REVISTA MULTIDISCIPLINARIA
DESARROLLO AGROPECUARIO, TECNOLOGICO, EMPRESARIAL Y HUMANISTA
UNIVERSIDAD TECNICA DE COTOPAXI - LA MANA. COTOPAXI. ECUADOR
ISSN: 2773-7527

Volumen 7. No. 2

Diciembre 2025

Blockchain para Mejorar la Seguridad y el Acceso Confiable a Datos: Aplicaciones en la Protección de Información

Blockchain to Improve Security and Reliable Data Access: Applications in Information Protection

Joseph Luis Rodríguez Bermudez[1], Kevin Paul Rivas Verástegui[1], Alberto Carlos Mendoza de los Santos[1]

[1]Universidad Nacional de Trujillo, Trujillo – Perú

Correo de correspondencia: jrodriguezbe@unitru.edu.pe

Información del artículo

Tipo de artículo:
Artículo original

Recibido:
11/08/2025

Aceptado:
06/11/2025

Publicado:
10/12/2025

Revista:
DATEH

Resumen

El presente trabajo analizó el uso de la tecnología blockchain para mejorar la seguridad y garantizar el acceso confiable a datos en sistemas digitales. Se investigó blockchain en la protección de datos, enfocado en su uso para reforzar la seguridad en entornos distribuidos. Las principales aplicaciones de blockchain consideradas fueron sistemas de votación electrónicos seguros, sistemas de IoT (en las revisiones analizadas existieron más redes inteligentes) y marcos para el trabajo con esta tecnología. La investigación empleó una revisión sistemática de la literatura utilizando la metodología PRISMA, con el objetivo de evaluar las ventajas, desafíos y oportunidades que presenta blockchain en la protección de la información. Los resultados obtenidos demostraron que blockchain, al ser una tecnología descentralizada e inmutable, ofrece una solución eficiente para mejorar la integridad y transparencia de los datos, reduciendo riesgos asociados a vulnerabilidades en sistemas tradicionales. Además, se identificaron soluciones criptográficas avanzadas, como la combinación de los algoritmos AES y RSA con blockchain, o los cifrados homomórficos que mejoran el funcionamiento en términos de privacidad y seguridad de los datos. A pesar de los beneficios, se destacaron desafíos en términos de escalabilidad y eficiencia cuando se aplica blockchain a sistemas con grandes volúmenes de transacciones. . En conclusión, blockchain es una herramienta poderosa para mejorar la protección de datos, pero su implementación a gran escala aún requiere optimizaciones tecnológicas adicionales.

Palabras clave: *blockchain, protección de datos, seguridad digital, contratos inteligentes, acceso confiable a datos*

Abstract

This study analyzed the use of blockchain technology to improve security and ensure reliable access to data in digital systems. Blockchain was investigated in data protection, particularly in reinforcing security in distributed environments. The main blockchain applications considered were secure electronic voting systems, IoT systems (in the reviews analyzed there were more smart grids), and frameworks for working with this technology... A systematic literature review was conducted using the PRISMA methodology to evaluate the advantages, challenges, and opportunities that blockchain presents in protecting information. The findings demonstrated that blockchain, as a decentralized and immutable technology, provides an efficient solution to enhance data integrity and transparency, reducing risks associated with vulnerabilities in traditional systems. Additionally, advanced cryptographic solutions, such as combining AES and RSA algorithms with blockchain, or homomorphic ciphers thatimprove operation in terms of privacy and data security. Despite the benefits, challenges in scalability and efficiency were highlighted when applying blockchain to systems with large transaction volumes. In conclusion, blockchain is a powerful tool to enhance data protection, but its large-scale implementation still requires further technological optimizations.

Keywords: *blockchain, data protection, digital security, smart contracts, reliable data access*

INTRODUCCIÓN

La seguridad de los datos y la protección de la información se han convertido en retos esenciales en el mundo digital actual. Con el crecimiento exponencial de las transacciones electrónicas y el aumento de los ciberataques, las amenazas como la manipulación de datos y los ataques a la privacidad han generado serias preocupaciones sobre la integridad y confidencialidad de

ISSN: 2773-7527
Volumen 7. No. 2
Diciembre 2025

la información. La digitalización masiva de servicios ha multiplicado los riesgos de exposición de datos sensibles, lo que pone en evidencia la necesidad urgente de soluciones que garanticen la seguridad de la información y la confianza en los sistemas. En este contexto, las tecnologías emergentes, como blockchain, se presentan como soluciones efectivas para mejorar la seguridad, la transparencia y la inmutabilidad de los datos. Blockchain, al ser una tecnología descentralizada, garantiza la integridad de la información mediante registros inalterables, lo que la convierte en una herramienta clave para mitigar los riesgos asociados con los sistemas tradicionales de almacenamiento y procesamiento de datos.

Blockchain ofrece varias ventajas sobre los sistemas centralizados, principalmente la capacidad de distribuir el control y la responsabilidad entre múltiples participantes, eliminando así los puntos de fallo centralizados. Esta descentralización no solo mejora la resiliencia del sistema, sino que también asegura la transparencia y auditabilidad de las operaciones realizadas dentro de la red. En particular, la aplicación de blockchain en áreas críticas como las votaciones electrónicas, la gestión de redes inteligentes y el acceso controlado a datos personales ha demostrado ser prometedora. La votación electrónica, por ejemplo, se ha beneficiado de las características de blockchain, ya que según Wahab et al. (2022) puede establecer la transparencia del proceso electoral, garantizar el recuento y evitar la duplicación de votos.

Además, la integración de blockchain con algoritmos criptográficos avanzados, como AES (Advanced Encryption Standard) y RSA, optimiza el procesamiento de grandes volúmenes de datos sin comprometer la seguridad. Estos algoritmos permiten cifrar los datos de manera eficiente, asegurando que solo las partes autorizadas puedan acceder a ellos. Esta combinación de tecnologías es crucial en sistemas con alta demanda de procesamiento de datos, como las elecciones nacionales, donde la velocidad y la seguridad del procesamiento de votos deben ser garantizadas para mantener la integridad del sistema como se aborda en la propuesta de Vinayachandra y Krishna Prasad (2025). Blockchain también se destaca por su capacidad para permitir el almacenamiento de datos de forma distribuida y segura, lo cual es esencial para sistemas como las redes inteligentes, que requieren una transmisión constante de datos en tiempo real.

A pesar de las ventajas prometedoras de blockchain, su implementación a gran escala presenta desafíos significativos. La escalabilidad y la eficiencia de los sistemas basados en blockchain siguen siendo dos de los mayores obstáculos para su adopción, especialmente en sistemas que requieren una alta tasa de transacciones, como los utilizados en votaciones electrónicas y redes inteligentes. La tecnología blockchain, si bien robusta en términos de seguridad, enfrenta limitaciones en términos de velocidad de procesamiento y costos asociados con el mantenimiento de su infraestructura descentralizada. Según Ohize et al. (2024), aunque blockchain mejora la integridad de los datos, aún existen problemas técnicos que deben ser resueltos para asegurar su desempeño en entornos críticos, de alta demanda y en tiempo real. La necesidad de mejorar los algoritmos de consenso y optimizar la infraestructura es esencial para hacer que blockchain sea más viable a gran escala, especialmente en sistemas que manejan grandes volúmenes de transacciones.

La pregunta central de esta investigación es: ¿Cómo influye la tecnología blockchain, combinada con algoritmos criptográficos avanzados, en la mejora de la ciberseguridad, la confiabilidad y la eficiencia de los sistemas que gestionan datos sensibles, especialmente en la votación electrónica y la gestión de redes inteligentes?

Para abordar esta pregunta de investigación, se plantean los siguientes objetivos específicos:

1. Analizar cómo blockchain y criptografía mejoran la ciberseguridad en sistemas críticos
2. Evaluar cómo blockchain y la criptografía mejoran la efectividad y confiabilidad en sistemas críticos
3. Explorar cómo el uso de blockchain y la criptografía mejora la automatización y control de datos.
4. Identificar los desafíos técnicos y económicos asociados con la implementación de blockchain y la criptografía a gran escala.

Nuestra hipótesis es que la tecnología blockchain, combinada con algoritmos criptográficos avanzados influirá de manera positiva brindando más seguridad, conservando la integridad de los datos, manteniendo un funcionamiento óptimo, aunque con retos de implementación para los sistemas críticos.

MATERIALES Y MÉTODOS

Como ya se ha dicho, la presente investigación es una revisión sistemática sobre la bibliografía existente que aborda el blockchain y su aplicación en la seguridad de la información en diferentes contextos. Para ello se hizo uso de la metodología PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), qué es ampliamente utilizada para garantizar rigurosidad en el análisis de la bibliografía. Su propósito es garantizar una

documentación transparente del motivo de la revisión, que se hizo y que se encontró (Page et al., 2021). La investigación se realizó a través de internet, consultando artículos y trabajos de investigación.

Para el desarrollo de este artículo se necesitó acceso a internet. Por supuesto el instrumento utilizado en la metodología PRISMA es el análisis documental.

Ecuaciones de búsqueda

El primer paso fue seleccionar las bases de datos a utilizar, ya que se requiere investigar trabajos que cumplan con un estándar de calidad. Por ello se eligió a Scopus y Scielo como plataformas en las cuales buscar.

Para realizar el proceso de búsqueda se utilizaron palabras clave y las funciones de búsqueda avanzada de las plataformas, las cuales se pueden representar como cadenas de texto plasmadas en la Tabla 1. Esto también asegura que la investigación pueda ser replicada y se entienda el proceso por el cual se llegó a los resultados, por supuesto, considerando que habrá cambios temporales o en los motores de búsqueda de las plataformas.

Tabla 1
Cadenas de búsqueda ingresadas en los repositorios.

Repositorio	Criterios de inclusión
Scopus	"blockchain AND (cryptograp* OR encrypt*) AND system* AND secur* AND (electronic voting OR e-voting OR intelligent OR (smart contract))"
Scielo	"((blockchain) OR (cadena de bloques)) AND ((tecno-lo-gias de la informacion) OR (ti) OR (tic))"

Criterios de inclusión y exclusión.

Lo siguiente que se hizo fue formular los criterios de inclusión y de exclusión las cuales son pautas específicas que nos permiten guiarnos para la selección de los trabajos de investigación. Los criterios de inclusión permiten determinar qué trabajos se incluirán en el análisis, se tiene que cumplir con todos ellos.

Tabla 2
Criterios de inclusión.

N°	Criterios de inclusión
CI1	Artículos que tienen el blockchain y su impacto en la seguridad de diferentes sistemas como tema
CI2	Artículos del top 20 relevantes de las bases de datos que reflejen los resultados de implementar la tecnología blockchain
CI3	Artículos en español e inglés
CI4	Artículos publicados entre los años 2020 y 2025

Los criterios de exclusión a su vez filtraron los resultados preliminares, descartaron del análisis aquellos que caigan en alguno de estos conceptos relacionados con tiempo, contexto, temática, forma, etc.

Tabla 3
Criterios de exclusión.

N°	Criterios de exclusión
CE1	Artículos no publicados entre los años 2020 y 2025
CE2	Artículos que no son finales y de libre acceso
CE3	Artículos sin el keyword ya sea de autor o de indexación blockchain
CE4	Documentos que no tienen relación con el tema central de investigación y duplicados

Proceso de recolección de información

Al final del proceso de filtrado se estableció que colse debía trabajar con 23 investigaciones. Los cuales cumplen con los criterios de inclusión y exclusión.

Algunos de ellos hablan de la implementación del blockchain para mejora de seguridad, otros proponen un modelo de software, y otros revisan las tendencias y soluciones en este campo.

En la Figura 1 se tiene un mapa echo en el software VOSviewer, utilizado para hacer Scoping Review, que representa la relación entre las palabras clave de los artículos antes de ser filtrado para un panorama amplio. Se utilizo número minimo de ocurrencias en 30, Se puede notar que todos los conceptos tienen alta relación entre sí, por lo que parece que el tema toca diferentes áreas a la vez.

REVISTA MULTIDISCIPLINARIA
DESARROLLO AGROPECUARIO, TECNOLOGICO, EMPRESARIAL Y HUMANISTA
UNIVERSIDAD TECNICA DE COTOPAXI - LA MANA. COTOPAXI. ECUADOR
ISSN: 2773-7527
Volumen 7. No. 2
Diciembre 2025

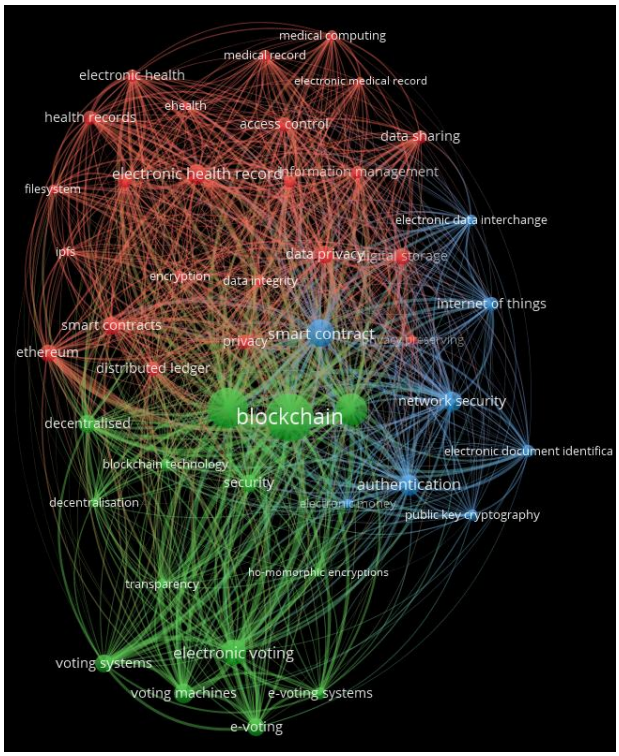

Figura 1. *Mapa de palabras clave de los artículos preseleccionados*

En la Figura 2 se tiene un resumen del proceso de la metodología PRISMA que se ha seguido hasta ahora. Reconociendo que plasma la idea detrás de la revisión sistemática, que según Morales (2022) es minimizar el riesgo de sesgo en el proceso de revisión, y por eso es importante que el protocolo previo sea detallado. Con las investigaciones ya definidas, se pasó a un análisis más exhaustivo de donde se sacaron los hallazgos más importantes y las conclusiones a las que estas llegaron.

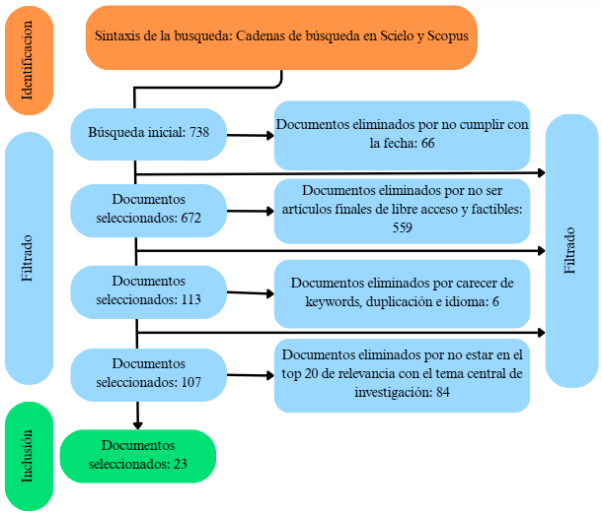

Figura 2. *Diagrama de flujo PRISMA aplicado a este artículo*

Cabe destacar que los criterios no siempre corresponden a los filtros de las bases de datos. Por ejemplo, como parte de la investigación se comprobó el estado de los artículos, y aún con los filtros de las plataformas puestos hubo uno en Scielo (no cargaba siempre) y dos del top 20 de relevancia en Scopus (uno no era disponible sin registrarse vía institución y otro no tenía el DOI correcto) que no fueron seleccionados. A continuación, en la Figura 3. Un mapa en VOSviewer ahora con los artículos resultantes del proceso de selección. Siendo de apoyo en nuestra afirmación de que los criterios y métodos utilizados nos han llevado a trabajos que se adecúan correctamente para ser trabajados en este artículo. Dándonos así una idea de la dirección a la que se inclina el campo. Se utilizo número mínimo de ocurrencias en 3. Donde se puede diferenciar dos *clusters*, uno sobre las votaciones electrónicas y otro sobre la tecnología utilizada.

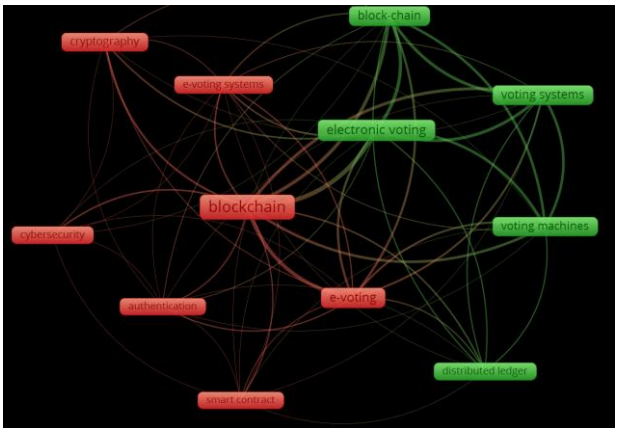

Figura 3. *Mapa de palabras clave de los artículos seleccionados*

RESULTADOS Y DISCUSIÓN

Los resultados del análisis de los 23 artículos seleccionados se presentan a continuación, donde se destacan los principales aportes de cada estudio y su mejora de acuerdo con los objetivos de investigación. A través de una evaluación sistemática, se ha identificado cómo la tecnología blockchain, combinada con algoritmos criptográficos avanzados, mejora la seguridad y confiabilidad de sistemas críticos como la votación electrónica y la gestión de redes inteligentes. En este análisis, se ha considerado la protección de los datos y la ciberseguridad, así como los desafíos asociados con la implementación de blockchain. Los hallazgos reflejan las ventajas de blockchain en términos de integridad de los datos, transparencia y auditoría descentralizada, aunque también se identificaron áreas donde se deben realizar mejoras, particularmente en la escalabilidad y eficiencia.

Tabla 4
Principal producto, y mejora o desafío en la que concluyen los artículos.

Estudio	Principal Producto	Mejora/Desafio
(Wahab et al., 2022)	Framework	Seguridad, Transparencia, Economía, Participación
(Anwar Ul Hassan et al., 2022)	Sistema	Rapidez, Economía, Seguridad, Transparencia, Legalidad, Escalabilidad, Participación
(Taş & Tanriöver, 2021)	Sistema	Transparencia, Seguridad, Privacidad, Escalabilidad
(Mullegowda et al., 2024)	Sistema	Seguridad, Rapidez, Economía, Escalabilidad
(González-Puetate et al., 2022)	Revisión	Economía, Rapidez, Transparencia, Adaptación
(Llanten-Lucio, et al., 2022a)	Framework	Seguridad, Adaptación, Escalabilidad
(Vinayachandra y K, 2025)	Sistema	Privacidad, Seguridad, Rapidez, Participación, Escalabilidad, Adaptación
(Ohize et al., 2024)	Revisión	Seguridad, Transparencia, Escalabilidad, Adaptación, Futuro
(Sharp et al., 2024)	Revisión, Sistema	Seguridad, Privacidad, Transparencia, Futuro
(Daraghmi et al., 2024)	Sistema	Seguridad, Privacidad, Transparencia, Escalabilidad, Futuro, Adaptación
(Majumder et al., 2024)	Sistema	Seguridad, Privacidad, Economía
(Alown et al., 2025)	Revisión	Futuro, Escalabilidad, Privacidad
(Singh et al., 2024)	Revisión	Escalabilidad, Legal, Privacidad, Adaptación
(Almeida et al., 2023)	Revisión	Adaptación, Escalabilidad
(Wang et al., 2024)	Sistema	Privacidad, Transparencia, Seguridad
(Umar et al., 2022)	Sistema	Seguridad, Privacidad
(Sallal et al., 2023)	Sistema	Privacidad, Transparencia, Seguridad, Escalabilidad
(Mohanaprakash et al., 2024)	Sistema	Seguridad, Transparencia, Rapidez
(Chentouf & Bouchkaren, 2023)	Sistema	Seguridad, Transparencia
(Salman et al., 2023)	Sistema	Seguridad, Privacidad
(Jaramillo & Piedra, 2021)	Framework	Transparencia, Seguridad, Adaptación
(Olivares-Rojas et al., 2023)	Sistema	Seguridad, Futuro, Adaptación
(Llanten-Lucio et al., 2022b)	Framework	Escalabilidad, Adaptación

Las mejoras y desafíos se estudiaron de las conclusiones. En los sistemas, se priorizaron sus aportes y no la parte teórica. Se consideraron conclusiones principales y no solo menciones.

Para comprender mejor la Tabla 4, se dan las siguientes aclaraciones: La economía prácticamente se refiere a la mejora en cuanto a gastos con propuestas anteriores. De similar forma la rapidez.

Con futuro se entiende a la tecnología y mirada a desafíos y oportunidades. Con adaptación se muestra lo que se podría hacer en el presente para que esto salga del laboratorio y diversas aplicaciones.

Que un estudio tenga pocos ítems en la tabla no significa que fue insuficiente. Por ejemplo, Almeida et al., 2023 concluyen con la necesidad de adaptación y escalabilidad, pero lo hacen de manera profunda y completa de acuerdo con todos sus artículos revisados.
La escalabilidad es el desafió que presentan muchos de los sistemas analizados, aunque por ejemplo Sallal et al. (2024) se atreven a concluir que su sistema si es escalable de acuerdo con los resultados iniciales.

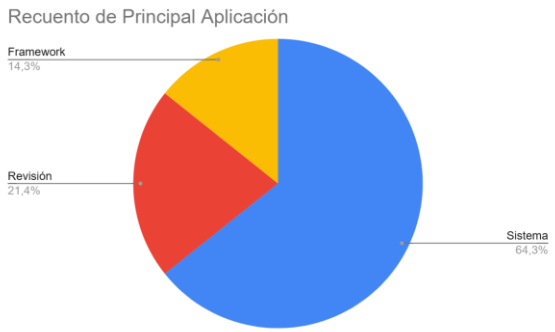

Figura 4. *Resumen del principal producto en los estudios revisados.*

Análisis de la mejora de la ciberseguridad en sistemas críticos con blockchain y algoritmos criptográficos

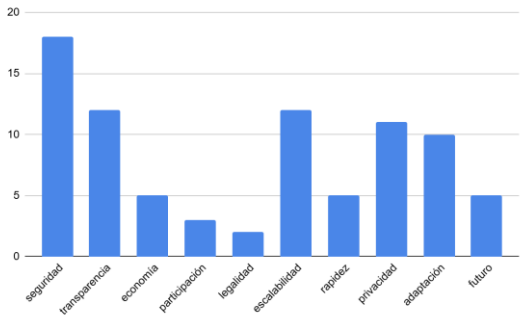

Figura 5. *Gráfico de barras con las principales conclusiones de mejoras o desafíos en los estudios revisados.*

Los estudios revisados muestran que la combinación de blockchain y algoritmos criptográficos avanzados mejora sustancialmente la ciberseguridad y la protección de datos en sistemas críticos, como votación electrónica y gestión de redes inteligentes. La mejora en seguridad es la que más presente está en las conclusiones de los artículos. La inmutabilidad de blockchain, combinada con criptografía de clave pública/privada y funciones hash, crea registros de datos inalterables, lo que aumenta la seguridad de los sistemas frente a manipulaciones o ataques. Este enfoque es particularmente valioso en entornos donde los datos son extremadamente sensibles, como los sistemas de votación electrónica.

Por ejemplo, el estudio realizado por Vinayachandra y Krishna Prasad (2025), en el que se consideró diferentes implementaciones de blockchain para votación electrónica, propuso que la criptografía avanzada, como AES y RSA, es una gran alternativa para proteger los datos durante la transmisión y el almacenamiento. El uso de firmas digitales y mecanismos de consenso distribuido proporciona una capa adicional de seguridad, eliminando el riesgo de un punto único de fallo. Según Ohize et al. (2024), este tipo de blockchain permite verificar las transacciones de manera descentralizada, lo que aumenta la confianza del usuario en el sistema.

Pero para aumentar la seguridad no solo necesitamos la tecnología sino la forma de aplicarla. Los marcos para desarrollar proyectos son de gran ayuda. Así lo constató Llanten-Lucio et al. (2022a) que propusieron un marco basado en estas tecnologías para la mitigación de amenazas cibernéticas. Concluyen con los desafíos que implica una red blockchain y su aplicación en ambientes reales.

Tabla 5
Ejemplos de características de seguridad implementada

Estudio	Sistema Analizado	Características de seguridad implementados
Vinayachandra y Krishna Prasad (2025)	Sistema de votación electrónica	Integración de AES y RSA, procesamiento eficiente de datos
Ohize et al. (2025)	Sistema de votación electrónica	Contratos inteligenres, monedas de voto, cadenas laterales

Evaluación de blockchain y la criptografía para mejorar la efectividad y confiabilidad en sistemas críticos

En este estudio identificamos que la implementación de tecnología blockchain no solo beneficia a los sistemas, sino que también impacta positivamente en los usuarios. Puesto que hay un antes y después notable en el tratamiento y vulnerabilidad de sus datos. Por ello la transparencia y privacidad son de los más mencionados en los artículos. Sin embargo, solo 5 concluyen principalmente sobre economía. Y solo tres sobre el aumento de la participación gracias a los avances en blockchain.

Como evidencias textuales tenemos que Vinayachandra y Krishna Prasad (2025) concluyen que su sistema de votación puede mejorar la participación de los votantes, puesto que un sistema encriptado híbrido y descentralizado es más confiable. El estudio de Taş y Tanriöver (2021) presenta una alternativa a los problemas de manipulación de resultados. Y como resultado está su modelo de seguridad de doble capa que utiliza blockchain y cifrado homomórfico, garantizando así un control de acceso confiable. El objetivo principal del trabajo de Jaramillo y Piedra (2021) fue mejorar la trazabilidad y confianza en el intercambio de información de instituciones superiores. Proponiendo apps descentralizadas (DApps) y demostrando en dos casos de aplicación el beneficio de estas para que los datos sean rastreables y seguros.

Vinayachandra y Krishna Prasad (2025) detallan que la combinación de los algoritmos AES (Advanced Encryption Standard) y RSA con blockchain proporciona una capa adicional de seguridad en el sistema de votación, donde la encriptación asegura la privacidad de los votos mientras que blockchain garantiza su integridad. Y nos lo muestran en la Figura 3. Que solo es un ejemplo de los muchos diagramas representativos de los sistemas en los estudios analizados. Este enfoque permite que el proceso electoral sea transparente, ya que los votos registrados en blockchain son accesibles y verificables para todas las partes interesadas, incluidas las autoridades electorales y los votantes, sin comprometer la

privacidad del votante (Vinayachandra & Krishna Prasad, 2025).

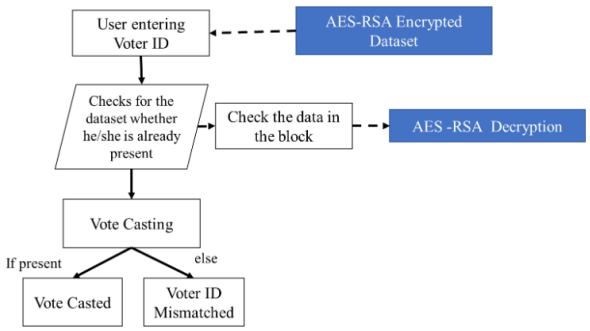

Figura 6. *Proceso general del mecanismo de votación segura*. Tomado de *Vinayachandra y Krishna Prasad (2025)*

En cuanto a la prevención de fraudes, varios estudios resaltan cómo blockchain puede evitar prácticas como el doble voto o la alteración de los resultados. Ohize et al. (2024) evidencian que las tecnologías de descentralización de blockchain permiten obtener los resultados de manera segura y reduciendo el peligro de manipulación. Además, la implementación de blockchain contribuye a la confiabilidad del sistema electoral, ya que la tecnología asegura que el sistema esté disponible de manera continua, sin depender de un único servidor centralizado susceptible a ataques.

Pero la efectividad también se constata en las aplicaciones que tiene en las diferentes industrias. Gonzales-Puetate et al. (2022) en su trabajo de investigación analizó las aplicaciones de la tecnología blockchain en la industria agroalimentaria. Encontraron que su uso se repartía en trazabilidad 26%, cadena de suministro 17.5%, desarrollo tecnológico 10.4%, confianza 9.8%, entre otros. Concluyen que la alta relación con la logística se debía a la alta integración de los procesos con los mediante automatización de documentos, sensores e información en tiempo real.

Exploración de blockchain y la criptografía para mejorar la automatización y control de datos.

En cuanto a la automatización no podemos dejar de mirar a los contratos inteligentes. El uso de contratos inteligentes en la tecnología blockchain ha demostrado ser una herramienta clave para mejorar la seguridad y la transparencia en la gestión de datos, especialmente en sistemas críticos como la votación electrónica y la gestión de redes inteligentes. Los contratos inteligentes son programas ejecutables que automatizan la ejecución de contratos bajo condiciones predefinidas, eliminando la necesidad de intermediarios. Este proceso asegura que solo las partes autorizadas tengan acceso a datos específicos, lo que reduce el riesgo de errores humanos y manipulaciones.

En el ámbito de la votación electrónica, los contratos inteligentes pueden asegurar que solo los votantes verificados puedan emitir su voto, cumpliendo con reglas de acceso claras y verificables por todas las partes involucradas. Según Jaramillo y Piedra (2020), el uso de contratos inteligentes es una parte primordial cuando trabajamos con blockchain.

Además, el uso de contratos inteligentes en la gestión de redes inteligentes permite la automatización de acuerdos de acceso a datos en tiempo real. Según Daraghmi et al. (2024), esta tecnología se utiliza para garantizar que solo autorizados tengan acceso a la información y para evitar votos repetidos.

Tabla 6
Ejemplos de aplicaciones de contratos inteligentes en sistemas blockchain

Estudio	Aplicación de Blockchain	Características de contratos inteligentes
Jaramillo & Piedra (2020)	Intercambio de información	Integración en la blockchain
Daraghmi et al. (2023)	Votación electrónica	Control de transacciones, aplicacion de reglas y gestion de datos ya enviados

Pero no es indispensable usar contratos inteligentes para la automatización, la tecnología por sí sola la ofrece en diferentes aplicaciones. Así lo constató Llanten Lucio et al. (2022) que presenta la importancia de la automatización de procesos para muchas empresas, y cómo esta se vuelve más sensible cuando se tratan con datos y ciberseguridad. Para ello se propuso un marco de trabajo que permita guiarse en la implementación de las nuevas tecnologías entre ellas el blockchain y el IoT para la generación automática de reglas y almacenamiento de alertas. Concluye con la importancia y gran oportunidad de incorporar los avances tecnológicos, pero también reconoce los muchos desafíos y percances que pueden surgir de ello.

Identificación de desafíos técnicos y económicos y propuestas de solución

A pesar de las ventajas evidentes de blockchain, su implementación a gran escala enfrenta diversos desafíos técnicos y económicos. En cuanto a los desafíos técnicos, uno de los principales problemas es la escalabilidad de la red. Pocos, como Olivares-Rojas et al. (2023) destacan que sus modelos son escalables y funcionarían sin mayor complicación en el nivel NAN. Para 12 artículos el tema de escalabilidad se volvió una conclusión principal. Esto

ISSN: 2773-7527
Volumen 7. No. 2
Diciembre 2025

se vuelve un desafío particularmente en elecciones nacionales o redes inteligentes que requieren procesar millones de transacciones en tiempo real.

Un problema adicional es la interoperatividad entre diferentes sistemas blockchain. Puesto que se crean diversos marcos y modelos como los análizados aquí. Destacamos a Alown et al. (2025) que dicen asimilar un marco común que da una comprensión integral de las capas en el blockchain para una comparación significativa con otros estudios
En términos económicos, la implementación y mantenimiento de blockchain sigue siendo costosa debido a los requerimientos de infraestructura necesarios para mantener una red descentralizada. Ohize et al. (2023) indican que los costos operativos relacionados con la infraestructura y el consumo de energía en sistemas blockchain pueden ser elevados sobre todo cuando se habla de escalabilidad. Para mitigar estos costos, se observaron soluciones como el uso de algoritmos de consenso más eficientes como Proof of Stake (PoS), que requieren menos recursos computacionales que los algoritmos tradicionales como Proof of Work (PoW).

Tabla 7
Ejemplos de desafíos técnicos y soluciones propuestas en la implementación de blockchain

Desafio tecnico	Estudio relevante	Solucion propuesta
Escalabilidad	Olivares-Rojas et al. (2023)	Implementación de blockchain de múltiples niveles
Interoperabilidad	Alow et al. (2025)	UUtilizar un marco común para entendimiento de las capas blockchain
Consumo Energético	Ohize et al. (2023)	Optimización mediante Proof of Stake (PoS)

Se puede mencionar naciente preocupación por la implementación legislativa como un desafío, el tema legal aparece como una de las principales conclusiones 2 veces.

Los hallazgos obtenidos en esta investigación han permitido responder a la pregunta central sobre cómo la tecnología blockchain, combinada con algoritmos criptográficos avanzados, mejora la ciberseguridad, la confiabilidad y la eficiencia de los sistemas que gestionan datos sensibles, particularmente en la votación electrónica y la gestión de redes inteligentes. En general, los estudios revisados confirmaron que blockchain ofrece una solución robusta para garantizar la seguridad de los datos en entornos críticos. La inmutabilidad de los registros, la transparencia y la auditoría descentralizada son características que contribuyen a una mayor protección de la información, lo que hace que blockchain sea especialmente adecuado para sistemas como el de votación electrónica, donde la integridad y la confianza son esenciales.

Los estudios revisados también subrayan que la combinación de blockchain con algoritmos criptográficos avanzados, como AES y RSA, mejora considerablemente la protección de los datos, tanto en términos de cifrado como de integridad. Este enfoque, utilizado en sistemas de votación electrónica, asegura que los votos sean registrados de manera segura y no puedan ser alterados sin que se detecte, lo que aumenta la confianza del electorado en la transparencia del proceso electoral. Esta mejora de la transparencia y seguridad también se refleja en la gestión de redes inteligentes, donde el uso de blockchain puede garantizar el acceso seguro a los datos en tiempo real, como se mostró en el estudio de Olivares-Rojas et al. (2023).

A pesar de los beneficios prometedores, los resultados de esta investigación también identificaron varios desafíos técnicos y económicos que deben abordarse para lograr una adopción masiva de blockchain en estos sistemas. Uno de los principales desafíos es la escalabilidad de los sistemas basados en blockchain, especialmente cuando se enfrentan a grandes volúmenes de transacciones, como en las elecciones nacionales o en redes inteligentes que requieren procesar datos en tiempo real. Estos problemas los enfrentan diversos sistemas blockchain y también influye en su interoperatividad que hace dificil no sacrificar la eficiencia, según Mullegowda et al. (2024).
Además, otro obstáculo importante es el consumo energético asociado con el uso de mecanismos de consenso como Proof of Work (PoW). Los estudios revisados, como el de Ohize et al. (2023), destacan que los costos operativos y el alto consumo de energía pueden ser una barrera significativa para la adopción de blockchain enescenarios de votación. Se ha propuesto el uso de Proof of Stake (PoS) por ejemplo como una solución más eficiente, que requiere menos recursos computacionales y reduce el impacto ambiental, lo que podría mejorar la viabilidad a largo plazo de blockchain en sistemas de votación electrónica y redes inteligentes.

En cuanto a la interoperabilidad, otro desafío clave mencionado ya en la investigación es la dificultad para integrar diferentes plataformas blockchain en un único sistema. Aunque marcos multicapa comunes que se adopten por la mayoría podrían proporcionar una solución a este problema, la implementación de este tipo de metodologías aún requiere más investigación, especialmente en la creación de estándares que permitan que distintas plataformas blockchain trabajen de manera conjunta. Allow et al. (2025) dicen que hay variaciones de diseño con muchos enfoques y modelos.

Se espera que este estudio contribuya a un mayor entendimiento de cómo blockchain y los algoritmos criptográficos avanzados pueden transformar la ciberseguridad y la protección de datos en sistemas críticos, particularmente en votación electrónica y redes inteligentes. Si bien blockchain ofrece numerosas ventajas en términos de seguridad y eficiencia, la adopción a gran escala aún enfrenta varios desafíos técnicos y económicos. Las soluciones propuestas, como los contratos inteligentes que puede proporcionar una elección rentable según Anwar ul Hassan et al. (2022) y la integración de blockchain híbrido que es la tercera preferida en el estudio de Sharp et al. (2024), podrían ser fundamentales para superar estos obstáculos y facilitar la implementación de blockchain en sistemas de alta demanda. Se sugiere que futuras investigaciones continúen explorando formas de mejorar la escalabilidad de blockchain, así como la interoperabilidad entre diferentes plataformas, lo que permitirá que blockchain se convierta en una solución viable y sostenible a largo plazo en estos contextos.

CONCLUSIONES

Este estudio confirmo la hipótesis que la tecnología blockchain, combinada con algoritmos criptográficos avanzados, mejora significativamente la ciberseguridad, la confiabilidad y la eficiencia de los sistemas que gestionan datos sensibles, especialmente en la votación electrónica y redes inteligentes. En conjunto la seguridad, transparencia y privacidad se mencionan como principales conclusiones por lo menos 41 veces. Los resultados confirman que blockchain ofrece una solución robusta para garantizar la inmutabilidad, transparencia y seguridad de los datos, pero su implementación a gran escala aún enfrenta desafíos como la escalabilidad y el consumo energético. Pero esto va mejorando, es por eso por lo que la economía, rapidez y escalabilidad se pueden observar cómo conclusiones principales 22 veces, ya sea para mostrar preocupación o para añadir una mejora. Se espera que este estudio aporte una comprensión más clara de los beneficios y limitaciones de blockchain. Finalmente, y en vista que, de la misma manera, la expectativa de más participación; y el interés por la adaptación y por el futuro aparecen 18 veces, se sugiere que futuras investigaciones se centren en mejorar la escalabilidad, la interoperatividad entre plataformas blockchain, la optimización de costos operativos y la búsqueda de innovadoras aplicaciones y soluciones para facilitar su adopción masiva.

CONTRIBUCIÓN DE LOS AUTORES

Rodriguez Bermudez Joseph Luis: Investigador de campo, redacción, recopilación de datos y análisis de resultados.

Rivas Verastegui Kevin Paul: Investigador de campo, redacción, recopilación de datos y análisis de resultados.

Mendoza de los Santos Alberto Carlos: Revisión del documento, mentor de investigación y metodología, supervisión del progreso.

AGRADECIMIENTOS

A Dios por permitirnos estudiar e investigar estas áreas del conocimiento.

REFERENCIAS BIBLIOGRÁFICAS

Almeida, R. L., Baiardi, F., Di Francesco Maesa, D., & Ricci, L. (2023). Impact of Decentralization on Electronic Voting Systems: A Systematic Literature Survey. *IEEE Access*, *11*, 132389-132423. Scopus. https://doi.org/10.1109/ACCESS.2023.3336593

Alown, M., Sabir Kiraz, M., & Ali Bingol, M. (2025). Enhancing Democratic Processes: A Survey of DRE, Internet, and Blockchain in Electronic Voting Systems. *IEEE Access*, *13*, 20512-20545. Scopus. https://doi.org/10.1109/ACCESS.2025.3531349

Anwar ul Hassan, C., Hammad, M., Iqbal, J., Hussain, S., Ullah, S. S., AlSalman, H., Mosleh, M. A. A., & Arif, M. (2022). A Liquid Democracy Enabled Blockchain-Based Electronic Voting System. *Scientific Programming*, *2022*(1), 1383007. https://doi.org/10.1155/2022/1383007

Chentouf, F. zahrae, & Bouchkaren, S. (2023). Security and privacy in smart city: A secure e-voting system based on blockchain. *International Journal of Electrical and Computer Engineering (IJECE)*, *13*(2), 1848-1857. https://doi.org/10.11591/ijece.v13i2.pp1848-1857

Daraghmi, E., Hamoudi, A., & Abu Helou, M. (2024). Decentralizing Democracy: Secure and Transparent E-Voting Systems with Blockchain Technology in the Context of Palestine. *Future Internet*, *16*(11), 388. https://doi.org/10.3390/fi16110388

González-Puetate, I., Marín Tello, C. L., & Reyes Pineda, H. (2022). Agri-food safety optimized by blockchain technology: review. Revista Facultad Nacional de Agronomía Medellín, 75(1). https://doi.org/10.15446/rfnam.v75n1.95760

Jaramillo, M. P., & Piedra, N. (2021). Un marco de trabajo basado en tecnología blockchain para mejorar la trazabilidad y la confianza en el intercambio de información entre Instituciones de Educación Superior. RISTI - Revista Ibérica de Sistemas E Tecnologias de Informação, 41, 97-111. https://doi.org/10.17013/risti.41.97-111

Llanten-Lucio, Y. I., Amador-Donado, S., & Márceles-Villalba, K. (2022a). Architecture of an intelligent cybersecurity Framework based on Blockchain technology for IIoT. *Ing. Compet.*, *24*(2). SciELO Colombia. https://doi.org/10.25100/iyc.v24i2.11761

Llanten-Lucio, Y. I., Amador-Donado, S., & Márceles-Villalba, K. (2022b). Validation of Cybersecurity Framework for Threat Mitigation. *Revista Facultad de Ingeniería*, *31*(62). https://doi.org/10.19053/01211129.v31.n62.2022.14840

Majumder, S., Ray, S., Sadhukhan, D., Dasgupta, M., Das, A. K., & Park, Y. (2024). ECC-EXONUM-eVOTING: A Novel Signature-Based e-Voting Scheme Using Blockchain and Zero Knowledge Property. *IEEE Open Journal of the Communications Society*, *5*, 583-598. Scopus. https://doi.org/10.1109/OJCOMS.2023.3348468

Mohanaprakash, T. A., Ranganayaki, V. C., Minu, M. S., Durga Devi, A., & Cinthuja, K. (2024). Secure Routing E-voting Protocol based on Wireless Sensor Network Platform with Block chain. *International Journal of Electrical and Electronics Research*, *12*(4), 1381-1390. Scopus. https://doi.org/10.37391/IJEER.120432

Morales, W. G. B. (2022). ANALISIS DE PRISMA COMO METODOLOGÍA PARA REVISIÓN SISTEMÁTICA: UNA APROXIMACIÓN GENERAL. Saúde Em Redes, 8(sup1), 339-360. https://doi.org/10.18310/2446-4813.2022v8nsup1p339-360

Mullegowda, R. C., Hiremani, N., Birje, M., & Ramaswamy, N. K. (2024). A novel smart contract based blockchain with sidechain for electronic voting. *International Journal of Electrical and Computer Engineering (IJECE)*, *14*(1), 617-630. https://doi.org/10.11591/ijece.v14i1.pp617-630

Ohize, H. O., Onumanyi, A. J., Umar, B. U., Ajao, L. A., Isah, R. O., Dogo, E. M., Nuhu, B. K., Olaniyi, O. M., Ambafi, J. G., Sheidu, V. B., & Ibrahim, M. M. (2024). Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges. Cluster Computing, 28(2). https://doi.org/10.1007/s10586-024-04709-8

Olivares-Rojas, J. C., Reyes-Archundia, E., & Gutiérrez-Gnecchi, J. A. (2023). A cybersecurity transaction energy system using Multi-Tier blockchain. Computación y Sistemas, 27(3). https://doi.org/10.13053/cys-27-3-4071

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., . . . Alonso-Fernández, S. (2021). Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas. Revista Española de Cardiología, 74(9), 790-799. https://doi.org/10.1016/j.recesp.2021.06.016

Sallal, M., de Fréin, R., & Malik, A. (2023). PVPBC: Privacy and Verifiability Preserving E-Voting Based on Permissioned Blockchain. *Future Internet*, *15*(4). Scopus. https://doi.org/10.3390/fi15040121

Salman, S., Janabi, S., & Sagheer, A. (2023). Security Attacks on E-Voting System Using Blockchain. *Iraqi Journal for Computer Science and Mathematics*, *4*(2), 179-192. https://doi.org/10.52866/ijcsm.2023.02.02.016

Sharp, M., Njilla, L., Huang, C.-T., & Geng, T. (2024). Blockchain-Based E-Voting Mechanisms: A Survey and a Proposal †. *Network*, *4*(4), 426-442. Scopus. https://doi.org/10.3390/network4040021

Singh, I., Kaur, A., Agarwal, P., & Idrees, S. M. (2024). Enhancing Security and Transparency in Online Voting through Blockchain Decentralization. *SN Computer Science*, *5*(7), 921. https://doi.org/10.1007/s42979-024-03286-2

Taş, R., & Tanrıöver, Ö. Ö. (2021). A Manipulation Prevention Model for Blockchain-Based E-Voting Systems. *Security and Communication Networks*, *2021*(1), 6673691. https://doi.org/10.1155/2021/6673691

Umar, B. U., Olaniyi, O. M., Olajide, D. O., & Dogo, E. M. (2022). Paillier Cryptosystem Based ChainNode for Secure Electronic Voting. *Frontiers in Blockchain*, *5*. https://doi.org/10.3389/fbloc.2022.927013

Vinayachandra, & Krishna Prasad, K. (2025). Blockchain Based Cryptographic Algorithm for Data Protection in Electronic Voting System. *EAI Endorsed Transactions on Internet of Things*, *11*. https://doi.org/10.4108/eetiot.7680

Wahab, Y. M., Ghazi, A., Al-Dawoodi, A., Alisawi, M., Abdullah, S. S., Hammood, L., & Nawaf, A. Y. (2022). A Framework for Blockchain Based E-Voting System for Iraq. *International Journal of Interactive Mobile Technologies (iJIM)*, *16*(10), 210-222. https://doi.org/10.3991/ijim.v16i10.30045

Wang, X., Feng, T., Liu, C., & Fang, J. (2024). Multi party confidential verifiable electronic voting scheme based on blockchain. *Journal of Cloud Computing*, *13*(1). Scopus. https://doi.org/10.1186/s13677-024-00723-8