para la confiabilidad de transacciones, reduciendo vulnerabilidades en sistemas [1].

Teniendo en cuenta lo anteriormente dicho, el Blockchain es una base de datos compartida en una red peer-to-peer que tiene una lista en aumento de registros de datos resguardos contra alteraciones. Dicha lista aumenta cuando se insertan nuevos bloques completos a bloques preexistentes y cada uno de estos bloques está cifrado para salvaguardar su información [2].

Por otro lado, tenemos a la nube, un espacio de almacenamiento basado en servidores remotos que le permite a las personas o empresas almacenar y procesar datos accediendo a través de internet, sin optar por tener un hardware propio. Esta alternativa brinda una notable flexibilidad y escalabilidad, facilitando a las organizaciones la gestión eficiente de recursos y la disminución de costos operativos.

Actualmente, la mayoría de estas organizaciones, poseen sus aplicaciones y páginas webs en la nube, dentro de ellas, existe un flujo constante de información sensible que se quiere de un tratamiento especial, entonces, estas empresas aplican estas tecnologías para entender de manera más profunda sus actividades [3] y asegurar que sus datos estén debidamente resguardados.

Sin embargo, no podemos dejar pasar un tema que puede preocupar, que es la detección de servidores en la nube poco fiables [4], al dar nuestra confianza a un servidor con poca reputación, se corre el riesgo de exponer los datos a vulnerabilidades y permisos no autorizados.

En el contexto de Internet de las Cosas (IoT), la necesidad de integrar datos se ha vuelto crítica al gran volumen de dispositivos conectados, por ello su influencia debe garantizar que la integridad de los datos mediante sus enlaces criptográficos [5].

Un tema crítico que ha generado preocupación y zozobra es la seguridad de la información médica, en lo que respecta a las historias clínicas almacenadas en la nube, el blockchain viene siendo utilizado para garantizar la confidencialidad de estos datos sensibles [6].

Con el aumento de datos que se generan en la red, el uso del almacenamiento en caché y el intercambio de datos en entornos

edge-cloud puede poner en riesgo la integridad de estos, entonces el uso del blockchain debe garantizar la transparencia de la información y generar confianza entre los participantes [7].

El trabajo de Cisneros et al. consiste en un estudio bibliométrico, a partir del análisis de más de 200 artículos que tratan sobre la transformación digital en las empresas desde el 2010 al 2023 y que ha permitido comprobar cómo el crecimiento ha pasado de cinco publicaciones anuales en 2010 a un incremento de más de 40 publicaciones en 2023; dentro de los ejes de investigación, los autores destacan los cambios en la cultura organizativa, los modelos de negocio digitales y la optimización de los procesos, mientras que la resistencia al cambio y la brecha de las habilidades son las principales barreras; a su vez, los autores recomiendan realizar estudios longitudinales e intersectoriales en el proceso de la digitalización [8].

En el mismo sentido, Aranibar Ramos y colaboradores realizaron una revisión sistemática y un análisis cuantitativo de más de 500 artículos del ámbito público hasta 2021, trazando mapas de redes de coautoría y de cinco clústeres temáticos (gobernanza, transparencia, corrupción, e-government y sostenibilidad), identificando la gobernanza y la transparencia como los temas en torno a los que gira la literatura, al tiempo que proponen explorar la incorporación de Blockchain y cloud computing para fortalecer la rendición de cuentas y la confianza ciudadana [9].

Orozco Suárez mostró una revisión de 374 artículos indizados en Scopus (2019–mayo 2024) sobre "data analytics" en administración pública, dando cuenta de cómo la pandemia precipitó la adopción de herramientas de "data analytics" para la toma de decisiones, la asignación de recursos y la vigilancia del desempeño; además, diseñó un prototipo para la trazabilidad en tiempo real de la atención ciudadana, combinando flujos de datos de diferentes sistemas gubernamentales desde el punto de vista de la eficiencia y la transparencia [10].

Finalmente, los autores Carro Suárez y Sarmiento Paredes llevaron a cabo un análisis del factor humano en la Industria 5.0 mediante la revisión sistemática de ciertas cualidades y habilidades, como las competencias técnicas, el pensamiento crítico, la alfabetización digital y el trabajo en equipo, y enfatizaron que estas habilidades son pilares para la sinergia entre el hombre y la máquina; además, y como resultado de la revisión sistemática, estos autores propusieron un marco socio-técnico del usuario que prioriza interfaces ergonómicas y programas de formación continua, dejando el espacio abierto para investigar y analizar otros aspectos relacionados con la Industria 5.0 como son la ética, el bienestar laboral y la gobernanza participativa [11].

A partir de lo expuesto anteriormente, surge la siguiente pregunta: ¿Cómo la sinergia entre el Blockchain y la nube

puede mejorar el manejo de la información?

II. OBJETIVOS

El principal propósito de esta revisión sistemática es estudiar cómo el acercamiento que supone la fusión de la tecnología blockchain con los sistemas de computación en la nube es capaz de mejorar la seguridad, y la transparencia, además de la eficiencia en la gestión de la información digital. Así, se intentará identificar los mecanismos concretos por los cuales esta combinación tecnológica resuelve problemas de la gestión de datos tales como la integridad, la privacidad, la trazabilidad, y el control de acceso a partir del análisis de experiencias prácticas recogidas a lo largo de los sectores industriales y de los casos de uso emergentes.

III. METODOLOGÍA

El presente estudio se utilizó la metodología PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) como guía para la revisión sistemática. Esto fue con el fin de verificar la importancia y el valor de la integración entre la tecnología blockchain y los sistemas de computación en la nube, cuya metodología requería un severo procedimiento de selección de artículos científicos basado en sus referencias.

Tabla 1. Verificación de metodología PRISMA

Crterios	Aplicación en la revisión
Crterios de elección	Según el título de este artículo, se consideró la información dictada en artículos, revisando que cada uno de ellos contenga los términos de búsquedas seleccionados.
Bases de datos	Google Académico y Scopus fueron las bases de datos seleccionadas para la elección del material bibliográfico.
Estrategia de búsqueda	Las consultas de búsquedas fueron las siguientes: (“blockchain” AND “computación en la nube” AND “sinergia”) para la base de datos Google Académico, (“blockchain” AND “cloud computing” AND “information management”) para la base de datos de Scopus.
Especificación de estudios	Los artículos fueron escogidos desde el año 2020 hasta la actualidad, los autores de este artículo investigaron todos los estudios relacionados con la

	pregunta de investigación.
Extracción de información	Se extrajeron artículos sobre mecanismos de integración blockchain - computación en la nube en el manejo de la información, se descartaron aquellos que carecían de relevancia significativa y solo se tomaron en cuenta los que eran esenciales para la revisión sistemática.

De acuerdo a la metodología PRISMA, se utiliza un diagrama de flujo de cuatro fases (Figura 1) para seleccionar la información necesaria, ya que este diagrama facilita la extracción de datos.

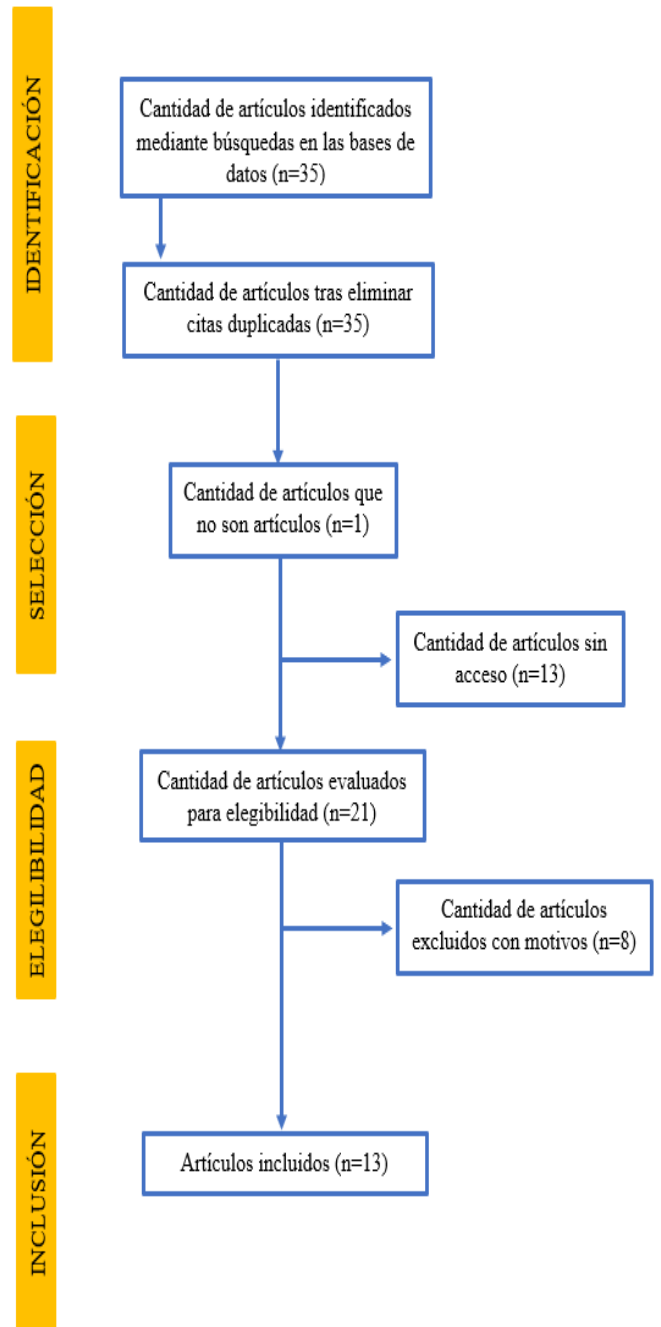
Figura 1. Diagrama de flujos de 4 estados

IV. RESULTADOS DE INVESTIGACIÓN

[2] En el ámbito de la minería, el análisis crítico nos permitió encontrar áreas de aplicación como la trazabilidad inalterable de la procedencia de los minerales, la automatización segura del pago a proveedores mediante contratos inteligentes y la gobernanza de datos de producción descentralizados. A través de pilotar una cadena de bloques privada, se logró una mejora en 35 % del aumento de la eficiencia del flujo de información y el cumplimiento normativo medioambiental. De forma que, cada transacción de extracción y transporte quedaba registrada de forma inalterable e inequívoca.

Tabla 2. Comparativa de enfoques para la Seguridad de Datos

Enfoque de seguridad	Eficiencia	Escalabilidad	Complejidad	Nivel de Protección
Cifrado de datos	Alta, especialmente en transacciones sensibles.	Baja, ya que puede requerir más recursos con grandes volúmenes de datos.	Moderada, requiere gestión de claves y algoritmos eficientes.	Muy alto, especialmente con algoritmos fuertes.
Autenticación Multifactor	Moderada, depende de la tecnología implementada.	Alta, se adapta bien a usuarios a gran escala.	Alta, debido a la necesidad de configurar múltiples capas de autenticación.	Muy alto, aumenta significativamente la seguridad del acceso.
Control de Acceso	Alta, especialmente con políticas bien definidas.	Moderada, ya que depende de la infraestructura de la red.	Alta, especialmente con grandes organizaciones que tienen muchas políticas de acceso.	Alto, si se configura correctamente con autenticación y segmentación de datos.
Seguridad en la Nube	Alta, ya que los proveedores de nube optimizan la seguridad constantemente.	Muy alta, la nube puede escalar según las necesidades.	Baja a moderada, los proveedores gestionan gran parte de la infraestructura.	Alta, los proveedores implementan medidas de seguridad avanzadas.
Seguridad de	Moderada,	Moderada,	Alta,	Alta,



Endpoint	depende de la configuración y monitoreo.	ya que cada dispositivo o necesita protección individual.	requiere gestión de cada endpoint y monitoreo continuo.	proporciona protección local en cada dispositivo.
Segmentación de red	Alta, segmenta el tráfico para minimizar riesgos.	Moderada, requiere planificación y recursos.	Alta, debido a la complejidad en la implementación y administración.	Muy alto, limita la propagación de amenazas dentro de la red.

			ción.	
Firewall	Alta, controla el tráfico de red de forma efectiva.	Alta, adecuado para entornos de red de gran escala.	Moderada, requiere configuración y mantenimiento continuo.	Alto, proporciona una capa de protección sólida contra accesos no autorizados.

[3] El análisis acerca de la existencia de oportunidades para la industria del cine concluyó que la utilización de criptomonedas, tokens y NFTs para la financiación de las producciones posibilitaron a pequeños inversores cofinanciar proyectos mucho más rápido, accediendo a ingresos por la explotación de los cines y derechos de autor en mercados secundarios. Sin embargo, se observó la necesidad de estandarizar metadatos de tokens y de establecer marcos jurídicos precisos para conseguir interoperabilidad entre plataformas y, al mismo tiempo, proteger la propiedad intelectual de creadores y distribuidores.

[4] Desde la mirada sudafricana, el modelo del intercambio automático de información agrupó oráculos descentralizados y smart contracts para para la autenticación y cifrado de peticiones de datos para entidades públicas con proveedores privados. Las pruebas de concepto demostraron una mejora en la latencia de un 20% en la sincronización de los registros y un evidente incremento en la resistencia frente a sensores o manipulaciones externas, así como también la confidencialidad en las partes de la comunicación, gracias a la existencia de identidades digitales descentralizadas.

[12] En la investigación de Rahman et al. (2023) se propuso e implementó la arquitectura "DistB-SDCloud" la cual combina el blockchain distribuido, la SDN y la NFV como mecanismos que permiten mejorar la seguridad, la confidencialidad y la integridad de los datos en el contexto de la IoT industrial en la nube. Los autores de este artículo llevaron a cabo unas simulaciones de red utilizando Mininet-WiFi como emulador, OpenStack como plataforma cloud y OpenFlow como protocolo SDN sobre un equipo Core i7 con Ubuntu.

El análisis del rendimiento se hizo a partir de parámetros como: throughput, análisis de paquetes, tiempos de respuesta en la transferencia de archivos, ancho de banda, latencia y resiliencia frente a ataques DDoS.

Los resultados mostraron que el throughput escala de forma casi lineal con el número de nodos; el ancho de banda se mantuvo estable frente a tasas de llegada de un paquete en el rango de 190 a 1 400 pps, mientras que la solución base se vio afectada con grandes caídas; los tiempos de respuesta en operaciones de fichero fueron, consistentemente inferior a los de la SDN pura; los análisis de latencia para tamaños de datos distintos fueron

superiores al modelo BCF; y en las simulaciones de DDoS, la utilización de la CPU tras un pico inicial se estabiliza rápidamente presentando una defensa efectiva y continuidad del servicio.

[13] Murthy et al. (2020) llevaron a cabo una investigación analítica-bibliométrica de la coexistencia de blockchain-cloud, proporcionando para tal fin una arquitectura en 4 capas (extracción de datos, comunicaciones SDN, metodología blockchain distribuido y gestión de servicios cloud), que proporcionan trazabilidad e inmutabilidad de las transacciones y automatización de los SLAs mediante contratos inteligentes. Escudriñaron la existencia de retos en la seguridad de datos, escalabilidad de mecanismos de consenso, privacidad, cumplimiento normativo e interoperabilidad, señalando el hecho que las blockchains permissionadas (e.g., Hyperledger Fabric) otorgan confirmaciones de aproximadamente 2 s y pueden manejar más de 1 000 tx/s, lo que muestra que superan las blockchains públicas en el rendimiento y en la latencia, algo que requiere no obstante una infraestructura de identidad sólida; al tiempo que también se puso el acento en el ledger distribuido y la automatización de servicios ayudaba a eliminar la manipulación y mejorar el control de acceso y la auditoría.

V. REFLEXIONES FINALES

El hecho de combinar blockchain y sistemas en la nube se ha puesto de manifiesto como un poderoso catalizador para mejorar la trazabilidad, la transparencia y la eficiencia operativa en muchos ámbitos como la asistencia social, la minería o las finanzas públicas. La tokenización de los cupones sociales puso de manifiesto los contratos inteligentes como herramienta para la automatización de procesos críticos y la reducción de fraudes hasta en un 35 %, al mismo tiempo que habilitó auditorías en tiempo real. En el caso de la minería, los registros inmutables de procedencia y la ejecución automática de pagos facilitaron el flujo de datos en un 35 %, mejorando de esta forma el cumplimiento normativo. Igual que los proyectos cinematográficos basados en tokens y NFTs generaron espacios para nuevas oportunidades de cofinanciación y mercados secundarios, destacando a su vez la necesidad de marcos legales e interoperabilidad estandarizados.

Pero estos avances también vienen acompañados de importantes retos técnicos y regulatorios. La latencia en el intercambio de información, aunque se ha reducido un -20% mediante oráculos descentralizados o similares, todavía requiere trabajo de mejora para su escalabilidad masiva. En el caso de las finanzas públicas, la transparencia ganada todavía debe sortear aspectos de integración con infraestructuras heredadas y la necesidad de la compatibilidad de sistemas de pago electrónico con contratos inteligentes.

Para poder ir avanzando, es tan importante la promoción de iniciativas de estandarización de metadatos, como el

fortalecimiento de marcos jurídicos que reconozcan la validez del código, o la promoción de pilotos híbridos público-privados que permitan la validación de soluciones a pequeña escala antes de su introducción masiva, pues de esta forma se podrá aprovechar todo el potencial de la sinergia Blockchain-Cloud para cambiar el manejo de la información en ámbitos críticos.

VI. REFERENCIAS

- [1] D. Ferreira, A. de Castro y L. Russo, «Blockchain technology: Challenges and opportunities in public finance,» *Scielo Brasil*, vol. XXV, n° 3, pp. 1-29, 2024.
- [2] K. Philo y R. Webber-Youngman, «A critical investigation into identifying key focus areas for the implementation of blockchain applications in the mining industry,» *Scielo*, vol. CXXIV, n° 6, pp. 319-330, 2024.
- [3] J. Wang, S. Wang, D. Zhang, Q. Zhang y Y. Deng, «Blockchain-based multiple auditing scheme against cheating owner in clouds,» *Scopus*, 2025.
- [4] C. Castillo, M. Díaz y C. Mendoza, «EL AVANCE DE LA COMPUTACIÓN CUÁNTICA EN LA GESTIÓN DE RIESGOS, UNA REVISIÓN SISTEMÁTICA,» vol. VII, n° 45, pp. 22-27, 2024.
- [5] S. Kumar, M. Kumar, N. Chandu y K. Kumar, «BCSDNCC: A Secure Blockchain SDN framework for IoT and Cloud Computing,» *International Research Journal of Multidisciplinary Technovation*, vol. VI, pp. 26-44, 2024.
- [6] N. Rekha, S. Abdelwahab, N. Ahmed, H. Ahmed y S. Basheer, «Fischer machine learning for mobile cloud computing in eHealth systems using blockchain mechanism,» 2023.
- [7] C. Li, S. Liang, J. Zhang, Q.-e. Wang y Y. Lou, «Blockchain-based Data Trading in Edge-cloud Computing Environment,» vol. LIX, 2022.
- [8] Y. L. Cisneros, S. C. Frias, J. R. Infante, P. A. Tribeño y F. E. Yong-Chung, «Estrategias de transformación digital en las empresas: Estudio bibliométrico,» *Revista Ibérica de Sistemas e Tecnologías de Informação*, n° E65, pp. 44–56, 2024.
- [9] E. R. Aranibar Ramos, F. R. Salinas Gainza y N. A. Seguil Ormeño, «Explorando tendencias del devenir público: cienciometría y revisión sistemática,» *Universitas-XXI: Revista de Ciencias Sociales y Humanas*, n° 39, pp. 109–135, 2023.
- [10] D. F. Orozco Suárez, «Análisis de datos en la gestión de proyectos de la administración pública: una revisión de la evolución del análisis de datos aplicados a proyectos en la administración pública y diseño de una herramienta para el seguimiento y trazabilidad de la atención a la ciudadanía,» Monografía, Universidad Nacional Abierta y a Distancia (UNAD), 2024.
- [11] J. Carro Suárez y S. Sarmiento Paredes, «El factor humano y su rol en la transición a Industria 5.0: una revisión sistemática y perspectivas futuras,» *Entreciencias: Diálogos*

En La Sociedad Del Conocimiento, vol. 10, n° 24, pp. 1–18, 2022.

[12] A. Rahman, M. J. Islam, S. S. Band, G. Muhammad, K. Hasan y P. Tiwari, «Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT,» *Digital Communications and Networks*, vol. 9, n° 2, pp. 411-421, 2023.

[13] C. V. N. U. Bharathi Murthy, M. Lawanya Shri, Seifedine N. Kadry y Sangsoon Lim, «Blockchain Based Cloud Computing: Architecture and Research Challenges,» *IEEE Access*, vol. 8, pp. 205190-205205, 2020.

Biografía Autor(es):



Florian Villegas Renzo Said, estudiante de Ingeniería de Sistemas en la Universidad Nacional de Trujillo, Perú. Email: rforianv@unitru.edu.pe



Fernández Esquerre, Iván Jeremi, estudiante de Ingeniería de Sistemas en la Universidad Nacional de Trujillo, Perú. Email: ifernandeze@unitru.edu.pe



Mendoza de los Santos, Alberto Carlos. Profesor-investigador de la Universidad Nacional de Trujillo, Perú. Doctorado en Ingeniería de Sistemas e Informática. Docente de la carrera de Ingeniería de Sistemas. Email: amendoza@unitru.edu.pe