

Santiago Augusto Hincapié Oliveros, Jhon Jader Díaz Gómez, Juan Esteban Molina Martínez (2023).

Voto electrónico como una alternativa al proceso de votación tradicional: Una revisión de literatura. Cuaderno Activa, 15, 61-69.



Voto electrónico como una alternativa al proceso de votación tradicional: Una revisión de literatura.

Electronic Voting as an Alternative to the Traditional Voting Process: A Review of the Literature

Santiago Augusto Hincapié Oliveros¹, Jhon Jader Díaz Gómez², Juan Esteban Molina Martínez³

Tipo de Artículo: Revisión de literatura

Recibido: 15/05/2023 **Aprobado:** 01/09/2023 **Publicado:** 22/12/2023

Resumen: Los sistemas de votación electrónica se exploran cada vez más como una forma de hacer que el proceso de votación sea más seguro, transparente y accesible. Buscando evitar los problemas del voto tradicional como el fraude, la piratería y la manipulación, se inicia una revisión de literatura que permita evaluar cuáles son las tendencias actuales relacionadas con la seguridad en el e-voting (Voto electrónico), el impacto de estas nuevas tecnologías en la lucha contra la corrupción en el proceso de votación y, finalmente, se busca cómo unir las tecnologías blockchain con el e-voting. Se encuentra, finalmente, que el blockchain puede garantizar la integridad general del proceso de votación electrónica unido de técnicas de encriptación y reconocimiento facial, entregando así tranquilidad para el pueblo en general a la hora de ejercer su derecho al voto.

Palabras clave: Blockchain, reconocimiento facial, voto electrónico.

Abstract: The electronic voting systems are being explored like an alternative to make the voting process more secure, reliable, and accessible. The current literature review is made looking how to avoid the issues with the traditional voting process like fraud piracy and vote manipulation, the review seek to evaluate the current tendencies related with the security in the e-voting (Electronic voting) process, this review also seeks how these new technologies can impact the corruption related with voting, and finally, the review looks for a way to apply blockchain technologies with the e-voting. The findings are that the blockchain technology can guaranty general integrity in the electronic voting using facial recognition and encryption

1 Autor correspondiente: Santiago Augusto Hincapié Oliveros. Filiación institucional: Universidad Católica Luis Amigó. País: Colombia, Ciudad: Medellín. Correo electrónico: santiago.hincapieol@amigo.edu.co

2 Autor correspondiente: Jhon Jader Díaz Gómez. Filiación institucional: Universidad Católica Luis Amigó. País: Colombia, Ciudad: Medellín. Correo electrónico: jhon.diazg21@outlook.com

3 Autor correspondiente: Juan Esteban Molina Martínez. Filiación institucional: Universidad Católica Luis Amigó. País: Colombia, Ciudad: Medellín. Correo electrónico: juan.molinama@amigo.edu.co

techniques, at the end this mix of technologies can make the voting right a peaceful process.

Keywords: Blockchain, facial recognition, electronic voting.

I. Introducción

Los sistemas de votación electrónica se exploran cada vez más como una forma de hacer que el proceso de votación sea más seguro, transparente y accesible. Los sistemas de votación tradicionales a menudo se asocian con desafíos como el fraude, la piratería y la manipulación. Sin embargo, el uso de cadenas de bloques y tecnologías biométricas en el voto electrónico tiene el potencial de abordar algunos de estos desafíos al proporcionar un registro de transacciones seguro y a prueba de manipulaciones, y mejorar la precisión de la verificación de la identidad del votante.

Esta investigación tiene como objetivo explorar el uso de blockchain y tecnologías biométricas en el voto electrónico y evaluar su impacto potencial en la seguridad, privacidad y accesibilidad del proceso de votación. Específicamente, esta investigación se centrará en identificar los riesgos y vulnerabilidades potenciales asociados con la implementación de sistemas de voto electrónico que utilizan tecnologías biométricas y de cadena de bloques, evaluar la eficacia de los controles de seguridad y privacidad, el cumplimiento de los requisitos legales y reglamentarios, y el impacto del sistema sobre los votantes.

La investigación se basará en una variedad de métodos, que incluyen revisiones de la literatura y estudios de casos. Los hallazgos de esta RSL se utilizarán para informar las recomendaciones para el diseño de la investigación, la implementación y la evaluación de los sistemas de votación electrónica que utilizan tecnologías biométricas y de cadena de bloques.

La arquitectura que se expondrá dentro de esta RSL está enfocada en la denominada como microservicios; esta es un enfoque de diseño de

software que se basa en la creación de aplicaciones a partir de un conjunto de servicios pequeños, independientes y altamente especializados, que se comunican entre sí mediante interfaces bien definidas y ligeras.

En esta arquitectura, cada microservicio es responsable de una tarea específica y se ejecuta de manera autónoma en su propio proceso. Esto permite una mayor flexibilidad, escalabilidad y mantenibilidad en comparación con las arquitecturas monolíticas tradicionales, ya que los microservicios pueden ser actualizados, escalados y desplegados de forma independiente, sin afectar al resto del sistema.

En última instancia, el objetivo de esta RSL es contribuir con las bases de conocimiento que nos darán paso al desarrollo de un sistema de voto electrónico que sea seguro, transparente y accesible, y que inspire confianza en el proceso de votación, con el fin de contribuir con un método más controlado de los diferentes desafíos que conlleva que una organización, o una población en específico, realice la selección o elección de un tema determinado por medio del sistema.

II. Materiales y Métodos

Materiales

La literatura existente en la base de datos Science Direct, la cual es suministrada por la Universidad Católica Luis Amigó.

Métodos

Se empleó el identificador booleano "AND" junto con las palabras clave mencionadas anteriormente, así: "Peace engineering and blockchain", "E-voting and Blockchain". La búsqueda de la documentación de las investigaciones ya existentes con respecto a la implementación del blockchain y de las creaciones o implementaciones de E-voting en la sociedad realizó durante los años del 2020 en adelante.

III. Resultados de búsqueda

Autores	Contribución
Srijanee Mookherji, Odelu Vanga y Rajendra Prasath	Reconocen la votación por medio del uso de papeletas (papel y cajas) como un método de malas prácticas y, en muchos casos, dan la oportunidad para la manipulación.
Kashif Mehboob Khan, Junaid Arshad y Muhammad Mubashir Khan	Desarrollaron un sistema de votación basado en <i>blockchain</i> enfocado a la votación pública con un modelo en específico.
Patricia Baudier, Galina Kondrateva y Chantal Ammi	El estudio analiza las contribuciones potenciales del <i>blockchain</i> al proceso de votación.
Pawlak, M. y Poniszewska-Marañda, A.	Tendencias en los sistemas de votación electrónica basados en <i>blockchain</i> .
Revathy, G., Bhavana Raj, K., Kumar, A., Adibatti, S., Dahiya, P. y Latha, T. M.	Aporta conocimiento para el planteamiento de sistemas de votación electrónicos con el uso de tecnologías como <i>blockchain</i> y reconocimiento facial usando IA.
Berdik, D., Otoum, S., Schmidt, N., Porter, D. y Jararweh, Y.	Nos cuentan sobre el aprovisionamiento de la tecnología <i>blockchain</i> en sistemas de manejo de la información y su seguridad.
Ullah, S., Zheng, J., Din, N., Hussain, M. T., Ullah, F. y Yousaf, M.	Explican qué es la criptografía de curva elíptica, sus aplicaciones, cambios recientes, avances a futuro y tendencias.
Anitha, V., Marquez Caro, O. J., Sudharsan, R., Yoganandan, S. y Vimal.	Nos relatan acerca de la transparencia que ofrecen los sistemas de votación electrónicos basados en <i>blockchain</i> en cuanto a la seguridad e inalterabilidad de la información (votos).
Golchha, R., Joshi, A. y Gupta, G. P.	Hablan de cómo mejorar la seguridad frente a ataques cibernéticos usando "Learning Approach" para detectarlos.
Gupta, S., Gupta, A., Pandya, I. Y., Bhatt, A. y Mehta, K.	Aportan conocimiento para el planteamiento de sistemas de votación electrónicos con el uso de tecnologías como <i>blockchain</i> y su famosa llave de distribución cuantificada.
Hauk, E., Oviedo, M. y Ramos, X.	Hablan sobre la percepción europea frente a la gestión pública y corrupción en América Latina.
Panja, S. y Roy, B.	Explican la seguridad que conlleva el uso de la tecnología "end to end" en los sistemas de votación electrónicos basados en <i>blockchain</i> .
Khazaei, S. y Rezaei-Aliabadi, M.	Plantean un análisis de la electrónica descentralizada y las virtudes de esta práctica.
Fan, X., Wu, T., Zheng, Q., Chen, Y., Alam, M. y Xiao, X.	Muestran la seguridad y eficiencia que aportan los sistemas de votación electrónica basados en "homomorphic signcryption" del autor Zhen.
Lee, E. Y. y Ha, W.	Nos cuentan sobre el voto electrónico y su aporte para los sistemas socio-políticos.

IV. Resultados de selección

Año	Título	Autores	Volumen	Fascículo
2021	Peace engineering: The contribution of blockchain systems to the e-voting process	Patricia Baudier, Galina Kondrateva y Chantal Ammi	162	Pronóstico tecnológico y cambio social
2020	Investigating performance constraints for blockchain based secure e-voting system	Kashif Mehboob Khan, Junaid Arshad y Muhammad Mubashir Khan	105	Sistemas informáticos de generación futura
2022	Chapter 9 - Blockchain-based e-voting protocols	Srijanee Mookherji, Odelu Vanga y Rajendra Prasath		Blockchain Technology for Emerging Applications
2021	Trends in blockchain-based electronic voting systems.	Pawlak, M. y Poniszewska-Marañda, A.	58(4)	Information Processing & Management
2022	Investigation of E-voting system using face recognition using convolutional neural network (CNN)	Revathy, G., Bhavana Raj, K., Kumar, A., Adibatti, S., Dahiya, P. y Latha, T. M.	925	Theoretical Computer Science
2021	A Survey on Blockchain for Information Systems Management and Security.	Berdik, D., Otoum, S., Schmidt, N., Porter, D. y Jararweh, Y.	58(1)	Information Processing & Management
2023	Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey	Ullah, S., Zheng, J., Din, N., Hussain, M. T., Ullah, F. y Yousaf, M.	47	Computer Science Review
2023	Transparent voting system using blockchain.	Anitha, V., Márquez Caro, O. J., Sudharsan, R., Yoganandan, S. y Vimal,	25	Measurement
2023	Voting-based Ensemble Learning approach for Cyber Attacks Detection in Industrial Internet of Things	Golchha, R., Joshi, A. y Gupta, G. P.	218	Procedia Computer Science
2021	End to end secure e-voting using blockchain & quantum key distribution	Gupta, S., Gupta, A., Pandya, I. Y., Bhatt, A. y Mehta, K.		Proceedings
2020	Blockchain Ethereum Clients Performance Analysis Considering E-Voting Application	Dhulavvagol, P. M., Bhajantri, V. H. y Totad, S. G.	167	Procedia Computer Science

Año	Título	Autores	Volumen	Fascículo
2021	Support for multicriteria group decision with voting procedures: Selection of electricity generation technologies	Marques, A. C., Machado, L. C., Alencar de Morais Correia, L. M., Leal Vieira, M. J., Luíza da Silva, M., Morais Galdino de Lima, M. F., Pontes do Espírito Santo, P. P., Morais, D. C. y Frej, E. A.	3	Cleaner Environmental Systems
2021	A secure end-to-end verifiable e-voting system using blockchain and cloud server	Panja, S. y Roy, B	59	Security and Applications
2018	A rigorous security analysis of a decentralized electronic	Khazaei, S. y Rezaei-Aliabadi, M.	43	Journal of Information Security and Applications
2020	A secure high-efficiency electronic voting scheme based on homomorphic signcryption	Fan, X., Wu, T., Zheng, Q., Chen, Y., Alam, M. y Xiao, X.	111	Future Generation Computer Systems
2018	Electronic voting and strategic disclosure before shareholder meetings	Lee, E. Y. y Ha, W.	219	Security and Applications

V. Discusión

1. ¿Cuáles son las tendencias usadas actualmente por los sistemas *e-voting* con relación a la seguridad de la información (votos)?

Los sistemas de votación electrónica enfrentan muchos desafíos, incluidos problemas con la autenticación, la privacidad, la integridad de los datos, la transparencia y la verificabilidad. Sin embargo, la tecnología *blockchain* desarrollada hace más de 10 años proporciona una solución lista para usar en muchos de esos desafíos [1]; las autoridades de certificación deben garantizar la transparencia y precisión del conteo de votos electrónicos asegurando que las boletas de los votantes electrónicos se almacenen en un

entorno confiable y nadie pueda acceder a ellas o modificarlas o determinar el resultado de la elección antes de que se termine el protocolo. Finalmente, la privacidad es una de las obligaciones fundamentales de un sistema de votación, protegiendo a los ciudadanos del acceso fraudulento a su información personal, como el contenido de su voto o perfil, incluida su dirección y correo electrónico [2].

La votación es el proceso principal de los sistemas de voto electrónico. El principal requisito para el sistema es guardar el anonimato del voto. Por esta razón, se utiliza la tecnología *blockchain* y dentro del sistema se utiliza la firma ciega de los letreros de votante y verifica que se proporcionen certificados X.509. *Blockchain* ayuda a contar y

a salvar la integridad de los votos. Además, hoy en día esta tecnología se utiliza en muchas áreas, como medicina, transporte, seguridad, etc. [3].

Los investigadores consideran que la tecnología *blockchain* tiene un impacto positivo en los sistemas de votación electrónica. Sus principales ventajas son la inmutabilidad de los datos y su naturaleza distribuida. El primero asegura que los votos contenidos en él no fueron manipulados, y el segundo que ninguna entidad tiene el control completo del sistema [1]; debido a que *blockchain* es, por diseño, descentralizada, la tecnología es un candidato maravilloso para validar datos y mantener la integridad de las transacciones. Actualmente, los enfoques utilizados en la industria para hacer esto no están descentralizados. En cambio, confían en un tercero de confianza. Este es, por supuesto, un sistema menos que perfecto para lograr el objetivo deseado [4].

Según Revathy y otros [3] "En el proceso de registro se ingresan los parámetros solicitados por los sistemas y estos parámetros son verificados por la base de datos ciudadana del país. Hay varios requisitos para los votantes en cada país. En la base de datos ciudadana del país se guarda información de confianza sobre los votantes. Luego, la información especial que se utiliza en el proceso de votación se guarda en la base de datos de votantes. El esquema propuesto se proporciona mediante el reconocimiento facial, por lo que los rostros de los votantes se guardan en esta base de datos". También, Panja y Roy nos aportan "Las tecnologías biométricas agregan un nuevo nivel de autenticación a varias aplicaciones; sin embargo, siempre existen riesgos y desafíos relacionados con la privacidad y la seguridad de la biométrica" [5].

Otra de las tendencias usadas o en estudio de implementación actualmente para la verificación de la identidad en los sistemas de *e-voting* es la criptografía de curva elíptica y firma digital. Según Ullah y otros [6] La transmisión de datos e información a través de redes no seguras

es vulnerable al robo y ataque de datos, lo que implica el estudio de la criptografía. La criptografía es la práctica de usar claves para cifrar información y correspondencia para que solo pueda ser interpretada y procesada por aquellos que se supone que la reciben. Una firma digital, una técnica criptográfica para la autenticación y la integridad de los datos, se basa en el mensaje que se envía al remitente y utiliza operaciones matemáticas para localizar la firma.

Las principales tendencias encontradas son los diferentes tipos de cifrado o encriptación de información usando tecnologías avanzadas; algunos tipos son:

Cifrado simétrico de búsqueda (SSE): SSE permite a una parte externalizar de forma segura su almacenamiento de datos a otra parte, mientras conserva el derecho de buscar sobre él de forma selectiva. En los últimos años, este tema ha sido objeto de investigación activa [6].

Symmetric Image Encryption (SIE): un novedoso método de cifrado de imágenes basado en una estructura compuesta caótica. Una clave externa y dos sistemas logísticos se utilizan para el cifrado, que baraja las ubicaciones y sustituye los valores grises por los píxeles de la imagen [6].

Cifrado de imagen: para proteger el contenido de la imagen, la mayoría de los algoritmos de cifrado actuales convierten la imagen original en una imagen similar a una textura o similar al ruido, que es un indicador visual obvio de la existencia de una imagen cifrada, lo que resulta en un número desproporcionadamente grande de ataques [6].

Cifrado dinámico de búsqueda (DSE): se completa utilizando las características de un esquema PEKS y un filtro Bloom; un mecanismo de búsqueda de texto cifrado se completa en un canal inseguro; la búsqueda de palabras clave difusas está habilitada utilizando un esquema de cifrado de búsqueda de clave pública. La invención admite

búsquedas de múltiples palabras clave en chino; las palabras clave de un documento se pueden agregar o eliminar dinámicamente [6].

2. ¿Qué tanto influye en el control de la corrupción electoral en una organización?

Las elecciones son representativas porque cambian la realidad de un país, es la forma en la que todos participan de la política en una democracia. La votación electrónica se presenta como una diáfanidad para la democracia por las siguientes ventajas [7]:

Manipulación sencilla: las personas no tienen necesidad de saber leer o escribir; solamente con presionar un botón que señala el candidato será suficiente para el voto [8].

Sistema Autónomo: las computadoras son creadas exclusivamente para el sistema de votación, no hay forma de acceder para robar o cambiar la información [9].

Desaparece el voto nulo: la votación, al ser por botones, no deja opción a marcar de forma incorrecta y dañar el papel de votación [10].

Permite auditorías: el software permite recoger y evaluar datos para demostrar qué tan confiable y seguro es en evitar la corrupción de los datos [11].

Control en tiempo real: cada voto tiene una huella de la hora exacta en la que el voto fue emitido. Esto es inmodificable, lo cual permite una verificación más precisa en caso de una auditoría [12].

Resultados ágiles: por el contrario del sistema de votación a papel, que toma mucho tiempo el conteo de los votos y puede ser corrompido fácilmente. El sistema electrónico puede soportar cantidades muy grandes de usuarios y realizar las operaciones muy rápidamente, entregando los resultados casi al instante [13].

3. ¿Cómo se relacionan el e-voting con el uso de tecnologías como *blockchain*?

A lo largo de los años el concepto de votación ha sido relacionado con las sociedades u organizaciones democráticas, siendo este un pilar fundamental (13); sin embargo, un gran problema que se ha manifestado constantemente en organizaciones y sociedades con la tradicional votación en papeletas, es que esta misma da lugar a malas prácticas y manipulaciones graves durante y después de la votación (242), con el fin de superar estos problemas planteados, que se podrían definir como corrupción, por los sistemas de votación o elección convencional; en 1981 Chuan introdujo el primer sistema de votación electrónica (*E-voting*) en los últimos años, el *blockchain*, el cual se puede definir como un sistema distribuido con tecnologías de registros inmutables (246), lo cual ha traído la atención de un número significativo de aplicaciones por ser una base de datos descentralizada distribuida que mantiene una lista de registros de datos en constante crecimiento (13); esto podría significar que el *blockchain* nos permite generar una votación por medio de un sistema seguro y verificable (15).

Además de esto, la implementación de un sistema de voto electrónico implica que la tecnología movilizadora esté alineada con los principios de la democracia. El advenimiento de tecnologías distribuidas como *blockchain* podrían potenciar resolver los problemas que enfrentan los actores del proceso de votación (2).

Una cadena de bloques es un conjunto de bloques compuestos por transacciones válidas que funcionan de forma descentralizada entre pares. En un sistema de cadena de bloques, cualquier nodo puede iniciar una transacción que se puede propagar a todos los nodos dentro de la red. Para evitar el no repudio, se utiliza una firma digital para verificar la identidad de un usuario (el nodo) y certificar su actividad dentro de la cadena de bloques; todos los demás nodos

pueden controlar la firma (3), Una vez que se valida la transacción, la función hash se moviliza para agregar el bloque a la cadena de bloques de forma inviolable (2).

Las cadenas de bloques se pueden segmentar de tres maneras: (1) la cadena de bloques pública, visible para todos en Internet; cualquiera puede verificar y agregar un bloque de transacciones a la cadena de bloques (); (2) la cadena de bloques privada, visible para todos en Internet, pero solo unas pocas personas pueden verificar y agregar bloques de transacciones (); y (3) el consorcio, compuesto por organizaciones o grupos que son los únicos que pueden acceder, verificar o agregar bloques () este último podría ser implementado dentro en un sistema cerrado de e-voting, para que aquellos encargado de las selecciones realicen un monitoreo exhaustivo de la legalidad de la acción de votar por parte de los usuarios.

VI. Conclusiones

Se observa que, en la evolución de los sistemas de votación y desde sus inicios, llegando hasta la actualidad, obtenemos los sistemas de votación electrónica, los cuales se buscan ajustar a la necesidades de los procesos de votación; partiendo de esto, podemos encontrar que la principales tendencias son el uso de tecnologías como criptografía o *blockchain* para garantizar la seguridad e inalterabilidad de la información,

y también el uso de la inteligencia artificial por medio de reconocimiento facial u otras tecnologías biométricas para verificar la identidad de los votantes y evitar casos de suplantación.

Se puede encontrar una estrecha relación entre un sistema de *e-voting* y el *blockchain*; todo esto debido al control y a la seguridad que el *blockchain* nos permite tener de las transacciones realizadas en un sistema, teniendo en cuenta que el *e-voting* es un sistema que intenta ser una mejora para las formas de votación o elección convencional; esta debe de partir de la idea de que el control de las excepciones o posibles fugas de veracidad que encontramos en un sistema de votación convencional, como es el del modelo físico, debe de mejorar; en este apartado es donde interviene el *blockchain*.

En conclusión, la votación electrónica se presenta como una solución efectiva y transparente para las elecciones en una democracia, ya que ofrece una serie de ventajas que mejoran la eficacia y la precisión del proceso electoral. Además, la votación electrónica elimina muchos de los problemas y riesgos asociados con el sistema de votación en papel, lo que hace que sea una opción viable para garantizar la integridad de las elecciones y la representatividad de los resultados. En resumen, la votación electrónica es una opción valiosa para mejorar la democracia y garantizar la participación de todos los ciudadanos en la política de su país.

VII. Referencias

- [1] M. Pawlak & A. Poniszewska-Marañda, "Trends in blockchain-based electronic voting systems", *Inf Process Manag*, vol. 58, n° 4, p. 102595, Jul. 2021. [En línea]. Disponible en: doi: 10.1016/J.IPM.2021.102595.
- [2] P. Baudier, G. Kondrateva, C. Ammi, & E. Seulliet, "Peace engineering: The contribution of blockchain systems to the e-voting process", *Technol Forecast Soc Change*, vol. 162, p. 120397, 2021. [En línea]. Disponible en: doi: 10.1016/J.TECHFORE.2020.120397.
- [3] G. Revathy, K. Bhavana Raj, A. Kumar, S. Adibatti, P. Dahiya, & T. M. Latha, "Investigation of E-voting system using face recognition using convolutional neural network (CNN)", *Theor Comput Sci*, vol. 925, pp. 61–67, 2022. [En línea]. Disponible en: doi: 10.1016/J.TCS.2022.05.005.
- [4] D. Berdik, S. Otoum, N. Schmidt, D. Porter, & Y. Jararweh, "A Survey on Blockchain for Information Systems Management and Security", *Inf Process Manag*, vol. 58, n° 1, p. 102397, 2021. [En línea]. Disponible en: doi: 10.1016/J.IPM.2020.102397.
- [5] S. Panja & B. Roy, "A secure end-to-end verifiable e-voting system using blockchain and cloud server", *Journal of Information Security and Applications*, vol. 59, p. 102815, 2021. [En línea]. Disponible en: doi: 10.1016/J.JISA.2021.102815.
- [6] S. Ullah, J. Zheng, N. Din, M. T. Hussain, F. Ullah, & M. Yousaf, "Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey", *Comput Sci Rev*, vol. 47, p. 100530, 2023. [En línea]. Disponible en: doi: 10.1016/J.COSREV.2022.100530.