Cryptographic Protocols and their Impact on Digital Election Security: An RSL

Jeremies Chinchay [1], Massiel Parvina[2], Carmen Cuba[3],Cesar Cabrera[4]
[1,2,3,4] Universidad Tecnológica del Perú, Perú, U20233293@utp.edu.pe, U20245397@utp.edu.pe, c20369@utp.edu.pe, c20259@utp.edu.pe

Abstract*– Digital electoral security has become fundamental to the development of reliable, integrated and available technological systems, driven by the growing demand for transparency and protection against threats. The purpose of this study is to analyze the impact of cryptographic protocols on the security of electoral processes, evaluating their effectiveness against traditional methods. For this purpose, a systematic review of the literature was carried out, considering 50 articles extracted from the Scopus database. The analysis focused on cryptographic techniques applied to blockchain-based environments, such as homomorphic encryption, zero-knowledge proofs and smart contracts, evaluating their contribution to design more secure, auditable and reliable voting systems. The results show that these protocols contribute to prevent recurring vulnerabilities, such as vote tampering, electoral fraud, impersonation and lack of validation, in addition to strengthening auditability and operational reliability Finally, the study concludes that the adoption and assessment of cryptographic protocols are essential to reduce risks in electronic voting, and promote more secure, transparent and efficient electoral processes.

Keywords—Cryptographic protocols, Electronic voting, Blockchain, Cryptography, Security.

Protocolos Criptográficos y su Impacto en la Seguridad Electoral Digital: Una RSL

Jeremies Chinchay [1], Massiel Parvina[2], Carmen Cuba[3],Cesar Cabrera[4]
[1,2,3,4] Universidad Tecnológica del Perú, Perú, U20233293@utp.edu.pe, U20245397@utp.edu.pe, c20369@utp.edu.pe, c20259@utp.edu.pe

Resumen*– La seguridad electoral digital se ha vuelto fundamental para el desarrollo de sistemas tecnológicos confiables, integro y disponible e impulsado por la creciente demanda de transparencia y protección contra amenazas. El propósito de este estudio es analizar el impacto de los protocolos criptográficos en la seguridad de los procesos electorales, evaluando su eficacia frente a los métodos tradicionales. Para ello, se realizó una revisión sistemática de la literatura, considerando 50 artículos extraídos de la base de datos Scopus. El análisis se enfocó en técnicas criptográficas aplicadas a entornos basados en blockchain, como la encriptación homomórfica, las pruebas de conocimiento cero y los contratos inteligentes, evaluando su contribución para diseñar sistemas de votación más seguros, auditables y confiables. Los resultados muestran que estos protocolos contribuyen a prevenir vulnerabilidades recurrentes, como la manipulación de votos, el fraude electoral, la suplantación de identidad y la falta de validación, además de fortalecer la auditabilidad y la fiabilidad operativa Finalmente, el estudio concluye que la adopción y avaluación de protocolos criptográficos son esenciales para reducir riesgos en las votaciones electrónicas, y promover procesos electorales más seguros, transparentes y eficientes.

Palabras clave-Protocolos criptográficos, Voto electrónico, Blockchain, Criptografía, Seguridad.

I. INTRODUCCIÓN

La seguridad electoral digital se ha convertido en un pilar fundamental dentro del desarrollo de sistemas tecnológicos confiable, integro y disponibles especialmente en un contexto global donde los procesos democráticos buscan cada vez mayor transparencia, eficiencia y protección ante amenazas cibernéticas. Históricamente, los métodos tradicionales han enfrentado desafíos relacionados con errores humanos y vulnerabilidades a la manipulación, lo que ha debilitado la confianza en los procesos electorales [1]. Los sistemas de votación físicos presentan numerosas deficiencias, y los sistemas de votación digital no son eficiente como para su implementación a gran escala [2]. Numerosos investigadores han propuesto sistemas de votación basados en blockchain para mejorar la seguridad y la transparencia electoral [3]. La votación electrónica (e-voting), sustentada en protocolos criptográficos y tecnología blockchain, se posiciona como una solución innovadora capaz de asegurar la integridad, confidencialidad y verificabilidad del voto digital [4]. Además, esta tecnología garantiza la igualdad de derechos en la participación de todos los votantes, permite mantener un registro seguro y permanente de cada voto emitido, haciendo posible revisar y verificar los resultados sin alterar la información original, lo que refuerza la confianza ciudadana en el proceso electoral [5][6][7]. El objetivo principal de estas propuestas es proporcionar el nivel necesario de seguridad y fiabilidad, manteniendo al mismo tiempo la transparencia y la confianza [8]. A pesar de ello, resulta difícil integrar el sistema de votación electrónica basado en blockchain con las plataformas actuales [9]. Aunque los sistemas de votación digital se encuentren en constante avance, estos continúan siendo objeto de controversia. En países como Colombia, la desconfianza en los sistemas electorales es histórica, exacerbada por casos de fraude, alteración de resultados y coacción a votantes [10]. Si bien la tecnología blockchain se presenta como una solución innovadora, su implementación aún enfrenta obstáculos clave como la escalabilidad, la protección de la privacidad del votante y la verificación robusta de identidades, limitando su adopción en elecciones de gran escala [11]. Aunque blockchain promete mejorar la transparencia y seguridad de los sistemas electorales, los problemas de rendimiento, almacenamiento y procesamiento de transacciones continúan dificultando su implementación en elecciones de gran magnitud [12]. En este escenario, se hace necesaria la realización de una Revisión Sistemática de la Literatura (RSL) que permita identificar, clasificar y analizar críticamente las soluciones criptográficas y tecnológicas existentes. Estudios recientes coinciden en que aún existen vacíos significativos en las revisiones previas, especialmente en lo referente a comparaciones técnicas detalladas, validaciones prácticas y la integración de contratos inteligentes como mecanismos de automatización [13][14]. Asimismo, se han identificado retos abiertos relacionados con la escalabilidad, la confianza y la transparencia en los procesos electorales digitales [15]. Por tanto, esta RSL busca aportar una visión integral sobre el impacto de los protocolos criptográficos en la seguridad electoral digital, contribuyendo con evidencia actualizada al diseño de sistemas más robustos, verificables y confiables.

II. METODOLOGÍA

El presente estudio adopta una revisión sistemática de la literatura (RSL) con el propósito de identificar, analizar y clasificar los protocolos criptográficos orientados a mejorar la seguridad en los sistemas de votación electrónica. El proceso incluye inicialmente la definición de las preguntas de investigación. En segundo lugar, se realizó una búsqueda exhaustiva de publicaciones, seguida de la identificación de fuentes relevantes según criterios predefinidos. Finalmente, se analizaron y clasificaron los estudios, sintetizando y resumiendo la información extraída [16]. Se consideraron artículos extraídos de bases de datos científica Scopus, priorizando aquellos con propuestas basadas en tecnologías como blockchain, cifrado homomórfico, contrato inteligente, firmas ciegas, redes mixtas y pruebas de conocimiento cero. Estas herramientas son fundamentales para comprender el alcance de cada protocolo analizado. Entre las propuestas identificadas, [17] presenta un sistema de votación basado en blockchain que incorpora cifrado homomórfico y

mecanismos de autenticación como reconocimiento facial, además de simular ataques cibernéticos para evaluar su robustez. El análisis se centra únicamente en aquellas propuestas basadas en técnicas criptográficas, excluyendo métodos no criptográficos, aunque puedan también contribuir a la seguridad electoral [18]. Además, se revisaron los trabajos más relevantes y similares de literatura sobre el tema seleccionado, lo que facilitó la comprensión compleja de los protocolos criptográficos [19]. Para el análisis comparativo de los artículos seleccionados, se tomaron en cuenta dos categorías principales: (A) Protocolos criptográficos y (B) Métrica de seguridad [20]. Este diseño metodológico garantiza una revisión exhaustiva y crítica de los protocolos criptográficos en seguridad electoral digital, aportando una visión integral que fundamenta las conclusiones y recomendaciones para futuros desarrollos en el área.

Determinar interrogantes de investigación

La búsqueda se realizó mediante preguntas de investigación PICO general y con sus preguntas específicas

TABLA I. PREGUNTAS DE INVESTIGACIÓN

Preguntas de investigación	**Palabras clave**
P: ¿Cuáles son los problemas de seguridad más relevantes en los procesos electorales electrónicos que pueden ser mitigados mediante el uso de protocolos criptográficos?	• Seguridad • Seguridad electoral • Seguridad digital • Privacidad de datos
I: ¿Qué tipos de protocolos criptográficos han sido propuestos o implementados para fortalecer la seguridad en los procesos de votación electrónica entre el 2020 y 2025?	• Protocolos criptográficos • Blockchain • Cifrado homomórfico • Contrato inteligente
C: ¿Cómo se comparan los protocolos criptográficos con los métodos de votación tradicionales en cuanto a niveles de seguridad?	• votación electrónica • Elecciones digitales • Votación por internet
O: ¿Qué métricas de seguridad evidencian un mayor impacto positivo tras la implementación de protocolos criptográficos en elecciones digitales?	• métricas de seguridad • transparencia • Integridad • verificabilidad
General: ¿Cómo impacta los protocolos criptográficos en la seguridad de los sistemas electorales digitales?	

A. Criterios de inclusión y exclusión:

Luego de formular la pregunta PICO junto con sus respectivas derivadas, se establecieron los criterios de inclusión y exclusión.

TABLA II. CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

Inclusión	
CRI01	Estudios enfocados en sistemas electorales digitales
CRI02	Estudios que presenten soluciones de seguridad criptográfica aplicadas a elecciones.
CRI03	Publicaciones entre 2020 y 2025.
CRI04	Artículos que ofrezcan resultados o modelos aplicables contra el fraude electoral.
CRI05	Artículos redactados en inglés o español para una comprensión precisa.
Exclusión	
CRE01	Estudios sin enfoque en seguridad criptográfica de los sistemas electorales.
CRE02	Estudios sin acceso al texto completo.
CRE03	Estudios centrados únicamente en criptografía general sin conexión con procesos de votación.
CRE04	Estudios enfocados en amenazas, sin vinculación con la aplicación de protocolos criptográficos
CRE05	Estudios con enfoque social, político o legal, sin propuestas criptográficas

Se definieron los criterios de inclusión y exclusión, y posteriormente se llevó a cabo la ejecución de la ecuación de búsqueda en la base de datos Scopus.

B. Ecuación de búsqueda:

A continuación, se presenta la fórmula empleada en la ecuación de búsqueda:

(TITLE-ABS-KEY ("Security" OR "Election security" OR "Digital security" OR "data privacy" OR "confidentiality" OR "Secrecy" OR "Anonymity" OR "Trustworthiness") AND TITLE-ABS-KEY ("Cryptographic protocols" OR "Blockchain" OR "Cryptography" OR "Homomorphic encryption" OR "smart contract" OR "Blind signatures" OR "Zero-Knowledge Proofs" OR "ZKP" OR "Mixnets" OR "Encryption") AND TITLE-ABS-KEY ("electronic voting" OR "e-voting" OR "Digital elections" OR "internet voting" OR "voting systems") AND TITLE-ABS-KEY ("security metrics" OR "transparency" OR "verifiability" OR "Integrity" OR "Privacy" OR "advantages" OR "robustness" OR "trust" OR "resilience" OR "accountability" OR "Security analysis" OR "Reliability" :)) AND PUBYEAR > 2019 AND PUBYEAR < 2026 AND PUBYEAR > 2019 AND PUBYEAR < 2026 AND (LIMIT-TO (OA , "all")) AND (LIMIT-TO (DOCTYPE , "ar") OR LIMIT-TO (DOCTYPE , "cp") OR LIMIT-TO (DOCTYPE , "re"))

C. Selección de datos:

Luego de determinar los criterios de inclusión y exclusión, y ecuación de búsqueda, se procedió a realizar el diagrama PRISMA.

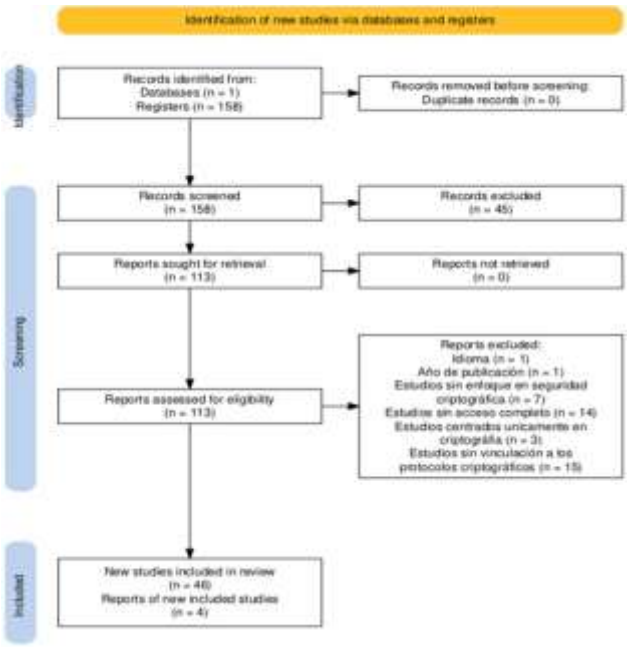

Fig. 1. Diagrama de Flujo Prisma

III. RESULTADOS

A. *Resultados bibliométricos*

Esta sección detalla los artículos que se revisaron y seleccionaron para el desarrollo de los estudios actuales. Cada artículo contiene información relevante, como el año de publicación, lugar de publicación, sector aplicado y los protocolos criptográficos utilizadas. Los artículos revisados provienen de diversos países y reflejan un creciente interés por mejorar la seguridad en los procesos electorales digitales. A través del uso de diferentes enfoques criptográficos, estas investigaciones aportan soluciones orientadas a fortalecer la integridad, privacidad y confiabilidad del voto electrónico.

TABLA III. ARTÍCULOS SELECCIONADOS

N°	Año	País	Ámbito de aplicación	Protocolos Criptográficos
21	2024	China	Electoral	Encriptación homomórfica y criptografía hash.
22	2022	Rumanía	Gobierno digital	Firmas ciegas, criptografía hash, llave pública y contratos inteligentes.
23	2024	Indonesia /Malasia	Electoral	Contratos inteligentes, llave pública y privada.
24	2024	China	Electoral	Encriptación homomórfica y contratos inteligentes
25	2024	Kazajistán	Electoral	Criptografía hash y firmas digitales.
26	2024	India / Corea del Sur	Electoral	Contratos inteligentes.
27	2023	Marruecos	Electoral	Contratos inteligentes, llave pública y privada.
28	2024	Irlanda	Electoral	Prueba de conocimiento cero (ZKP), encriptación homomórfica, llave pública y privada
29	2023	Bangladesh / Finlandia	Electoral	Contratos inteligentes, llave pública y privada.
30	2020	Polonia/ España	Electoral	Firmas ciegas, llave pública y privada
31	2022	Malasia	Electoral	Firma de anillo.
32	2024	Marruecos	Electoral	Contratos inteligentes
33	2024	China	Electoral	Firmas ciegas, pruebas de conocimiento cero (ZKPs)
34	2024	Alemania	Electoral	Pruebas de conocimiento cero (ZKPs)
35	2024	Marruecos	Electoral	Contratos inteligentes y Pruebas de conocimiento cero (ZKPs).
36	2024	China	Electoral	Cifrado homomórfico
37	2024	India /Noruega	Electoral	Contratos inteligentes.
38	2024	Italia	Electoral	Contratos inteligentes.
39	2024	Estados Unidos	Electoral	Pruebas de conocimiento cero (ZKPs) y las firmas de anillo
40	2022	Indefinido	Electoral	Contratos inteligentes, llave pública y privada.
41	2023	Estados Unidos	Electoral	Criptografía Hash, firmas ciegas y pruebas de conocimiento cero (ZKPs).
42	2021	Australia/ Luxemburgo / Noruega	Electoral	Encriptación homomórfica
43	2023	Italia / Corea de Sur	Electoral	Llave pública.
44	2024	Kazajistán	Electoral	Firmas digitales y contratos inteligentes
45	2024	Irak /Arabia Saudita/Emiratos Árabes Unidos/Reino Unido	Electoral	Firmas digitales, cifrado homomórfico, pruebas de conocimiento cero
46	2024	China	Electoral	Encriptación homomórfica y llave pública
47	2023	China	Electoral	Prueba de conocimiento cero, criptografía hash y contratos inteligentes.
48	2023	Reino Unido / Irlanda	Electoral	Cifrado homomórfico, prueba de conocimiento cero (ZKPs) y contratos inteligentes.
49	2023	India / Corea del Sur	Electoral	Prueba de conocimiento cero, firma ciega y contratos inteligentes.
50	2023	Italia	Electoral	Prueba de conocimiento cero (ZKPs) y contratos inteligentes.

B. *Hallazgos obtenidos de la revisión*

En la figura 2, se presenta un mapa mental de términos clave extraído del conjunto de estudios seleccionados en esta revisión sistemática. La visualización fue generada mediante la herramienta VosViewer, permitiendo identificar las relaciones semánticas entre palabras que aparecen con mayor frecuencia conjunta en los artículos analizados. El análisis se centra en investigaciones relacionadas con el uso de protocolos criptográficos en sistemas de votación electrónica, destacando términos como "blockchain", "criptografía", "voto electrónico", "seguridad", y "autenticación". Estos conceptos se organizan en clústeres temáticos diferenciados por colores.

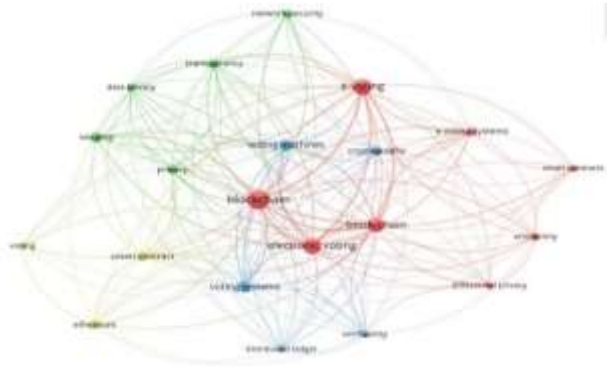

Fig. 2. Mapa de concurrencia

En la Figura 3 se presenta la distribución anual de un total de 50 publicaciones sobre protocolos criptográficos en procesos de votación electrónica. En 2020 y 2021, la participación fue de 4% en cada año, con estudios centrados en la seguridad electoral y la integridad del voto. En 2022, la producción aumentó al 20%, destacando protocolos como contratos inteligentes y firmas ciegas. En 2023, se alcanzó un 24%, con artículos que profundizaron en la integración de múltiples mecanismos criptográficos para mejorar la seguridad electoral. El año 2024 fue el más productivo, con un 42%, concentrando investigaciones orientadas a la implementación de sistemas seguros de votación electrónica. Finalmente, en 2025 se ha alcanzado un 6%, que continúan fortaleciendo el desarrollo de soluciones criptográficas, con expectativas de crecimiento durante del año. Este crecimiento refleja una tendencia creciente y sostenida en la investigación sobre la seguridad electoral digital mediante criptografía.

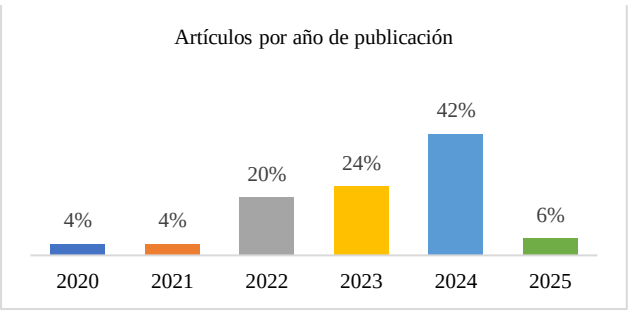

Fig. 3. Artículos por año de publicación

Por otro lado, la Figura 4 muestra la distribución geográfica de las publicaciones analizadas. China, con una participación del 12%, se centra en el desarrollo de protocolos criptográficos avanzados, como pruebas de conocimiento cero y cifrado homomórfico, orientados a mejorar la verificabilidad del voto. De manera similar, Malasia, también con un 12%, destaca por la incorporación de contratos inteligentes y firmas ciegas en plataformas de votación electrónica. Sin embargo, sus investigaciones muestran una constante preocupación por los ataques cibernéticos, lo que indica que, a pesar del uso de criptografía, este tipo de amenazas sigue representando una vulnerabilidad persistente. Italia, con un 10%, se orienta hacia el fortalecimiento de la transparencia en los procesos electorales digitales. Por su parte, Marruecos, con el mismo porcentaje (10%), contribuye con investigaciones centradas en criptografía hash, promoviendo una mayor integridad en el sistema. Por otro lado, Portugal, con un 2%, aporta mejoras en la robustez de los sistemas de votación, mediante enfoques que refuerzan su seguridad y resiliencia

Fig. 4. Distribución de publicaciones por ubicación geográfica

Esta sección presenta las amenazas de seguridad más relevantes que afectan a los sistemas de votación electrónica, tal como se ilustra en la Figura 5. Entre los problemas más frecuentes se encuentran la manipulación de votos (20%), evidenciando la necesidad de garantizar la integridad del sufragio mediante robustos mecanismos de cifrado. De igual manera, el riesgo a la privacidad (19%) señala la persistente dificultad para garantizar el anonimato del votante, aspecto fundamental para preservar tanto la confianza como la libertad del votante. Le sigue la falta de transparencia (13%), que limita la capacidad de verificación ciudadana y compromete la legitimidad del proceso. Por último, aunque con menor incidencia, la falta de verificación (4%) y el fraude electoral (4%) siguen siendo amenazas relevantes, que exigen sistemas de monitoreo más rigurosos para preservar la legitimidad y exactitud del proceso.

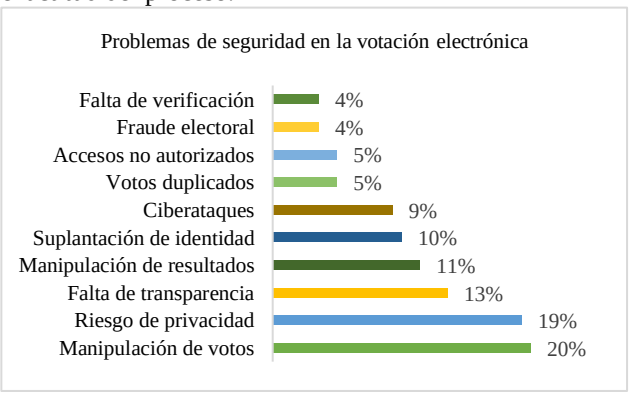

Fig. 5. Problemas de seguridad en la votación electrónica

La Figura 6 muestra la frecuencia de aparición de cada protocolo. Destacan, en primer lugar, los contratos inteligentes, con un 23%, cuya amplia adopción se asocia con su capacidad para automatizar procesos electorales, garantizar la inmutabilidad de los registros y facilitar la verificabilidad de los resultados. Le siguen la encriptación homomórfica, con un 17%, que permite contar los votos sin tener que descifrarlos, protegiendo así la privacidad del votante y evitando la revelación del contenido de su elección. Las pruebas de conocimiento cero, con un 15%, permiten verificar la validez de un voto sin revelar su contenido. Asimismo, se identifican las firmas ciegas, con un 12%, que ayudan a mantener el anonimato al impedir que el sistema relacione un voto con la identidad de su emisor. También se observa el uso de funciones hash criptográficas, con un 6%, utilizadas para crear identificadores únicos que detectan cualquier alteración en los datos. En un nivel de menor frecuencia, se encuentran las llaves privadas, con un 5%, que complementan a las públicas permitiendo la desencriptación; las firmas de anillo, con un 4%, que refuerzan el anonimato al ocultar la identidad del votante dentro de un grupo; y las redes mixtas, con un 2%, empleadas para dificultar el rastreo del camino seguido por un voto, protegiendo su transmisión. Estos resultados evidencian una clara tendencia hacia la combinación de técnicas criptográficas para abordar múltiples dimensiones de la seguridad electoral digital.

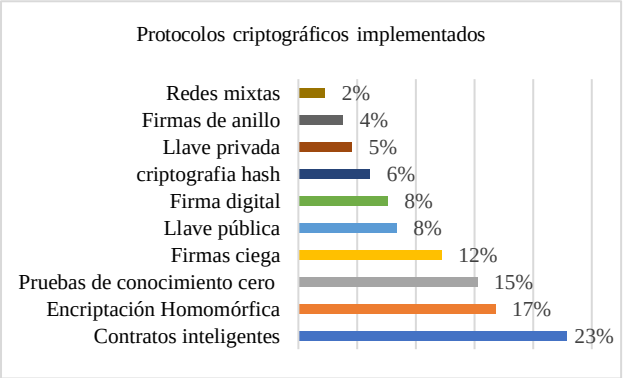

Fig. 6. Protocolos criptográficos implementados

La Figura 7 presenta una comparación entre los protocolos criptográficos y los métodos tradicionales de votación desde una perspectiva de seguridad, basada en los artículos revisados. Los resultados evidencian una clara superioridad de los enfoques criptográficos en múltiples dimensiones clave. Las características más destacadas son la resistencia al fraude electoral (23.68%), que evidencia la potente capacidad de la criptografía para proteger la integridad del proceso. Asimismo, la resistencia a manipulaciones (22.8%) subraya su capacidad para proteger la integridad del proceso electoral frente a intentos de alteración maliciosa. Además, se observa una mejora significativa en transparencia electoral (14.91%), que permiten a los votantes y observadores verificar el funcionamiento del sistema de manera más abierta. De igual forma, se observa un incremento en la confianza electoral (9.65%), un indicador clave para la legitimidad del sistema. Por último, aunque con menor frecuencia, se menciona una mejora en la trazabilidad del voto (4.39%), aspecto que refuerza la capacidad de seguimiento del proceso sin comprometer el

anonimato del elector. Estos hallazgos confirman que los protocolos criptográficos no solo refuerzan la seguridad, sino que también potencian la transparencia, verificabilidad y confianza en los procesos electorales digitales.

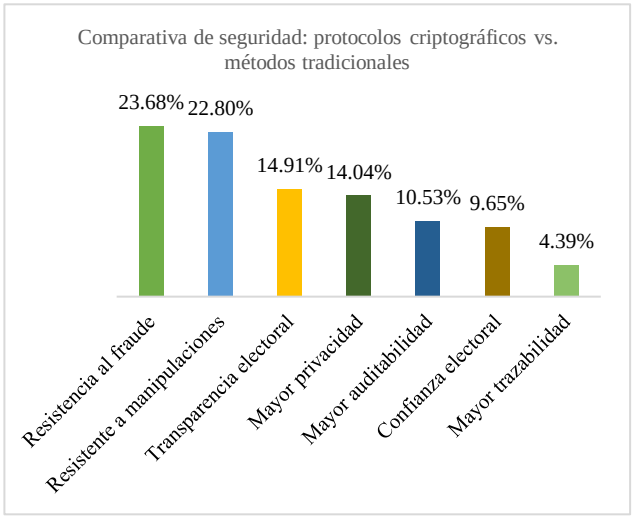

Fig. 7. Comparativa de seguridad: protocolos criptográficos vs. métodos tradicionales

La Figura 8 ilustra el impacto relativo de estos protocolos en cada métrica de seguridad. Las más beneficiadas son la integridad 30%, donde la mayoría de los estudios se enfocan en asegurar que los votos no sean modificados ni alterados después de ser emitidos. De manera similar, la verificabilidad 29%, destacando la importancia de que tanto los votantes como terceros puedan confirmar que los resultados son correctos. Por otro lado, la privacidad también representa un atributo relevante, con un 22% demostrando la efectividad de estos mecanismos para proteger la identidad del votante sin comprometer la transparencia del proceso. En una proporción menor, se observan mejoras en robustez 8%, mostrando la preocupación por crear sistemas que resistan fallos o ataques. Además, la trazabilidad 5% se refiere a la capacidad de seguir el camino del voto dentro del sistema, ayudando a detectar problemas sin revelar el contenido del voto. Por su parte, la confidencialidad 5% se relaciona con proteger la información que se transmite entre los distintos componentes del sistema electoral, para que no sea interceptada o modificada. Finalmente, la disponibilidad alcanza solo un 1%, lo que indica que pocos estudios se centran en asegurar que los sistemas estén siempre funcionando y accesibles durante toda la elección.

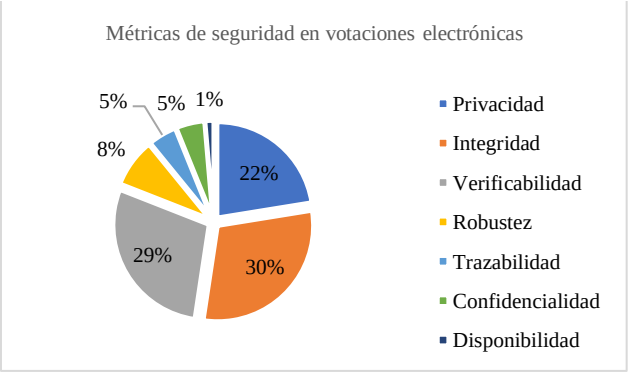

Fig. 8. Métricas de seguridad en votaciones electrónicas

La Figura 9 presenta las vulnerabilidades que aún persisten en los sistemas de votación electrónica a pesar de los protocolos criptográficos. La mayor preocupación es la posibilidad de sufrir ataques 24%, lo que muestra que, aunque los datos estén cifrados, existen otras formas de comprometer el sistema. En segundo lugar, la implementación insegura representa un 16%, debido a fallos en la forma en que se diseñan o se configuran de forma incorrecta. La desanonimización alcanza un 13% y evidencia el riesgo de que se pueda revelar la identidad del votante, afectando la privacidad. También se observa que debilidad ante la coacción 11%, donde los votantes pueden ser presionados para votar de cierta manera y la pérdida de disponibilidad 10%, que implica que el sistema puede dejar de funcionar o estar inaccesible durante el proceso electoral. Por otra parte, la falta de confianza y la falta de transparencia, ambas con un 8%, muestran que la criptografía, por sí sola, no garantiza credibilidad si no se complementa con mecanismos claros de verificación y auditoría. Finalmente, la centralización 5% y el riesgo de manipulación 5% evidencian la existencia de puntos de fallo únicos y posibles acuerdos fraudulentos entre participantes, lo que requiere controles adicionales y normas para reducir su impacto.

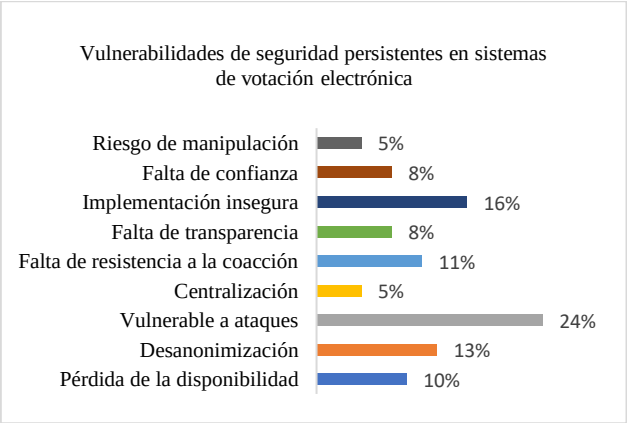

Fig. 9. Vulnerabilidades de seguridad persistentes en sistemas de votación electrónica

IV. Discusión

En esta revisión sistemática sobre protocolos criptográficos aplicados a la votación electrónica, se evidenció un marcado liderazgo en la producción científica relacionada con este campo. El análisis de la Figura 4 sobre la distribución geográfica de las publicaciones refleja que continentes como Asia 44% y Europa 31% concentran mayor parte de producción científica. En contraste, Oceanía presenta el menor nivel de contribución, con apenas un 3% de publicaciones. Esta diversidad geográfica evidencia que cada región representa características distintas en su avance tecnológico y en las necesidades específicas de sus sistemas de votación. Por lo tanto, es necesario adaptar los protocolos criptográficos a cada entorno electoral específico. Continuando con el análisis, la Figura 5 evidencia los problemas que enfrentan los sistemas de votación electrónica. La manipulación de votos, con un 20%, se presenta como la amenaza principal,

reflejando deficiencias en la protección de los datos. Por otro lado, la falta de verificación, con un 4%, subraya la necesidad de incorporar mecanismos que permitan al votante confirmar su sufragio. En conjunto, estos hallazgos refuerzan la necesidad de aplicar protocolos criptográficos más robustos que garanticen la integridad, privacidad y verificabilidad del proceso, fortaleciendo la confianza ciudadana en el voto electrónico. A partir de lo anterior, la Figura 6 muestra que los contratos inteligentes, con un 23%, destacan por su capacidad para automatizar procesos y asegurar registros inmutables, lo que favorece la transparencia del voto electrónico. Por su parte, las redes mixtas, con un 2%, ayudan a mantener el anonimato al ocultar el origen y destino de los votos. Esta comparación muestra que cada protocolo aporta en diferentes etapas del voto electrónico, y su uso depende de qué tan práctico y seguro sea aplicarlo. Se sugiere crear soluciones que combinen automatización, privacidad y protección contra amenazas, adaptadas a las necesidades de cada elección. Asimismo, la Figura 7 presenta una comparación entre los niveles de seguridad que ofrecen los distintos protocolos criptográficos frente a los métodos tradicionales, destacando que la resistencia al fraude electoral representa un 23.68%, lo cual es clave para garantizar la integridad y legitimidad del proceso de votación, evitando manipulaciones. Por otro lado, la mayor trazabilidad 4.39%, permite un seguimiento transparente y verificable de cada voto, facilitando la detección de posibles irregularidades. En conjunto, estos hallazgos indican que, aunque se prioriza la protección contra manipulaciones, es fundamental mejorar los mecanismos que aseguren la transparencia y la confianza en el sistema electoral. Por su parte, la Figura 8 muestra que los protocolos criptográficos han reforzado principalmente la integridad, con un 30%, garantizando que los datos no sean modificados durante el proceso electoral. En contraste, la disponibilidad ha recibido menor atención, con un 1% lo que indica vulnerabilidad potencial a ataques que podrían interrumpir el sistema. Por ello, importante complementar las medidas de seguridad con soluciones que aseguren la disponibilidad, garantizando así un proceso electoral estable y sin interrupciones, La Figura 9 muestra que, a pesar del uso de sistemas de votación electrónica basados en protocolos criptográficos, aún persisten vulnerabilidades de seguridad, siendo el 24% de los sistemas vulnerable a ataques como la interceptación de datos, suplantación de identidad y alteración del contenido electoral, lo que pone en riesgo la integridad del proceso. Asimismo, el riesgo de manipulación representa un 5%, asociado a intentos de alterar los resultados mediante accesos no autorizados o modificaciones maliciosas en los registros, evidenciando la necesidad de reforzar los mecanismos de protección y detección temprana de anomalías.

V. CONCLUSIÓN

Esta revisión sistemática identificó cómo el uso de protocolos criptográficos ha evolucionado para reforzar la seguridad en los sistemas de votación electrónica. Se evidenció que estos protocolos, en particular los contratos inteligentes, son importantes para automatizar procesos y asegurar la inmutabilidad de los registros, lo que contribuye a la transparencia y confianza en el sistema electoral. En paralelo, la integridad se posiciona como el principio más fortalecido, al asegurar que la información electoral no sea alterada durante su transmisión o procesamiento. Por su parte, la confidencialidad representa un componente que requiere mayor atención, ya que su fortalecimiento permitiría garantizar el secreto del voto frente a posibles vulneraciones. Asimismo, la disponibilidad se presenta como un aspecto con oportunidades de mejora, especialmente en contextos donde factores técnicos o de conectividad pueden limitar el acceso estable al sistema electoral. Esta investigación ofrece una visión general de los avances en protocolos criptográficos para votación digital, resaltando beneficios y limitaciones. Por lo tanto, se recomienda que futuros estudios busquen soluciones más equilibradas, que combinen eficiencia, privacidad y accesibilidad según el contexto electoral.

AGRADECIMIENTO/RECONOCIMIENTO

Agradecemos a la docente asesora, por su orientación constante y sus valiosos comentarios durante el desarrollo de esta investigación. También reconocemos el trabajo de todos los investigadores cuyas publicaciones fueron fundamentales para llevar a cabo esta revisión sistemática, y que aportan significativamente al avance de la seguridad electoral digital.

REFERENCIAS

[1] M. Alown, M. Sabir Kiraz and M. Ali Bingol, "Enhancing Democratic Processes: A Survey of DRE, Internet, and Blockchain in Electronic Voting Systems," *IEEE Access*, vol. 13, pp. 20512-20545, 2025, doi: 10.1109/ACCESS.2025.3531349.

[2] M. S. Farooq, U. Iftikhar and A. Khelifi, "A Framework to Make Voting System Transparent Using Blockchain Technology," *IEEE Access*, vol. 10, pp. 59959-59969, 2022, doi: 10.1109/ACCESS.2022.3180168.

[3] B. M. B. Pereira, J. M. Torres, P. M. Sobral, R. S. Moreira, C. P. d. A. Soares, and I. Pereira, "Blockchain-Based Electronic Voting: A Secure and Transparent Solution," Cryptography, vol. 7, no. 2, p. 27, 2023, doi: 10.3390/cryptography7020027.

[4] T. Aidynov, N. Goranin, D. Satybaldina, and A. Nurusheva, "A systematic literature review of current trends in electronic voting system protection using modern cryptography," Applied Sciences, vol. 14, no. 7, p. 2742, 2024, doi: 10.3390/app14072742.

[5] H. O. Ohize, A. J. Onumanyi, B. U. Umar, L. A. Ajao, R. O. Isah, E. M. Dogo, B. K. Nuhu, O. M. Olaniyi, J. G. Ambafi, V. B. Sheidu, and M. M. Ibrahim, "Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges," Cluster Computing, vol. 28, no. 2, 2025, doi: 10.1007/s10586-024-04709-8.

[6] Y.-X. Kho, S.-H. Heng, and J.-J. Chin, "A review of cryptographic electronic voting," Symmetry, vol. 14, no. 5, p. 858, 2022, doi: 10.3390/sym14050858.

[7] E. Daraghmi, A. Hamoudi, and M. Abu Helou, "Decentralizing democracy: Secure and transparent e-voting systems with blockchain technology in the context of Palestine," Future Internet, vol. 16, no. 11, p. 388, 2024, doi: 10.3390/fi16110388.

[8] H. Baniata and G. Caluna, "BP-Vot: Blockchain-based e-voting using smart contracts, differential privacy, and self-sovereign identities," IEEE Access, vol. 13, pp. 46106–46123, 2025, doi: 10.1109/ACCESS.2025.3548404.

[9] A. Marouan, M. Badrani, N. Kannouf, A. Zannou, and A. Chetouani, "Blockchain-based e-voting system in a university," Indonesian

Journal of Electrical Engineering and Computer Science, vol. 34, no. 3, pp. 1915–1923, 2024, doi: 10.11591/ijeecs.v34.i3.pp1915-1923.

[10] C. Satizábal, R. Páez, and J. Forné, "Secure Internet Voting Protocol (SIVP): A secure option for electoral processes," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 6, pp. 3647–3660, 2022, doi: 10.1016/j.jksuci.2020.12.016.

[11] R. Fatih, S. Arezki, and T. Gadi, "A review of blockchain-based e-voting systems: Comparative analysis and findings," International Journal of Interactive Mobile Technologies (iJIM), vol. 17, no. 23, pp. 49–67, 2023, doi: 10.3991/ijim.v17i23.45257.

[12] U. Jafar, M. J. Ab Aziz, Z. Shukur, and H. A. Hussain, "A systematic literature review and meta-analysis on scalable blockchain-based electronic voting systems," Sensors, vol. 22, no. 19, p. 7585, 2022, doi: 10.3390/s22197585.

[13] M. Hajian Berenjestanaki, H. R. Barzegar, N. El Ioini, and C. Pahl, "Blockchain-based e-voting systems: A technology review," Electronics, vol. 13, no. 1, p. 17, 2024, doi: 10.3390/electronics13010017.

[14] Jumaa, M. H., & Shakir, A. C. (2023). Review study of e-voting system based on smart contracts using blockchain technology. *Iraqi Journal of Science*, *64*(4), 2001–2022. https://doi.org/10.24996/ijs.2023.64.4.36

[15] U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for electronic voting system—Review and open research challenges," Sensors, vol. 21, no. 17, p. 5874, 2021, doi: 10.3390/s21175874.

[16] R. Taş and Ö. Ö. Tanrıöver, "A systematic review of challenges and opportunities of blockchain for e-voting," Symmetry, vol. 12, no. 8, p. 1328, 2020, doi: 10.3390/sym12081328.

[17] S. Salman, S. Al-Janabi, and A. Sagheer, "Security attacks on e-voting system using blockchain," Iraqi Journal for Computer Science and Mathematics, vol. 2, no. 2, pp. 179–188, 2023, doi: 10.52866/ijcsm.2023.02.02.016.

[18] R. L. Almeida, F. Baiardi, D. Di Francesco Maesa, and L. Ricci, "Impact of decentralization on electronic voting systems: A systematic literature survey," IEEE Access, vol. 11, pp. 132389–132423, 2023, doi: 10.1109/ACCESS.2023.3336593.

[19] A. M. Larriba and D. López, "SUVS: Secure unencrypted voting scheme," Informatica, vol. 33, no. 4, pp. 749–769, 2022, doi: 10.15388/22-INFOR503.

[20] A. Benabdallah, A. Audras, L. Coudert, N. El Madhoun, and M. Badra, "Analysis of blockchain solutions for e-voting: A systematic literature review," IEEE Access, vol. 10, pp. 70746–70759, 2022, doi: 10.1109/ACCESS.2022.3187688.

[21] J. Ye, L. Wang, Z. Wang, Z. Zhang, Z. Xu, and J. Zhao, "An electronic voting scheme with privacy protection," Procedia Computer Science, vol. 243, pp. 1248–1256, 2024, doi: 10.1016/j.procs.2024.09.147.

[22] C. Toma, M. Popa, C. Boja, C. Ciurea, and M. Doinea, "Secure and anonymous voting D-App with IoT embedded device using blockchain technology," Electronics, vol. 11, no. 12, p. 1895, 2022, doi: 10.3390/electronics11121895.

[23] Tedyyana, A., Ghazali, O., Asnafi, T., Purbo, O., Harun, N., & Riza, A. Tedyyana, O. Ghazali, T. Asnafi, O. Purbo, N. Harun, and F. Riza, "Transforming the voting process: Integrating blockchain into e-voting for enhanced transparency and security," TELKOMNIKA (Telecommunication Computing Electronics and Control), vol. 22, no. 2, p. 311, 2024, doi: 10.12928/telkomnika.v22i2.25758.

[24] Y. Hu and P. Su, "A decentralized voting system on the Polygon blockchain," Procedia Computer Science, vol. 247, pp. 1304–1313, 2024, doi: 10.1016/j.procs.2024.10.156.

[25] J. Ainur, M. Gulzhan, T. Amandos, R. Venera, S. Bulat, Y. Zauresh, and S. Aizhan, "The impact of blockchain and artificial intelligence technologies in network security for e-voting," *International Journal of Electrical and Computer Engineering*, vol. 14, no. 6, pp. 6723–6733, 2024, doi: 10.11591/ijece.v14i6.pp6723-6733.

[26] A. Shukla, D. Mishra, A. Pattnaik, and S. R. Salkuti, "Analysis and design on acceptance of blockchain-based e-voting system," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 33, no. 3, pp. 1793–1801, 2024, doi: 10.11591/ijeecs.v33.i3.pp1793-1801.

[27] F. Chentouf and S. Bouchkaren, "Security and privacy in smart city: A secure e-voting system based on blockchain," International Journal of Electrical and Computer Engineering (IJECE), vol. 13, no. 2, pp. 1848–1857, 2023, doi: 10.11591/ijece.v13i2.pp1848-1857.

[28] A. K. Vangujar, B. Ganesh, A. Umrani, and P. Palmieri, "A novel approach to e-voting with group identity-based identification and homomorphic encryption scheme," IEEE Access, vol. 12, pp. 162825–162843, 2024, doi: 10.1109/ACCESS.2024.3408670.

[29] M. N. Neloy, M. A. Wahab, S. Wasif, A. All Noman, M. Rahaman, T. H. Pranto, A. K. M. B. Haque, and R. M. Rahman, "A remote and cost-optimized voting system using blockchain and smart contract," IET Blockchain, vol. 3, no. 1, pp. 1–17, 2023, doi: 10.1049/blc2.12021.

[30] S. Barański, J. Szymański, A. Sobecki, D. Gil, and H. Mora, "Practical I-voting on Stellar blockchain," *Applied Sciences*, vol. 10, no. 21, p. 7606, 2020, doi: 10.3390/app10217606.

[31] N. Kassim and N. Ibrahim, "UTHM e-voting system using blockchain," *Journal of Soft Computing and Data Mining*, vol. 3, no. 1, 2022, doi: 10.30880/jscdm.2022.03.01.004.

[32] T. Chafiq, R. Azmi, and M. Ouadoud, "Blockchain-based electronic voting systems: A case study in Morocco," *International Journal of Intelligent Networks*, vol. 5, p. 100163, 2024, doi: 10.1016/j.ijin.2024.01.004.

[33] B. Wang, F. Guo, Y. Liu, B. Li, and Y. Yuan, "An efficient and versatile e-voting scheme on blockchain," *Cybersecurity*, vol. 7, Art. no. 26, 2024, doi: 10.1186/s42400-024-00226-8.

[34] Huber, N., Küsters, R., Liedtke, J., & Rausch, D. (2024). ZK-SNARKs for ballot validity: A feasibility study. In *Electronic Voting: 9th International Joint Conference, E-Vote-ID 2024, Tarragona, Spain, October 2–4, 2024, Proceedings* (pp. 107–123). Springer. https://doi.org/10.1007/978-3-031-72244-8_7

[35] F. Rabia, A. Sara, and G. Taoufiq, "ZkSNARKs and ticket-based e-voting: A blockchain system proof of concept," *Data and Metadata*, vol. 3, 2024, doi: 10.56294/dm2024.341.

[36] Y. Zhan, W. Zhao, C. Zhu, Z. Zhao, N. Yang, and B. Wang, "Efficient electronic voting system based on homomorphic encryption," Electronics, vol. 13, no. 2, p. 286, 2024, doi: 10.3390/electronics13020286.

[37] I. Singh, A. Kaur, P. Agarwal, and S. M. Idrees, "Enhancing security and transparency in online voting through blockchain decentralization," *SN Computer Science*, vol. 5, no. 7, 2024, doi: 10.1007/s42979-024-03286-2.

[38] D. Granata, M. Rak, P. Palmiero, and A. Pastena, "A methodology for vulnerability assessment and threat modelling of an e-voting platform based on Ethereum blockchain," *IEEE Access*, vol. 12, pp. 176598–176614, 2024, doi: 10.1109/ACCESS.2024.3495981.

[39] M. Sharp, L. Njilla, C.-T. Huang, and T. Geng, "Blockchain-based e-voting mechanisms: A survey and a proposal," *Network*, vol. 4, no. 4, pp. 426–442, 2024, doi: 10.3390/network4040021.

[40] V. Neziri, I. Shabani, R. Dervishi, and B. Rexha, "Assuring anonymity and privacy in electronic voting with distributed technologies based on blockchain," *Applied Sciences*, vol. 12, no. 11, p. 5477, 2022, doi: 10.3390/app12115477.

[41] M.-V. Vladucu, Z. Dong, J. Medina, and R. Rojas-Cessa, "E-voting meets blockchain: A survey," *IEEE Access*, vol. 11, pp. 23293–23308, 2023, doi: 10.1109/ACCESS.2023.3253682.

[42] Boyen, X., Haines, T., & Müller, J. (2021). Epoque: Practical end-to-end verifiable post-quantum-secure e-voting. In *2021 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 272–291). IEEE. https://doi.org/10.1109/EuroSP51992.2021.00027

[43] Esposito, C., & Choi, C. (2023). Design and implementation of a blockchain-based e-voting system by using the Algorand platform. In *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing (SAC '23)* (pp. 715–723). Association for Computing Machinery. https://doi.org/10.1145/3555776.3577750

[44] A. Jumagaliyeva, E. Abdykerimova, A. Turkmenbayev, G. Muratova, A. Talgat, and A. Shekerbek, "Analysis of research on the implementation of blockchain technologies in regional electoral processes," *International Journal of Electrical and Computer Engineering*, vol. 14, no. 3, pp. 2854–2867, 2024, doi: 10.11591/ijece.v14i3.pp2854-2867.

[45] W. A. Mahmood, J. Waleed, A. R. Abbas, H. Alaskar, M. Altulyan, and A. J. Hussain, "Intelligent gesture-enhanced blockchain voting: A new era of secure and accessible e-voting," *IEEE Access*, vol. 12, pp. 144055–144068, 2024, doi: 10.1109/ACCESS.2024.3468338

[46] K. Yuan, P. Sang, S. Zhang, X. Chen, W. Yang, and C. Jia, “An electronic voting scheme based on homomorphic encryption and decentralization,” *PeerJ Computer Science*, vol. 9, p. e1649, 2023, doi: 10.7717/peerj-cs.1649.

[47] W. Tang, W. Yang, X. Tian, and S. Yuan, “Distributed anonymous e-voting method based on smart contract authentication,” *Electronics*, vol. 12, no. 9, p. 1968, 2023, doi: 10.3390/electronics12091968.

[48] M. Sallal, R. de Fréin, and A. Malik, “PVPBC: Privacy and verifiability preserving e-voting based on permissioned blockchain,” Future Internet, vol. 15, no. 4, p. 121, 2023, doi: 10.3390/fi15040121.

[49] 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. https://doi.org/10.1109/OJCOMS.2023.3348468

[50] C. Spadafora, R. Longo, and M. Sala, “A coercion-resistant blockchain-based e-voting protocol with receipts,” Advances in Mathematics of Communications, vol. 17, no. 1, 2021, 10.3934/amc.2021005.