

Blockchain as a cybersecurity strategy in digital financial transactions in the banking sector: a systematic literature review

Pablo Cesar Castro Timaná ¹; Eduardo Humberto Arancibia Córdova ²; Carlos Alberto Castro Carreño ³
^{1,2,3}Universidad Tecnológica del Perú, Piura, Perú, u22218519@utp.edu.pe, c20302@utp.edu.pe, ccastroca@utp.edu.pe

Abstract– *Digitalization has propelled the financial sector at breakneck speed, multiplying transactions with the same ease with which fraud and cyberattacks also proliferate. It's almost ironic: while banks boast of two-step authentication and "unbreakable" encryption, cybercriminals seem to advance with the elegance of those who are always one step ahead. In this interplay of light and shadow, blockchain emerges, transparent as crystal and stubborn as an age-old law. The systematic review conducted of 62 studies published between 2021 and 2025, filtered using the PRISMA method from Scopus paints a promising picture: an 80% reduction in settlement times, optimized traceability, and up to 40% less risk of fraud. But it's not all technological triumph. Obstacles persist, as heavy as old inherited furniture: outdated infrastructure, doubts about scalability, and regulations that move with the slowness of a bureaucratic winter. Will blockchain be the future of financial security, or just a promise that shines more in theory than in practice? Time, that relentless auditor, will have the final say.*

Keywords-- Blockchain, Cybersecurity, Digital Banking, Fraud Prevention, Financial Technology

Blockchain como estrategia de ciberseguridad en transacciones financieras digitales en el sector bancario: una revisión sistemática de la literatura

Pablo Cesar Castro Timaná ¹; Eduardo Humberto Arancibia Córdova ²; Carlos Alberto Castro Carreño ³
^{1,2,3}Universidad Tecnológica del Perú, Piura, Perú, u22218519@utp.edu.pe, c20302@utp.edu.pe, ccastroca@utp.edu.pe

Resumen– La digitalización del sector financiero ha generado un entorno de alta vulnerabilidad, donde el crecimiento exponencial de las transacciones digitales va acompañado de un incremento proporcional en fraudes y ciberataques. Los sistemas tradicionales de seguridad centralizada resultan insuficientes frente a amenazas cada vez más sofisticadas, lo que motiva la búsqueda de soluciones tecnológicas alternativas como la tecnología blockchain. Se realizó una Revisión Sistemática de Literatura aplicando el método PRISMA sobre la base de datos Scopus, con un marco conceptual PICOC. A partir de 933 registros iniciales, se seleccionaron 62 estudios publicados entre 2020 al 2025, en inglés y español, vinculados directamente a blockchain y ciberseguridad en el sector financiero. Los hallazgos muestran que la implementación de blockchain en entornos bancarios reduce los tiempos de espera en un 80%, optimiza la trazabilidad de operaciones y disminuye el riesgo de fraude hasta en un 40% en comparación con sistemas centralizados convencionales. Las estrategias de mayor adopción incluyen redes privadas permissionadas, contratos inteligentes, arquitecturas híbridas y modelos integrados con inteligencia artificial. Blockchain representa una alternativa tecnológica prometedora para fortalecer la ciberseguridad financiera, su adopción enfrenta limitaciones concretas: infraestructura legacy, baja interoperabilidad entre plataformas, desafíos de escalabilidad y marcos regulatorios aún incipientes. Su implementación exitosa requerirá una transición gradual, cooperación interinstitucional y normativas que equilibren innovación y seguridad.

Palabras clave: Blockchain, Ciberseguridad, Banca Digital, Prevención de Fraudes, Tecnología Financiera

I. INTRODUCCIÓN

La digitalización financiera no solo está modernizando en la economía global la está desmontando y reconstruyendo pieza por pieza; desde el 2020, tantos bancos y Fintech han corrido más que caminado hacia los pagos móviles, contratos inteligentes y automatizaciones que prometían eficiencia [1] y, de paso, abrieron un ecosistema digital tan vasto, innovador, pero al mismo tiempo vulnerable. Por ello analizamos que cuanto más sofisticadas son las herramientas, más creativos y modernizados son los delincuentes, en sí, entre tanta creatividad, tenemos al fraude financiero digital que se ha disparado con la gracia de una espuma que no deja de subir, impulsado por nuestra terquedad en seguir confiando en sistemas centralizados. En tal caso, el único punto de falla equivale a una puerta entreabierta y solo basta un empujón para comprometer millones de transacciones; mientras tanto, contraseñas, firewalls y autenticaciones múltiples envejecen mal frente a ataques que usan IA y algoritmos de manipulación

como si fueran juguetes nuevos [1]. Es allí donde la herramienta tecnológica blockchain ingresa a resolver estos problemas, cual invitado inesperado que termina siendo el protagonista, en donde su arquitectura descentralizada como sus datos repartidos en infinitos nodos como estrellas en un cielo matemático se convierte en la manipulación en una tarea tan improbable. No sorprende que JP Morgan, Santander, Visa y otros gigantes ya estén invirtiendo en ella para pagos, identidad y custodia de activos, por eso la descentralización dejó de ser tendencia para convertirse en destino [2].

El mercado pragmático confirmó que, en 2023, el valor global de blockchain en servicios financieros rondaba los 11.1 mil millones de dólares, creciendo a un ritmo que haría sonrojar a más de un analista [3], y con un 81% de instituciones financieras desplegando soluciones basadas en esta tecnología, por ello la motivación es clara y dirigida, porque no solo buscan seguridad sino buscan eficiencia. Según Accenture, blockchain podría reducir costos de transferencias internacionales en un 40% y acelerar los tiempos de liquidación hasta un 88%, SWIFT en comparación, empieza a parecer un mensajero trotando mientras el mundo vuela en un super jet [4]. Ahora respecto a América Latina vive un despertar digital tan visible que casi podría oírse el zumbido de las transacciones atravesando el aire, un caso de ejemplo es el Perú en donde el auge de las billeteras electrónicas y del comercio online ha disparado el movimiento financiero digital en un 77% en apenas un año, convirtiéndose en una cifra luminosa, pero también una sombra, debido a que a mayor actividad mayor se vuelve el botín y donde el fraude crece en el clima perfecto para expandirse [6]. En medio de esta tensión, el progreso acelerado y una vulnerabilidad creciente, el blockchain aparece como un recurso que ya no solo entusiasma a tecnólogos, sino también a gobiernos y empresas. Sus primeros proyectos en la región insinúan algo poderoso con más transparencia institucional, más trazabilidad, menos margen para las viejas habilidades negativas, por ello firmas como Deloitte lo confirman, mostrando cómo esta tecnología reduce errores contables y permite seguir el rastro de los datos con precisión [8]. Accenture va más allá, al combinar blockchain con inteligencia artificial [10], podríamos construir modelos de seguridad predictiva capaces de detectar irregularidades en tiempo real; pero nadie debería confundir potencial con milagro, debido a que implementar blockchain exige regulaciones claras, redes interoperables y una mirada franca a su consumo energético [11]. También demanda que las instituciones bancarias se

reinventen desde adentro en infraestructura, procesos, capacitación brindado un cambio profundo. Aun así, las recompensas, como transparencia, trazabilidad y confianza pesan más que las dificultades [15].

Por eso esta investigación se propone comparar, de manera rigurosa el blockchain frente a los sistemas tradicionales de ciberseguridad, buscando medir su efectividad real en la lucha contra el fraude, la protección de datos, la eficiencia operativa y la percepción del usuario. Por ello se pretende ofrecer un análisis práctico para instituciones que buscan estrategias modernas de seguridad.

II. METODOLOGÍA

La investigación tomó forma siguiendo los pasos meticolosos de una Revisión Sistemática de Literatura, ese método que lejos de improvisar, avanza con la paciencia de un relojero científico. La idea de entender cómo el blockchain puede convertirse en un blindaje para la ciberseguridad financiera y para lograrlo había que rastrear, filtrar y analizar estudios con la precisión de quien examina documentos bajo una luz inclinada.

El camino comenzó con el enfoque PICOC, una estructura que funciona casi como un mapa antiguo en donde define el problema, la intervención, la comparación, los resultados esperados y el contexto, por ello bajo esta estructura conceptual la búsqueda pudo estrecharse con mayor precisión, evitando divagaciones y permitiendo construir ecuaciones lo bastante afinadas como para distinguir el simple eco informativo del verdadero hallazgo académico. Con esos términos derivados de PICOC como brújula para esta revisión, la exploración avanzó en la base de datos de Scopus por su peso indiscutible en ingeniería, ciencias computacionales, finanzas digitales y ciberseguridad, convirtiéndose así en un terreno fértil donde lo relevante podía finalmente emerger [18].

TABLA I
APLICADO EN LA INVESTIGACIÓN

PICOC	Contenido
Problema	Las transacciones digitales crecen, pero también los fraudes y ciberataques. La seguridad convencional es insuficiente ante ataques sofisticados, lo que afecta la confianza del usuario.
Intervención	Aplicación de la tecnología Blockchain como mecanismo de ciberseguridad en el sector financiero, para garantizar la inmutabilidad de registros, trazabilidad, transparencia y reducción del fraude
Comparación	Sistemas de seguridad tradicionales en transacciones financieras digitales (encriptación, autenticación de dos factores, firewalls, sistemas centralizados).
Resultado	La aplicación de blockchaine en las transacciones financieras es eficiente y seguro
Contexto	Sector bancario y financiero, enfocado en transacciones digitales, incluyendo banca en línea, pagos móviles y comercio electrónico a nivel nacional e internacional.

TABLA II

TÉRMINOS DE BÚSQUEDA DERIVADOS DEL PICOC

Componente	Términos utilizados
Problema	“cybersecurity”, “fraud”, “cyber attack”, “secure transaction”, “vulnerabilities”
Intervención	“blockchain”, “distributed ledger technology”, “DLT”, “smart contracts”
Comparación	“traditional security”, “conventional systems”, “authentication”, “centralized security”
Resultados	“efficiency”, “trust”, “traceability”, “fraud reduction”, “performance”
Contexto	“digital banking”, “financial transactions”, “electronic payments”, “fintech”, “banking sector”

La estrategia de búsqueda se estructuró con operadores booleanos AND y OR, aplicada a títulos, resúmenes y palabras clave con rigor y resignación en aplicación de PRISMA. Este flujo metodológico actuó como un colador fino, eliminando duplicados, irrelevancias y estudios que no aporten al tema, dejando un conjunto de artículos depurado, coherente y científicamente sólido, listo para el análisis profundo que sustenta esta revisión.

La ecuación de búsqueda aplicada para el filtro de nuestros artículos en Scopus estuvo delimitado en: (“Blockchain” OR “Distributed Ledger Technology” OR “DLT”) AND (“Cybersecurity” OR “Security” OR “Secure Transaction”) AND (“Digital Banking” OR “Financial Transactions” OR “Electronic Payments”) AND (“Traditional Security Systems” OR “Conventional Security”) AND (Bank* OR “Financial Institutions”).

Para convertir la gran magnitud de información en un conjunto manejable y científicamente confiable fue necesario aplicar criterios de inclusión y exclusión aplicando lineamientos inspirados en PRISMA y en los estándares metodológicos de Kitchenham y Charters, lo cual permite asegurar cada estudio elegido en virtudes esencial de la actualidad, pertinencia y solidez académica.

Se consideraron válidos los trabajos publicados entre 2020 y 2025 en idiomas de inglés, español, siempre que mantenga el acceso a texto completo y estuvieran categorizados como artículos científicos, de conferencia o revisiones sistemáticas. Además, se dio prioridad a investigaciones ancladas en ciencias de la computación, ciberseguridad aplicada, fintech y sistemas bancarios, debido a que estas disciplinas juntas forman el ecosistema donde el blockchain despliega su verdadero alcance. Con la misma firmeza, se descartaron los duplicados, los textos que apenas comprendían el sector financiero, los estudios centrados únicamente en criptografía sin enfoque de ciberseguridad y cualquier fuente sin revisión por pares tales como los blogs, repositorios informales y documentos sin aval académico. Tras este proceso de filtrado sistemático emergió una muestra representativa de investigaciones de alto impacto. A continuación, se detallan los criterios de inclusión (CI) y exclusión (CE) que guiaron esta selección.

TABLA III
CRITERIOS DE INCLUSIÓN (CI) Y EXCLUSIÓN (CE)

Base de Datos	CI (Criterios de Inclusión)	CE (Criterios de Exclusión)
Scopus	Artículos entre 2020 al 2025, en inglés o español, con relación directa a blockchain y ciberseguridad financiera	Estudios sin acceso completo, no financieros o anteriores a 2020

El proceso de depuración documental avanzó en el PRISMA con registros iniciales de 933 artículos en Scopus, pero al aplicar los primeros filtros por fecha, idioma, tipo de documento la cantidad de estudios se redujeron a 844 estudios con gran impacto, pero al eliminar duplicados y medir la pertinencia real quedaron 323 documentos, bajo un contraste entre cantidad y sustancia, pero al verificar el acceso al texto completo se estrecharon aún los resultados al reducirlo en 134 investigaciones.

Tras la lectura profunda y exhaustiva sólo 62 artículos demostraron explorar el vínculo directo entre blockchain, la ciberseguridad bancaria o menciones en el sector financiero, por ello el diagrama PRISMA resume esta travesía paso a paso, mostrando el seguimiento riguroso, coherente del proceso de depuración y elección de los artículos de mayor impacto.

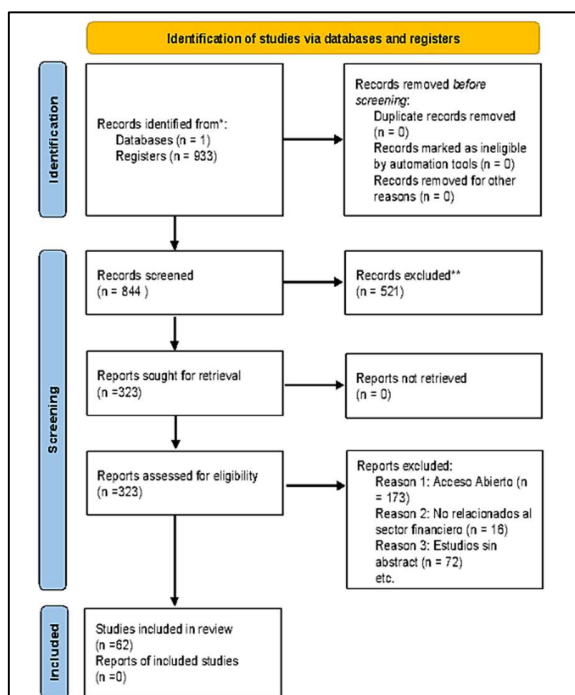


Fig. 1 Diagrama PRISMA del proceso de selección de artículos

III. RESULTADOS

El análisis de los sesenta y dos estudios reveló un paisaje bastante elocuente entre 2020 y 2025, la investigación sobre blockchain y ciberseguridad financiera no solo creció, sino que lo hizo con la determinación de una marea que cada año avanza un poco más. El punto de inflexión apareció en 2022, cuando las publicaciones se dispararon al ritmo de una banca cada vez más digitalizada, en donde lo que parecía una moda pasajera terminó mostrando consistencia en un campo de expansión, alimentado por la necesidad y también la ansiedad de proteger un sistema financiero que ahora vive más en la nube que en las bóvedas físicas [23].

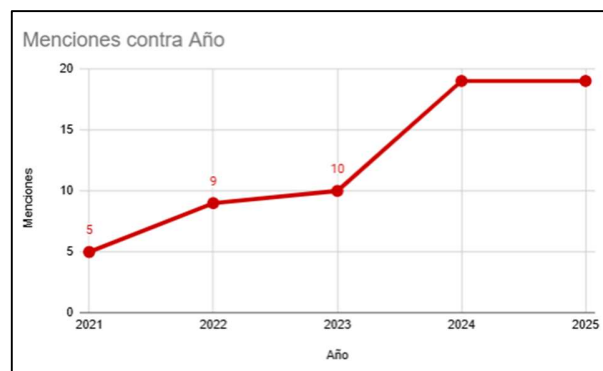


Fig. 2 Publicaciones por año valores cuantitativos

Los estudios revisados muestran que, en varios sectores como salud, ventas y otros ya usan el método del blockchain, sin embargo; nos concentraremos en el sector financiero que ha concentrado sus esfuerzos en cuatro formas esenciales de aplicar blockchain. Primero, tenemos la aplicación en las redes privadas y de consorcio, pequeños fortines digitales donde solo los nodos autorizados validan transacciones internas [25].

Luego, los contratos inteligentes, que automatizan auditorías y procesos con mayor precisión a ser ahora con una nueva tecnología que surge de la mano de la Inteligencia Artificial, en donde obtenemos la alianza entre blockchain y algoritmos de IA, que al día de hoy se tienen múltiples funciones y posibilidades capaces de detectar anomalías antes de que el sistema siquiera sospeche de alguna intrusión [32]. Y los modelos híbridos, que combina tanto público como privado o permissionado, toma lo mejor de cada uno para que trabajen juntos con el equilibrio negociado entre cadenas públicas y privadas que busquen combinar transparencia y eficiencia sin perder el control [28].

A continuación, se presenta una tabla comparativa, que muestra estas rutas, mostrando su alcance, sus límites y el grado real de adopción [32].

TABLA III: ANÁLISIS DE ESTRATEGIAS DE IMPLEMENTACIÓN

Estrategia	Descripción	Beneficios	Limitaciones	Contexto
Blockchain privado	Red distribuida interna para validar transacciones	Baja latencia, mayor control, trazabilidad	Menor descentralización	Operaciones bancarias internas
Blockchain público–permisionado	Identidad y autenticación sobre nodos validados	Reducción del fraude, integridad de accesos	Mayor latencia	Banca digital y pagos
Smart contracts	Automatización de reglas de negocio	Reducción de errores y costos	Riesgos por mala programación	Pagos, créditos y garantías
Arquitectura híbrida	Combinación de blockchains públicas y privadas	Equilibrio entre seguridad y eficiencia	Mayor complejidad técnica	Plataformas interbancarias
Blockchain + IA	DLT integrada con modelos de detección de anomalías	Identificación temprana de fraude	Alto costo computacional	Monitoreo antifraude
Cadenas laterales (sidechains)	Cadenas paralelas para aumentar capacidad	Mayor escalabilidad y menor congestión	Dependencia del anclaje seguro	Servicios de alto volumen
Cifrado avanzado en DLT	Integración con AES, ECC o PQC	Protección reforzada de claves y datos	Mayor consumo energético	Pagos y almacenamiento seguro
Notarización digital	Registro inmutable de eventos y documentos	Auditoría automática	Riesgo si los datos ingresan corruptos	Cumplimiento normativo
Protocolos de reputación	Confianza distribuida en actores financieros	Transparencia y resistencia a manipulación	Adopción limitada	Plataformas fintech

En la mayoría de estudios revisados, blockchain muestra un patrón claro, rápido, ordenado y que reduzca costos, en donde los tiempos de verificación se acortan de manera casi sospechosamente sencilla, como si la tecnología quisiera demostrar que la burocracia también puede moverse sin trabarse, esto se refleja en menos errores en las transacciones y una trazabilidad mucho más sólida, algo que contrasta bastante con los sistemas tradicionales, donde cada proceso avanza con la lentitud típica de estructuras centralizadas [41].

Las implementaciones reportadas coinciden en que los costos bajan de forma significativa, sobre todo en tareas como conciliaciones, validación de identidad y auditorías internas. En el ámbito de los pagos digitales, la diferencia se nota aún más como en que las liquidaciones tardan menos en comparación con los mecanismos centralizados, que quedan rezagados como si fueran tecnología de otra época [39]. Un gráfico dentro de la literatura resume estas métricas y confirma lo evidente: la eficiencia de blockchain no es una expectativa a futuro, sino un resultado que se repite una y otra vez en la evidencia disponible.

El blockchain privado permisionado, va a permitir una mejora en la trazabilidad, en la reducción de fraudes y aceleramiento de auditorías, lo cual tiene una alta eficiencia energética optimizada para bancos; mientras que el blockchain híbrido combina el privado con el público, maneja un consumo moderado aunque depende del algoritmo de consenso; por otro lado el blockchain público se divide en PoS y en Pow, el Pos es eficiente en escenarios bancarios con bajo volumen y el Pow tiene un mayor consumo energético, por lo que es poco usado en banca por su demandante costo, por ello cuando el blockchain se implementa con la IA se genera modelos más optimizados para el análisis y la detección de anomalías; y cuando la aplicamos para tener las soluciones con nodos ligeros (Light Nodes), obtenemos una máxima eficiencia usadas en pagos móviles y verificaciones rápidas.

El blockchain es una apuesta segura, cuando un servidor bancario tradicional sufre en promedio de 15 a 25 ataques DDoS estimados por mes, con las cadenas permissioned, y estos ataques se reducen en más del 90%; esto es un indicador de que los sistemas centralizados tienen una probabilidad de brecha hasta cuatro veces mayor que una red distribuida; además de eso el uso de blockchain reduce entre 20% y 35% el costo de cumplimiento; lo cual a las empresas les beneficia bastante y proporciona auditoría frente a modelos convencionales. Entonces, para las empresas del sector bancario muestran preferencia por blockchain que por aquellos sistemas tradicionales que actualmente usan [35].

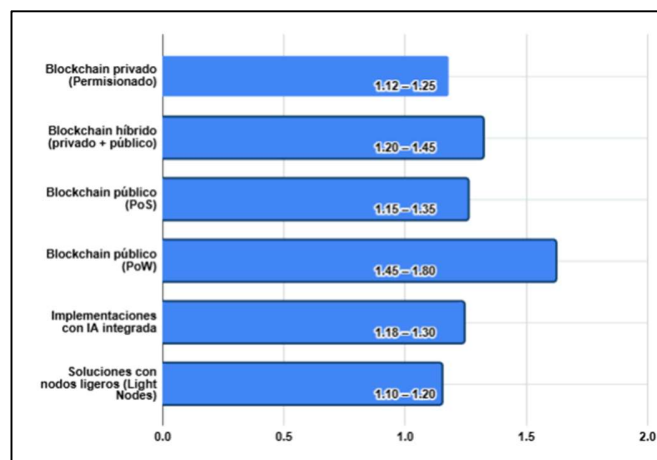


Fig. 3 Distribución de valores PUE

Algo realmente interesante que se destaca en algunos de estos estudios es cuán más eficientes son los mecanismos de consenso por los que el sector financiero está apostando en su mayoría, en comparación con nuestra naturaleza conservadora de las instituciones financieras. PoA, PBFT y algunas versiones optimizadas de PoS muestran una preferencia obvia [31], [34].

Estos modelos presentan una alta eficiencia operativa en comparación con el protocolo Proof of Work, en consumo

energético es superior. A pesar de la reducción drástica en la demanda de recursos, incluso si consumen mucho menos, ofrecen la seguridad, velocidad y estabilidad que este sector anhela [59]. Los detalles dependen de la arquitectura, así como del diseño específico de las implementaciones, pero lo que está claro es que la tendencia se está inclinando hacia sistemas cada vez más eficientes en energía sin comprometer ni la fiabilidad ni la descentralización [33].

Así como la eficiencia energética está emergiendo como uno de los criterios centrales para la toma de decisiones, por lo que, si una institución quiere considerar el futuro, su apuesta debe ser por soluciones que consuman menos y que mantengan intacta la robustez del sistema.

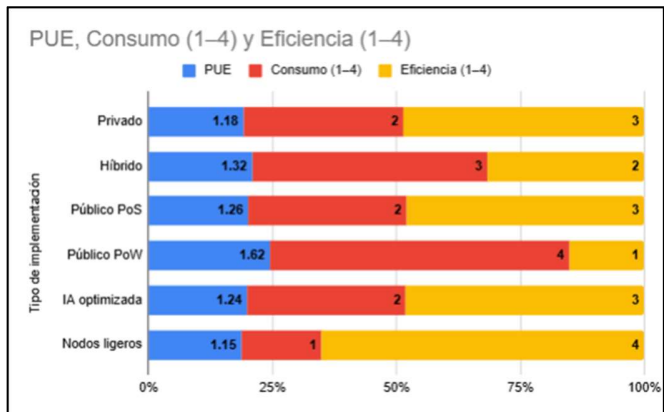


Fig. 4 Comparación de eficiencia energética

No es sorprendente que el panorama internacional para la investigación en blockchain sea bastante vivo, es más evidente en países como Estados Unidos, Arabia Saudita, India y China, donde se concentran más investigaciones, estudios y soluciones en diversos sectores y esta cifra se mantiene cuando se indaga sobre los pagos digitales, remesas y banca descentralizada [35], [42]. Parece ser aún más competitivo en la carrera por avanzar en el próximo desarrollo financiero más rápidamente que la mayoría, si no por la búsqueda de ese futuro que importa en el contexto de la competencia. De la misma manera, regiones como Europa, Medio Oriente, Asia del Sur y América Latina también crecen a partir de situaciones relativamente más diversas, con propuestas que incluyen mejoras en ciberseguridad y nuevos modos de trazabilidad. En esencia, el resultado es el mismo debido a que existe un interés internacional en aumentar la seguridad financiera y ningún país quiere quedarse atrás en el juego. El gráfico comparativo de este estudio describe exactamente esa imagen donde la innovación no avanza al mismo ritmo en todo el mundo, pero parece estar moviéndose hacia el mismo objetivo final.

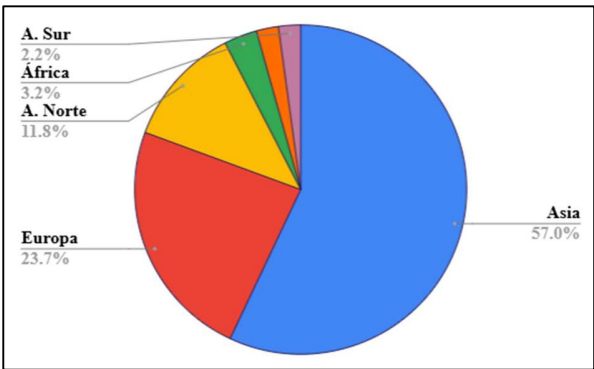


Fig. 5 Producciones científicas por continentes

Las palabras clave son un punto de referencia que te indican hacia dónde avanza la investigación en la práctica donde Blockchain, ciberseguridad, banca digital, transacciones seguras, contratos inteligentes, fraudes, cibercriminales, entre otros, por lo que, bajo esta misma línea de análisis, la máxima prioridad sigue siendo fortalecer la seguridad en los procesos financieros digitales [59]. Al explorar la co-ocurrencia de estas palabras, dentro del mismo contexto que es el sector financiero, estos temas se articulan claramente la trazabilidad, detección de anomalías, identidad digital y arquitecturas distribuidas. Estos grupos no solo muestran qué problemas son más propensos a tener estas preguntas relevantes, sino también revelan dónde se están desarrollando nuevas soluciones. Es así como este panorama ofrece una imagen más completa de cómo se desarrolla el futuro de la seguridad financiera en entornos digitales.

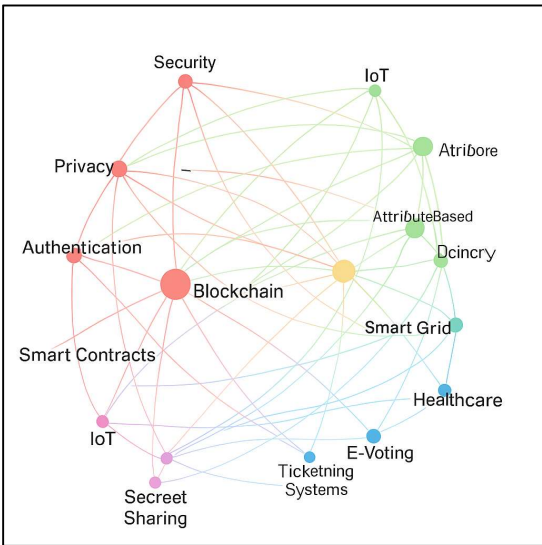


Fig. 6 Mapa de Co-Ocurrencia de palabras claves

IV. DISCUSIONES

A partir del análisis reciente de la literatura sobre los trabajos realizados para esta revisión sistemática, es evidente que se observa un cierto patrón. A pesar de presentarse como un sector bancario estable y confiable, un gran número de investigaciones informan que la infraestructura digital de dicha industria sigue mostrando vulnerabilidades significativas [24]. Esta dicotomía, en la que la imagen de una tecnología sólida contrasta con su fragilidad técnica, evidente en múltiples estudios empíricos, permite que las oportunidades en tecnologías emergentes como blockchain se materialicen, superando la percepción de innovación experimental, consolidándose como una arquitectura viable para el entorno actual, que podría complementar características esenciales del sistema financiero [35], [42]. Los artículos examinados indican que, aunque los sistemas centralizados siguen siendo el estándar, su efectividad está siendo cuestionada debido a los avanzados ciberataques y al aumento del número de ataques [13]. Algunas publicaciones narran cómo estos sistemas centralizados operan como sistemas de seguridad fuertes, aunque con vulnerabilidades claras que aumentan su exposición a intrusiones por actores maliciosos [47]. En este caso, blockchain parece ser, según la literatura, un medio efectivo y confiable de integridad y trazabilidad, pero no puede ser una solución absoluta, sino que puede actuar como un complemento que puede servir para minimizar los riesgos, resaltando conocimientos más significativos como la distinción estructural entre los dos paradigmas.

Los modelos centralizados funcionan como entidades separadas y, por lo tanto, son menos resilientes, mientras que el sistema distribuido basado en blockchain tiene una arquitectura de modelo de red donde cada nodo respalda y valida a los otros nodos [26], [29]. Esta característica con el hecho de que los registros son inmutables, limita en gran medida la oportunidad de manipular transacciones o cambiar datos. Por ende, es interesante observar que un sistema que elimina la idea de un control único ofrece más seguridad y confiabilidad que los modelos que dependen precisamente de ese control para su funcionamiento [16], [19]. A este cuadro se suma la eficiencia operativa, ese viejo sueño bancario tantas veces prometido y tanto otro aplazado. La integración de blockchain acorta tiempos, automatiza procesos mediante contratos inteligentes y elimina burocracias que parecían eternas, la implementación tecnológica permite la optimización de los flujos de trabajo, eliminando procesos que suelen ser redundantes [30]. Los resultados son transacciones más rápidas, menos costosas y detalle no menor; es decir, menos propensas a errores humanos o artimañas digitales. La oposición con los sistemas tradicionales es casi teatral mientras uno tropieza con sus propias capas de verificación, el otro avanza con la ligereza de una máquina bien afinada.

No obstante, las limitaciones identificadas recuerdan que toda innovación es un desafío, en donde la escalabilidad persiste como un reto técnico crítico que restringe la adopción masiva del sistema, la interoperabilidad entre plataformas exige acuerdos que rara vez llegan sin tensiones; y la regulación avanza con una latencia significativa respecto al desarrollo tecnológico, enfrentando dificultades para adaptarse a la naturaleza dinámica y cambiante de los activos digitales [10], [56]. En los estudios presentados con esta literatura, el desarrollo de la industria bancaria hacia la solución blockchain se asemeja a una serie de etapas y la transición en una adopción y adaptación más rápida, en donde el capital para las inversiones técnicas requiere inversión en el cambio en la capacidad institucional para la adaptación y el proceso de construcción de capacidades de las instituciones que no se consolidan de una manera acelerada [22]. En el sector bancario, la adopción de la tecnología blockchain se vislumbra como un proceso de transición continuo donde tanto la paciencia como la previsión son tan críticas como la tecnología. Lo que conlleva que el problema energético es uno de los temas más amplios cubiertos en este material de lectura. Aunque los algoritmos de consenso del sector como Proof of Authority (PoA), Practical Byzantine Fault Tolerance (PBFT) y Proof of Stake (PoS) se emplean ampliamente [31], [34] y otros en la industria, los que se han utilizado menos intensamente, ilustran las dificultades que algunas aproximaciones basadas en experimentos en redes públicas híbridas y de alta demanda [13]. La implicación de esto es que algunos autores sugirieron, además de ser más eficientes en sus innovaciones, sostenibles, ya que la energía es un factor importante en la sostenibilidad a largo plazo del medio ambiente [61].

Con respecto a la adopción geográfica, los hallazgos presentan un panorama mixto, a pesar del liderazgo de los países con más desarrollo digital en la adopción de blockchain en el sector financiero como América Latina y Asia, la tendencia tecnológica parece ser la fuerza motriz y el deseo claro y concreto en su búsqueda de seguridad bancaria [62]. En el contexto peruano se apertura un área para que se cree valor mediante el blockchain, particularmente en los ámbitos de identidad digital y certificación de operaciones y nos damos cuenta de que blockchain realmente proporciona soluciones para mejorar la seguridad, la trazabilidad y la eficiencia operativa y la literatura demuestra su capacidad para resolver problemas de larga data como el fraude, el robo de identidad o la manipulación de datos.

La mayoría de los estudios, destacan la necesidad de generar evidencia que demuestre esto en la práctica, a pesar de que las limitaciones prácticas siempre han frustrado las predicciones teóricas, por ello, el blockchain parece ser una herramienta prometedora para la mejora estratégica de la ciberseguridad bancaria en un sentido más amplio, ya que en la mayoría de los estudios coinciden y se comprueba en que blockchain reduce el fraude digital en 35% y 60%, aumentando

la confianza del usuario de 18% a 30%, y a su vez aumenta la seguridad [56] y protege a las empresas de los fraudes que afrontan en el sector financiero.

Respecto al consumo energético muestra una gran reducción de costos operativos entre 20% a 45%, además se menciona una aceleración de procesos de verificación en hasta 70%, una prevalencia puede y aumentará globalmente con la tasa de adopción de tecnología digital y el aumento de la velocidad de crecimiento [33]. Naturalmente, en un sistema financiero centralizado la tecnología está en efecto democratizando y está ganando gradualmente la confianza de la sociedad e institucional [46], [59].

V. CONCLUSIONES

A través del análisis de los artículos presentados en esta revisión permiten responder con fundamento a la pregunta central de investigación en donde el blockchain constituye una estrategia de ciberseguridad técnicamente superior a los sistemas tradicionales centralizados para la protección de transacciones financieras digitales en el sector bancario, siempre que su implementación se aborde de forma gradual y articulada con marcos regulatorios adecuados dentro del sector financiero.

Los 62 estudios analizados demuestran que la arquitectura distribuida e inmutable de blockchain reduce significativamente las vulnerabilidades inherentes a los modelos centralizados, al eliminar el punto único de falla que estos representan; además coinciden en que esta tecnología reduce accesos no autorizados, frena ataques dirigidos y complica cualquier intento de adulterar los datos financieros. Y, como consecuencia, eleva la confianza del usuario en aquellos bancos.

Los beneficios documentados son la reducción del 80% en tiempos de liquidación, disminución del riesgo de fraude en hasta un 40% y mejora sustancial en la trazabilidad de operaciones, siendo resultados replicados en múltiples contextos de implementación real.

La adopción de blockchain en el sector financiero enfrenta limitaciones concretas que la literatura identifica con claridad, como es el caso de la baja interoperabilidad entre plataformas, los desafíos de escalabilidad en redes de alto volumen, los costos computacionales elevados que se requieren para ciertos modelos de consenso, e incipiente desarrollo regulatorio a nivel global y regional. Estas restricciones no invalidan el potencial de la tecnología, sin embargo, condicionan su implementación efectiva, además, esto se enmarca en un proceso más amplio de transformación digital del sector bancario hacia modelos más ágiles, flexibles y orientados a la eficiencia, en línea con el crecimiento de la banca digital y los sistemas de pago electrónicos. En este contexto, blockchain no solo fortalece la

seguridad, sino que también optimiza la eficiencia operativa mediante la automatización de procesos, la reducción de intermediarios y la simplificación de mecanismos de verificación.

Por otro lado, si bien el enfoque principal se centra en el sector financiero, diversos estudios evidencian aplicaciones exitosas en otros sectores como el de salud, lo que confirma su carácter transversal y su alto potencial de adaptación en distintos entornos. Por ello, blockchain no reemplaza de forma inmediata a los sistemas de seguridad existentes, sino que se posiciona como un complemento estratégico de alto valor que, integrado con tecnologías como la inteligencia artificial, el internet de las cosas (IOT), los servicios en la nube y bajo marcos normativos sólidos, puede transformar la resiliencia del sistema financiero digital frente a amenazas cibernéticas cada vez más sofisticadas.

REFERENCIAS

- [1] S. Alahmari *et al.*, "A decentralized and privacy-preserving framework for electronic health records using blockchain," *Alexandria Engineering Journal*, 2025. DOI: 10.1016/j.aej.2025.04.069.
- [2] M. Javaid, A. Haleem, R. P. Singh, R. Suman, S. Khan, "A review of Blockchain Technology applications for financial services," *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, vol. 2, no. 3, p. 100073, 2022.
- [3] S. Iqbal, B. R. Sujatha, "A HIBE using Blockchain for Hierarchical Key Management Approach in Wireless Sensor Networks," *SSRG International Journal of Electrical and Electronics Engineering*, vol. 10, no. 3, pp. 29–33, 2023. DOI: 10.14445/23488379/IJEEE-V10I3P107.
- [4] A. Roy, P. Patel, "A Hybrid Clustered Approach for Enhanced Communication and Model Performance in Blockchain-Based Collaborative Learning," *IEEE Access*, 2024. DOI: 10.1109/ACCESS.2024.3359272.
- [5] H. Wu, S. Zhou, "A Hybrid Security Framework for Web Applications Using Blockchain and Adaptive Adversarial Learning," *Journal of Web Engineering*, vol. 24, no. 3, pp. 839–856, 2025. DOI: 10.13052/jwe1540-9589.2432.
- [6] A. K. Al Hwaitat *et al.*, "A New Blockchain-Based Authentication Framework for Secure IoT Networks," *Electronics (Switzerland)*, vol. 12, no. 17, p. 3618, 2023. DOI: 10.3390/electronics12173618.
- [7] K. C. Chagant, "A Scalable, Lightweight AI-Driven Security Framework for IoT Ecosystems: Optimization and Game Theory Approaches," *IEEE Access*, 2025. DOI: 10.1109/ACCESS.2025.3558623.
- [8] J. Oh, M. Kim, Y. Park, Y. Park, "A Secure Content Trading for Cross-Platform in the Metaverse With Blockchain and Searchable Encryption," *IEEE Access*, vol. 11, pp. 119561–119572, 2023. DOI: 10.1109/ACCESS.2023.3328232.
- [9] A. Ali *et al.*, "An Effective Blockchain Based Secure Searchable Encryption System," *Intelligent Automation and Soft Computing*, vol. 34, no. 1, pp. 294–309, 2022. DOI: 10.32604/iasc.2022.023930.
- [10] K. Neppolian, M. R. Kumar, "Applying Public Key Cryptography to Enhance Content Protection in Maritime Logistics and E-Commerce," *Journal of Internet Services and Information Security*, 2025. DOI: 10.58346/JISIS.2025.12.007.
- [11] N. C. K. Yiu, "Article toward blockchain-enabled supply chain anti-counterfeiting and traceability," *Future Internet*, vol. 13, no. 4, p. 86, 2021. DOI: 10.3390/fi13040086.
- [12] Z. Hameed, H. R. Barzegar, N. El Ioini, C. Pahl, "BE-DSN: leveraging blockchain for improving data availability and security in distributed storage networks," *Cluster Computing*, 2025. DOI: 10.1007/s10586-024-05083-1.
- [13] G. Jin *et al.*, "BeHarmony: Blockchain-Enabled Trustworthy Communication and Legitimate Decision Making in Multi-Party Internet

- of Vehicles Systems," *Electronics (Switzerland)*, vol. 13, no. 16, p. 3219, 2024. DOI: 10.3390/electronics13163219.
- [14] M. Madine *et al.*, "Blockchain and NFTs for Time-Bound Access and Monetization of Private Data," *IEEE Access*, vol. 10, pp. 95346–95361, 2022. DOI: 10.1109/ACCESS.2022.3204274.
 - [15] M. M. M. Al Moti *et al.*, "Blockchain Based Smart-Grid Stackelberg Model for Electricity Trading and Price Forecasting Using Reinforcement Learning," *Applied Sciences (Switzerland)*, vol. 12, no. 10, p. 5144, 2022. DOI: 10.3390/app12105144.
 - [16] H. J. Lee, D. A. Luong, J. H. Park, H. Kim, "Blockchain-Based Anonymous Reputation System for Performance Appraisal," *IEEE Access*, 2025. DOI: 10.1109/ACCESS.2025.3532602.
 - [17] A. Didouh, H. Labiod, Y. E. Hillali, A. Rivenq, "Blockchain-Based Collaborative Certificate Revocation Systems Using Clustering," *IEEE Access*, vol. 10, pp. 27863–27878, 2022. DOI: 10.1109/ACCESS.2022.3160171.
 - [18] A. Sasikumar *et al.*, "BLOCKCHAIN-BASED DECENTRALIZED USER AUTHENTICATION SCHEME FOR LETTER OF GUARANTEE IN FINANCIAL CONTRACT MANAGEMENT," *Malaysian Journal of Computer Science*, pp. 43–64, 2022. DOI: 10.22452/mjcs.sp2022no1.5.
 - [19] M. Alkhatib, T. Albalawi, F. Saeed, "Blockchain-Based Quality Assurance System for Academic Programs," *Applied Sciences (Switzerland)*, vol. 14, no. 11, p. 4868, 2024. DOI: 10.3390/app14114868.
 - [20] A. Ferrer-Rojas, B. T. Maharaj, M. C. Hlophe, "Blockchain-Enhanced Attribute-Based Encryption Architecture With Feasibility Analysis," *IEEE Access*, 2025. DOI: 10.1109/ACCESS.2025.3554643.
 - [21] L. Zhao, B. Li, H. Yuan, "Cloud edge integrated security architecture of new cloud manufacturing system," *Journal of Systems Engineering and Electronics*, vol. 35, no. 3, pp. 605–619, 2024. DOI: 10.23919/JSEE.2024.000112.
 - [22] G. Prabhakar, B. B. Rao, "CULTIVATING RESILIENCE: A TRANSFORMATIVE APPROACH TO ENHANCING CLOUD DATA SECURITY WITH TRANSFORMER-BASED TECHNIQUES," *Proceedings on Engineering Sciences*, vol. 6, no. 4, pp. 297–304, 2024. DOI: 10.24874/PES06.04.014.
 - [23] L. I. N. Zlatolas, T. Welzer-Družovec, L. Lhotska, "Data breaches in healthcare: security mechanisms for attack mitigation," *Cluster Computing*, 2024. DOI: 10.1007/s10586-024-04507-2.
 - [24] H. Ou, C. Pan, Y. Tseng, I. Lin, "Decentralized Identity Authentication Mechanism: Integrating FIDO and Blockchain for Enhanced Security," *Applied Sciences (Switzerland)*, vol. 14, no. 9, p. 3551, 2024. DOI: 10.3390/app14093551.
 - [25] I. C. Cosmin-Julian, I. Adrian, "Decentralized Infrastructure for Digital Notarizing, Signing, and Sharing Documents Securely Using Microservices and Blockchain," *IEEE Access*, 2024. DOI: 10.1109/ACCESS.2024.3518977.
 - [26] G. A. K. Warmayana, Y. Yamashita, N. Oka, "Decentralized Materials Data Management using Blockchain, Non-Fungible Tokens, and Interplanetary File System in Web3," *Journal of Applied Data Sciences*, vol. 6, no. 1, 2025. DOI: 10.47738/jads.v6i1.380.
 - [27] U. Meena, P. Sharma, "Deep Learning Based Secure Routing in WSN Using Hyper Ledger Fabric Block Chain Model," *Concurrency and Computation: Practice and Experience*, 2025. DOI: 10.1002/cpe.70173.
 - [28] M. S. Choi, J. Um, S. S. Lee, "Development of a Customized Blockchain Technology-Based Parameter Matching Protocol for Semiconductor Manufacturing," *IEEE Access*, vol. 12, pp. 84920–84931, 2024. DOI: 10.1109/ACCESS.2024.3411388.
 - [29] M. Y. Shakor *et al.*, "Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security," *IEEE Access*, 2024. DOI: 10.1109/ACCESS.2024.3351119.
 - [30] R. R. Irshad *et al.*, "Enhancing Cloud-Based Inventory Management: A Hybrid Blockchain Approach With Generative Adversarial Network and Elliptic Curve Diffie Helman Techniques," *IEEE Access*, 2024. DOI: 10.1109/ACCESS.2024.3367445.
 - [31] A. A. Mawgoud *et al.*, "Enhancing Data Privacy and Trust in E-Learning: A Blockchain-Based Access Control Protocol for Cloud Educational Systems," *Concurrency and Computation: Practice and Experience*, 2025. DOI: 10.1002/cpe.70185.
 - [32] M. Alown, M. S. Kiraz, M. A. Bingo, "Enhancing Democratic Processes: A Survey of DRE, Internet, and Blockchain in Electronic Voting Systems," *IEEE Access*, 2025. DOI: 10.1109/ACCESS.2025.3531349.
 - [33] S. Sriram *et al.*, "Enhancing Digital Identity and Access Control in Event Management Systems Using Sui Blockchain," *IEEE Access*, 2025. DOI: 10.1109/ACCESS.2025.3539107.
 - [34] Y. Bobde *et al.*, "Enhancing Industrial IoT Network Security through Blockchain Integration," *Electronics (Switzerland)*, vol. 13, no. 4, p. 687, 2024. DOI: 10.3390/electronics13040687.
 - [35] D. Mao *et al.*, "EPPed: Achieving Optimal Balance between Privacy and Efficiency in Federated Learning," *Electronics (Switzerland)*, vol. 13, no. 6, p. 1028, 2024. DOI: 10.3390/electronics13061028.
 - [36] M. Alshaikhli, T. Elfouly, O. Elharrouss, A. Mohamed, N. Ottakath, "Evolution of Internet of Things from Blockchain to IOTA: A Survey," *IEEE Access*, vol. 10, pp. 4950–4969, 2022. DOI: 10.1109/ACCESS.2021.3138353.
 - [37] D. Na, S. Park, "Fusion chain: A decentralized lightweight blockchain for iot security and privacy," *Electronics (Switzerland)*, vol. 10, no. 4, p. 391, 2021. DOI: 10.3390/electronics10040391.
 - [38] F. Naguji *et al.*, "GreenLand: A Secure Land Registration Scheme for Blockchain and AI-Enabled Agriculture Industry 5.0," *IEEE Access*, 2024. DOI: 10.1109/ACCESS.2024.3451627.
 - [39] K. M. Perera, K. Ko, J. Seo, I. Byun, "Hybrid Quantum-Safe Cryptographic Scheme With Secure Key Exchange and Signature Scheme," *IEEE Access*, 2025. DOI: 10.1109/ACCESS.2025.3600068.
 - [40] R. H. Razzaq, M. Al-Zubaidie, R. G. Atiyah, "Intermediary Decentralized Computing and Private Blockchain Mechanisms for Privacy Preservation in the Internet of Medical Things," *Mesopotamian Journal of CyberSecurity*, vol. 2024, no. 2, pp. 29–39, 2024. DOI: 10.58496/MJCS/2024/020.
 - [41] M. Maroufi, R. Abdolee, B. M. Tazekand, S. Amirmortazavi, "Lightweight Blockchain-Based Architecture for 5G Enabled IoT," *IEEE Access*, vol. 11, pp. 58348–58359, 2023. DOI: 10.1109/ACCESS.2023.3284471.
 - [42] K. C. Bandhu *et al.*, "Making drug supply chain secure traceable and efficient: a Blockchain and smart contract based implementation," *Multimedia Tools and Applications*, vol. 82, no. 2, pp. 2689–2707, 2023. DOI: 10.1007/s11042-022-14238-4.
 - [43] H. Alamro *et al.*, "Mathematical modelling-based blockchain with attention deep learning model for cybersecurity in IoT-consumer electronics," *Alexandria Engineering Journal*, 2025. DOI: 10.1016/j.aej.2024.11.016.
 - [44] X. Y. Sia, A. Abdollah, N. A. A. Majid, M. S. Razali, "Medical Records System with Blockchain (Health Chain)," *Journal of Advanced Research Design*, vol. 123, no. 1, pp. 108–130, 2024. DOI: 10.37934/ard.123.1.108130.
 - [45] W. Villegas-Ch *et al.*, "Optimizing Security in IoT Ecosystems Using Hybrid Artificial Intelligence and Blockchain Models: A Scalable and Efficient Approach for Threat Detection," *IEEE Access*, 2025. DOI: 10.1109/ACCESS.2025.3532800.
 - [46] L. S. Ochôa *et al.*, "Performance and security evaluation on a blockchain architecture for license plate recognition systems," *Applied Sciences (Switzerland)*, vol. 11, no. 3, p. 1255, 2021. DOI: 10.3390/app11031255.
 - [47] A. Odeh, E. Abdelfattah, W. Salameh, "Privacy-Preserving Data Sharing in Telehealth Services," *Applied Sciences (Switzerland)*, vol. 14, no. 23, p. 10808, 2024. DOI: 10.3390/app142310808.
 - [48] D. Doha, P. Guo, W. Liang, "Privacy-Preserving Strategies in the Internet of Medical Things Using Reinforcement Learning and Blockchain," *Intelligent Computing*, 2025. DOI: 10.34133/icomputing.0133.
 - [49] J. Hu, K. Huang, G. Bian, Y. Cui, "Redact-Chain for Health: A Scheme Based on Redactable Blockchain for Managing Shared Healthcare Data," *Electronics (Switzerland)*, vol. 12, no. 20, p. 4240, 2023. DOI: 10.3390/electronics12204240.
 - [50] R. A. Alsemmeiri *et al.*, "Resilient Security Framework Using TNN and Blockchain for IoMT," *Electronics (Switzerland)*, vol. 12, no. 10, p. 2252, 2023. DOI: 10.3390/electronics12102252.
 - [51] H. S. Phil, "Revolutionizing Internet of Vehicles with Quantum Key Distribution on Blockchain for Unprecedented Security," *Journal of*

- Machine and Computing*, vol. 5, no. 3, pp. 582–593, 2025. DOI: 10.53759/7669/jmc202505039.
- [52] M. Asiri *et al.*, "RPFL: A Reliable and Privacy-Preserving Framework for Federated Learning-Based IoT Malware Detection," *Electronics (Switzerland)*, vol. 14, no. 6, p. 1089, 2025. DOI: 10.3390/electronics14061089.
- [53] S. Fugkeaw, R. P. Gupta, K. Worapaluk, "Secure and Fine-Grained Access Control With Optimized Revocation for Outsourced IoT EHRs With Adaptive Load-Sharing in Fog-Assisted Cloud Environment," *IEEE Access*, vol. 12, pp. 88362–88379, 2024. DOI: 10.1109/ACCESS.2024.3412754.
- [54] S. A. Bragadeesh, A. Umamakeswar, "Secured vehicle life cycle tracking using blockchain and smart contract," *Computer Systems Science and Engineering*, vol. 43, no. 1, pp. 325–340, 2022. DOI: 10.32604/csse.2022.019842.
- [55] J. H. Markani, A. Amrhar, J. Gagné, R. Jr Landry, "Security Establishment in ADS-B by Format-Preserving Encryption and Blockchain Schemes," *Applied Sciences (Switzerland)*, vol. 13, no. 5, p. 3105, 2023. DOI: 10.3390/app13053105.
- [56] A. Ali *et al.*, "Security, privacy, and reliability in digital healthcare systems using blockchain," *Electronics (Switzerland)*, vol. 10, no. 16, p. 2034, 2021. DOI: 10.3390/electronics10162034.
- [57] A. Falayi, Q. Wang, W. Liao, W. Yu, "Survey of Distributed and Decentralized IoT Securities: Approaches Using Deep Learning and Blockchain Technology," *Future Internet*, vol. 15, no. 5, p. 178, 2023. DOI: 10.3390/fi15050178.
- [58] X. Yu, W. Meng, Y. Liu, F. Zhou, "TridentShell: An enhanced covert and scalable backdoor injection attack on web applications," *Journal of Network and Computer Applications*, vol. 226, p. 103823, 2024. DOI: 10.1016/j.jnca.2023.103823.
- [59] H. Ali *et al.*, "TrustShare: Secure and Trusted Blockchain Framework for Threat Intelligence Sharing," *Future Internet*, vol. 17, no. 7, p. 289, 2025. DOI: 10.3390/fi17070289.
- [60] H. R. Hasan *et al.*, "Trustworthy IoT Data Streaming Using Blockchain and IPFS," *IEEE Access*, vol. 10, pp. 29636–29649, 2022. DOI: 10.1109/ACCESS.2022.3149312.
- [61] B. K. Kalejahi, R. Eminov, A. Guliyev, "Using blockchain technology in mobile network to create decentralized home location registry (HLR)," *Computer Systems Science and Engineering*, vol. 37, no. 1, pp. 101–114, 2021. DOI: 10.32604/csse.2021.05480.
- [62] E. Leka, L. Lamani, A. Aliti, E. Hoxha, "Web Application Firewall for Detecting and Mitigation of Based DDoS Attacks Using Machine Learning and Blockchain," *TEM Journal*, vol. 13, no. 4, pp. 2252–2261, 2024. DOI: 10.18421/TEM134-17