www.editada.org

International Journal of Combinatorial Optimization Problems and Informatics, 17(3), 2026, 190-198. ISSN: 2007-1558. https://doi.org/ 10.61467/2007.1558.2026.v17i3.1272

Development of a Blockchain for voting: A security approach in the student process at UAEH

Miguel Enrique De-La-Rosa-Lopez, Evangelina Lezama-León, Alonso Ernesto Solís-Galindo, Israel Acuña-Galván
Universidad Autónoma del Estado de Hidalgo, Carretera Tizayuca-Pachuca Km. 2.5, 43800 Fuentes de Tizayuca Hidalgo.
Email address(es): *de421564@uaeh.edu.mx, evangeli@uaeh.edu.mx, soliser@uaeh.edu.mx, israel_acuna4738@uaeh.edu.mx*
✉Corresponding author: Evangelina Lezama-León

Abstract. This paper proposes an electronic voting system based on blockchain technology with the aim of guaranteeing the integrity, transparency, and automation of the electoral process. The developed solution uses smart contracts for the decentralized registration and counting of votes, eliminating human intervention in results processing and ensuring the immutability of the stored information. The results obtained demonstrate that the system prevents duplicate votes, preserves the traceability of each record, and generates high levels of trust among participating users. The research demonstrates the viability of blockchain technology as an alternative to strengthen the reliability of digital electoral processes and establishes a solid foundation for future large-scale implementations.

Keywords: Blockchain, Electronic voting, Cybersecurity, Decentralization, Data integrity.

Article information
Received: April 9, 2026
Accepted: May 9, 2026

1 Introduction

Traditional electoral processes have been questioned due to their dependence on intermediaries, the possibility of manipulation in the counting process, and the absence of verifiable citizen audit mechanisms. The incorporation of decentralized technologies represents an opportunity to transform these processes by enabling distributed registration, public verification, and automation of vote counting (Antonio, 2016; Huckle et al., 2016). Among these technologies, blockchain is positioned as an ideal alternative thanks to its properties of immutability, transparency, decentralization, and resistance to data alteration (Treiblmaier & Sillaber, 2021; Mejía & Múnera, 2022).

Several studies have demonstrated the feasibility of applying Blockchain in the electoral sphere to increase public confidence and reduce third-party intervention (Antonio, 2016; Mejía & Múnera, 2022; Gates, 2017; López & Unda, 2018). Additionally, international institutions and organizations have pointed out its potential to strengthen democratic integrity through distributed vote verification (López & Unda, 2018; Susnjara & Smalley, 2021; INE, 2024).

In this context, this paper develops a Blockchain-based electronic voting system, whose purpose is to guarantee the uniqueness of the vote, prevent its subsequent modification, and automate the counting of results through smart contracts. This article presents the design, validation, and results obtained in the implementation of the prototype, as well as the analysis of users' perceptions regarding the level of trust and ease of use of the system.

2 Background information

Blockchain is being widely explored as a foundation for electronic voting to improve security, transparency, and trust in elections while enabling remote and online voting (table 1).

Core Design Elements

- Distributed ledger and immutability: Votes are stored on an append-only ledger replicated across many nodes, making tampering extremely difficult and audit trails natural (Ohize et al., 2024; Jafar et al., 2021; Hjalmarsson et al., 2018; Ayed, 2017; Khan et al., 2018; Hassan et al., 2022; Balkenov et al., 2026).
- Smart contracts: Voting rules (eligibility, one-vote-per-voter, tally logic) are encoded in smart contracts on platforms like Ethereum or Hyperledger Fabric (Hjalmarsson et al., 2018; Gokul, 2025; Tanwar et al., 2023; Ahn, 2022; Pawlak & Poniszewska-Marańda, 2021; S et al., 2025; Hassan et al., 2022).
- Cryptography and privacy: Systems use encryption, blind signatures, zero-knowledge proofs, and sometimes ring signatures to keep ballots secret while allowing verification (Patil et al., 2025; Ihm & Kim, 2022; Tahboub et al., 2025; Gokul, 2025; Khan et al., 2018).

Table 1: Typical design choices in blockchain voting systems

Aspect	Common Approach	Citations
Identity/auth	Digital IDs, certificates, encrypted passwords, MFA	(Ohize et al., 2024; Jafar et al., 2021; Hjalmarsson et al., 2018; Ihm & Kim, 2022; Yadav et al., 2025; Gokul, 2025)
Ledger type	Public, private, or hybrid / permissioned	(Ohize et al., 2024; Berenjestanaki et al., 2023; Tahboub et al., 2025; Gokul, 2025; Pawlak & Poniszewska-Marańda, 2021; Hassan et al., 2022)
Platform	Ethereum, Hyperledger Fabric, Multichain, custom chains	(Berenjestanaki et al., 2023; Hjalmarsson et al., 2018; Gokul, 2025; Tanwar et al., 2023; Pawlak & Poniszewska-Marańda, 2021; Khan et al., 2018; Hassan et al., 2022)
Interface	Web/mobile DApps, REST APIs, open-source prototypes	(Jafar et al., 2021; Hjalmarsson et al., 2018; Tahboub et al., 2025; Tanwar et al., 2023; Ahn, 2022)

Reported Benefits

- Security and integrity: Resistance to vote tampering, double voting, and single points of failure is a central claim across implementations and surveys (Ohize et al., 2024; Mehta & Sinclair, 2025; Jafar et al., 2021; Hjalmarsson et al., 2018; Yadav et al., 2025; Gokul, 2025; Tanwar et al., 2023; Ch. et al., 2022; Hassan et al., 2022; Anand et al., 2024).
- Transparency and auditability: Real-time or post-election auditing by voters and observers is enabled through public or permissioned ledgers and verifiable receipts (Ohize et al., 2024; Mehta & Sinclair, 2025; Hjalmarsson et al., 2018; Tahboub et al., 2025; Ahn, 2022; Pawlak & Poniszewska-Marańda, 2021; Khan et al., 2018; Anand et al., 2024; Balkenov et al., 2026).
- Remote access and efficiency: Online participation, faster counting, and reduced operational cost are frequently highlighted (Patil et al., 2025; Jafar et al., 2021; Hjalmarsson et al., 2018; Yadav et al., 2025; Ayed, 2017; Ch. et al., 2022; Hassan et al., 2022).

Main Technical and Practical Challenges

- Scalability and performance: High transaction volumes and speed constraints are recurring limitations; transaction throughput and latency must be improved for national-scale use (Patil et al., 2025; Jafar et al., 2021; Ihm & Kim, 2022; Ayed, 2017; Gokul, 2025; Ch. et al., 2022).

- Privacy vs. transparency trade-off: Balancing voter anonymity with public verifiability remains non-trivial, especially on public chains (Berenjestanaki et al., 2023; Patil et al., 2025; Ihm & Kim, 2022; Tahboub et al., 2025; Gokul, 2025).
- Integration and usability: Many works note limited focus on accessibility, usability, and compatibility with legacy election infrastructure (Berenjestanaki et al., 2023; Jafar et al., 2021; Hjalmarsson et al., 2018; Ihm & Kim, 2022).
- Regulatory and trust issues: Several papers emphasize that legal frameworks, certification, and public confidence are as critical as technical soundness (Ohize et al., 2024; Patil et al., 2025; Hjalmarsson et al., 2018; Tahboub et al., 2025; Ahn, 2022; Balkenov et al., 2026).

Research converges on a basic architecture: a (often permissioned) blockchain ledger, smart contracts for vote logic, strong cryptography for privacy, and auditable interfaces for voters and observers. Prototypes and case studies show feasibility and security gains, but real-world, large-scale deployment must still solve scalability, privacy, usability, and regulatory challenges.

In recent years, various studies have explored the implementation of Blockchain technology in electronic voting systems as a secure and auditable alternative to traditional methods. (Antonio, 2016) proposed a distributed voting model based on smart contracts, highlighting the ability of Blockchain to guarantee the immutability of votes. (Mejía & Múnera, 2022) developed BlockID, a university platform that demonstrated the feasibility of using blockchain to record votes in a decentralized and transparent manner.

For their part, (Huckle et al., 2016) and (Treiblmaier & Sillaber, 2021) analyzed the relationship between technological decentralization and trust in digital electoral processes. These studies agree treduce use of distributed networks reduces the possibility of fraud and increases citizen verifiability of the results. Finally, (López & Unda, 2018) argue that digital trust in complex environments depends directly on the transparency and traceability of information systems, principles that Blockchain technology natively fulfills.

In this sense, the present study builds on these previous advances, proposing its own architecture oriented toward the practical application of electronic voting with immutable, automated, and publicly verifiable registration.

3 Proposition || Submission

The general architecture of the proposed voting system, which consists of four main elements (see Figure 1):
1. User interface for casting votes.
2. Smart contract that validates and records votes.
3. Private blockchain network that stores each transaction in a distributed manner.
4. Module for public consultation and verification of the registry (Mejía & Múnera, 2022; Gates, 2017).

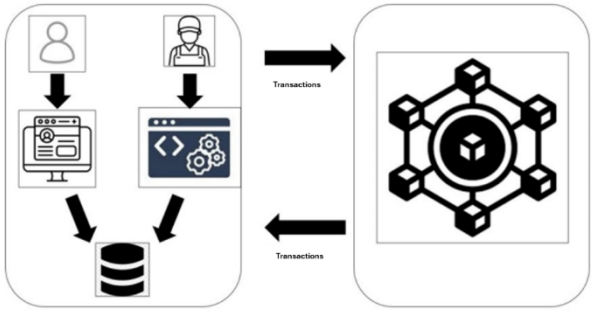


Figure 1. General architecture of the Blockchain-based electronic voting system.

The process ensures that each recorded transaction corresponds to a single vote and that once stored, it cannot be altered or deleted, thereby guaranteeing immutability. The system was implemented on a private Ethereum-

based blockchain network using the Ganache framework, configured with 10 distributed nodes operating under a Proof of Work (PoW) consensus mechanism. Smart contracts were developed in Solidity and deployed through the Remix IDE, while Web3.js enabled interaction between the application interface and the blockchain. Although the network operated in a local simulated environment without real gas expenditure, transaction execution times were measured, with average block confirmation ranging between 1 and 3 seconds. Public verification of the hash associated with each vote allows its existence to be validated without exposing the voter's identity. This configuration provides sufficient technical details to allow reproducibility of the proposed architecture in comparable controlled blockchain environments.

The complete process of issuing, validating, and recording votes is illustrated in Figures 2 to 9, detailing each stage of the flow: authentication, candidate selection, single vote validation, submission to the blockchain network, block registration, and confirmation to the user.

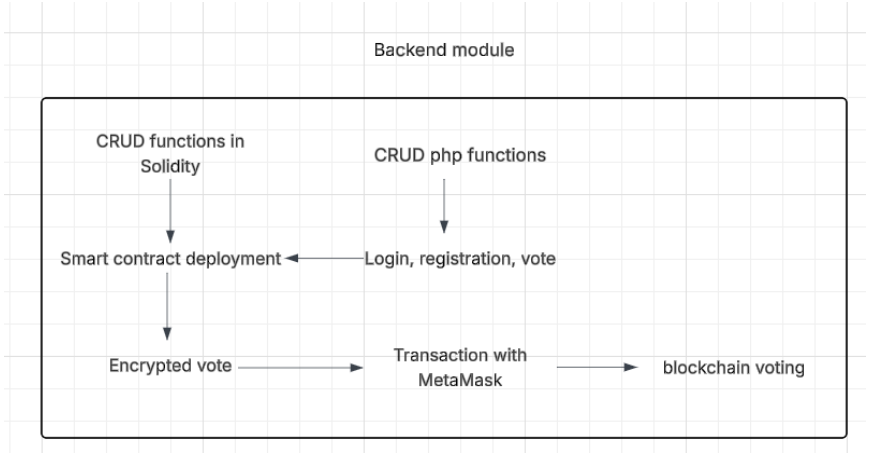


Figure 2. Flow of the voting process implemented in the system.

Figures 3 to 9 collectively illustrate the operational implementation of the proposed architecture, covering authentication, candidate selection, vote submission, smart contract validation, block registration, and public verification. Rather than representing isolated interface stages, these figures demonstrate the sequential enforcement of vote uniqueness, transaction immutability, and hash traceability within the blockchain environment. The integration of frontend interaction with backend validation and distributed ledger recording ensures that each step is cryptographically secured and programmatically controlled, eliminating manual intervention throughout the process.

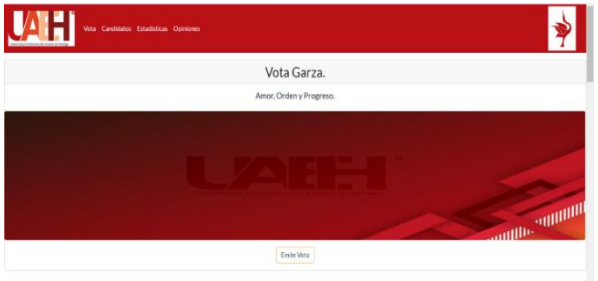


Figure 3. System 1.

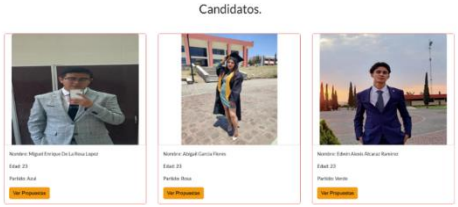


Figure 4. System 2.

Figure 5. System 3.

Figure 6. System 4.

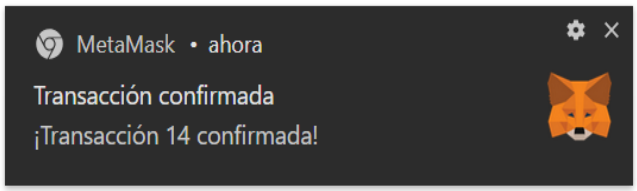


Figure 7. System 5.

Figure 8. System 6.

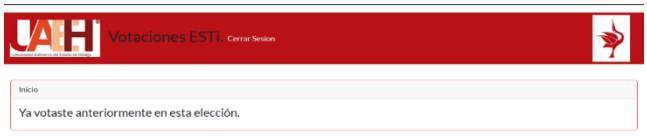


Figure 9. System 7.

This flow was implemented to guarantee the uniqueness of the vote and the automation of the counting process, eliminating human intervention in the critical stages of voter registration.

From a security standpoint, the system was examined under a simplified threat model to assess potential vulnerabilities inherent to blockchain-based voting architectures. Given that the implementation operates on a private Ethereum network composed of 10 nodes under a Proof of Work consensus mechanism, a 51% attack would require majority computational control over internal validators. While this scenario is unlikely in a controlled institutional deployment, it remains theoretically possible within distributed ledger systems.

Sybil attacks are mitigated by restricting node participation to authorized and pre-configured instances within the private network. Vote uniqueness is enforced at the smart contract level through state validation mechanisms

that prevent duplicate submissions from the same address. Nevertheless, as with any Ethereum-based implementation, vulnerabilities associated with insufficient contract auditing must be considered. Additionally, denial-of-service conditions and insider manipulation represent relevant risks in privately governed networks, underscoring the importance of governance policies, access control mechanisms, and periodic security evaluation in real-world adoption contexts.

The smart contract prevents users from casting more than one vote, guaranteeing the uniqueness of each vote (Mejía & Múnera, 2022; Gates, 2017). It was verified that, once registered, the vote cannot be modified or deleted due to the immutability properties of the Blockchain (Huckle et al., 2016). In addition, the system allows the hash associated with each transaction to be consulted, which publicly confirms that the vote was correctly registered without revealing the voter's identity (see Figures 10 and 11).

In addition to functional validation, basic performance indicators were measured within a controlled experimental environment consisting of a private Ethereum network simulated through Ganache and configured with 10 distributed nodes operating locally. Under normal load conditions, the average block confirmation time ranged between 1 and 3 seconds per transaction. The system processed approximately 15–20 transactions per minute without observable instability.

Scalability was evaluated through incremental transaction submission, simulating voter interaction under academic testing conditions rather than a real institutional election. The system maintained stable behavior under moderate load; however, large-scale stress testing was not conducted. Storage growth remained proportional to the number of recorded votes, as each transaction generated a new block entry without excessive data overhead. These results suggest that the prototype is operationally viable within small-to-medium electoral contexts, although broader deployment would require extended performance evaluation.

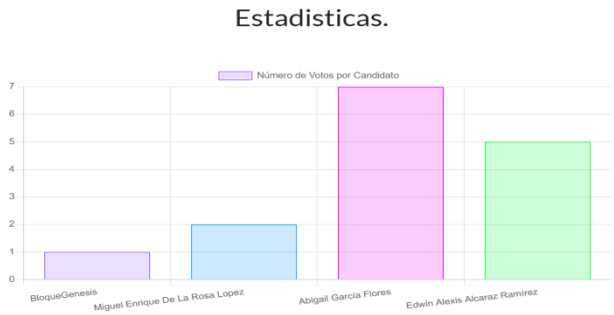
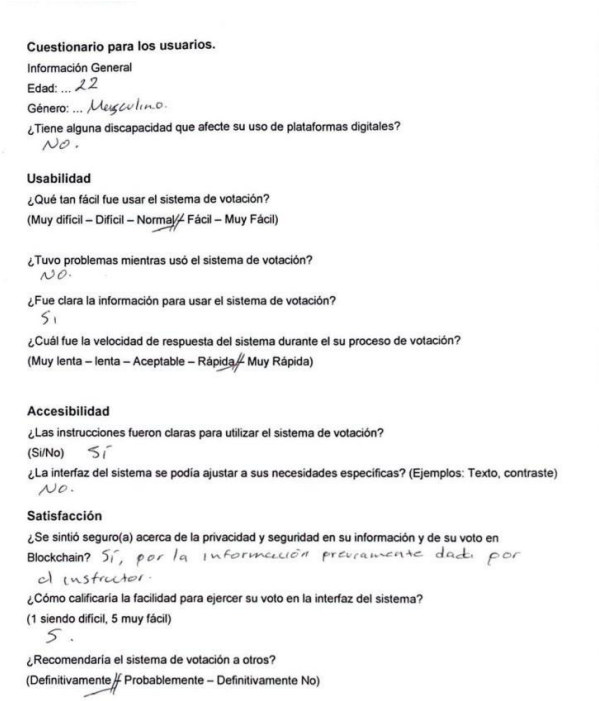


Figure 10. Votes recorded by candidate.



Cuestionario para los usuarios.

Información General

Edad: ... 22

Género: ... Masculino.

¿Tiene alguna discapacidad que afecte su uso de plataformas digitales?

No.

Usabilidad

¿Qué tan fácil fue usar el sistema de votación?

(Muy difícil – Difícil – Normal // Fácil – Muy Fácil)

¿Tuvo problemas mientras usó el sistema de votación?

No.

¿Fue clara la información para usar el sistema de votación?

Si

¿Cuál fue la velocidad de respuesta del sistema durante el su proceso de votación?

(Muy lenta – lenta – Aceptable – Rápida // Muy Rápida)

Accesibilidad

¿Las instrucciones fueron claras para utilizar el sistema de votación?

(Si/No) Si

¿La interfaz del sistema se podía ajustar a sus necesidades específicas? (Ejemplos: Texto, contraste)

No.

Satisfacción

¿Se sintió seguro(a) acerca de la privacidad y seguridad en su información y de su voto en Blockchain? Si, por la información previamente dada por el instructor.

¿Cómo calificaría la facilidad para ejercer su voto en la interfaz del sistema?

(1 siendo difícil, 5 muy fácil)

5.

¿Recomendaría el sistema de votación a otros?

(Definitivamente // Probablemente – Definitivamente No)

Figure 11. Users' perception of the voting system.

After administering the questionnaire to 30 participants (10 students from each undergraduate program offered at ESTi), a highly positive assessment of the proposed system was observed. The instrument consisted of 10 questions combining closed-format items, true/false statements, difficulty-scale evaluations (Very difficult–Difficult–Normal–Easy–Very easy), and a limited number of open-ended questions aimed at collecting qualitative feedback. Results indicated that 100% of respondents considered the system secure and reliable, 93% rated it as easy to use, and 86% stated they would prefer this method over traditional voting. In general terms, participants agreed that the automation of the process and the transparency of the count generate greater confidence compared to conventional electoral procedures.

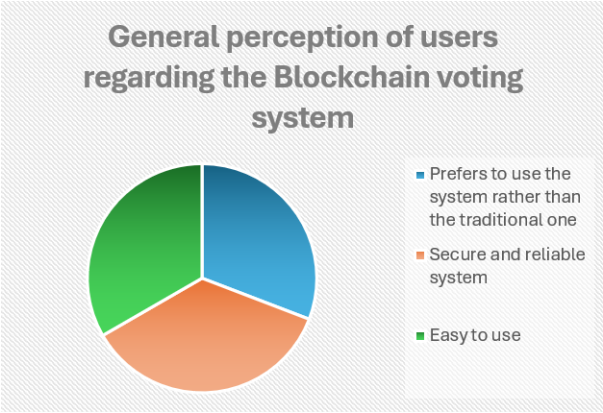


Figure 12. Pie chart shows users' overall perception of the Blockchain-based voting system.

The results show that the use of Blockchain allows the election counting process to be automated without human intervention, guarantees the integrity of the record, and increases the user's perception of security. Functional validation confirms that the system prevents duplicate votes and maintains the traceability of each transaction. The values obtained in the survey reflect a high acceptance of the proposed model, which supports its viability in real environments.

4 Conclusions

The electronic voting system based on blockchain technology demonstrated functional viability within a controlled experimental environment. The decentralization of the registry and the use of smart contracts for vote validation and counting reduced manual intervention in critical stages of the electoral process, contributing to procedural transparency. However, these findings should be interpreted within the scope of the experimental configuration and not as definitive evidence of readiness for large-scale institutional deployment.

The results confirmed that the proposal complies with fundamental security principles: each vote is unique, cannot be modified once stored, and can be publicly verified without compromising the voter's identity. Likewise, the perception evaluation showed high levels of trust and acceptance by users.

However, the system presents limitations inherent to its experimental nature. It was validated in a private Ethereum network environment, without biometric authentication mechanisms and without large-scale stress testing. Additionally, regulatory and legal interoperability with national electoral frameworks remains an open challenge, as the adoption of blockchain-based voting systems must comply with institutional norms, electoral transparency requirements, and data protection regulations. Ethical considerations related to digital identity management and governance structures also require careful evaluation before real-world implementation. While the prototype shows promising characteristics for secure digital voting, its adoption in real electoral systems would require comprehensive regulatory alignment, institutional governance frameworks, and extended empirical validation.

References

Ahn, B. (2022). Implementation and Early Adoption of an Ethereum-Based Electronic Voting System for the Prevention of Fraudulent Voting. *Sustainability*. https://doi.org/10.3390/su14052917

Allende López, M., & Colina Unda, V. (2018). *Blockchain: How to Develop Trust in Complex Surroundings to Generate Social Impact Value*. Inter-American Development Bank. https://doi.org/10.18235/0001139

Anand, A., Lakhwani, K., & Mathur, S. (2024). A Blockchain Technology Based Voting System. *International Journal For Multidisciplinary Research*. https://doi.org/10.36948/ijfmr.2024.v06i06.32871

Ayed, A. (2017). A Conceptual Secure Blockchain Based Electronic Voting System. *International Journal of Network Security & Its Applications, 9*, 01-09. https://doi.org/10.5121/ijnsa.2017.9301

Balkenov, A., Yun, T., Khizirova, M., Kasimov, A., & Karibaev, B. (2026). Development of a Blockchain-Based Electronic Voting System. *Trudy Universiteta*. https://doi.org/10.52209/1609-1825_2026_1_453

Berenjestanaki, M. H., Barzegar, H., Ioini, N. E., & Pahl, C. (2023). Blockchain-Based E-Voting Systems: A Technology Review. *Electronics*. https://doi.org/10.3390/electronics13010017

Caballero Gimeno, J. Á. (2018). *Estudio de tecnologías Bitcoin y Blockchain* [Trabajo final de máster, Universitat Oberta de Catalunya]. Repositorio Institucional UOC. https://hdl.handle.net/10609/81268

Ch., R., D, J. K., Gadekallu, T., & Iwendi, C. (2022). Distributed-Ledger-Based Blockchain Technology for Reliable Electronic Voting System with Statistical Analysis. *Electronics*. https://doi.org/10.3390/electronics11203308

Gates, M. (2017). *Blockchain: Ultimate guide to understanding blockchain, Bitcoin, cryptocurrencies, smart contracts and the future of money*. CreateSpace Independent Publishing Platform.

Gokul, C. (2025). Blockchain-Based Distributed Electronic Voting System Ensuring Privacy and Integrity through Smart Contracts. *International Journal for Research in Applied Science and Engineering Technology*. https://doi.org/10.22214/ijraset.2025.71401

Hassan, C. A. U., Hammad, M., Iqbal, J., Hussain, S., Ullah, S. S., Alsalman, H., Mosleh, M. A. A., & Arif, S. M. (2022). A Liquid Democracy Enabled Blockchain-Based Electronic Voting System. *Sci. Program., 2022*, 1383007:1-1383007:10. https://doi.org/10.1155/2022/1383007

Hjalmarsson, F. P., Hreioarsson, G. K., Hamdaqa, M., & Hjálmtýsson, G. (2018). Blockchain-Based E-Voting System. *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, 983-986. https://doi.org/10.1109/cloud.2018.00151

Huckle, S., Bhattacharya, R., White, M., & Beloff, N. (2016). Internet of Things, Blockchain and Shared Economy Applications. *Procedia Computer Science, 98*, 461–466. https://doi.org/10.1016/j.procs.2016.09.074

IBM. (n.d.). *What is blockchain?* Retrieved June 3, 2026, from https://www.ibm.com/think/topics/blockchain

Ihm, Y.-S., & Kim, S.-H. (2022). Development of a Blockchain-Based Online Secret Electronic Voting System. *IEICE Trans. Inf. Syst., 105-D*, 1361-1372. https://doi.org/10.1587/transinf.2021edk0005

Instituto Nacional Electoral. (n.d.). *Urna Electrónica*. Retrieved June 3, 2026, from https://portal.ine.mx/voto-y-elecciones/urna-electronica/

Jafar, U., Aziz, M. J. A., & Shukur, Z. (2021). Blockchain for Electronic Voting System—Review and Open Research Challenges. *Sensors (Basel, Switzerland), 21*. https://doi.org/10.3390/s21175874

Khan, K. M., Arshad, J., & Khan, M. M. (2018). Secure Digital Voting System Based on Blockchain Technology. *Int. J. Electron. Gov. Res., 14*, 53-62. https://doi.org/10.4018/ijegr.2018010103

Marín Bermúdez, A. (2016). *Estudio de la utilización de protocolos blockchain en sistemas de votación electrónica* [Projecte/Treball Final de Carrera, Universitat Politècnica de Catalunya]. UPCommons. https://hdl.handle.net/2117/98545

Mehta, H. C., & Sinclair, K. (2025). Blockchain-Based Solutions for Secure Voting Systems. *ITSI Transactions on Electrical and Electronics Engineering*. https://doi.org/10.65521/itsi-teee.v13i1.68

Mejía Herrera, D. S., & Múnera Sánchez, J. P. (2022). *BlockID diseño de un sistema de votaciones basado en la tecnología blockchain* [Trabajo de grado de maestría, Universidad Tecnológica de Pereira]. Repositorio Institucional UTP. https://repositorio.utp.edu.co/entities/publication/8df9491d-b038-4d11-b52b-6226937224a2

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

Patil, M., Mote, A., Patil, D., Patil, P., & Patil, R. (2025). Blockchain-Based Online Voting System: Enhancing Security and Transparency in Elections Through Advanced Cryptographic Integration. *2025 IEEE International Conference on Advances in Computing Research On Science Engineering and Technology (ACROSET)*, 1-6. https://doi.org/10.1109/acroset66531.2025.11281000

Pawlak, M., & Poniszewska-Marańda, A. (2021). Implementation of Auditable Blockchain Voting System with Hyperledger Fabric. 642-655. https://doi.org/10.1007/978-3-030-77961-0_51

S, M., N, N., & M, N. (2025). Design and Implementation of a Blockchain-Based Secure and Transparent Electronic Voting System. *2025 3rd International Conference on Inventive Computing and Informatics (ICICI)*, 584-590. https://doi.org/10.1109/icici65870.2025.11069694

Tahboub, Y., Revilla, A., Lynch, J., & Floyd, G. (2025). Blockchain-Based Secure Online Voting Platform Ensuring Voter Anonymity, Integrity, and End-to-End Verifiability. *ArXiv, abs/2509.22965*. https://doi.org/10.48550/arxiv.2509.22965

Tanwar, S., Gupta, N., Kumar, P., & Hu, Y. (2023). Implementation of blockchain-based e-voting system. *Multimedia Tools and Applications, 83*, 1449-1480. https://doi.org/10.1007/s11042-023-15401-1

Treiblmaier, H., & Sillaber, C. (2021). The impact of blockchain on e-commerce: A framework for salient research topics. *Electronic Commerce Research and Applications, 48*, Article 101054. https://doi.org/10.1016/j.elerap.2021.101054

Yadav, S., Pechetti, J., G, T., & Belwal, M. (2025). A Secure and Distributed Blockchain-Based E-Voting System for Multi-Level Elections with Encrypted Authentication. *2025 9th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS)*, 1-6. https://doi.org/10.1109/csitss67709.2025.11294662