Revista Politécnica ISSN 1900-2351 (Impreso), ISSN 2256-5353 (En línea), Año 20, Número 40, páginas 09-29, Julio-Diciembre 2024

DOI: https://doi.org/10.33571/rpolitec.v20n40a1

# IDENTIFICACIÓN DE VARIABLES RELACIONADAS A LA SEGURIDAD INFORMÁTICA A PARTIR DE TENDENCIAS INVESTIGATIVAS DE LA TECNOLOGÍA BLOCKCHAIN

**John Edward Rueda-Castañeda [1], Natalia Gallego-Gómez [2], Edward Estanling-Cárdenas[3], Jerson Samuel Tello[4], Vanessa García Pineda[5]**

[1]Ingeniero de Sistemas en formación, Corporación Universitaria Americana, ruedajohn7588@americana.edu.co, https://orcid.org/0009-0009-9615-3311.
[2]Ingeniera de Sistemas, Instituto Tecnológico Metropolitano, nataliagallego255620@correo.itm.edu.co, https://orcid.org/0009-0001-5472-2856.
[3]Ingeniería de Sistemas en formación, Corporación Universitaria Americana, cardenasedward3579@americana.edu.co, https://orcid.org/0009-0000-7675-8764.
[4]Ingeniero de Sistemas en formación, Corporación Universitaria Americana, tellojerson7176@americana.edu.co, https://orcid.org/0009-0001-4488-1175.
[5]M. Res. En Gestión de Innovación Tecnológica, Cooperación y Desarrollo Regional, Docente Ocasional Tiempo Completo, Instituto Tecnológico Metropolitano, vanessagarciap@itm.edu.co, https://orcid.org/0000-0003-3418-8956.

## RESUMEN

La protección de los datos y la información se ha convertido en un aspecto de prioridad tanto para personas como para organizaciones. Con la difusión, apropiación y alfabetización cada vez mayor respecto al uso de las tecnologías de la información y la comunicación, los datos de las personas están cada vez más expuestos. Esto, se ha convertido en un aspecto de discusión debido a la fragilidad en los diferentes sistemas de información que pueden permitir la exposición de información delicada y personal, demandando más herramientas y estrategias de ciberseguridad. Por lo anterior, el objetivo de este trabajo es identificar las variables relacionadas a la seguridad informática a partir de las tendencias investigativas de blockchain en diferentes aplicaciones a través de una revisión sistemática de literatura. Entre los principales resultados, se encuentra la aplicación de diferentes técnicas de inteligencia artificial y la Automatización Robótica de Procesos (RPA) en el ecosistema blockchain.

**Palabras clave:** Blockchain, seguridad informática, ciberseguridad, seguridad de la información, ciberataques

Recibido: 07 de febrero de 2024. Aceptado: 21 de Mayo de 2024
*Received: February 07, 2024. Accepted: May 21, 2024*

## IDENTIFICATION OF VARIABLES RELATED TO CYBERSECURITY BASED ON BLOCKCHAIN RESEARCH TRENDS

## ABSTRACT

*The protection of data and information has become a priority for both individuals and organizations. With the increasing dissemination, appropriation and literacy regarding the use of information and communication technologies, people's data is increasingly exposed. This has become an aspect of discussion due to the fragility of the different information systems that can allow the exposure of sensitive and personal information, demanding more cybersecurity tools and strategies. Therefore, the objective of this work is to identify the variables related to computer security from blockchain research trends in different applications through a systematic literature review. Among the main results is the application of different artificial intelligence techniques and Robotic Process Automation (RPA) in the blockchain ecosystem.*

**Keywords:** *Blockchain, computer security, cybersecurity, information security, cyber attacks*

*Cómo citar este artículo: J. Rueda-Castañeda, et al. "Identificación de variables relacionadas a la seguridad informática desde la aplicación de la tecnología blockchain", Revista Politécnica, vol.20, no.40 pp.09-29, 2024. DOI:10.33571/rpolitec.v20n40a1*

## 1. INTRODUCCIÓN

Blockchain se ha convertido en una tecnología crucial, ya que permite la preservación segura, descentralizada y rentable de información que debe mantenerse inalterable y accesible. De acuerdo con un artículo publicado por la empresa Seguridad esencial contra amenazas en evolución (Essential Security against Evolving Threats - ESET), esta tecnología posibilita el almacenamiento seguro y descentralizado de prácticamente cualquier tipo de información que deba mantenerse inalterable y accesible, a menudo a un costo más bajo que a través de intermediarios [1]. Además, si la información se almacena cifrada, se garantiza su confidencialidad, ya que solo las personas con la clave de cifrado pueden acceder a ella. El impacto de esta tecnología es notable en varios sectores, como las finanzas, la cadena de suministro, la atención médica y el Internet de las Cosas, al mejorar la seguridad, la eficiencia y la transparencia en diversas aplicaciones [1].

Así, recientemente ha emergido como una tecnología innovadora que ha cobrado fuerza durante la última década. Su función principal radica en simplificar el proceso de registro de transacciones y el seguimiento de activos en una red empresarial. Sea que se trate de un activo físico, como una vivienda o dinero en efectivo, o de un activo intangible, como propiedad intelectual o derechos de autor, blockchain puede rastrear y gestionar prácticamente cualquier elemento de valor. Este enfoque conlleva una significativa reducción de riesgos y costos para todas las partes involucradas en una transacción [2]. Adicionalmente, esta tecnología ha encontrado aplicaciones en diferentes campos, por ejemplo, en la cadena de suministro principalmente en industria de alimentos.

La tecnología Blockchain ha emergido como una tecnología transformadora en la cadena de suministro, especialmente en la industria alimentaria. Mediante la asignación de códigos de rápida respuesta (Quick Response QR) que contienen información detallada acerca del origen de los productos y su trayectoria en la cadena de suministro, las empresas pueden rastrear productos perecederos desde su origen en la granja hasta el consumidor final. Este proceso fomenta una mayor claridad y eficiencia en la gestión. No solamente facilita la identificación y retirada selectiva de productos del mercado, reduciendo así el desperdicio y los gastos, sino que también empodera a minoristas y consumidores al proporcionarles información esencial sobre los productos, como su procedencia y características. Además, la tecnología blockchain ha demostrado ser altamente prometedora en la monitorización de suministros médicos, permitiendo la autenticación de los envíos de medicamentos [3].

Por esta razón, la tecnología Blockchain emerge como una estrategia innovadora que proporciona seguridad, rapidez y transparencia en el ámbito digital. Visionarios como los autores Tapscott y Tapscott [4] sugieren que tiene el potencial de revolucionar significativamente no solo el sector de servicios financieros, sino también en los demás sectores económicos, industriales y académicos. De esta manera, se reconoce como una tecnología disruptiva para el registro de sucesos por medio de un sistema distribuido y replicado, como indica Bartolomé [5]. Este impacto se ha manifestado de manera notable en el ámbito financiero, con ejemplos destacados como el Banco de Inglaterra, Visa, Santander, USB, BNY Mellon y Deutsche Bank[6]. De esta manera, la Blockchain engloba una amplia gama de aplicaciones, siendo las criptomonedas, especialmente Bitcoin, las más destacadas. El éxito de Bitcoin se fundamenta en su sistema descentralizado y en el uso de pruebas que se almacenan en toda la red, preservando el anonimato de los usuarios. Este atributo ha suscitado un interés generalizado en la potencialidad de Blockchain en diversos campos, como la gestión de la identidad digital, la atención a comunidades desfavorecidas, el registro de historiales médicos y, sin lugar a duda, la educación [7].

Es por lo anterior por lo que esta esta tecnología surge como una revolución en la seguridad y confiabilidad del entorno digital. Además, su capacidad para asegurar la integridad de los datos y proteger contra amenazas cibernéticas la convierte en un recurso valioso para empresas e industrias de diversa índole. A medida que sigue avanzando, su impacto en la sociedad y la seguridad en línea continua siendo de gran relevancia. Así, la importancia de Blockchain en el ámbito de la ciberseguridad radica en que, durante el año 2023, se han producido eventos significativos de ciberataques en todo el mundo. Estos incidentes enfatizan la necesidad apremiante de fortalecer la ciberseguridad a nivel global y aumentar la concienciación sobre las amenazas cibernéticas en todos los sectores [8].

Según el Reporte Global de Ransomware 2023 se informa que el 84% de las empresas a nivel mundial ha enfrentado incidentes de seguridad cibernética en el último año, con un promedio de tres violaciones

de seguridad por organización en la región de América Latina y el Caribe [9]. De manera similar, se registró una filtración de información que afectó a más de 200,000 usuarios durante la emergencia médica en el caso del Casmu [10].

También, el Instituto Nacional de Ciberseguridad (INCIBE) identificó una campaña de phishing que suplantaba a Endesa, empleando enlaces maliciosos para instalar el troyano bancario Grandoreiro [11]. Paralelamente, en el contexto actual en el cual se viene dando una rápida transformación digital, se ha destacado la necesidad de un enfoque completo de ciberseguridad. Además, se han registrado múltiples casos de hackers que atacaron cuentas verificadas en Facebook y distribuyeron malware mediante anuncios engañosos. En otro escenario, un troyano de suscripción conocido como Fleckpe afectó a más de 620,000 dispositivos a través de aplicaciones disponibles en la Google Play Store. Estos incidentes subrayan la urgente necesidad de fortalecer la ciberseguridad a nivel global y aumentar la conciencia sobre las amenazas cibernéticas en todos los sectores [8].

En el contexto latinoamericano, la región experimentó un incremento considerable en intentos de ciberataques en 2022, con más de 360,000 millones de intentos en el segundo semestre del año. Según la Asociación de Bancos de México y la American Chamber, México sufrió el 66% de los ataques cibernéticos en América Latina entre 2021 y 2022, lo que resultó en pérdidas anuales estimadas en un rango de 3,000 a 5,000 millones de dólares. De hecho, los directores de empresas mexicanas identifican la ciberseguridad como su principal preocupación en el presente año, según el Global CEO Survey 2022 [12].

En Chile, el ejército experimentó un ataque cibernético en su red interna, lo que implicó la implementación de medidas de precaución [13]. Por su parte, Colombia enfrentó un aumento significativo en los intentos de ciberataques, llegando a 20,000 millones en un año, lo que representó un incremento del 80% en comparación con 2021. Además, se mantiene un alto nivel de amenazas de ransomware, junto con la persistente utilización de malware antiguo y botnets en los ataques cibernéticos. Según el Informe Global de Brecha de Habilidades en Ciberseguridad de 2023, un 53% más de organizaciones experimentaron cinco o más violaciones de seguridad de 2021 a 2022 debido a la falta de personal y la presión sobre los equipos de ciberseguridad [14]. Es por lo anterior, por lo que este trabajo tuvo como objetivo identificar las variables relacionadas a la seguridad informática a partir de tendencias investigativas de blockchain por medio de una revisión sistemática de literatura.

El documento se estructura de la siguiente manera; inicialmente, se proporciona información relacionada con la seguridad en la aplicación de la tecnología blockchain, destacando su importancia en un contexto donde la ciberseguridad es una preocupación creciente. Posteriormente, se presenta la metodología utilizada para abordar la investigación, luego se presentan los resultados y finalmente se abordan la discusión y conclusiones.

## 2. MATERIALES Y METODO

Las revisiones sistemáticas de literatura han sido uno de los métodos más utilizados por los investigadores para la comprensión conceptual de una temática estudiada y para identificar las tendencias y avances investigativas respecto al objeto de estudio. La revisión de literatura desempeña un papel central en la investigación de blockchain debido a la naturaleza dinámica y compleja de esta tecnología. Dado el constante avance en el campo de la tecnología blockchain, llevar a cabo una revisión de literatura se convierte en una herramienta esencial para mantenerse al día con los últimos desarrollos, identificar desafíos recurrentes y evaluar soluciones propuestas [15].

Las revisiones sistemáticas de literatura son un proceso metodológico en el cual se recopilan, evalúan, sintetizan y analizan rigurosamente todos los estudios relevantes existentes sobre un tema o pregunta específica. Su propósito principal es proporcionar una visión completa y objetiva de la evidencia científica disponible para abordar preguntas de investigación o resolver problemas particulares. Estas revisiones son fundamentales para la toma de decisiones basadas en evidencia y son esenciales en la práctica clínica e investigación [16].

Pasos para realizar una Revisión Sistemática en la Investigación Tecnológica, se deben seguir varios pasos:

1. Definir una Pregunta de Investigación Clara: La formulación de una pregunta específica de investigación estructurada utilizando el enfoque PICO (Población, Intervención, Comparación, Resultados) es esencial para delimitar los componentes clave de la pregunta [17]. En este caso, se formuló como pregunta de investigación la siguiente ¿Cuáles son las variables que influyen en la mejora de la seguridad cibernética a través del uso de blockchain?

2. Especificar Criterios de Inclusión y Exclusión: Establecer criterios que determinen qué estudios serán considerados para la revisión y cuáles serán excluidos. Esto incluye el tipo de estudio, el año de publicación y otros factores relevantes. Para esta ocasión, se formularon los siguientes criterios:

    - Criterios de Inclusión:
        - Estudios académicos y científicos publicados en la Biblioteca Científica Scielo y Redalyc del 2020 al 2023.
        - Investigaciones que aborden específicamente la relación entre seguridad cibernética y la aplicación de blockchain.
        - Sin restricciones de idioma para garantizar inclusividad global.
        - Enfoque en variables específicas que impactan la efectividad de la seguridad cibernética mediante la implementación de blockchain.

    - Criterios de Exclusión:
        - Estudios no académicos o sin revisión por pares.
        - Investigaciones no relacionadas directamente con la intersección de seguridad cibernética y blockchain.
        - Estudios anteriores al año 2020.
        - Trabajos que no abordan explícitamente variables clave o carezcan de rigurosidad metodológica.

3. Estrategia de Búsqueda

En una revisión sistemática de la literatura sobre seguridad cibernética y la tecnología blockchain, se implementa una estrategia de búsqueda específica para identificar estudios pertinentes. La ecuación de búsqueda utilizada es "(seguridad OR security) AND 'blockchain". Las bases de datos académicas de Redalyc y Scielo se seleccionaron estratégicamente debido a su enfoque en la producción de contenido científico. Esta selección permitió abordar la temática desde una perspectiva global, sin restricciones de idioma o año de publicación. Las bases de datos académicas de Redalyc y Scielo se seleccionaron estratégicamente debido a su enfoque en la producción de contenido científico. Esta selección permitió abordar la temática desde una perspectiva que abarca una amplia gama de estudios, independientemente de su idioma de publicación. Luego de usar la ecuación de búsqueda en las bases de datos seleccionadas, se obtuvo un conjunto de resultados los cuales se procedió a revisar los títulos y resúmenes de los artículos encontrados y luego a leer detenidamente los textos completos. Como resultado de este proceso, se seleccionaron 25 artículos que se ajustaban a los criterios que se tenían previamente establecidos. Cada uno de estos artículos se examinó de cerca y se resumió, lo que brindó una comprensión más completa de las investigaciones relacionadas con la seguridad en la tecnología blockchain, desde distintos puntos de vista.

4. Registro y Evaluación de la Calidad de los Estudios Seleccionados: Es importante registrar y evaluar en detalle las características de los estudios incluidos, incluyendo su metodología y posibles sesgos.

5. Presentación de los Resultados: Después de revisar los 25 artículos elegidos y organizar la información en una base de datos en formato Excel, los datos se categorizaron en función de diversas variables. Estas variables incluyeron; el título, los autores, el año de publicación, la revista, la metodología, el país de origen, variables relacionadas con la seguridad, blockchain, herramientas y aplicaciones específicas. Esta clasificación por variables facilitó un análisis efectivo y proporciona una visión estructurada de la investigación relacionada con la seguridad y la tecnología blockchain. El registró se realizó de la siguiente manera;

- Título: Se registró el título de cada artículo seleccionado, lo que permite identificar rápidamente el tema central de cada estudio.
- Autores: Se registraron los nombres de los autores de los artículos seleccionados, lo que facilita la atribución de la autoría y la identificación de expertos en el campo.
- Año: Se anotó el año de publicación de cada artículo, lo que puede ser importante para evaluar la relevancia temporal de la investigación.
- Revista: Se registró el nombre de la revista en la que se publicó cada artículo, lo que ayuda a contextualizar la fuente de la investigación.
- Metodología: Se documentó la metodología de investigación utilizada en cada artículo, lo que puede ayudar a entender cómo se llevó a cabo el estudio y evaluar su calidad metodológica.
- País: Se anotó el país de origen de los autores o el país de afiliación de la institución, lo que puede proporcionar información sobre la ubicación geográfica de la investigación.
- Variables Relacionadas a Seguridad: Se registraron las variables específicas relacionadas con la seguridad que se abordaron en cada artículo, lo que facilita la identificación de los aspectos de seguridad tratados en la literatura.
- Variables relacionadas a Blockchain: Se documentaron las variables específicas relacionadas con la tecnología blockchain que se exploraron en cada artículo, lo que ayuda a comprender los aspectos de blockchain en el contexto de la investigación.
- Variables relacionadas a Herramienta: Se anotaron las herramientas o tecnologías específicas que se mencionaron o utilizaron en los estudios, lo que puede ser relevante para comprender cómo se llevaron a cabo las investigaciones.
- Aplicación: Se registró la aplicación o el caso de uso concreto que se abordó en cada artículo, lo que permite entender en qué contextos se aplicó la tecnología blockchain en relación con la seguridad.

6. Conclusión y Presentación de Resultados: Se revisaron los 25 artículos publicados en revistas donde los resultados fueron sometidos a un análisis de acuerdo con los criterios de inclusión y exclusión. Posteriormente, se procedió a organizar la información en una base de datos en formato Excel donde se sintetizaron los documentos por:

    - Nombres de los autores
    - País
    - Revista donde fueron publicados
    - Metodología que utilizaron
    - Año en el que fue publicado
    - Variables Relacionadas a Seguridad
    - Variables relacionadas a Blockchain
    - Variables relacionadas a Herramienta
    - Variables relacionadas a Aplicación.

Adicionalmente, se presenta un análisis de tendencias y análisis de variables a partir de los términos clave encontrados en la base de datos Scopus. Para ello se utiliza la ecuación de búsqueda “TITLE ( ( "seguridad informática" OR "information security" ) AND blockchain )” y los datos extraídos se analizan utilizando el software VosViewer y Biblioshiny de Bibliometrix de R°. En total se encontraron 59 artículos relacionados para el tema objeto de estudio entre los años 2017 y 2024.

## 3. RESULTADOS

Esta investigación destaca el creciente papel de la tecnología blockchain en la era digital, abordando desafíos cambiantes. A lo largo de los años, se ha observado un aumento en la productividad investigativa y la diversidad de aplicaciones a nivel global. La revisión de literatura se destaca como la metodología predominante, subrayando la necesidad de comprender y contextualizar blockchain en un mundo en constante cambio. En última instancia, blockchain no solo resuelve desafíos en una variedad de sectores, sino que también respalda la seguridad, eficiencia y sostenibilidad en la empresa global. La Figura 1 muestra cómo la investigación en seguridad en Blockchain ha evolucionado a lo largo de los años. Cada año en el gráfico representa una etapa diferente en la historia de esta tecnología.

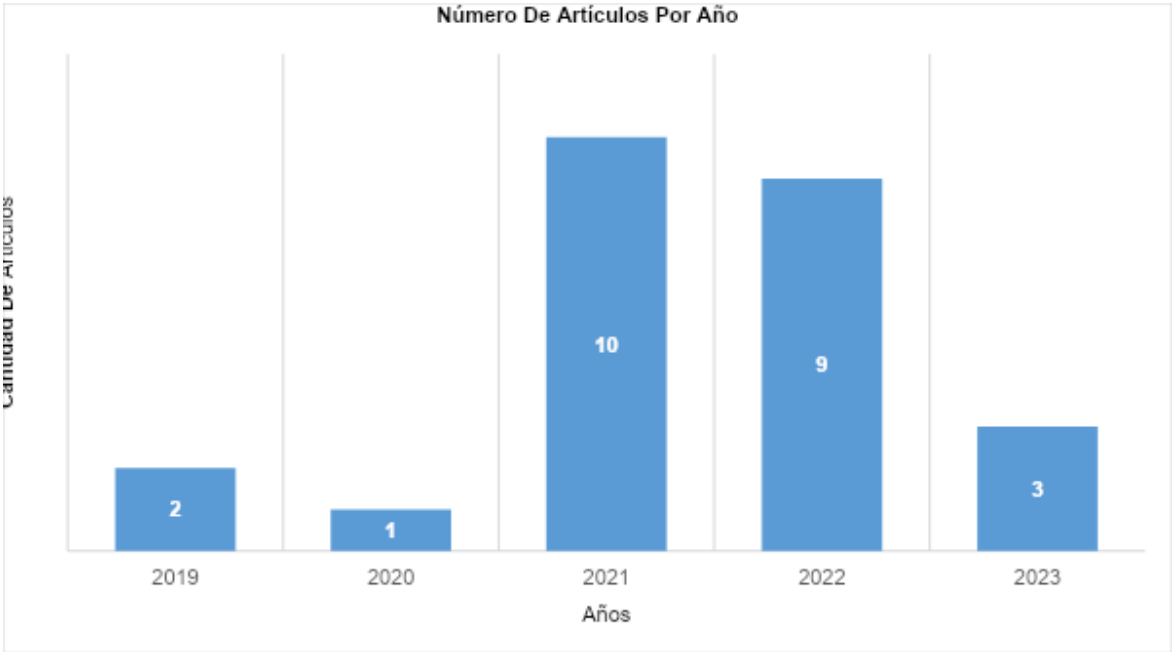


Figura 1. Productividad investigativa respecto a Blockchain y ciberseguridad por año.

En 2019, la investigación se centró en la privacidad y la publicidad en línea. Uno de los artículos exploró cómo la tecnología blockchain podría abordar los desafíos en la publicidad digital, mejorando la privacidad y la confiabilidad en este campo en constante evolución. A medida que la publicidad en línea creció exponencialmente, se hizo evidente la necesidad de soluciones que protegieran la privacidad de los usuarios y garantizaran la transparencia en la recopilación de datos. Además, sugiere que blockchain podría desempeñar un papel crucial al ofrecer soluciones que mejoren la confiabilidad y la seguridad de la privacidad en el entorno de la publicidad digital.

El año 2020 destacó la relevancia de la tecnología blockchain en la educación y la seguridad en línea. Se exploró cómo blockchain garantiza la autenticidad de las credenciales educativas y protege la integridad de los registros académicos en un mundo cada vez más digitalizado. Con la pandemia de COVID-19 impulsando la educación en línea, la verificación de títulos y certificados se volvió crucial. Los empleadores y las instituciones educativas necesitaban una forma confiable de verificar la autenticidad de las credenciales en un entorno digital, y blockchain emergió como una tecnología que ofrece esta confiabilidad y seguridad.

En 2021, la regulación de las criptomonedas y monedas digitales fue un tema importante. Se reflejó la creciente atención a la regulación de estas tecnologías, especialmente a medida que las criptomonedas se volvieron más comunes. La regulación es esencial para garantizar la estabilidad financiera y la protección del consumidor en este nuevo panorama digital. Con la creciente adopción de criptomonedas como Bitcoin, los gobiernos y las entidades reguladoras han estado trabajando en marcos legales y regulaciones para supervisar y garantizar la seguridad de estas monedas digitales. El año 2022 se caracterizó por un enfoque en la ciberseguridad y la atención médica. Se exploró cómo blockchain contribuye a la mitigación de amenazas cibernéticas y a la protección de datos sensibles en un mundo digitalmente conectado. La ciberseguridad ha tomado un rol prioritario en las organizaciones a medida que las amenazas en línea aumentan en sofisticación. Además, la aplicación de blockchain en la atención médica se volvió relevante para la gestión segura de registros médicos y datos de salud. El uso de blockchain puede brindar mayor integridad y confidencialidad de los registros de salud en un entorno donde la seguridad de los datos es fundamental.

En el año 2023, se enfatizó la importancia de la certificación de energía renovable. Se exploró cómo blockchain se utiliza para rastrear y verificar la producción de energía limpia, lo que es esencial en la transición hacia fuentes de energía renovables y el cambio de fuentes fósiles hacia energías sostenibles. Los certificados de energía renovable desempeñan un papel crítico en la garantía de la autenticidad de

la energía producida de manera ecológica. Blockchain proporciona una solución eficiente y confiable para rastrear y verificar estos certificados, lo que contribuye a la transición global hacia una energía más sostenible. Con relación a la productividad por países, la Figura 2 brinda una representación visual de la relación entre la cantidad de artículos de investigación sobre seguridad en Blockchain y los países en los que se han realizado. Cada país en el gráfico muestra su nivel de compromiso y actividad en la investigación en esta tecnología emergente.

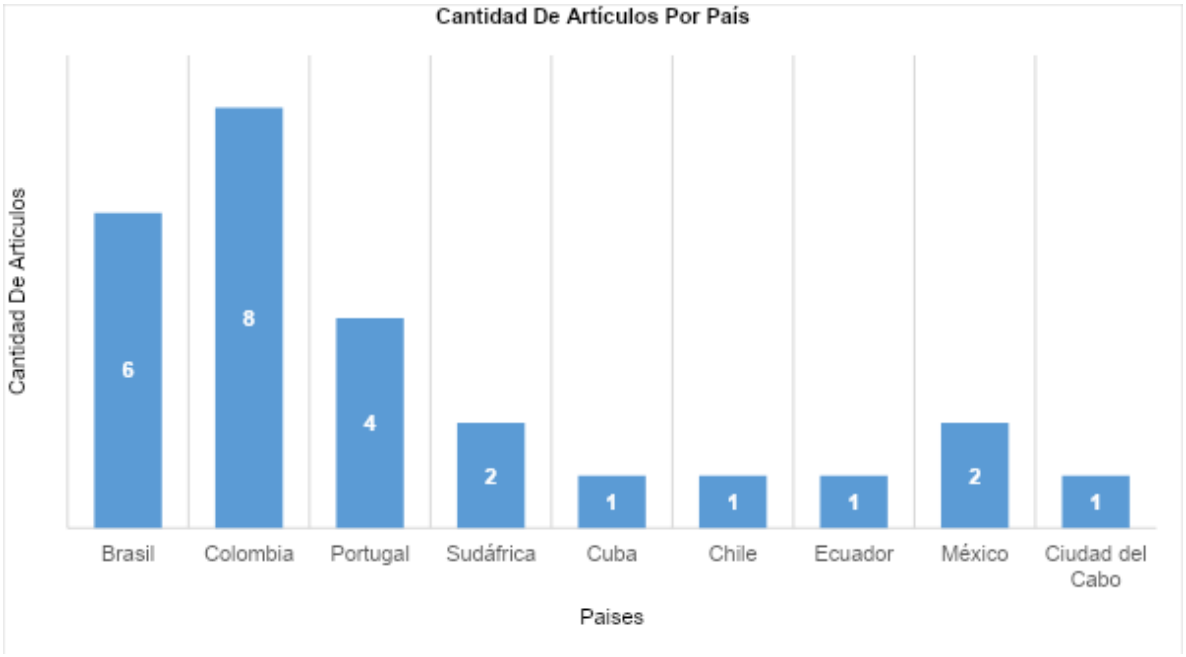


Figura 2. Productividad investigativa respecto a Blockchain y ciberseguridad por país

Colombia indica un compromiso significativo con esta tecnología emergente. Los artículos colombianos abordan una amplia gama de áreas, incluyendo la seguridad alimentaria, la atención médica, las finanzas y más. Colombia se ha destacado como un actor importante en la exploración y aplicación de blockchain en América Latina, con una fuerte presencia en la investigación y desarrollo de soluciones basadas en blockchain. Luego se encuentra Brasil, que demuestra un fuerte interés en la tecnología blockchain y su aplicación en diversas áreas. Los artículos brasileños abordan temas que van desde la certificación de energía renovable hasta la educación y la ciberseguridad. Esto refleja la diversidad de aplicaciones de blockchain que se están investigando y desarrollando en el país. Brasil se destaca como un centro de innovación y experimentación en el campo de la tecnología blockchain en América Latina.

Portugal por su parte, aborda una variedad de temas, desde la educación hasta la arquitectura de certificados digitales. Esto refleja la diversidad de aplicaciones de blockchain que se investigan en Portugal. El país está explorando cómo blockchain puede mejorar la educación y promover la descentralización en tecnologías como los certificados digitales. Luego, se encuentran México y Sudáfrica, dónde, México, el impacto de blockchain en la energía y la educación, analiza la innovación tecnológica de blockchain en el sector energético, mientras que el otro se centra en su aplicación en la educación. Esto muestra el interés de México en aprovechar la tecnología blockchain para abordar desafíos en estos sectores clave. Sudáfrica, relaciona la gestión de la información de salud y otro en la innovación en la atención médica. Esto indica un enfoque en la mejora de la atención médica y la gestión de datos de salud utilizando blockchain. Sudáfrica está investigando cómo blockchain puede abordar desafíos en el sector de la salud y promover la innovación en la atención médica. Finalmente, se encuentran Cuba, Ecuador, México y Ciudad del Cabo. Dónce, Cuba presenta un interés creciente en la convergencia de Internet de las cosas (IoT) y blockchain en el ámbito de la atención médica. Esto sugiere un enfoque en la mejora de la atención médica y la gestión de datos de salud utilizando blockchain. Cuba está explorando cómo estas tecnologías pueden contribuir a la mejora en la calidad de la prestación de servicios de salud en el país.

Chile muestra un interés en la aplicación de blockchain en servicios financieros electrónicos. Esto refleja la búsqueda de soluciones tecnológicas innovadoras en el sector financiero chileno y la exploración de cómo blockchain puede mejorar la eficiencia y la seguridad en las transacciones financieras. Ecuador se centra en la regulación de monedas digitales y su relación con blockchain. El artículo de Ecuador proporciona una perspectiva legal sobre este tema, lo que indica una preocupación por la regulación en el ámbito de las criptomonedas. Ecuador está investigando cómo establecer marcos regulatorios efectivos para las monedas digitales.

Respecto a la diversidad de aplicaciones como se puede ver en la Figura 3. hallada en la investigación realizada revela su versatilidad y capacidad para abordar desafíos en una variedad de sectores, desde energía renovable y salud hasta cadena de suministro y publicidad digital. La seguridad emerge como un elemento central, destacándose en contextos como ciberseguridad, integridad de datos en IoT y firma electrónica. Además, la tecnología se percibe como una herramienta para mejorar la sostenibilidad en la cadena de suministro y el sector energético. Las expectativas de implementación futura en diversos sectores empresariales subrayan su potencial transformador. El abordaje de desafíos específicos, como la eliminación de intermediarios y fraudes en publicidad digital, resalta la capacidad de blockchain para ofrecer soluciones concretas. De esta manera, la adopción extendida de blockchain refleja su papel central en la resolución de problemas multidisciplinarios, respaldando la seguridad, eficiencia y sostenibilidad en diversas industrias.

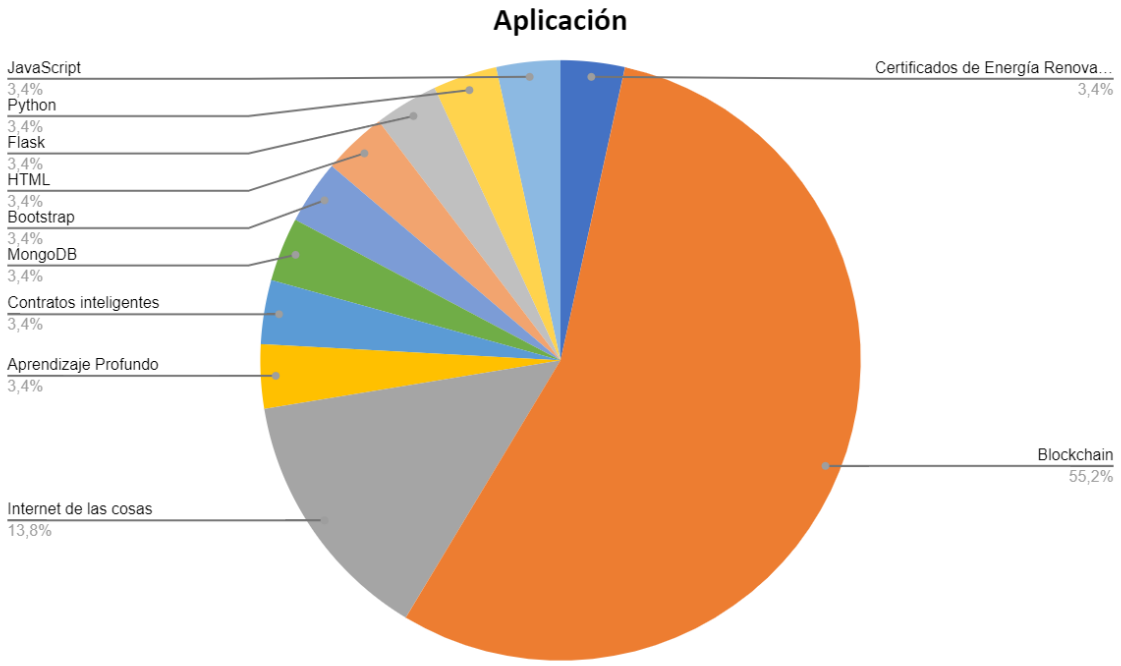


Figura 3. Aplicaciones utilizadas en el tema seguridad en Blockchain

La Figura presenta las variables relacionadas a las diferentes aplicaciones de Blockchain, entre las cuales se destacaron Blockchain para la industria con 55,2%, aplicaciones para Internet de las cosas con 13,8% aplicaciones para la industria como; como certificados de energía y contratos inteligentes, con 3,4%. Y algunas aplicaciones para la integración con otras herramientas como; Python, MongoDB, Bootstrap, HTML, Flask y JavaScript con 3,4%. Estos diversos enfoques de aplicaciones se explican a continuación de acuerdo a sus enfoques correspondientes a continuación:

Seguridad en Transacciones: La seguridad en las transacciones blockchain desempeña un papel fundamental en la confianza depositada en esta tecnología descentralizada. La agilidad en las transacciones se vuelve imperativa para asegurar que los usuarios puedan llevar a cabo intercambios de activos digitales de manera eficaz y segura [18]. Este grupo de variables se enfoca entonces en cómo la tecnología blockchain contribuye a esta agilidad al establecer un entorno de confianza para las transacciones, al eliminar intermediarios y reducir el riesgo de fraudes. Esto resulta esencial para

impulsar la adopción generalizada de blockchain en aplicaciones financieras y otros campos [19]. De este modo, la aportación de la tecnología blockchain a la celeridad de las transacciones resulta crucial, ya que se centra en cómo esta tecnología puede agilizar y simplificar la verificación y ejecución de las transacciones. Esto, a su vez, mejora la eficacia y, en última instancia, fortalece la seguridad de la red blockchain al reducir el período de exposición a posibles amenazas [20].

Control y Vigilancia: La supervisión y el monitoreo en el contexto de blockchain son elementos críticos para garantizar su seguridad y funcionamiento ininterrumpido. Estos componentes se encargan de supervisar la red, identificar actividades sospechosas y prevenir ataques maliciosos. La importancia reside en el hecho de que, sin un control eficaz y una vigilancia constante, la integridad y la seguridad de la blockchain podrían verse comprometidas [21]. Por esto, este grupo de variables se enfoca en la implementación de medidas de control y vigilancia destinadas a proteger la integridad de la red blockchain y salvaguardarla contra posibles amenazas. Esta protección es esencial para fomentar su adopción generalizada y su utilidad en diversos campos, que van desde transacciones financieras hasta registros médicos [22]. Esto permite entender que el papel del control y la vigilancia es crucial, ya que desempeñan un papel fundamental en la supervisión de la actividad en la blockchain, la detección de patrones inusuales y la respuesta a las amenazas de seguridad, garantizando así una gestión efectiva de la seguridad en las redes blockchain [21].

Elementos Para la Industria: El enfoque de este grupo de variables, se dirige hacia elementos esenciales de la tecnología blockchain, entre los que se incluyen Bitcoin, los contratos inteligentes y la automatización de procesos. La relevancia de abordar estos componentes radica en su papel fundamental dentro de la estructura y la ejecución y rendimiento de las redes blockchain [23]. Tanto Bitcoin como los activos criptográficos sirven como cimientos para diversas aplicaciones blockchain, mientras que los contratos inteligentes automatizan acuerdos y transacciones [23]. La seguridad de estas áreas se convierte en un factor vital, ya que cualquier vulnerabilidad podría tener repercusiones significativas desde el aspecto financiero y legal. Mediante la exploración de cómo se protegen estos elementos, se adquiere una comprensión más profunda sobre la forma de resguardar y fortalecer la seguridad en las aplicaciones basadas en la tecnología blockchain [24], [25].

Tecnologías y Herramientas Técnicas: La relevancia de este grupo de variables, se centra en las herramientas y tecnologías que respaldan la infraestructura de la blockchain, como AWS, Suricata, Docker y otros elementos similares. Estas herramientas desempeñan un papel crítico en el despliegue y funcionamiento de los nodos blockchain y deben ser utilizadas con seguridad para evitar posibles vulnerabilidades [26]. La seguridad en estos niveles técnicos resulta de suma importancia para garantizar que la infraestructura subyacente sea resistente a posibles ataques y amenazas. Al abordar la seguridad de estas herramientas, se contribuye a fortalecer la robustez y la confiabilidad de la red blockchain, aspectos cruciales para su adopción y su éxito continuado en una amplia gama de escenarios [27].

Dentro de este grupo, se destacan varias herramientas y tecnologías relevantes, tales como AWS (Amazon Web Services) para garantizar la seguridad en la infraestructura de los nodos blockchain, así como IoT (Internet of Things) Devices para lograr una integración segura de dispositivos en la red blockchain. Suricata cumple una función esencial en la detección de intrusiones, mientras que Hyperledger-Fabric, Docker, ARP Poisoning, Backdoor y Free Tier contribuyen a la seguridad de los nodos y servicios en la nube [28].

Integración de IoT y Blockchain: La convergencia de IoT (Internet de las Cosas) y blockchain se manifiesta como una tendencia de gran relevancia, destacándose por su capacidad para transformar industrias enteras. La seguridad en esta intersección desempeña un papel crítico, ya que aborda la comunicación y el intercambio de datos entre los dispositivos interconectados y la tecnología blockchain. Los retos de seguridad en este contexto son únicos y necesitan ser abordados de manera adecuada para asegurar la confiabilidad de las soluciones basadas en IoT y blockchain. Al explorar cuestiones relacionadas con la seguridad y la criptografía en este ámbito, se contribuye a una comprensión más profunda de cómo estas tecnologías pueden trabajar de manera conjunta y segura para impulsar la eficiencia y la confianza en diversas aplicaciones [19]. Para este grupo de variables, se exploran temas relacionados con la integración de IoT y blockchain, con un enfoque especial en elementos como "Internet de las Cosas (IoT)," "Arquitecturas IoT," "Dispositivos y Sensores IoT," así como "Seguridad y Criptografía" para garantizar la protección de datos en el punto de confluencia de estas tecnologías.

En cuanto a los componentes clave de implementación, este grupo se dedica a aspectos técnicos esenciales para asegurar soluciones blockchain sólidas. Elementos como "Tecnología Blockchain (BT)," "Contratos Inteligentes" y "Seguridad de Datos" son fundamentales. Estos componentes conforman la base de cualquier aplicación blockchain, y su seguridad es esencial para prevenir posibles ataques y garantizar la integridad de los datos almacenados en la blockchain. Abordar estas temáticas contribuye a la comprensión de cómo diseñar e implementar soluciones blockchain seguras y robustas [19]. En el contexto de la implementación de blockchain, "Tecnología Blockchain (BT)" y "Contratos Inteligentes" adquieren una importancia crítica, al igual que la "Seguridad de Datos" para salvaguardar la confidencialidad de la información almacenada en la blockchain. Además, "Computación en la Nube" se convierte en un aspecto relevante al discutir la implementación segura de nodos blockchain en entornos de nube [29].

Aspectos de Control de Acceso y Seguridad: La administración de atributos de seguridad, el control de acceso y la autenticación representan conceptos de vital importancia para garantizar la seguridad en el contexto de blockchain. La relevancia de estos conceptos radica en su capacidad para determinar quién tiene autorización para acceder y ejecutar acciones en la red blockchain. Este aspecto es fundamental para prevenir intrusiones no autorizadas y salvaguardar la confidencialidad de la información almacenada en la plataforma [30].

Al profundizar en estos tópicos, se contribuye a una comprensión más detallada de cómo se pueden establecer políticas de seguridad efectivas en entornos basados en blockchain. Esto resulta esencial para fomentar la adopción de esta tecnología en aplicaciones que requieren un alto nivel de seguridad y cumplimiento de regulaciones [30]. Dentro de este grupo, se destacan conceptos como "Atributos de Seguridad," "Control de Acceso," "Algoritmos de Encriptación," "Control de Acceso en Blockchain," "Validez de Accesos" y "Autenticación y Autorización" como elementos cruciales para definir y administrar políticas de seguridad efectivas en el ámbito de la blockchain. Estos conceptos garantizan un acceso seguro y una gestión adecuada de la red blockchain [31]. Por otro lado, es posible identificar algunas variables desde los desafíos soluciones e impacto que pueden darse:

- Privacidad y Publicidad en Línea

  Desafíos: Protección de la privacidad de los usuarios y transparencia en la recopilación de datos.
  Soluciones: Blockchain mejora la privacidad y la confiabilidad en la publicidad digital.
  Impacto: Asegura la privacidad de los usuarios y garantiza la transparencia en la publicidad digital.

- Autenticidad de Credenciales y Seguridad en la Educación

  Desafíos: Verificación de títulos y certificados educativos en entornos digitales.
  Soluciones: Blockchain garantiza la autenticidad y la integridad de los registros académicos.
  Impacto: Facilita la verificación de credenciales, especialmente crucial durante la pandemia de COVID-19.

- Regulación de Criptomonedas

  Desafíos: Estabilidad financiera y protección del consumidor en el ámbito de las criptomonedas.
  Soluciones: Desarrollo de marcos legales y regulaciones específicas.
  Impacto: Asegura la estabilidad y seguridad en el uso y adopción de criptomonedas.

- Ciberseguridad y Atención Médica

  Desafíos: Mitigación de amenazas cibernéticas y protección de datos sensibles.
  Soluciones: Blockchain asegura la gestión de registros médicos y protege datos de salud.
  Impacto: Incrementa la seguridad en la atención médica y la ciberseguridad en general.

- Certificación de Energía Renovable

Desafíos: Rastrear y verificar la producción de energía limpia.
Soluciones: Blockchain proporciona una solución eficiente y confiable para la certificación de energía renovable.
Impacto: Facilita la transición hacia energías sostenibles, asegurando la autenticidad de la energía producida.

También es posible resumir los enfoques específicos en Seguridad Blockchain, según las variables y su importancia:

- Seguridad en Transacciones

  Variables: Agilidad y seguridad en las transacciones, eliminación de intermediarios, y reducción de fraudes.
  Importancia: Establece un entorno de confianza y mejora la eficiencia y seguridad de las transacciones.

- Control y Vigilancia

  Variables: Supervisión de la red, identificación de actividades sospechosas, y prevención de ataques maliciosos.
  Importancia: Garantiza la integridad y seguridad continua de la red blockchain.

- Elementos para la Industria

  Variables: Bitcoin, contratos inteligentes, automatización de procesos.
  Importancia: Seguridad en la estructura y ejecución de aplicaciones blockchain.

- Tecnologías y Herramientas Técnicas

  Variables: AWS, Suricata, Docker, y otras herramientas de infraestructura.
  Importancia: Garantiza la seguridad en el despliegue y funcionamiento de nodos blockchain.

- Integración de IoT y Blockchain

  Variables: Seguridad y criptografía en la comunicación y datos entre dispositivos IoT y blockchain.
  Importancia: Asegura la confiabilidad de soluciones basadas en la integración de IoT y blockchain.

- Control de Acceso y Seguridad

  Variables: Atributos de seguridad, control de acceso, autenticación y autorización.
  Importancia: Previene accesos no autorizados y protege la confidencialidad de la información.

Por otro lado, el relacionamiento entre variables puede ser observado en la Figura 4, en dónde se observa los principales cluster de términos clave. Estos cluster se forman de acuerdo a la co-ocurrencia entre términos clave en los diferentes artículos publicados. Para el caso de este análisis se extrajeron los términos clave de la base de datos Scopus.

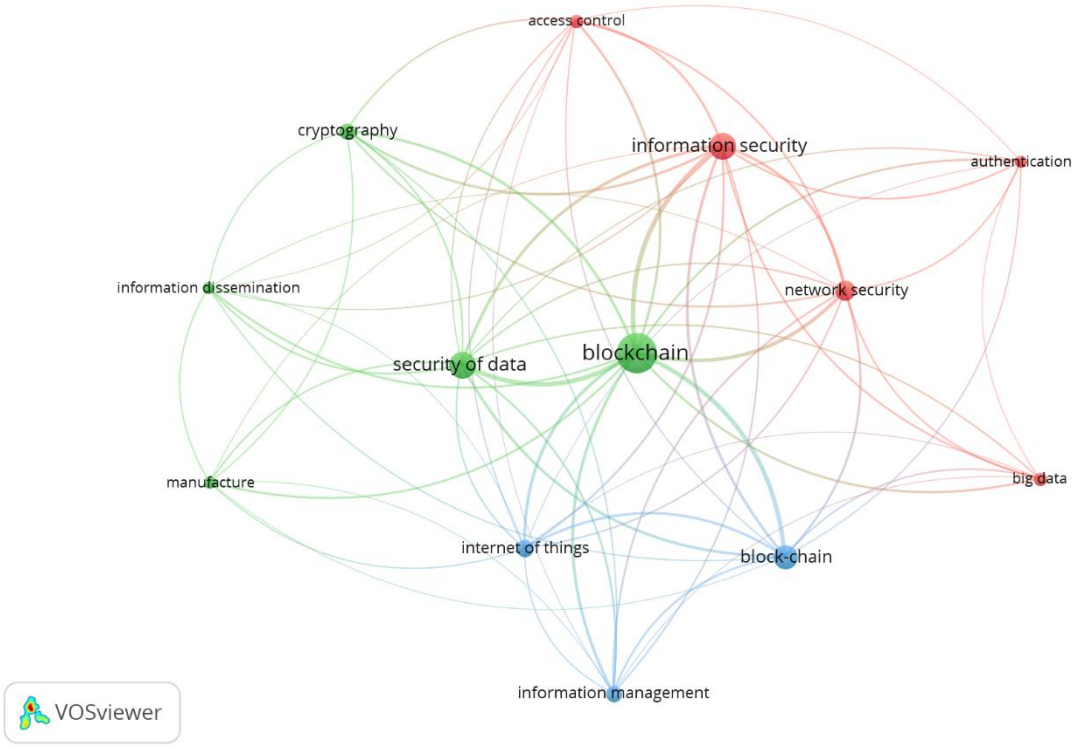


Figura 4. Co-ocurrencia de palabras clave para seguridad informática y blockchain.
Fuente. Elaboración propia a partir de la base de datos Scopus y el análisis en VosViewer.

De acuerdo con los términos clave y las redes conformadas, se puede observar un clúster principal conformado por blockchain, seguridad de los datos, manufactura, diseminación de la información y criptografía. Este grupo de términos se conforman principalmente por el enfoque que se da desde el blockchain en la cadena de suministro y la seguridad de la información a nivel empresarial. Por ejemplo [32] evalúan si el papel mediador del intercambio de información apoya la relación en la industria inmobiliaria en los Emiratos Árabes Unidos. También [33] exploran los impactos multifacéticos de la tecnología blockchain en la valoración empresarial y la seguridad de la información a partir de una revisión de estudios de casos, encuestas y análisis estadísticos. También en otro estudio, se propone un esquema de intercambio de seguridad de información de privacidad basado en blockchain en el Internet industrial de las cosas (IIoT) para resolver el problema de compartir información privada en fábricas inteligentes [34].

Luego, se encuentra un clúster conformado por los términos seguridad de la información, seguridad de la red, control de acceso, big data y autenticación. Este clúster de términos clave esta orientado principalmente a aspectos de seguridad cibernética procurando la seguridad de acceso a la red directamente, evitando infiltraciones en la red de datos. Uno de los trabajos más recientes que reúne estos términos, estudia la seguridad de la información de la red a través del algoritmo SM2. El principio del software de firewall para proteger el contenido de información de big data es que el software puede distinguir claramente las redes internas y externas, lo que no solo garantiza la seguridad del entorno interno de la computadora, sino que también reduce la posibilidad de que virus del entorno externo invadan la computadora [35]. En otro trabajo de investigación, se crea una plataforma de gestión de IoT basada en blockchain basada en el marco Hyperledger Fabric. La plataforma utiliza blockchain como tecnología subyacente, coopera con el almacenamiento de datos de origen en la red IPFS, carga el valor hash devuelto a la red blockchain y aplica la tecnología blockchain al campo de la seguridad de la información [36]. En otro proyecto, se examina cómo la tecnología blockchain puede mejorar la seguridad y confiabilidad de los datos para aplicaciones web [37].

El último cluster de términos clave, esta conformado por los términos internet de las cosas, blockchain y gestión de la información. Entre los trabajos que comprenden el uso de estos términos, se encuentran

inicialmente como uno de los trabajos más citados, un estudio que introduce el concepto de tecnología Blockchain, proponiendo la aplicación de la tecnología Blockchain en la seguridad de la información de la cadena de suministro de alimentos y comparándola con el sistema de cadena de suministro tradicional [38]. Por otro lado, [39] propusieron un mecanismo de almacenamiento de datos de modo dual adecuado para él, los datos de la cadena de suministro fueron almacenados por la combinación de almacenamiento blockchain y almacenamiento de bases de datos fuera de la cadena. Por otro lado, [34] proponen un esquema de intercambio de seguridad de información de privacidad basado en blockchain en el Internet industrial de las cosas (IIoT) para resolver el problema de compartir información privada en fábricas inteligentes.

## 4. DISCUSIÓN

El análisis de los resultados revela un panorama interesante en cuanto a la adopción y aplicación de la tecnología Blockchain en diferentes países de América Latina y otras regiones. Colombia emerge como un actor destacado en la exploración y desarrollo de soluciones basadas en Blockchain, con un fuerte enfoque en áreas como la seguridad alimentaria, la atención médica y las finanzas. Esta tendencia sugiere un compromiso significativo con la tecnología emergente y su potencial para abordar desafíos en una amplia gama de sectores.

Brasil también muestra un fuerte interés en Blockchain, y su aplicación abarca desde la certificación de energía renovable hasta la educación y la ciberseguridad. Esta diversidad de aplicaciones destaca la versatilidad de Blockchain y su capacidad para abordar desafíos en diferentes campos. Brasil se presenta como un centro de innovación y desarrollo en el ámbito de Blockchain en América Latina. Portugal se suma a la lista de países comprometidos con Blockchain, explorando su aplicación en áreas que van desde la educación hasta la arquitectura de certificados digitales. Esto refleja la diversidad de aplicaciones que se investigan en Portugal y su enfoque en la mejora de la educación y la promoción de la descentralización en tecnologías como los certificados digitales.

México y Sudáfrica también muestran interés en Blockchain, con enfoques específicos en el sector de la energía y la educación. México se centra en la innovación tecnológica en el sector energético, mientras que Sudáfrica se enfoca en la gestión de la información de salud y la innovación en la atención médica. Estos enfoques demuestran cómo Blockchain se utiliza para abordar desafíos en sectores clave de ambos países. Cuba y Ecuador exploran la convergencia de Internet de las cosas (IoT) y Blockchain en el ámbito de la atención médica. Esta tendencia refleja un compromiso con la mejora de la atención médica y la gestión de datos de salud utilizando tecnologías Blockchain. Chile muestra un interés particular en la aplicación de Blockchain en servicios financieros electrónicos, lo que subraya la búsqueda de soluciones tecnológicas innovadoras en el sector financiero chileno. Ecuador se enfoca en la regulación de monedas digitales y su relación con Blockchain, lo que indica una preocupación por establecer marcos regulatorios efectivos para las criptomonedas.

En cuanto a la diversidad de aplicaciones de Blockchain en estos países destaca su versatilidad y capacidad para abordar desafíos en una amplia gama de sectores, desde la energía renovable y la salud hasta la cadena de suministro y la publicidad digital. La seguridad se destaca como un elemento central, especialmente en contextos como la ciberseguridad, la integridad de datos en IoT y la firma electrónica. La tecnología Blockchain se percibe como una herramienta para mejorar la sostenibilidad en la cadena de suministro y el sector energético. Además, se espera que tenga un papel transformador en diversos sectores empresariales en el futuro. La capacidad de abordar desafíos específicos, como la eliminación de intermediarios y fraudes en la publicidad digital, destaca la capacidad de Blockchain para ofrecer soluciones concretas en estos campos. Además, entre las diferentes herramientas y tecnologías presentadas en los artículos para las diferentes aplicaciones presentadas en Blockchain, se encontraron las siguientes:

- Access Control: El control de acceso es esencial en la seguridad de Blockchain para asegurar que únicamente los usuarios con los permisos otorgados accedan a la red y sus recursos [40], [41], [42].

- AdEx y AdHive: Son plataformas que podrían estar relacionada con la publicidad en Blockchain [43], [44].

- ARP Poisoning: Es una técnica que puede utilizarse para ataques de suplantación en la red, y su seguridad es crucial [45].

- Arquitecturas IoT: En el contexto de IoT (Internet de las Cosas), las arquitecturas son fundamentales para garantizar una comunicación segura y eficiente entre dispositivos y Blockchain [46].

- Authentication and Authorization: La autenticación y la autorización son conceptos críticos para garantizar que solo usuarios autorizados puedan interactuar con la red Blockchain [47].

- Automatización Robótica de Procesos (RPA): La RPA puede utilizarse en aplicaciones Blockchain para automatizar procesos, y su seguridad es esencial para prevenir riesgos [48].

- AWS (Amazon Web Services): AWS proporciona servicios en la nube y puede ser utilizado para alojar nodos de Blockchain, por lo que su seguridad es fundamental [49], [50].

- Backdoor: Las puertas traseras son una vulnerabilidad de seguridad y su prevención es vital [51].

- Base de datos (MongoDB): Las bases de datos son utilizadas en aplicaciones Blockchain, y MongoDB es una de las opciones. La seguridad de la base de datos es esencial [52].

- Billetera Virtual: Las billeteras virtuales son fundamentales en Blockchain para el almacenamiento de criptomonedas. Su seguridad es crítica [53].

- Bitcoin: Como una de las criptomonedas más conocidas, la seguridad de Bitcoin es vital [54].

- Cloud Computing (Computación en la Nube): La nube se usa para alojar nodos Blockchain, y su seguridad es esencial [55].

- Data Security: La seguridad de los datos es un aspecto crucial en todas las aplicaciones de Blockchain [56].

- Dispositivos y Sensores IoT: Estos dispositivos son fundamentales en aplicaciones de IoT y Blockchain y deben ser seguros [57].

- Docker: Docker es utilizado para contener nodos Blockchain y su seguridad es esencial [58].

- Encryption Algorithms: Los algoritmos de cifrado son fundamentales para proteger los datos en Blockchain [59].

- Ethereum: Como otra de las principales criptomonedas, la seguridad de Ethereum es crítica [60].

- Firma Electrónica: La firma electrónica se utiliza en muchas aplicaciones de Blockchain y debe ser segura [61].

- Hyperledger: Hyperledger es una plataforma de Blockchain empresarial, y su seguridad es fundamental [62].

- Inteligencia Artificial (Machine Learning): La IA se utiliza en Blockchain para diversos fines, y su seguridad es vital [63].

- Navegador Brave: Brave es un navegador centrado en la privacidad que utiliza Blockchain. Su seguridad es crucial [64].

- Plataformas como BAT (Basic Attention Token): Las plataformas que utilizan tokens, como BAT, deben ser seguras para garantizar la integridad de los tokens [65].

- Public Key Infrastructure (PKI): La infraestructura de clave pública es fundamental para la seguridad de Blockchain [66].

La seguridad se mantiene como un pilar central en la adopción de esta tecnología, especialmente en ámbitos críticos como la ciberseguridad, la integridad de datos en IoT y la firma electrónica. La percepción de Blockchain como una herramienta transformadora para la sostenibilidad en la cadena de suministro y el sector energético destaca su importancia a futuro. La capacidad de resolver desafíos específicos, como la eliminación de intermediarios y la lucha contra el fraude en la publicidad digital, pone de relieve la versatilidad de Blockchain.

Además, entre las diversas herramientas y tecnologías presentadas en los artículos para las diferentes aplicaciones de Blockchain, se encuentran elementos cruciales para garantizar la seguridad y el funcionamiento eficaz de la tecnología. Desde el control de acceso hasta las bases de datos y la infraestructura de clave pública, cada componente desempeña un papel vital en la protección de la red Blockchain y los datos sensibles que alberga. La seguridad de estas herramientas es fundamental para prevenir amenazas y garantizar la confianza en las aplicaciones de Blockchain. En conjunto, esta diversidad de aplicaciones y la atención a la seguridad de las herramientas subrayan la importancia en constante crecimiento de Blockchain en el panorama tecnológico global. Teniendo en cuenta lo anterior, se realiza un análisis de tendencias de investigación que parte de la evaluación de los principales términos clave. En este sentido, se presentan en la Figura 5 los temas que son tendencia en el área de la seguridad informática y el blockchain de acuerdo con el año de mayor aprovechamiento del término.

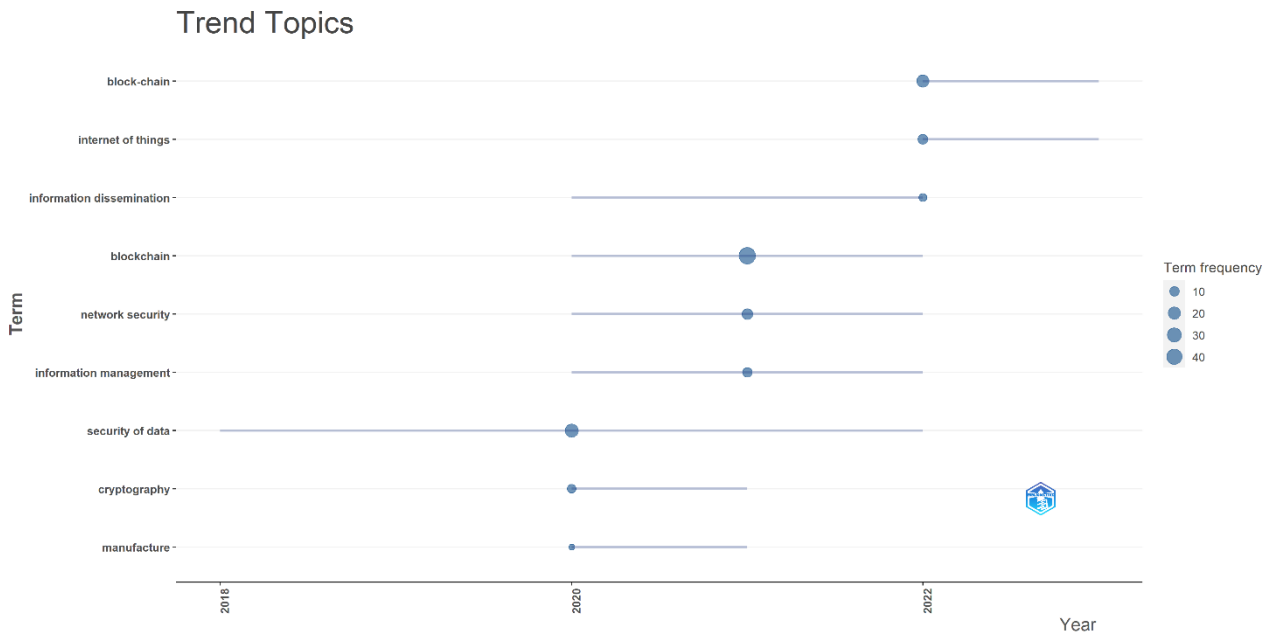


Figura 5. Términos tendencia en el área de la seguridad informática y el blockchain
Fuente. Elaboración propia a partir de Scopus y Bibliometrix

Se observa como término que surge aproximadamente en el año 2018 y manteniéndose hasta el 2022 la seguridad de los datos. Este término tuvo mayor relevancia aproximadamente en el año 2020, dónde una de las investigaciones más relevantes se enfoca en el análisis de los problemas de seguridad de la información existentes en Internet de la energía desde las cuatro perspectivas: capa de control del sistema, acceso a dispositivos, transacciones de mercado y privacidad del usuario. Luego se introduce la tecnología blockchain y se analizan sus principios de funcionamiento y características técnicas [67]. Luego, en el año 2020 surgen los términos criptografía y manufactura, teniendo mayor protagonismo el término criptografía. Estos términos se mantienen aproximadamente hasta el año 2021. Uno de los trabajos más relevantes que involucra criptografía, presenta una metodología para brindar seguridad de

la información a los usuarios de una manera innovadora mediante la integración de las características más importantes de la industria del procesamiento de datos digitales, como: blockchain, criptografía, control de acceso y algunas características de seguridad de los datos [68].

Posteriormente, se encuentran los términos blockchain, seguridad en la red y gestión de la información. Estos términos surgen aproximadamente en el año 2020, pero su mayor ocurrencia fue en el año 2021 y se mantienen hasta el año 2022. Como uno de los trabajos con el mayor impacto se presenta una investigación que propone un esquema conjunto de agrupación en clústeres y blockchain para la transmisión de seguridad de información en tiempo real para evitar que algunos vehículos envíen mensajes maliciosos para alterar el orden del tráfico en los cruces de las redes celulares de vehículo a todo C-V2X [69]. Por último, uno de los términos más recientes y vigentes además de blockchain, se encuentra el internet de las cosas. Uno de los trabajos con mayor impacto fue el de [70], dónde presentan una descripción general del concepto de uso de cifrado con una clave asimétrica para proteger los datos desde los sensores a los lagos de datos antes de reenviarlos a una infraestructura blockchain interconectada y descentralizada.

## 5. CONCLUSIONES

La tecnología blockchain ha demostrado ser altamente versátil y capaz de abordar desafíos en una amplia gama de sectores, desde la energía renovable y la salud hasta la cadena de suministro y la publicidad digital. La seguridad emerge como un elemento central en estas aplicaciones, destacándose en contextos como la ciberseguridad, la integridad de datos en el Internet de las cosas (IoT) y la firma electrónica. Además, la tecnología se percibe como una herramienta para mejorar la sostenibilidad en la cadena de suministro y el sector energético. Las expectativas de implementación futura en diversos sectores empresariales subrayan su potencial transformador. El abordaje de desafíos específicos, como la eliminación de intermediarios y fraudes en la publicidad digital, resalta la capacidad de blockchain para ofrecer soluciones concretas.

El uso de la tecnología blockchain ha transformado la industria al convertirse en una herramienta fundamental en la seguridad cibernética y en diversos sectores. Esta tecnología ha demostrado su versatilidad al abordar desafíos relacionados con la integridad de datos, la autenticidad de transacciones y la protección contra amenazas cibernéticas además un enfoque significativo en la seguridad de las transacciones, el control y la vigilancia, los elementos clave de la implementación, las tecnologías y herramientas técnicas, la integración de IoT , así como aspectos de control de acceso y seguridad. Además, se destaca que países como Brasil, Colombia, Cuba, Ecuador, México y Portugal han demostrado un compromiso significativo con la exploración y aplicación de blockchain en diversas áreas, lo que refleja su importancia a nivel global. También se observa un aumento en la atención hacia herramientas específicas utilizadas en el contexto de blockchain, lo que indica un enfoque en la mejora de la seguridad y eficiencia de esta tecnología.

En un entorno donde la ciberseguridad es una preocupación creciente, esta tecnología se presenta como una solución revolucionaria que ofrece seguridad, agilidad y transparencia en el mundo digital. Su capacidad para garantizar la integridad de los datos y las transacciones, así como su aplicabilidad en una amplia gama de sectores, lo convierte en una herramienta esencial para abordar los desafíos de seguridad cibernética en la actualidad. Su adopción extendida demuestra su potencial transformador en la resolución de problemas multidisciplinarios, respaldando la seguridad, eficiencia y sostenibilidad en diversas industrias.

Es evidente que la tecnología blockchain no solo ha tenido un impacto positivo en la seguridad y la eficiencia en diversos sectores, sino que también ha fomentado la colaboración a nivel global. La naturaleza descentralizada de la blockchain ha permitido una mayor cooperación entre países y organizaciones, promoviendo estándares y mejores prácticas en la implementación de esta tecnología. La comunidad internacional se ha unido en la exploración y aplicación de blockchain, reconociendo su capacidad para abordar desafíos compartidos en un mundo cada vez más interconectado. Este espíritu colaborativo no solo fortalece la seguridad cibernética, sino que también allana el camino hacia un futuro más sostenible y seguro en una variedad de sectores. Esta colaboración global es fundamental para impulsar la adopción generalizada de blockchain y garantizar un enfoque cohesivo para abordar los desafíos y oportunidades que esta tecnología presenta.

Finalmente, la tecnología blockchain se ha destacado como una herramienta verdaderamente transformadora en una amplia variedad de sectores, abarcando desde la publicidad en línea hasta la atención médica y la certificación de energía renovable. La notable adopción y adaptación de esta tecnología por diferentes países subraya su innegable potencial para abordar desafíos específicos en diversas áreas. La revisión de la literatura emerge como una metodología crítica para mantenerse actualizado respecto a los desarrollos más recientes y para comprender los aspectos técnicos y de gobernanza relacionados con la seguridad en blockchain. Además, la implementación de una serie de herramientas y tecnologías se revela como fundamental en todo el proceso de desarrollo, implementación y mantenimiento de soluciones basadas en blockchain.

## 6. REFERENCIAS BIBLIOGRÁFICAS


[1] C. Pastorino, “Blockchain: qué es y cómo funciona esta tecnología”, ESET, 2022, https://www.welivesecurity.com/la-es/2022/05/13/blockchain-que-es-como-funciona-y-como-se-esta-usando-en-el-mercado/

[2] IBM, “¿Qué es la seguridad de blockchain?”, 2024, https://www.ibm.com/es-es/topics/blockchain-security#:~:text=Se%20basa%20en%20principios%20de,o%20un%20paquete%20de%20transacciones.

[3] SAP, “¿Qué es la tecnología de blockchain?”, 2024, https://www.sap.com/latinamerica/products/artificial-intelligence/what-is-blockchain.html#:~:text=Al%20blockchain%20se%20lo%20suele,es%20la%20propiedad%20de%20qu%C3%A9%E2%80%93..

[4] D. , & T. A. Tapscott, “Blockchain revolution”, Senai-SP Editora. 2018. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://itig-iraq.iq/wp-content/uploads/2019/05/Blockchain_Revolution.pdf

[5] A. Bartolomé, “Cambiando el futuro ‘blockchain’ y Educación,” *Comunicación y Pedagogía: nuevas tecnologías y recursos didácticos*, vol. 303–304, pp. 7–12, 2017. https://doi.org/10.12795/pixelbit.82546

[6] P. Rivera and C. Lindin, “Blockchain en Educación. Entre la búsqueda de seguridad en el mundo digital y el determinismo tecnológico,” *Revista de la educación superior*, vol. 27, 2020. https://doi.org/10.36857/resu.2020.194.1129159

[7] A. Wright and P. De Filippi, “Decentralized Blockchain Technology and the Rise of Lex Cryptographia,” *SSRN Electronic Journal*, 2015, doi: 10.2139/ssrn.2580664.

[8] Hacknoid, “Estadísticas Ciberseguridad Mayo 2023 | Lo que debes saber,” 2023, https://www.hacknoid.com/hacknoid/estadisticas-ciberseguridad-mayo-2023/#:~:text=El%20informe%20destaca%20la%20escasez,informaci%C3%B3n%20y%20casos%20de%20ransomware.

[9] Fortinet, “Informe global sobre el ransomware 2023 INFORME,” 2023. Accessed: Nov. 01, 2023. https://global.fortinet.com/ai-la-lp-es-ap-global-ransomware-report2023?utm_source=website&utm_medium=LATHERO&utm_campaign=LATHERO-BAN3-Ransomware-LATAM-LAT&utm_content=LATHERO-BAN3-Ransomware

[10] J. De Marco, “Filtran datos de 200 mil usuarios de la emergencia medica del Casmu y hackers los ponen a la venta en internet,” *Robo de Información*, El Observador, Uruguay, May 22, 2023, https://www.elobservador.com.uy/nota/filtran-datos-de-200-mil-usuarios-de-la-emergencia-medica-del-casmu-y-hackers-los-ponen-a-la-venta-en-internet-202352295653#:~:text=Los%20datos%20filtrados%20del%20Casmu,venta%20en%20un%20foro%20especializado.

[11] Instituto Nacional de Ciberseguridad, “Distribución malware a través de un phishing que suplanta a Endesa,” España, May 2023, https://www.incibe.es/ciudadania/avisos/distribucion-malware-traves-de-un-phishing-que-suplanta-endesa#:~:text=Se%20ha%20detectado%20una%20campa%C3%B1a%20de%20malware%2C%20la%20cual%20est%C3%A1,el%20dispositivo%20de%20la%20v%C3%ADctima.

[12] X. Duque, “Ciberseguridad y estándares en el cuidado,” *El Tiempo*, 2023. [Online]. Available: https://www.eltiempo.com/opinion/columnistas/ximena-duque/ciberseguridad-y-estandares-en-el-cuidado-columna-de-ximena-duque-765439

[13] J. Muñoz, “Masivo ciberataque secuestra los datos de cientos de portales en Chile, Colombia y Panamá,” *BioBio Chile*, Chile, Sep. 15, 2023

https://www.biobiochile.cl/noticias/internacional/america-latina/2023/09/15/masivo-ciberataque-secuestra-los-datos-de-cientos-de-portales-en-chile-colombia-y-panama.shtml.

[14] L. Lesmes, “Colombia recibió 20.000 millones de ciberataques en 2022,” *El Tiempo*, Bogotá, Apr. 10, 2023, https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberseguridad-en-colombia-datos-sobre-ciberataques-en-el-pais-757651.

[15] D. Amo, M. Alier, F. García-Peñalvo, D. Fonseca, and M. J. Casañ, “Privacidad, seguridad y legalidad en soluciones educativas basadas en Blockchain: Una Revisión Sistemática de la Literatura,” *RIED. Revista Iberoamericana de Educación a Distancia*, vol. 23, no. 2, p. 213, Jul. 2020, doi: 10.5944/ried.23.2.26388.

[16] Ó. A. Beltrán, “Revisiones sistemáticas de la literatura,” *Rev Colomb Gastroenterol*, vol. 20, pp. 60–69, 2005, Accessed: Jun. 05, 2019. [Online]. Available: http://www.scielo.org.co/pdf/rcg/v20n1/v20n1a09.pdf

[17] C. Mamédio, C. Santos, C. Andrucioli De Mattos Pimenta, M. Roberto, and C. Nobre, “ESTRATEGIA PICO PARA LA CONSTRUCCIÓN DE LA PREGUNTA DE INVESTIGACIÓN Y LA BÚSQUEDA DE EVIDENCIAS,” *Rev Latino-am Enfermagem*, vol. 15, no. 3, 2007, www.eerp.usp.br/rlaeArtigodeAtualização

[18] O. R. Akinyemi, M. N. Sibiya, and O. Oladimeji, “Communication model enhancement using electronic health record standard for tertiary hospital,” *SA Journal of Information Management*, vol. 24, no. 1, Apr. 2022, doi: 10.4102/sajim.v24i1.1472.

[19] P. A. Astorga and Y. G. Garcia, “Internet de las cosas en el ámbito de la atención médica: tendencias y desafíos,” *Revista Cubana de Informática Médica*, vol. 14, no. 1, 2022, http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1684-18592022000100014.

[20] N. L. Marques, L. L. Gomes, and L. E. Brandão, “A blockchain-based model for token renewable energy certificate offers,” *Revista Contabilidade & Finanças*, vol. 34, no. 91, 2023, doi: 10.1590/1808-057x20221582.en.

[21] R. Pava, J. N. Perez Castillo, and L. F. Niño Vasquez, “Perspectiva para el uso del modelo P6 de atención en salud bajo un escenario soportado en IoT y blockchain,” *Tecnura*, vol. 25, no. 67, pp. 112–130, Jan. 2021, doi: 10.14483/22487638.16159.

[22] P. E. Romero, A. [1] Elizardo, and S. Costa, “Control and surveillance in digital capitalism: an analysis of blockchain technologies and their business implementation Controle e vigilância no capitalismo digital: uma análise da tecnologia blockchain e sua implementação empresarial Resumo,” pp. 1–13, 2023, doi: 10.1590/1679-395120220020x.

[23] E. Rodrigues, W. Lourenzani, and E. Satolo, “Blockchain in Supply Chain Management: Characteristics and Benefits,” *BAR - Brazilian Administration Review*, vol. 18, no. spe, 2021, doi: 10.1590/1807-7692bar2021200065.

[24] I. González-Puetate, C. L. Marín Tello, and H. Reyes Pineda, “Agri-food safety optimized by blockchain technology: review,” *Rev Fac Nac Agron Medellin*, vol. 75, no. 1, Jan. 2022, doi: 10.15446/rfnam.v75n1.95760.

[25] E. Rodrigues, W. Lourenzani, and E. Satolo, “Blockchain in Supply Chain Management: Characteristics and Benefits,” *BAR - Brazilian Administration Review*, vol. 18, no. spe, 2021, doi: 10.1590/1807-7692bar2021200065.

[26] Y.-I. Llanten-Lucio, S. Amador-Donado, and K. Marceles-Villalba, “Validation of Cybersecurity Framework for Threat Mitigation,” *Revista Facultad de Ingeniería*, vol. 31, no. 62, p. e14840, Oct. 2022, doi: 10.19053/01211129.v31.n62.2022.14840.

[27] B. García, M. A. Sánchez, and J. Abadía, “Herramienta web con tecnología de cadena de bloques para un sistema de facturación electrónica en Colombia,” *Información tecnológica*, vol. 32, no. 3, pp. 15–24, Jun. 2021, doi: 10.4067/S0718-07642021000300015.

[28] I. Gallardo, P. Bazan, and P. Venosa, “Arquitectura de Certificados Digitales: de una arquitectura jerárquica y centralizada a una distribuida y descentralizada,” *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, no. 32, pp. 49–66, Jun. 2019, doi: 10.17013/risti.32.49-66.

[29] I. González-Puetate, C. L. Marín Tello, and H. Reyes Pineda, “Agri-food safety optimized by blockchain technology: review,” *Rev Fac Nac Agron Medellin*, vol. 75, no. 1, Jan. 2022, doi: 10.15446/rfnam.v75n1.95760.

[30] I. Gallardo, P. Bazan, and P. Venosa, “Arquitectura de Certificados Digitales: de una arquitectura jerárquica y centralizada a una distribuida y descentralizada,” *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, no. 32, pp. 49–66, Jun. 2019, doi: 10.17013/risti.32.49-66.

[31] F. R. Cádima, “A Publicidade face aos novos contextos da era Digital: privacidade, transparência e disrupção,” *Media & Jornalismo*, vol. 19, no. 34, pp. 35–46, Jun. 2019, doi: 10.14195/2183-5462_34_3.

[32] S. Hamadneh, H. M. Alzoubi, E. K. Alquqa, A. Al Shraah, M. T. Alshurideh, and B. Al Kurdi, “The Mediating Role of Information Sharing in the Effect of Blockchain Strategy Information Security on E-Supply Chain in the UAE Real Estate Industry,” 2024, pp. 387–407. doi: 10.1007/978-3-031-31801-6_24.
[33] R. Udayakumar, B. Sivakuma, D. L. Femilin Jana, G. Simi Margarat, and T. Nathiya, “An Analytical Exploration of Blockchain Technology’s Impacts on Business Valuation and Information Security,” in *2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS)*, IEEE, Nov. 2023, pp. 192–196. doi: 10.1109/ICTACS59847.2023.10390018.
[34] Y. Wang, T. Che, X. Zhao, T. Zhou, K. Zhang, and X. Hu, “A Blockchain-Based Privacy Information Security Sharing Scheme in Industrial Internet of Things,” *Sensors*, vol. 22, no. 9, p. 3426, Apr. 2022, doi: 10.3390/s22093426.
[35] R. Ren, M. Ma, and W. Liu, “Design of Network Information Security Optimal Defense System Based on SM2 Algorithm and Blockchain Technology,” in *2023 2nd International Conference on Artificial Intelligence and Autonomous Robot Systems (AIARS)*, IEEE, Jul. 2023, pp. 223–227. doi: 10.1109/AIARS59518.2023.00052.
[36] C. Chen, Y. Chen, and Y. Gong, “Research on Internet of Things information security based on blockchain,” in *Third International Conference on Green Communication, Network, and Internet of Things (CNIoT 2023)*, S. Zhang and H. Wang, Eds., SPIE, Oct. 2023, p. 81. doi: 10.1117/12.3010663.
[37] B. Aliya, U. Olga, B. Yenlik, and I. Sogukpinar, “Ensuring Information Security of Web Resources Based on Blockchain Technologies,” *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 6, 2023, doi: 10.14569/IJACSA.2023.0140689.
[38] D. Tse, B. Zhang, Y. Yang, C. Cheng, and H. Mu, “Blockchain application in food supply information security,” in *2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, IEEE, Dec. 2017, pp. 1357–1361. doi: 10.1109/IEEM.2017.8290114.
[39] J. Xu, P. Sun, X. Zhang, X. Wang, J. Kong, and Z. Zhao, “Prototype System of Information Security Management of Cereal and Oil Food Whole Supply Chain Based on Blockchain,” *Nongye Jixie Xuebao/Transactions of the Chinese Society for Agricultural Machinery*, vol. 51, no. 2, pp. 341–349, 2020, 10.6041/j.issn.1000-1298.2020.02.037.
[40] T. Liu, P. Qin, L. Li, and Y. Tang, “Software-defined converged access network with cross-layer intelligent control architecture,” *Optical Fiber Technology*, vol. 50, pp. 242–249, Jul. 2019, doi: 10.1016/j.yofte.2019.04.001.
[41] G. He, C. Li, Y. Shu, and Y. Luo, “Fine-grained access control policy in blockchain-enabled edge computing,” *Journal of Network and Computer Applications*, vol. 221, p. 103706, Jan. 2024, doi: 10.1016/j.jnca.2023.103706.
[42] J. Seo and S. Park, “SBAC: Substitution cipher access control based on blockchain for protecting personal data in metaverse,” *Future Generation Computer Systems*, vol. 151, pp. 85–97, Feb. 2024, doi: 10.1016/j.future.2023.09.022.
[43] S. M. N. Sakib, “Navigating the New Frontier of Finance, Art, and Marketing,” 2023, pp. 64–90. doi: 10.4018/978-1-6684-9919-1.ch005.
[44] W. Sardjono, A. Cholidin, and Johan, “Applying Digital Advertising in Food and Beverage Industry for McDonald’s with Marketing 5.0 Approach,” *E3S Web of Conferences*, vol. 426, p. 02009, Sep. 2023, doi: 10.1051/e3sconf/202342602009.
[45] A. H. Karbasi and S. Shahpasand, “A post-quantum end-to-end encryption over smart contract-based blockchain for defeating man-in-the-middle and interception attacks,” *Peer Peer Netw Appl*, vol. 13, no. 5, pp. 1423–1441, Sep. 2020, doi: 10.1007/s12083-020-00901-w.
[46] V. J. Aski, V. S. Dhaka, A. Parashar, S. kumar, and I. Rida, “Internet of Things in healthcare: A survey on protocol standards, enabling technologies, WBAN architectures and open issues,” *Physical Communication*, vol. 60, p. 102103, Oct. 2023, doi: 10.1016/j.phycom.2023.102103.
[47] D. P. Krishna *et al.*, “SSH-DAuth: secret sharing based decentralized OAuth using decentralized identifier,” *Sci Rep*, vol. 13, no. 1, p. 18335, Oct. 2023, doi: 10.1038/s41598-023-44586-6.
[48] C. Sharma, S. S. Bharadwaj, N. Gupta, and H. Jain, “Robotic process automation adoption: contextual factors from service sectors in an emerging economy,” *Journal of Enterprise Information Management*, vol. 36, no. 1, pp. 252–274, Jan. 2023, doi: 10.1108/JEIM-06-2021-0276.
[49] S. Mitrevska, E. Vrangalovska, S. Baloska, D. Mechkaroska, and E. Domazet, “Blockchain as a Service, an overview on AWS and its BaaS,” in *2022 30th Telecommunications Forum (TELFOR)*, IEEE, Nov. 2022, pp. 1–4. doi: 10.1109/TELFOR56187.2022.9983746.
[50] A. J. Cabrera-Gutiérrez, E. Castillo, A. Escobar-Molero, J. Cruz-Cozar, D. P. Morales, and L. Parrilla, “Blockchain-Based Services Implemented in a Microservices Architecture Using a Trusted

Platform Module Applied to Electric Vehicle Charging Stations," *Energies (Basel)*, vol. 16, no. 11, p. 4285, May 2023, doi: 10.3390/en16114285.

[51] S. Li *et al.*, "Backdoor-Resistant Public Data Integrity Verification Scheme Based on Smart Contracts," *IEEE Internet Things J*, vol. 10, no. 16, pp. 14269–14284, Aug. 2023, doi: 10.1109/JIOT.2023.3285939.

[52] S. Lin, Z. Li, S. Zhao, H. Zhao, Y. Li, and S. Wang, "Design and Implementation of Blockchain-based College Education Integrity System," in *2022 IEEE 5th International Conference on Information Systems and Computer Aided Education (ICISCAE)*, IEEE, Sep. 2022, pp. 276–281. doi: 10.1109/ICISCAE55891.2022.9927601.

[53] R. T, A. A, D. G, and D. K, "Intelligent Crypto Currency Mining Farm for E-Vehicle," in *2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*, IEEE, Aug. 2023, pp. 1869–1875. doi: 10.1109/ICAISS58487.2023.10250588.

[54] G. Bindu, H. M. Moyeenudin, and R. Anandan, "Blockchain of Cryptocurrency Using a Proof-of-Work-Based Consensus Algorithm with an SHA-256 Hash Algorithm to Make Secure Payments," 2024, pp. 243–252. doi: 10.1007/978-3-031-35751-0_17.

[55] N. Khanam and M. S. Islam, "Role of cloud computing and blockchain technology in paradigm shift to modern online teaching culture in the education sector," in *Artificial Intelligence and Blockchain in Industry 4.0*, Boca Raton: CRC Press, 2023, pp. 263–276. doi: 10.1201/9781003452591-18.

[56] N. us Sehar *et al.*, "Blockchain enabled data security in vehicular networks," *Sci Rep*, vol. 13, no. 1, p. 4412, Mar. 2023, doi: 10.1038/s41598-023-31442-w.

[57] K. Godewatte Arachchige, P. Branch, and J. But, "Evaluation of Blockchain Networks' Scalability Limitations in Low-Powered Internet of Things (IoT) Sensor Networks," *Future Internet*, vol. 15, no. 9, p. 317, Sep. 2023, doi: 10.3390/fi15090317.

[58] S. Wang, N. Karandikar, K. E. Knutsen, X. G. Tony Tong, T. Edseth, and Z. X. Zile, "Enhancing Maritime Data Standardization and Integrity using Docker and Blockchain," in *2023 IEEE/ACM 45th International Conference on Software Engineering: Companion Proceedings (ICSE-Companion)*, IEEE, May 2023, pp. 370–374. doi: 10.1109/ICSE-Companion58688.2023.00105.

[59] I. Keshta *et al.*, "Blockchain aware proxy re-encryption algorithm-based data sharing scheme," *Physical Communication*, vol. 58, p. 102048, Jun. 2023, doi: 10.1016/j.phycom.2023.102048.

[60] A. Jain, C. Jain, and K. Krystyniak, "Blockchain transaction fee and Ethereum Merge," *Financ Res Lett*, vol. 58, p. 104507, Dec. 2023, doi: 10.1016/j.frl.2023.104507.

[61] H. Wang, Z. Zheng, S. Xie, H. N. Dai, and X. Chen, "Blockchain challenges and opportunities: a survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, p. 352, 2018, doi: 10.1504/IJWGS.2018.10016848.

[62] A. Hombalimath, N. Mangla, and A. Balodi, "Designing A Permissioned Blockchain Network For The Insurance Claim Process Using Hyperledger Fabric And Composer," *Informatica*, vol. 47, no. 3, Jun. 2023, doi: 10.31449/inf.v47i3.4158.

[63] B. Deena Divya Nayomi, S. Suguna Mallika, P. Laxmikanth, and M. Bhavsingh, "A Cloud-Assisted Framework Utilizing Blockchain, Machine Learning, and Artificial Intelligence to Countermeasure Phishing Attacks in Smart Cities," in *Original Research Paper International Journal of Intelligent Systems and Applications in Engineering IJISAE*, 2023, pp. 313–327. [Online]. Available: www.ijisae.org

[64] A. Serada, J. Grym, and T. Sihvonen, "The Economy of Attention on Blockchain in the Brave Browser," in *Futures of Journalism*, Cham: Springer International Publishing, 2022, pp. 49–62. doi: 10.1007/978-3-030-95073-6_4.

[65] T. Yuvaraj *et al.*, "Comparative analysis of various compensating devices in energy trading radial distribution system for voltage regulation and loss mitigation using Blockchain technology and Bat Algorithm," *Energy Reports*, vol. 7, pp. 8312–8321, Nov. 2021, doi: 10.1016/j.egyr.2021.08.184.

[66] W. Liang, L. You, and G. Hu, "LRS_PKI: A novel blockchain-based PKI framework using linkable ring signatures," *Computer Networks*, vol. 237, p. 110043, Dec. 2023, doi: 10.1016/j.comnet.2023.110043.

[67] Z. Zeng *et al.*, "Blockchain Technology for Information Security of the Energy Internet: Fundamentals, Features, Strategy and Application," *Energies (Basel)*, vol. 13, no. 4, p. 881, Feb. 2020, doi: 10.3390/en13040881.

[68] A. I. Taloba, A. Elhadad, R. M. A. El-Aziz, and O. R. Shahin, "Prediction of data threats over web medium using advanced blockchain based information security with crypto strategies," *J Ambient Intell Humaniz Comput*, pp. 1026–1034, Apr. 2021, doi: 10.1007/s12652-021-03109-9.

[69] H. Xiao, W. Zhang, W. Li, A. T. Chronopoulos, and Z. Zhang, “Joint Clustering and Blockchain for Real-Time Information Security Transmission at the Crossroads in C-V2X Networks,” *IEEE Internet Things J*, vol. 8, no. 18, pp. 13926–13938, Sep. 2021, doi: 10.1109/JIOT.2021.3068175.
[70] S. Efendi, B. Siregar, and H. Pranoto, “Concept Designs of Patient Information Security Using e-Health Sensor Shield Platform on Blockchain Infrastructure,” 2018, pp. 641–646. doi: 10.1108/978-1-78756-793-1-00100.