

ONLINE VOTING SYSTEM USING BLOCKCHAIN

Ms. Intesar Fatima ¹, K. Guruteja ², B. Sripooja ², P. Sai Vardhan ²

¹Assistant Professor, ²UG student, ^{1,2}Department of Computer Science and
Engineering (Artificial Intelligence and Machine Learning)

^{1,2}J.B. Institute of Engineering and Technology

*Corresponding author: Ms. Intesar Fatima(fatima162903@gmail.com)

ABSTRACT

Secure, transparent, and real-time voting should be used in college and institutional elections where traditional methods are often subject to fraud, manipulation and inefficiency. To guarantee the impossibility of tampering with record keeping, this paper suggests a blockchain-based online voting system that stores voter, candidate, and election data in Ethereum smart contracts, which is impossible to alter. Ethereum-based smart contracts automate vote casting and counting, eliminating the need for manual intervention and reducing errors. To avoid impersonation and unauthorized access, voter authentication is based on a two-layer authentication process, which incorporates an OTP with email and facial recognition.

The system has strict voting windows that only allow one vote per election and allows the user to vote only during the normal hours. Some administrative features include secure voter and candidate management, election timing, real-time monitoring of the election. Although all the transactional information is stored on the blockchain, to ensure security, transparency, and auditability, face encodings are stored locally, to ensure the privacy of users. This can fit academic institutions and organizational voting situations because it is a seamless integration of online accessibility and verification of the identity. Scalable and secure institutional election processes are confirmed to be effective through experimentation results which demonstrate reliable authentication, valid vote counting, and timely results monitoring.

The proposed system enhances accessibility by allowing students to vote remotely while maintaining high security standards. It also

improves efficiency by providing instant and accurate results. Overall, this solution offers a reliable, secure, and user-friendly platform for conducting institutional elections, addressing the limitations of traditional voting methods

Keywords: Blockchain, e-voting, Ethereum, facial recognition, OTP, real-time elections, secure authentication, election transparency.

1.INTRODUCTION

College and institutional decision making processes cannot be done without elections since they ensure that the elected people are elected in a fair and legitimate way. They have to be trusted by the participants, and they should be correct and truthful. The common methods of voting are paper-based ballots and centralized electronic systems, which have some disadvantages: human error, tampering, slow processing of results and limited auditability reducing trust in the outcome of elections. The flaws of the traditional voting systems have become even more evident as the groups adopt the digital technologies in their administrative operations. Consequently, there is growing need to have safe and convenient voting processes that are both integrity and accessibly available to everyone involved.

Blockchain technology has demonstrated the ability to overcome these problems by decentralizing and protecting the process of voting. Its distributed ledger helps to keep the voting records in an unchangeable and tamper-resistant manner. The fact that all the transactions made in the voting process can be verified and checked makes this feature very effective in enhancing accountability and transparency. Consequently, it enhances trust, transparency, security in college / institutional

election processes among the players and administrators.

Security and privacy are vital issues that any voting system should consider especially in the online systems where cyber attacks are prevalent. Blockchain-based systems secure the privacy of voting information through cryptographic means without anonymity of the voter. These systems effectively prevent impersonation, duplicate voting and unwanted access when used in conjunction with modern authentication methods such as biometric verification and OTP to enhance election integrity.

Also, voting systems on blockchain make the process more inclusive and efficient within institutions. Those enable voters to vote without losing the sense of security and reliability as they encourage both in-person and internet-based voting. Moreover, the real-time completion of the administrative tasks like voter monitoring, elections preparation, and calculation of the results reduce the number of manual interactions and delays.

This change enhances the flexibility of the voting process as well as the transparency of voting and the utilization of resources is optimized.

The aim of the project is to develop an online voting system, which is secure, open, and reliable to be used in institutions, which will result in more users feeling safe and involved. The solution will ensure voter anonymity, prevent fraud, and can monitor results quickly by integrating blockchain technology and rigorous identity verification processes. Ultimately, this plan enhances organizational governance and decision-making through encouraging more effective and dependable institutional elections.

2. LITERATURE SURVEY

Verma described a decentralized and blockchain-based secure voting system that reduces the likelihood of fraud and point-of-failure. The paper demonstrated how distributed ledgers are capable of enhancing the integrity of the vote through ensuring that the

ballots are verifiable and cannot be changed. Meanwhile, the privacy of voters is ensured through the cryptography that enhances confidence in computerized voting situations. Salman and Al-Janabi reviewed all the models of vote based on blockchain and discussed the advantages and disadvantages regarding transparency, scale and privacy. They found out that blockchain-based strategies increase trust significantly as opposed to controlled systems. They however indicated that there were performance issues and the inclusion of them in the existing voting systems.

The discussion by Kho, Heng, and Chin was largely based on cryptographic electronic voting. They discussed the privacy of voters and polls that is ensured through encryption, digital signatures, and keeping of keys. They also talked about the application of the decentralized ledger technologies and the significance of strong cryptographic primitives in the construction of secure voting systems in their review. In their study on the opportunities of the distributed blockchain technology to be used in the voting settings, Sahib and Al-Shamery highlight the importance of consensus methods to ensure that the change of votes cannot be made without authorization. However, based on their findings, decentralization enables voting systems to be resilient to both internal and external attack on the system by enhancing transparency and tolerance to mistakes.

Sabharwal and his colleagues analyzed the differences and similarities of various blockchain methods of electronic voting. In their performance evaluation and analysis of security assurances and complexity of implementation, they provide different trade-offs between scalability and transparency, based on the election requirements, according to the permitted and public blockchain models. The interest of Singh, Wable, and Kharose was the effectiveness of the voting systems based on blockchain and the percentage of voter trust in them. They discovered that blockchain removes the aspect of centralised governments and inspections done manually. They were however also concerned with scalability, network latency and transaction costs.

Huang and his associates have critically discussed the use of blockchain technology in the voting system. They put into consideration privacy-saving solutions, security objectives, and design principles. The most important advantages they have discussed are end-to-end verifiability and auditability, in which blockchain can address the long-standing issues of digital voting and guarantee the voter trust. Marath headed a group of scholars that researched the digital voting system on the cloud and blockchain. They demanded that they ensure that they have votes that are safely stamped and verified. They concluded in their study that the combination of enabling infrastructures with distributed ledgers enhances availability, as well as integrity of data, but it creates coordination and system reliability issues.

Considering blockchain-based voting systems, Majeed paid attention to such aspects as trust, anonymity, and the challenge of hacking. Impossibility of alteration of records and decentralization of evidence makes cheating very hard as has been pointed out in this paper. Nevertheless, it also shed light on some issues, which were how to implement the system and obtain the consent of regulators during the actual elections. Diaconita, Belciu, and Stoica in their article proposed a blockchain-based system that is based on trust, and the citizens may vote in public areas and preserve their privacy. Their endeavor showed how clever procedures and cryptographic security may reconcile transparency and voter privacy. This demonstrated that it is possible to conduct elections with the help of the technology of blockchain and generated confidence in the voting on the Internet.

3. PROPOSED SYSTEM

The proposed solution provides a blockchain-based voting mechanism that is not at the expense of security, lacks transparency, and lacks trust, allowing to participate in college and institutional elections safely through the online and physical platforms. It employs email-based OTP and facial recognition in the two-tier authentication, which ensures only qualified voters vote and eliminate repeat

voting. To ensure that the governance is executed and the elections are managed effectively, the administrators will receive a safe interface to control the voter registration, candidate lists, election schedule, and the activation controls. Voter privacy is ensured and votes, other election-related information are stored on Ethereum blockchain that ensures immutability, easy verification, and non-tampering.

The system has a mechanism that only allows a single ballot to be cast by a particular voter in an election and puts strict time restrictions on voting. To reduce the number of human contacts and optimize the work process, the election results are automatically recalculated. The solution aims to enhance both accessibility and election integrity and confidence in institutional digital voting operations by combining biometric authentication with decentralized ledger technology.

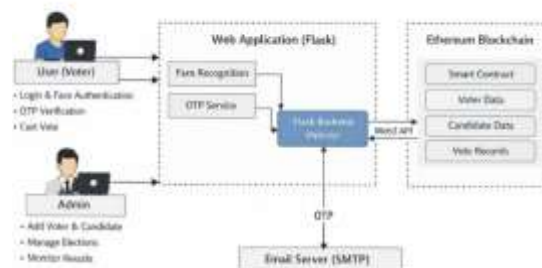


Figure 1: Proposed Architecture

Figure 1 presents the architecture of an online voting system based on the blockchain that is aimed at the institutional and college elections. The voters are capable of authenticating through OTP verification and facial recognition through a Flask-based web application. The backend communicates with the Ethereum blockchain via the Web3 API to store voter credentials and vote data in an unchangeable manner, to ensure their safety. The administrators are in charge of all the operations of an election including scheduling, management of candidates and voter registration. The transparency and efficiency is guaranteed.

3.1 Authentication and Registration Workflow:

In ensuring that authorized users are the only ones who can access the institutional online voting platform, the process begins with orderly authentication and registration system. The credentials are applied to protect administrative access, which allows a limited number of operations, such as election setup and voter registration.

The personal data is collected, checked against uniqueness, and securely stored when registering voters. Facial data is recorded in the process of biometric registration and stored in the local memory to be used in further verification whilst ensuring privacy. User credentials are verified at the time of logging in and this is followed by real-time facial recognition whereby the acquired facial data is compared with the stored records. There is an OTP verification done through email within a set time to enhance security.

This multi-layered authentication process ensures that each of the participants can be uniquely recognized, impersonation is minimized, and unauthorized entry is prevented. To eliminate any residual data reached after authentication has been done, session management systems eliminate any residual data so as to evade conflicts and maintain secure and reliable access.

3.2 Election Management and Control Process:

The institutional elections are ensured by the systematic and systematic election administration process in terms of fairness and operational integrity. Administrators define election elements such as title, duration and operating status.

Validation procedures ensure that a single election is running at a time and are not scheduled to collide. In order to make sure that the candidates and parties are ready to take part, their details are enrolled prior to the activation of the election. Once activated, the election enters into a monitored state and the voter turnout can be tracked in real time. Depending on the time, voting is only allowed within this

time; any attempt to turn up after this period is automatically rejected. It is switched off and the computation of the results starts upon election being complete.

Administrative dashboards do not reveal any particular voting preferences, but they provide such facts as voter turnout and election status. This structured control system ensures proper sequencing, timing of elections, equity and effective monitoring of the election process.

3.3 Vote Casting and Blockchain Recording:

The voting process is supposed to ensure verifiability, security and transparency. Participants are presented with a list of candidates in the current institutional election once the identity of the voter has been confirmed.

Besides checking the eligibility and election status of the voters, the technology ensures that the voter has not submitted a vote. The selected alternative is converted into a blockchain transaction and a record is placed on the distributed ledger when the vote is submitted. This makes sure that the votes recorded are not manipulated or deleted and they are not mutable. Duplication of voting is also prevented before submission of transactions through the inbuilt validation processes.

The storage offered by blockchain is decentralized, so the centralization of the systems is not required, reducing the risk of loss or manipulation of data. Voter identities are also secured but all votes can be verified which ensures privacy and enhances systemic trust.

3.4 Result Computation and Dissemination:

Once the voting process is completed the system automatically initiates the result computing process. Vote data is obtained in the blockchain, in which all the transactions have already been verified and stored in a secure location.

This ensures that results are immutable and eliminates the use of human intervention. The votes of each candidate are accurately tabulated and therefore provide reliable and consistent results. With secured dashboards, administrators would be able to access detailed

reports on the outcomes that would include the number of votes and successful candidates.

The automated process reduces the number of mistakes, minimizes the number of time wastes, and enhances the trust in the outcome. The technology ensures quick, precise and irreversible results through the use of blockchain database.

4. RESULTS & DISCUSSIONS

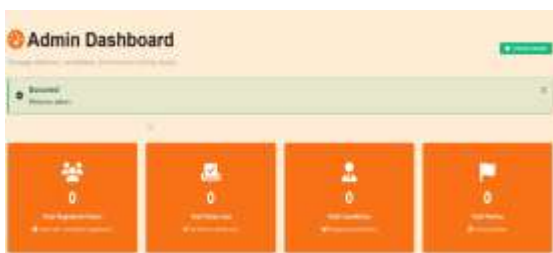


Fig.2 Admin Dashboard

As part of the institutional e-voting solution, the Admin Dashboard (Fig. 2) provides real-time information on voters, candidates, and blockchain-verified votes.



Fig.3 Add Candidate

Figure 3 shows the backend interface of adding a candidate with such information as name, party, and department/area.



Fig.4 Candidate List

The candidates who are running in the institutional election are displayed on a list posted on the screen in Figure 4.



Fig.5 Add Voter

Figure 5 displays the Add Voter form, that the administrators use to add new users to the electronic voting system.



Fig.6 Voter List

Figure 6 demonstrates the voter management interface where the details of all the registered voters in the system can be seen.



Fig.7 Create New Election

Figure 7 is the interface that the administrators use to configure and initiate a new institutional election.



Fig.10 Election Countdown

Figure 10 presents a real-time countdown timer on the remaining time of the ongoing institutional election.



Fig.8 User Dashboard

Figure 8 demonstrates the user interface that will enable the participants to track the election information and to get access to secure voting options.



Fig.11 Election Results

Figure 11 illustrates the final election results of each candidate and it has been verified and recorded on the blockchain to ensure integrity and transparency.



Fig.9 Cast Vote

The voting interface as identified in Figure 9 enables authorized users to vote securely and cast their ballots.

5. CONCLUSION

The developed blockchain-based online voting system by combining web-based accessibility with identification verification displays a secure, transparent, and live approach to conducting college and institutional elections. The Ethereum smart contracts ensure the unreliability of voter, candidate, and election data, and no one can make changes to it without authorization, which ensures reliable audit trails. Dual-layer authentication with email-based OTP and facial recognition is effective in reducing the risks of impersonation and duplicate voting by making a participant have one vote per time frame.

Administrative features help in making election management easier, including the monitoring of voter turnout and automated calculation of results.

Whereas blockchain is used to store data with integrity and transparency, biometric data is stored locally to secure the privacy of the user. The results of the experiment prove the reliability and scalability of the system in the institutional contexts ensuring the accuracy of voter identification, the smoothness of vote casting, and the consistency of results. Altogether, blockchain technology and biometric and OTP-based identification to address the challenges of security, transparency, and fraud prevention and enable efficient and reliable digital and hybrid voting processes meet the key goals.

Further future modifications might focus on making the system more accessible, scaled and interoperable with institutional installations. Authorized blockchain adoption may enhance latency and performance. Examples of advanced biometrics that may enhance authentication are iris and voice recognition.

The accessibility can be enhanced by supporting decentralized applications (dApps) and mobile devices to provide access to more distant users. Two additional privacy-protective techniques that may enhance the reliability of the system and data security are stronger administrative security and zero-knowledge proofs.

6. REFERENCES

- [1] Ohize, H. O., Onumanyi, A. J., Umar, B. U., Ajao, L. A., Isah, R. O., Dogo, E. M., ... & Ibrahim, M. M. (2025). Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges. *Cluster Computing*, 28(2), 132.
- [2] Subah, Z., Rozario, S., Islam, N., & Amir, S. A. B. (2022, March). Blockchain Technology Integrated Electronic Vote Casting System. In *Proceedings of the 2nd International Conference on Computing Advancements* (pp. 133-137).
- [3] Marian, C. V., Mitrea, D. A., Rusu, D. S., & Vasilateanu, A. (2025). Transparent digital governance: A blockchain-based workflow audit application. *Applied Sciences*, 15(21), 11694.
- [4] Braz, B. F. (2021). A proposal for the use of blockchain in the portuguese voting system (Master's thesis, Universidade NOVA de Lisboa (Portugal)).
- [5] Hammad, A. A. (2025). Blockchain Technology for Secure Data Sharing. *Al-Furat Journal of Innovations in Electronics and Computer Engineering*, 4(1), 120-140.
- [6] Ikrissi, G., Mazri, T.: *Electronic Voting: Review and Challenges*, pp. 110–119. Springer, Cham (2024).
- [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] Geng, T., Njilla, L., Huang, C.-T.: *A survey of blockchain-based electronic voting mechanisms in sensor networks*. In: *Proceedings of the 20th ACM Conference on Embedded Networked Sensor Systems*. SenSys '22, pp. 1222–1228. Association for Computing Machinery, New York, NY, USA (2023).
- [9] Viji, D.C., Kumar, A., Noorayen, A., Amjad, H., Abrar, M.: *Blockchain voting: a comparative analysis*. *Int. J. Res. Appl. Sci. Eng. Technol.* 10(3), 1886–1890 (2022).
- [10] Varaprasada Rao, K., Panda, S.K.: *Secure electronic voting (e-voting) system based on blockchain on various platforms*. In: *Computer Communication, Networking and IoT: Proceedings of 5th ICICC 2021*, vol. 2, pp. 143–151. Springer (2022).
- [11] Verma, G.: *A secure framework for e-voting using blockchain*. In: *2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA)*, pp. 1–5. IEEE (2022).
- [12] Salman, S.A.-B., Al-Janabi, S., Sagheer, A.M.: *A review on e-voting based on blockchain models*. *Iraqi J. Sci.* (2022).

- [13] Kho, Y.-X., Heng, S.-H., Chin, J.-J.: A review of cryptographic electronic voting. *Symmetry* 14(5), 858 (2022).
- [14] Sahib, R.H., Al-Shamery, E.S.: A review on distributed blockchain technology for e-voting systems. *J. Phys. Conf. Ser.* 1804, 012050 (2021).
- [15] Sabharwal, A., Saifullah, M., Grover, P., Batra, N.: Comparative study of blockchain techniques in electronic voting. *System* (2021).
- [16] Singh, S., Wable, S., Kharose, P.: A review of e-voting system based on blockchain technology. *Int. J. New Pract. Manag. Eng.* 10(04), 09–13 (2021).
- [17] Huang, J., He, D., Obaidat, M.S., Vijayakumar, P., Luo, M., Choo, K.-K.R.: The application of the blockchain technology in voting systems: a review. *ACM Comput. Surv. (CSUR)* 54(3), 1–28 (2021).
- [18] Marath, R., Sachin, C., Sanjay, S., Sagar, D., Annigeri, S.F., Abhinav, R., Bangalore, D.: A review on e-stamping in digital voting system using block chain and cloud server. *Int. J. Inno. Sci. Res. Tech.* 8(1), 1851–1855 (2023).
- [19] Majeed, N.A.: Review on blockchain based e-voting systems. *Konferenzband zum Scientific Track der Blockchain Autumn School 2021(004)*, 001–008 (2021)
- [20] Diaconita, V., Belciu, A., Stoica, M.G.: Trustful blockchain-based framework for privacy enabling voting in a university. *J. Theor. Appl. Electron. Commer. Res.* 18(1), 150–169 (2023).
- [21] Baudier, P., Kondrateva, G., Ammi, C., Seulliet, E.: Peace engineering: the contribution of blockchain systems to the e-voting process. *Technol. Forecast. Soc. Change* 162, 120397 (2021).
- [22] Gupta, S., Gupta, A., Pandya, I.Y., Bhatt, A., Mehta, K.: End to end secure e-voting using blockchain & quantum key distribution. *Mater. Today: Proc.* 80, 3363–3370 (2023).
- [23] Jafar, U., Aziz, M.J.A., Shukur, Z.: Blockchain for electronic voting system-review and open research challenges. *Sensors* 21(17), 5874 (2021).
- [24] Panja, S., Roy, B.: A Secure End-to-End Verifiable E-Voting System Using Zero-Knowledge Proof and Blockchain. Springer, Singapore (2021).
- [25] Faruk, M.J.H., Alam, F., Islam, M., Rahman, A.: Transforming online voting: a novel system utilizing blockchain and biometric verification for enhanced security, privacy, and transparency. *Clust. Comput.* (2024).