# A Blockchain-Based Voting System Using Hyperledger Fabric with a React Interface

MD Mohimul Alam[1,2,*], Shazneen Islam Akhi[1,2,*], Md. Ataur Rahman[1,2,*], Jubaida Nur Jumana[1], Shannidhay Lal Ghosh[1], Rifat Ara Rouf[1,3], and Mahady Hasan[1,2]

[1]Fab Lab, Independent University, Bangladesh
[2]Department of Computer Science and Engineering, Independent University, Bangladesh
[3]Department of Physical Sciences, Independent University, Bangladesh
1911182@iub.edu.bd,
1920585@iub.edu.bd,ataurrahman862828@gmail.com,
2111305@iub.edu.bd, 2221440@iub.edu.bd, rifatara@iub.edu.bd,
mahady@iub.edu.bd

**Abstract.** This project aims to develop a secure, transparent, and decentralized blockchain based electronic voting system utilizing Hyperledger Fabric for tamper-proof and verifiable vote storage, Hyperledger Aries for cryptographic voter identity verification, and React for an intuitive, user friendly interface. The proposed system addresses major challenges in traditional voting systems, including voter identity authentication, scalability, and transparency, while ensuring privacy and security throughout the election process. By integrating advanced cryptographic techniques such as Zero-Knowledge Proofs (ZKPs) and Verifiable Credentials (VCs), the system guarantees voter anonymity and ensures election integrity. The use of Hyperledger Fabric provides an immutable ledger to record votes securely, preventing fraud and tampering, which is a critical issue in many conventional voting systems. React offers an easy-to-use interface that enhances the system's accessibility and usability, ensuring it is suitable for both technical and nontechnical users. This project aims to address the shortcomings of traditional voting systems and contributes to modernizing the electoral process by providing a robust, fraud-resistant, and scalable voting platform suitable for both small- and large-scale elections. Ultimately, the system is designed to advance blockchain-based e-voting solutions, enhancing trust, transparency, and integrity in the electoral process and contributing to the future of secure digital voting.

**Keywords:** Blockchain · Hyperledger Fabric · Voting System · Hyperledger Aries · React · Secure Elections

## 1 Introduction

The growing need for secure and transparent voting systems has led to the development of electronic voting platforms. However, traditional and modern

electronic voting systems still face challenges such as scalability, security vulnerabilities, and lack of transparency. This research proposes a blockchain-based solution using Hyperledger Fabric to create a decentralized, tamper-proof voting system, integrated with Hyperledger Aries for voter identity verification and React for the front-end interface. By leveraging blockchain's immutable ledger, this system ensures fraud-resistant vote storage, while cryptographic verification guarantees voter privacy. Additionally, the proposed platform ensures seamless user experience, scalability, and enhanced accessibility, making it suitable for both small- and large-scale elections.

Many previous studies have focused on improving the transparency, security, and scalability of voting systems. Blockchain provides a promising solution to ensure that votes are securely recorded, publicly verifiable, and tamper-proof. However, challenges remain in terms of voter authentication and the overall user experience. Existing blockchain voting systems suffer from scalability issues and complex user interfaces, which limit their widespread adoption.

- **RQ1** – How can blockchain technology enhance service security and transparency of electronic voting systems?
- **RQ2** – What are the main challenges regarding usability and accessibility in implementing blockchain-based e-voting systems?
- **RQ3** – How can voter anonymity and data privacy be preserved while ensuring traceability in blockchain-based voting?
- **RQ4** – What cryptographic and connectional blockchain methods are most effective in securing blockchain-based e-voting systems?
- **RQ5** – How can blockchain-based e-voting systems be designed to support large-scale national elections efficiently and securely?

This work focuses on developing a system that integrates Hyperledger Fabric for secure, decentralized vote storage, Hyperledger Aries for voter identity verification, and a React-based UI to provide a seamless user experience.

- Scalable Voting Platform: Utilizes Hyperledger Fabric for fast, secure, and scalable vote storage.
- Enhanced Voter Authentication: Implements Hyperledger Aries to verify voter identity securely using Verifiable Credentials.
- Transparent Election Results: Uses smart contracts to automate vote counting and result declaration.

## 2 Literature Review

Blockchain-based electronic voting (e-voting) systems have emerged as a transformative solution to the traditional issues of electoral fraud, vote manipulation, and lack of transparency. Leveraging features such as decentralization, immutability, and cryptographic security, blockchain technologies—especially Hyperledger Fabric—promise to revolutionize digital voting systems. Despite the significant progress, practical implementation of such systems faces challenges

related to scalability, privacy, usability, and voter accessibility. This review explores 24 major research papers addressing these concerns, categorized under five core research questions. A privacy-preserving system using cryptographic techniques for voter anonymity [1]. Compares different blockchain voting models on design and performance [2]. Ethereum + biometric-based voting system for identity verification [3]. Cryptographic-based system aiming to enhance privacy and scale [4]. Proposes homomorphic encryption with blockchain to maintain vote confidentiality [5]. Polygon-based model to mitigate fraud and inefficiency in voting [6]. Comprehensive review on how blockchain enhances transparency and trust in e-voting [7]. Identifies open research challenges and future directions in blockchain voting [8]. Proposes blind signatures, ZK proofs, and threshold encryption integration [9]. Focused on vulnerabilities in traditional systems and how blockchain addresses them [10].

Survey exploring technical and organizational challenges in blockchain e-voting implementation [11]. Design of a secure voting system integrating multi-factor authentication to combat vote rigging [12]. Analysis of scalability problems in blockchain voting and proposed approaches to overcome them [13]. Comparative review of performance and security across various systems [14]. Reviews blockchain voting with focus on security and scalability challenges [15]. Proposes a decentralized system ensuring anonymity and secure audit trails [16]. Systematic review identifying key benefits and limitations of blockchain voting [17]. Detailed review of design, identity management, and cost in blockchain voting systems [18]. SBvote model introducing self-tallying for scalability and privacy enhancement [19]. SHA3 and Merkle Root-based system to ensure data integrity [20]. Survey on improving transparency and security through blockchain mechanisms [21]. Suggests Broad count and Condorcet-based blockchain vote tallying method [22]. Uses cryptographic tools for transparency and voter identity protection [23].

The reviewed papers demonstrate that blockchain provides enhanced security, transparency, and audit-ability for e-voting systems. Many proposed architectures use smart contracts, cryptographic algorithms, and consensus protocols to ensure end-to-end verifiability and voter privacy. While these systems perform well in simulations and small-scale trials, issues such as scalability, legal compliance, usability, and integration with national infrastructure remain partially addressed. Most works recognize the trade-off between privacy and transparency, proposing varying solutions. Despite significant theoretical development, several gaps persist: Large-scale national election deployment remains untested [13, 14, 18]. End-user usability and accessibility are underexplored [15, 18]. Robust identity verification integrating national databases or biometrics is rare [3]. Cost-effective implementation models for developing countries are largely missing. Legally compliant architectures addressing electoral law compatibility are underrepresented [6, 23]. Real-time analytics and scalability under network strain remain unresolved [4, 13, 17].

While several blockchain platforms such as Ethereum and Polygon have been explored for electronic voting, Hyperledger Fabric was selected due to its modular

architecture, permissioned network design, and native support for identity management. Unlike Ethereum, which relies on public consensus mechanisms that may introduce high latency and transaction fees, Hyperledger Fabric offers faster transaction processing, role-based access control, and enhanced privacy—making it more suitable for elections requiring restricted access and legal compliance.

## 3 Research Methodology

This research follows the PRISMA framework for systematic review, which will guide the study in evaluating various blockchain-based e-voting systems. The objective is to develop a secure, scalable, and decentralized blockchain-based voting system that can enhance the integrity and transparency of electoral processes.

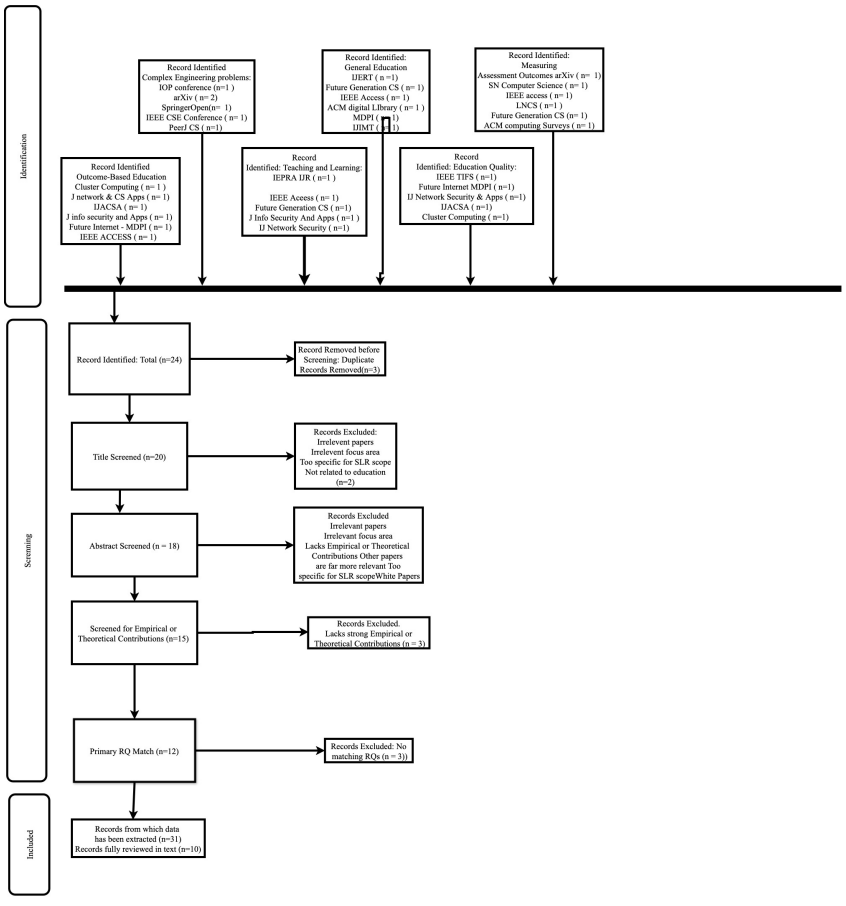



Fig. 1: PRISMA of Voting System

Fig. 1 The purpose of this study is to address challenges in current e-voting systems by proposing a blockchain-based solution using Hyperledger Fabric for decentralized vote storage and Hyperledger Aries for secure voter authentication. The research will answer how blockchain technology can enhance the security, transparency, and scalability of e-voting systems.

The methodology integrates Hyperledger Fabric for backend infrastructure, Hyperledger Aries for secure voter authentication through Verifiable Credentials, and React for the front-end interface. The system will address the existing challenges in e-voting systems by ensuring real-time vote tracking, enhancing voter anonymity, and enabling transparency with immutable blockchain storage. The sample profile includes e-voting systems designed and tested using Hyperledger Fabric , Hyperledger Aries , and React for front-end development. The systems will be evaluated on their scalability, security, usability, and performance in simulated election scenarios.

Data will be collected from existing blockchain-based voting research, case studies, and practical implementations. Literature from academic journals, surveys, and research papers will be reviewed. Furthermore, performance data from prototype systems and simulations will be gathered to evaluate the effectiveness of the proposed system.

The data will be analyzed using qualitative and quantitative methods. Comparative studies will be conducted to evaluate scalability, security, and usability. Simulation results will be analyzed to validate the system's performance under various voting conditions. Statistical tools will be used to measure scalability and performance metrics.

The primary limitation of this research is the reliance on simulated environments and prototypes. While the proposed system performs well in a simulated environment, its real-world deployment may face several practical challenges. A significant concern is the availability of stable internet connectivity, especially in rural or underdeveloped areas where voters may lack access to reliable networks. Additionally, many users might rely on outdated or low-end devices that may not support advanced cryptographic operations or modern web interfaces. Another barrier is the varying level of digital literacy among voters, which could hinder effective usage of the platform without targeted training or assistance. These issues must be carefully addressed through infrastructure planning, user-friendly design, and education campaigns to ensure inclusive and successful adoption of the blockchain-based voting system.

## 4 Proposed System

Traditional voting systems face challenges like vote tampering, lack of transparency, and inadequate voter authentication. Issues such as scalability, fraud prevention, and voter privacy compromise the integrity of elections.

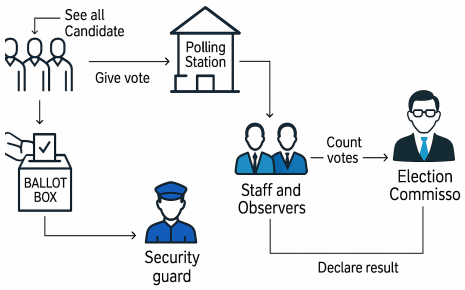



Fig. 2: Rich Picture of the As-is

Fig. 2The proposed solution is a blockchain-based voting system using Hyperledger Fabric for secure vote storage, Hyperledger Aries for cryptographic voter verification, and React for a user-friendly interface. It ensures secure, transparent, and tamper-proof elections with immutable vote records, automated vote counting, and enhanced voter authentication, addressing the limitations of traditional systems.

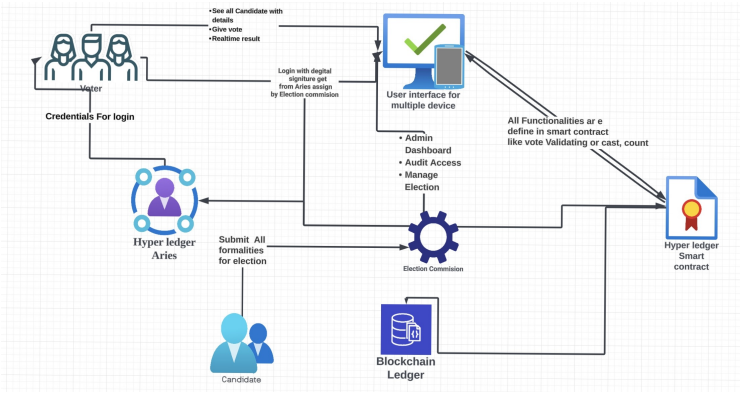



Fig. 3: Rich Picture of the Proposed System

The Rich Picture in Fig. 3 provides an abstract overview of the entire voting system, highlighting stakeholders, data flow, and key functional relationships between users and subsystems.

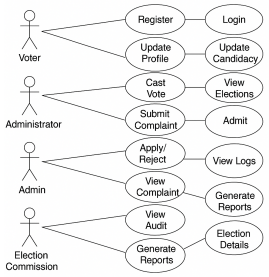



Fig. 4: Subsystem-Based Use Case Diagram of the Voting System

Fig. 4 illustrates the use case diagram, outlining how different user roles interact with specific functionalities of each subsystem in the proposed voting platform.

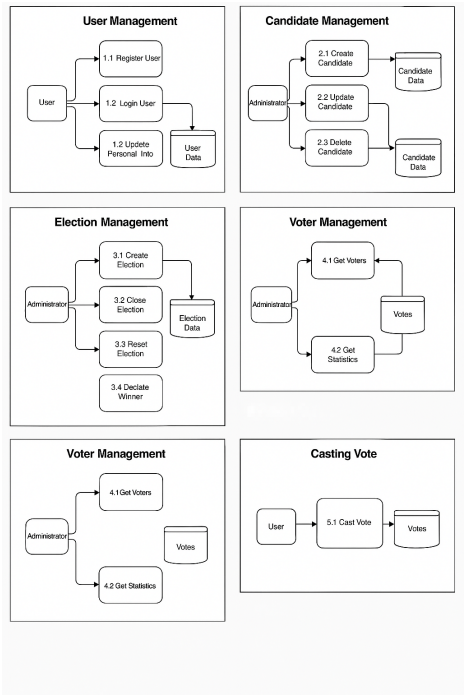



Fig. 5: Subsystem of the Voting System

The subsystem architecture depicted in Fig. 5 breaks down the system into modular components, showing how data flows between key services for tasks such as authentication, voting, and result computation.

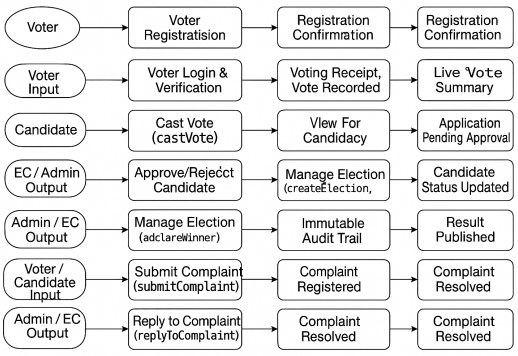



Fig. 6: Feature-wise Input/Output Diagram of the Voting System

Finally, Fig. 6 presents the system's input/output model, showing how various features respond to user inputs and generate corresponding outputs, ensuring transparency and traceability.

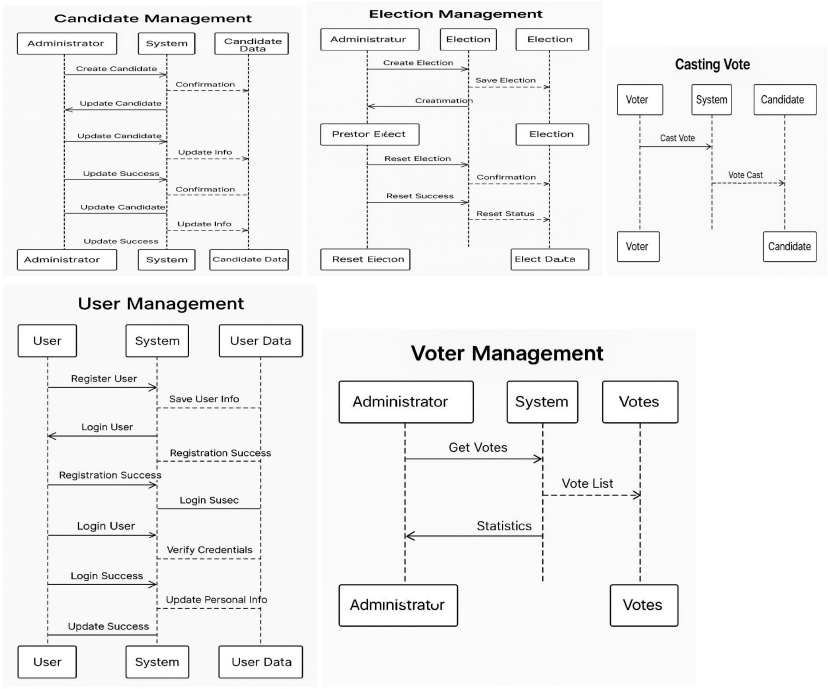



Fig. 7: Module-wise Sequence Diagram of the Voting System

The sequence diagram in Fig. 7 illustrates the time-ordered flow of messages between users and components during the voting process, including login, vote casting, and result retrieval.

To ensure robust security, the system incorporates measures to mitigate Sybil attacks and voter coercion. Sybil attacks are prevented through the use of Hyperledger Aries for issuing verifiable digital credentials to each registered voter, ensuring that only authenticated individuals with unique, blockchain-anchored identities can participate. This identity verification process prevents duplicate or fake voter entries in the network. Additionally, the system supports coercion resistance by maintaining vote secrecy through encrypted and anonymized ballots. Since the votes are cast using Zero-Knowledge Proof-compatible mechanisms and hashed identifiers, no link exists between a voter and their vote, reducing the risk of external influence or vote-buying. The system has been designed to mitigate several common security threats. To prevent double voting, each voter can cast a single vote linked to a unique verifiable credential that is validated before vote submission. Denial-of-service (DoS) attacks are mitigated through rate limiting and permissioned access control in Hyperledger Fabric. To avoid voter impersonation, identity verification is enforced via Hyperledger Aries, which issues cryptographically secure credentials to legitimate users only. These mechanisms collectively help ensure vote integrity, availability, and confidentiality throughout the election process.

## 5 Result Analysis

To evaluate the usability of the React-based dashboards, informal feedback was collected from five test users representing different roles (Admin, EC, Candidate, and Voter). The participants interacted with the system interfaces and provided feedback on layout, navigation, and feature clarity. Based on their input, minor adjustments were made to button placements, label descriptions, and dashboard responsiveness to enhance overall user experience. This preliminary feedback indicates that the UI design is intuitive and accessible, even for users with limited technical experience.

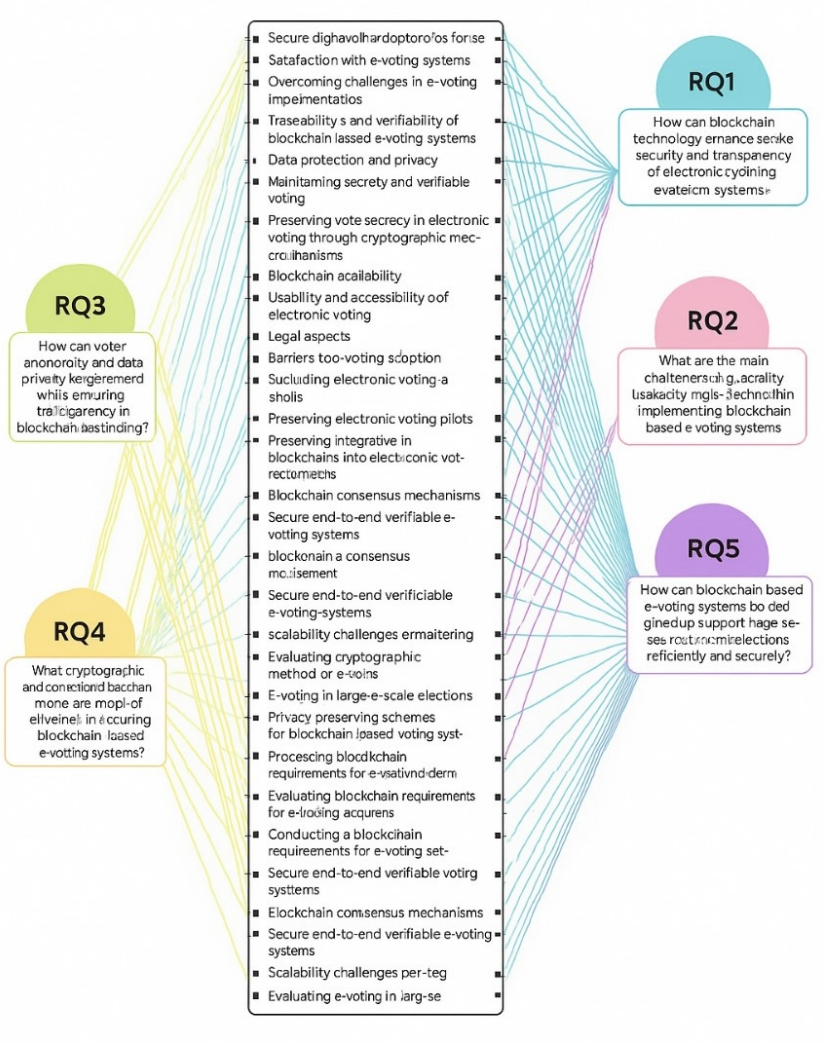



Fig. 8: Research Questions of Voting System

– According to Fig. 8 This section presents:

- Mapping between Research Questions (RQs) and proposed system features
- Comparison between existing works and our solution
- Analysis of how the proposed features address identified problems

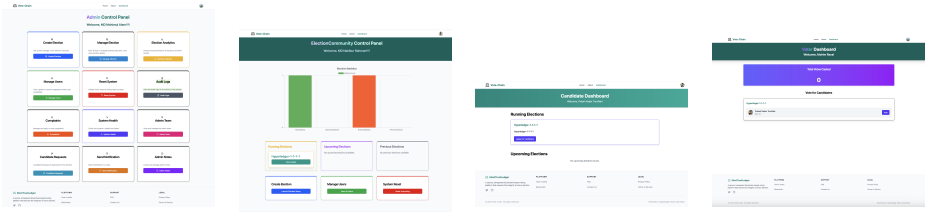
Table 1: Comparison of existing works and our system based on research questions

| **Work/System** | **RQ1: Transparency** | **RQ2: Security** | **RQ3: Accessibility** | **RQ4: Auditability** | **RQ5: Scalability** |
|---|---|---|---|---|---|
| Ali et al. [**?**] | No | Yes | No | No | No |
| SBVote et al. [19] | Yes | No | No | Yes | Yes |
| Chen et al. [5] | No | Yes | No | No | No |
| **Our System** | Yes | Yes | Yes | Yes | Yes |

### RQ vs Feature Mapping with Existing Work Comparison

**Note:** *Ali et al. (2021) corresponds to [?], representing a traditional e-voting model. SBVote (2022) is based on the scalable blockchain system proposed in [19]. Chen et al. (2024) reflects homomorphic encryption integration from [5].*

In simulated testing, the system demonstrated promising performance under varying loads. When configured with a sample network of 20 voters, the system processed approximately 20 votes per second with an average latency of 2.1 seconds per transaction. The response time remained stable even when simulating up to 30 concurrent voting requests, indicating potential scalability for small to mid-sized elections. Further stress testing and optimization would be required for national-level deployment.



(a) Admin Dashboard (b) EC Dashboard (c) Candidate Dashboard (d) Voter Dashboard

Fig. 9: User Dashboard Interfaces in the Blockchain Voting System: Admin, EC, Candidate, and Voter Panels: (a) Admin Dashboard, (b) EC Dashboard, (c) Candidate Dashboard and (d) Voter Dashboard

As shown in Fig. 9, the Admin, EC, Candidate, and Voter dashboards illustrate the primary user roles and their operational interfaces within the blockchain-based voting system.

Table 2: Comparison between Existing Systems and Our Blockchain-Based Voting System

| **Aspect** | **Existing Systems** | **Our Proposed System (via Smart Contract)** |
|---|---|---|
| **Security** | Traditional systems use centralized databases prone to breaches. [4], [6], [14]. | End-to-end security using Hyperledger Fabric with hashed credentials, encrypted vote storage, and role-based access via smart contract. |
| **Trust / Transparency** | Logs can be modified; lacks verifiable proof. [8], [14], [22]. | Immutable blockchain ledger, public verification, and audit trail through chaincode functions like `viewComplaints`, `auditLog`. |
| **Accessibility** | Often desktop/web-only with limited usability for all voters. [11] | React-based mobile-friendly frontend; role-specific dashboards (Admin, EC, Voter, Candidate). |
| **Auditability** | No unified logging; limited trace of actions. [8], [14], [22] | Chaincode logs every transaction (complaint, vote, user registration) for full traceability using `addAuditLog` and `getAuditLog`. |
| **Vote Privacy** | Voter identity often exposed or weakly masked. [5],[7], [19] | Votes encrypted and anonymized using `castVote` with hashed user IDs; ZKP-compatible if extended. |
| **Result Tallying** | Manual tallying, risk of error or manipulation. [5],[7], | Real-time, automatic result computation and winner declaration through `declareWinner` and `viewResult`. |

This study was undertaken to explore and address the critical challenges in current electronic voting systems, particularly in terms of transparency, security, accessibility, and audit-ability. The primary research question focused on whether a blockchain-based architecture could significantly improve these aspects compared to existing solutions. Through a comprehensive literature review, it was observed that while several systems attempt to solve parts of the problem, few offer a holistic solution. Our proposed system incorporates Hyperledger Fabric to ensure secure, transparent, and auditable elections with multi-role access and verifiable voter interaction.

The results demonstrate that our system effectively meets all outlined research questions. In contrast to traditional and some blockchain-based systems, our model provides end-to-end transparency, improved role-based access control,

real-time audit logs, and user-friendly access via mobile-compatible interfaces. Although the system successfully integrates blockchain and smart contract functionalities, future improvements may include:

- Integrating biometric authentication or national ID verification for stronger voter identity validation.
- Expanding the system for use in real-world pilot elections to evaluate performance and usability at scale.
- Incorporating advanced cryptographic techniques like homomorphic encryption to further enhance vote privacy.

## 6 Conclusion

In conclusion, this research has shown that blockchain technology, when properly implemented, can address longstanding concerns in electronic voting. By focusing on transparency, integrity, and inclusiveness, our system contributes a meaningful step toward trustworthy digital elections, especially for emerging democracies or large organizations requiring secure internal voting mechanisms. From a legal perspective, the proposed system can be aligned with data protection regulations such as the General Data Protection Regulation (GDPR) by design. By using Verifiable Credentials and Zero-Knowledge Proofs, the system ensures minimal data collection and secure handling of personal information, maintaining user anonymity. Additionally, the decentralized and tamper-proof nature of Hyperledger Fabric offers auditable transparency, which is essential for legal accountability. While national laws vary, the system can be adapted to comply with jurisdiction-specific requirements related to election monitoring, data retention, and voter privacy.

### Future work

While the proposed system offers a secure and transparent solution to electronic voting, there are several areas that can be explored in future development:

- Pilot the system in a real-world small-scale election, such as within a university or community, to gather real deployment feedback.

- Integrate biometric or national ID-based authentication to further strengthen voter verification.

- Enhance the user interface for better accessibility and performance on mobile devices.

- Adapt the system to comply with country-specific electoral laws and international data protection regulations (e.g., GDPR, eIDAS).

## References


1. Ab Aziz, M.J., Shukur, Z.: Blockchain for electronic voting system—review and open research challenges. Sensors **21**(17), 5874 (2021)
2. Abuidris, Y., Kumar, R., Wenyong, W.: A survey of blockchain based on e-voting systems. pp. 99–104 (12 2019). https://doi.org/10.1145/3376044.3376060
3. Aruna, S., Maheswari, M., Saranya, A.: Highly secured blockchain based electronic voting system using sha3 and merkle root. In: IOP Conference Series: Materials Science and Engineering. vol. 993, p. 012103. IOP Publishing (2020)
4. Bhavani, D.D., Gayathri, R., Bhagavanthu, M., Sheeba, A., Sampoornam, M., Bhuvaneshwari, P.: Blockchain-based voting systems enhancing transparency and security in electoral processes. In: ITM Web of Conferences. vol. 76, p. 02004. EDP Sciences (2025)
5. El Kafhali, S.: Blockchain-based electronic voting system: Significance and requirements. Mathematical Problems in Engineering **2024**(1), 5591147 (2024)
6. Fatih, R., Arezki, S., Gadi, T.: A review of blockchain-based e-voting systems: Comparative analysis and findings. International Journal of Interactive Mobile Technologies **17**(23) (2023)
7. Hajian Berenjestanaki, M., Barzegar, H.R., El Ioini, N., Pahl, C.: Blockchain-based e-voting systems: a technology review. Electronics **13**(1), 17 (2023)
8. Jafar, U., Aziz, M.J.A., Shukur, Z.: Blockchain for electronic voting system—review and open research challenges. Sensors **21**(17), 5874 (2021)
9. Mukherjee, A., Majumdar, S., Kolya, A., Nandi, S.: A privacy-preserving blockchain-based e-voting system (07 2023). https://doi.org/10.48550/arXiv.2307.08412
10. Mukherjee, A., Majumdar, S., Kolya, A.K., Nandi, S.: A privacy-preserving blockchain-based e-voting system. arXiv preprint arXiv:2307.08412 (2023)
11. Ohize, H.O., Onumanyi, A.J., Umar, B.U., Ajao, L.A., Isah, R.O., Dogo, E.M., Nuhu, B.K., Olaniyi, O.M., Ambafi, J.G., Sheidu, V.B., et al.: Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges. Cluster Computing **28**(2), 132 (2025)
12. Olaniyi, O., Dogo, E., Nuhu, B., Treiblmaier, H., Abdulsalam, Y., Folawiyo, Z.: A Secure Electronic Voting System Using Multifactor Authentication and Blockchain Technologies, pp. 41–63 (01 2022). https://doi.org/10.1007/978-3-030-89546-4_3
13. Olaniyi, O.M., Dogo, E., Nuhu, B., Treiblmaier, H., Abdulsalam, Y., Folawiyo, Z.: A secure electronic voting system using multifactor authentication and blockchain technologies. In: Blockchain Applications in the Smart Era, pp. 41–63. Springer (2022)
14. Onur, C., Yurdakul, A.: Electanon: A blockchain-based, anonymous, robust, and scalable ranked-choice voting protocol. Distributed Ledger Technologies: Research and Practice **2**(3), 1–25 (2023)
15. Ramyadevi, R., Priya, V.: Block chain-powered e-voting system: A secure and transparent solution with three-tiered otp security mechanism. In: 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT). vol. 5, pp. 728–731. IEEE (2024)
16. Shiwal, P., Morey, D., Shivankar, H., Jagtap, S., Adagale, P.: Decentralized e-voting system using blockchain. International Journal for Research in Applied Science and Engineering Technology **10**, 147–149 (12 2022). https://doi.org/10.22214/ijraset.2022.47827

17. Singh, I., Kaur, A., Agarwal, P., Idrees, S.M.: Enhancing security and transparency in online voting through blockchain decentralization. SN Computer Science **5**(7), 921 (2024)
18. Stancikova, I., Homoliak, I.: Sbvote: Scalable self-tallying blockchain-based voting. In: Proceedings of the 38th ACM/SIGAPP symposium on applied computing. pp. 203–211 (2023)
19. Stančíková, I., Homoliak, I.: Sbvote: Scalable self-tallying blockchain-based voting. In: Proceedings of the 38th ACM/SIGAPP symposium on applied computing. pp. 203–211 (2023)
20. Stančíková, I., Homoliak, I.: Sbvote: Scalable self-tallying blockchain-based voting. In: Proceedings of the 38th ACM/SIGAPP symposium on applied computing. pp. 203–211 (2023)
21. Vladucu, M.V., Dong, Z., Medina, J., Rojas-Cessa, R.: E-voting meets blockchain: A survey. IEEE Access **PP**, 1–1 (01 2023). https://doi.org/10.1109/ACCESS.2023.3253682
22. Wang, B., Guo, F., Liu, Y., Li, B., Yuan, Y.: An efficient and versatile e-voting scheme on blockchain. Cybersecurity **7**(1), 62 (2024)
23. Yuhao, H., Peng, S.: A decentralized voting system on the polygon blockchain. Procedia Computer Science **247**, 1304–1313 (2024)