IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN:2349-2163
Volume 13, Issue 04, April https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2026.v1304.06

Secure and Transparent E-Voting System Using Block chain, Smart Contracts, Differential Privacy & Email-Based Voter Authentication

Illendula Sai Krishna
Assistant Professor, Department of CSE
Guru Nanak Institute of Technology, Hyderabad, India
saikrishnai.csegnit@gniindia
https://orcid.org/0009-0007-4764-1082
Bandari Vasanth,Balineni Nanda Sai,Bilakanti Mohan
UG Student, Department of CSE,
Guru Nanak Institute of Technology, Hyderabad, India
orgvasanthbandari7@gmail.com, nandasaibalineni@gmail.com,Mohanbillakanti911@gmail.com

Publication History
Manuscript Reference No: IJIRAE/RS/Vol.13/Issue04/AEAP26.APAE10085
Research Article | Open Access | Double-Blind Peer-Reviewed| Article ID: IJIRAE/RS/Vol.13/Issue04/AEAP26.APAE10185
Received:02,March 2026, Revised: 29, March 2026, Accepted: 10,April 2026,Published Online: 22, April 2026.
https://www.ijirae.com/volumes/Vol13/iss-04/06.AEAP26.APAE10085.pdf
Article Citation:Illendula,Bandari,Balineni,Bilakanti(2026),Secure and Transparent E-Voting System Using Block chain, Smart Contracts, Differential Privacy & Email-Based Voter Authentication,IJIRAE: International Journal of Innovative Research in Advanced Engineering, Volume 13, Issue 04 of 2026 pages 766-771
Doi:> https://doi.org/10.26562/ijirae.2026.v1304.06 **BibTeX Key: Illendula@2026Secure**
IJIRAE papers should be cited as IJIRAE (International Journal of Innovative Research in Advanced Engineering, AM Publications, India 2025, ISSN 2349-2163, https://doi.org/10.26562/ijirae.2026.v1304.06 The journal's official abbreviation is IJIRAE. Orcid: https://orcid.org/0009-0004-9398-7488

Abstract: Electronic voting is an important part of modern democratic systems that helps keep things open and honest. Traditional voting methods depend a lot on manual processes, which can take a long time, be prone to mistakes, be unsafe, and not be very clear. This paper discusses an e-voting system based on blockchain that uses smart contracts, Differential Privacy, and Self-Sovereign Identity (SSI) to make voting safer, more private, and more reliable. Blockchain technology makes sure that votes are stored in a way that can't be changed and that they can be easily verified. Smart contracts automate the process of checking who voted, casting a vote, and counting the votes. To keep voters' identities secret, Differential Privacy is used. To keep user authentication safe, decentralized identity management techniques are used. Putting these technologies together makes the system work better and more reliably. Compared to traditional voting systems, experimental results show that this one is more accurate, has less lag time, and can handle more users. The BP-Vot system that has been suggested is a reliable and effective way to hold secure and open digital elections.
Keywords: Blockchain, E-Voting, Smart Contracts, Differential Privacy, Self-Sovereign Identity (SSI), Security, Privacy, Decentralization

I. INTRODUCTION

Electronic voting systems are a necessary part of modern democracies because they need safe and dependable ways to hold elections. A lot of people still use traditional voting systems, but they often have problems like being hard to understand, costing too much to run, and being open to fraud and mistakes. Handling ballots by hand and having a central authority make the process take longer and be less efficient, especially in big elections. Recent improvements in blockchain technology have made it possible to create safe and decentralized e-voting systems. Blockchain makes sure that data storage is secure, that transactions are clear, and that transactions can be verified by many people. But just using blockchain might not be enough to solve problems like protecting voter privacy, managing identities, and making the system run faster. To make sure that authentication is safe and to protect private voter information, more methods are needed.

II. LITERATURE SURVEY

M.Hossain and T.Alam (2025) suggested a blockchain voting system that uses differential privacy to find a balance between privacy and openness. The system makes sure that votes are sent safely, stops people from voting twice, and lets people check the results in real time. Got better latency and accuracy than older systems. Strong relevance: combines privacy, performance, and scalability; works well in the real world.

S.Mehta and D.Patel (2024) created a hybrid blockchain-based e-voting system with multi-factor authentication to make it safer and more open. The system uses encryption and safe authentication methods to keep people from getting in without permission. Achieved better security and less fraud. Relevance: good for authentication and security, but not so good for performance optimization. **Park,J.&Nguyen,H.(2023)** Decentralized voting system via SSI and verifiable credential for secure user authentication. Improved security and identity verification.

This decentralized identity management scheme makes user data control more effective by eliminating the need for central identity providers. Practical use: extremely practical but poses challenges with regard to system integration.

R.Kumar & S.Verma (2023) suggested an e-voting system using blockchain technology which incorporated homomorphic encryption techniques to conduct computations on votes in a safe and anonymous manner. It ensures that the votes can be counted without knowing each voter's decision, thus achieving full anonymity of voters. The automated process for voting through smart contracts includes voter authentication, casting votes, and counting results. Gained better security and efficiency in vote calculations. Highly relevant: applies encryption methods along with blockchain to ensure higher privacy and automation but with high computational cost.

III. METHODOLOGY

The proposed system uses a secure e-voting method based on blockchain. The workflow includes voter registration, authentication, casting votes, and calculating results using decentralized technologies.

A. Data Collection: The system captures the details of users such as the voter ID, username, and credentials during the registration process. The election data, such as the candidate details and the voting information, are also captured by the database.

B. Data Preprocessing: User input data is checked and formatted correctly, with passwords being encrypted for added security and validations done to prevent duplicate entries in the database.

C. User Authentication: The system implements secure methods of authenticating the identity of voters, with login credentials and token verification methods used to confirm authorized users of the voting platform.

D. Blockchain Vote Storing: Votes will be captured and stored in the database using the blockchain technology to prevent any form of manipulation and make them tamper-proof.

E. Privacy Protection: Methods such as encryption and Differential Privacy will be employed to protect the privacy and anonymity of voters, ensuring that their identities remain confidential.

F. Smart Contracts: Voting will be automated through the use of smart contracts which will help in validating votes and computing results.

G. Result Computation: Votes are counted automatically using secure aggregation methods. The results are generated in real-time and displayed to the admin in a transparent and accurate manner.

IV. SYSTEM ARCHITECTURE

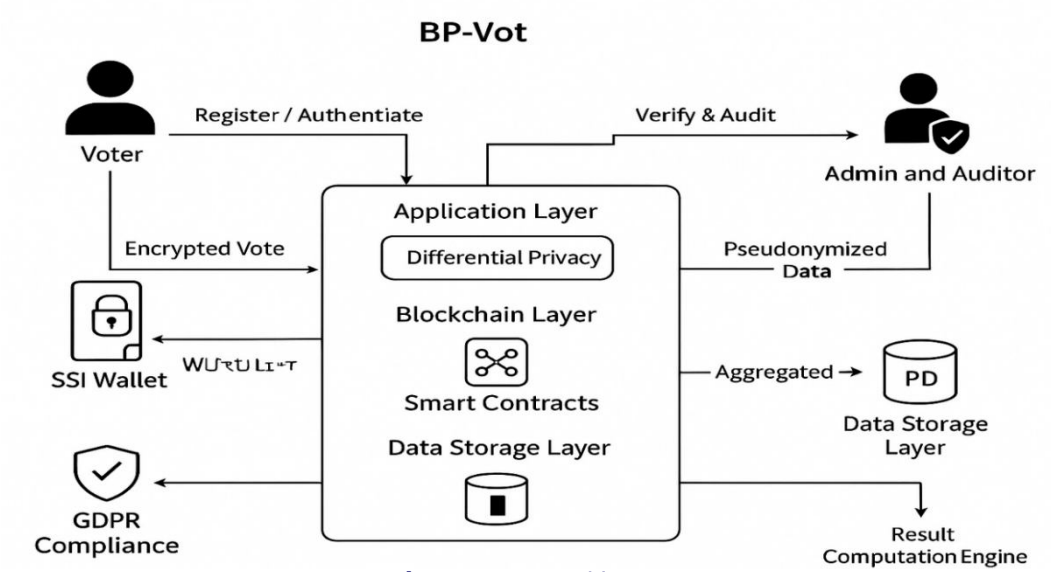

Fig 1: System Architecture

V. IMPLEMENTATION

The implementation process of the suggested system takes place through a secure e-voting framework based on blockchain technology. This means that the use of decentralized databases, secure authentication and automatic vote counting is involved in the process to ensure the reliability of the election process. The architecture splits the system into various modules, including user management, authentication, voting process, and results. This division ensures that the software is scalable, modular, and highly performant. Blockchain technology is used for storing all transactions done during voting to prevent any manipulation and unauthorized access. Smart contracts are deployed for automating critical operations like vote verification and calculation of voting results. The architecture also allows the use of voting processes and the processing of big data in election activities. It allows for smooth integration between the front end and back end of the system (designed using Java, JSP, and Servlets) and the MySQL database. On the whole, the system creates a secure and efficient platform for conducting electronic elections.

Existing System

Current voting systems depend mostly on conventional voting procedures that make use of conventional methods of ballots and voting or e-voting systems, which are centralized databases that store voting information.

In conventional systems, voters participate through physical voting procedures like distributing ballot papers, casting votes, and counting the votes cast, which are slow and subject to human error. Centralized e-voting systems have weak security features since most of these systems are database-driven, making it easy for any party with malicious intent to manipulate the voting system. These systems can be compromised in terms of unauthorized access, data tampering, and even a single point of failure, which is due to centralized administration. Current systems fail to provide adequate privacy protection to the voters and also cannot prevent fraudulent voting.

Proposed System

The suggested design proposes an electronic voting system framework using the blockchain concept to authenticate users, provide data storage capabilities, and ensure privacy protection features during the voting process. The proposed framework will use blockchain technology to store votes as unalterable transaction records and integrate the use of smart contracts to verify users, cast votes, and tally results. The combination of these components will ensure the integrity of the data stored and prevent any form of manipulation or tampering within the framework. The architecture is designed in a modular fashion to facilitate user management, authentication, voting process, and result analysis tasks independently. The design also incorporates security features such as encryption and Differential Privacy to maintain the anonymity of voters.

VI. RESULTS

LOGIN PAGE

Fig 1: Login Page

This is the main homepage of the entire system, which serves to introduce the whole secure e-voting system. The importance of maintaining transparency, security, and reliability in the process by adopting blockchain technology is emphasized in this homepage. There are two options available here for differentiating between voters and administrators. This page has a very simple interface.

REGISTRATION PAGE

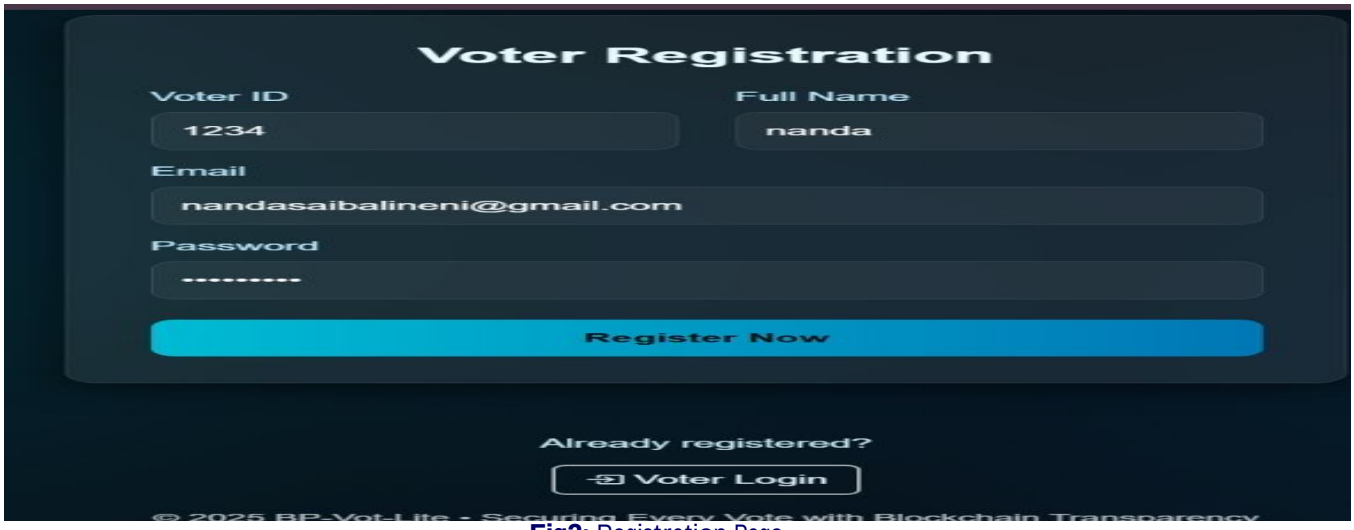

Fig2: Registration Page

The current section highlights voter registration, where users can register themselves by providing their details such as Voter ID number, full name, email address, and password. The purpose is to keep all data safe and validated for accuracy and duplicacy. This section is the easiest part to follow.

ADMIN PAGE

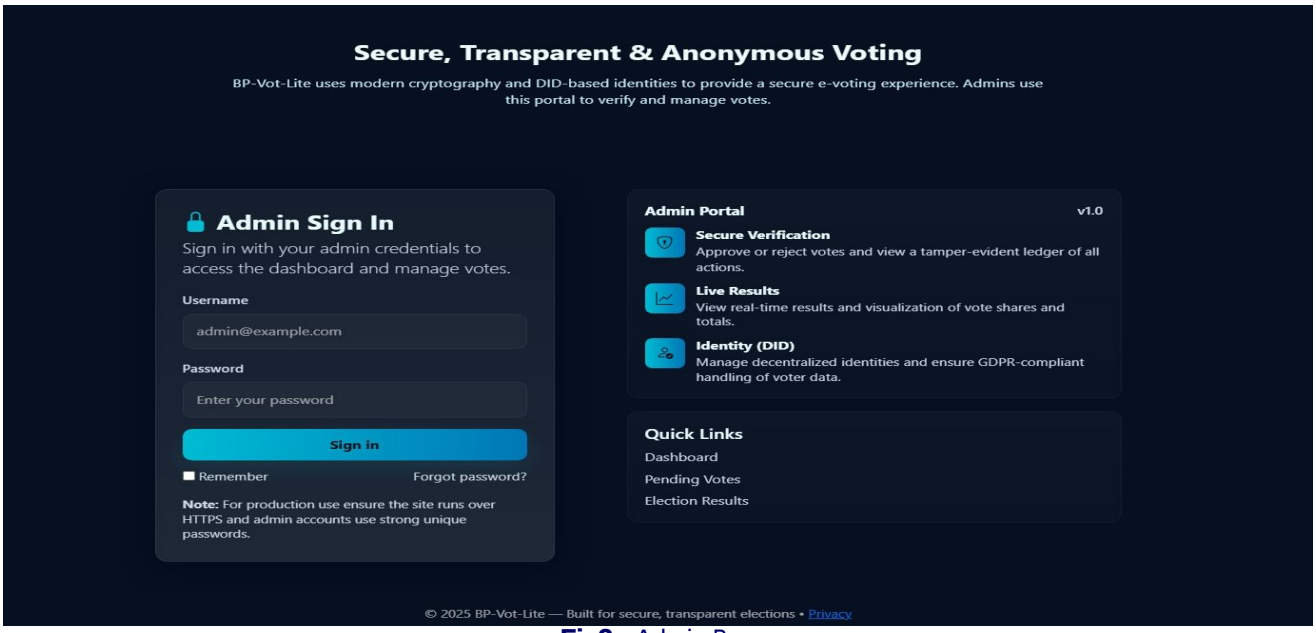

Fig3 : Admin Page

The module is responsible for handling the logging and managing of admins in the system, giving the logged-in admins secure access to the system. Admins can be able to monitor and keep track of voting processes, verifying voters and tracking results.

ADMIN DASHBOARD

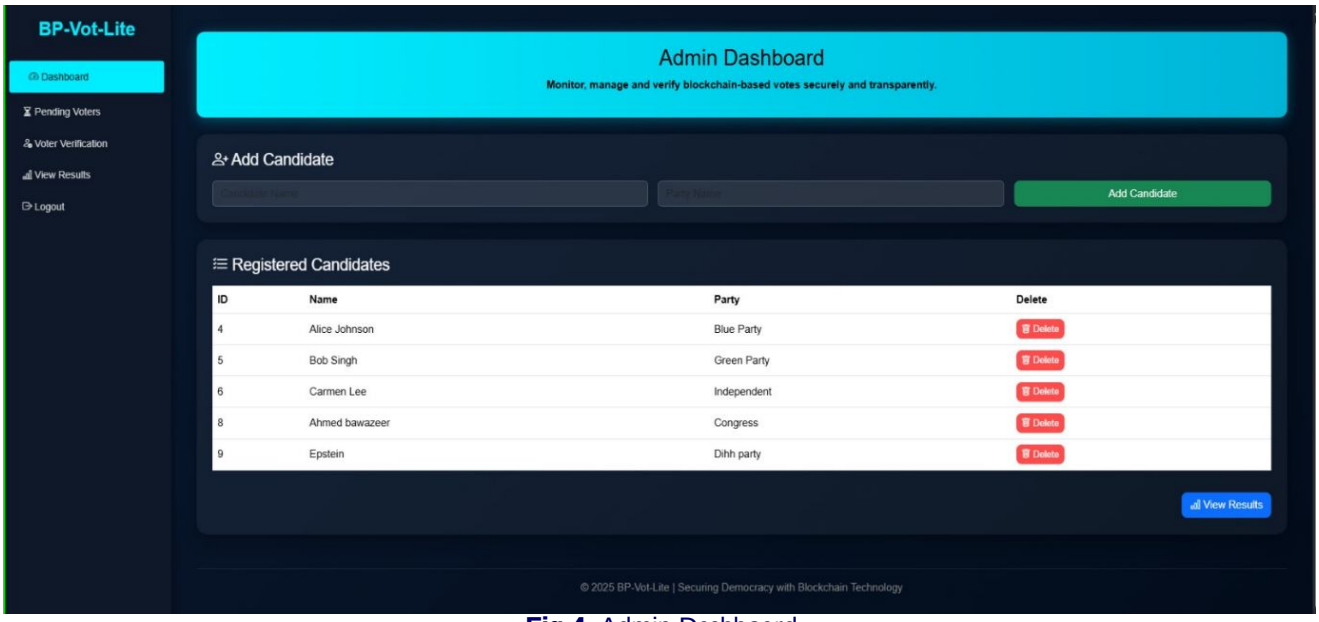

Fig 4: Admin Dashboard

This part constitutes the administrator interface, which serves as an easy platform for managing the entire voting process. The administrators will be able to add, view, and delete candidates from here while keeping track of all activities related to elections.

ADMIN APPROVAL

This is the part that shows the list of the users who have registered to vote but are waiting for admin approval. It gives the admin the opportunity to verify the voter information such as the ID number, name, and email address. Every entry contains the status of the user as well as the date and time of registration. This is the user login module, which helps registered users log into the system with the use of their email addresses and passwords. This ensures that only authorized users are able to access the application. In general, the module makes sure that the login process is easy for the voters.This module represents the voting interface where authenticated users can cast their votes by selecting their preferred candidate. It displays candidates and their details clearly, ensuring a simple and user-friendly voting process. Overall, it provides a secure and transparent environment for recording votes accurately. This module serves as the voting verification part, which appears right after an individual manages to cast their vote. The verification message is clearly indicated alongside some basic information about the voter. On the whole, it is reassuring for the voters that their votes have been properly recorded.

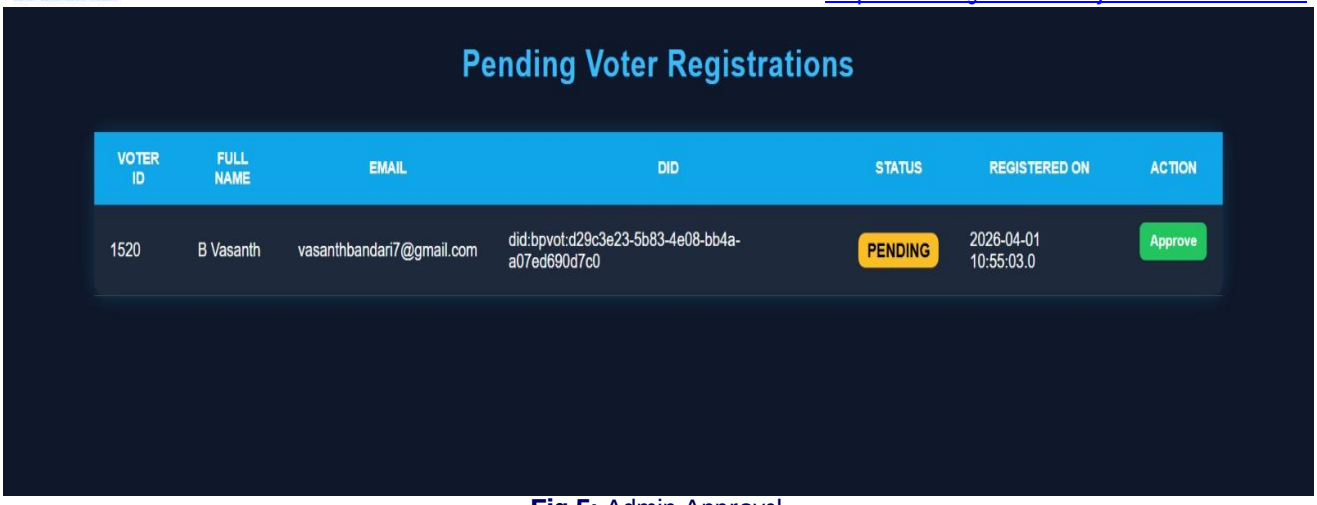

Fig 5: Admin Approval

USER LOGIN PAGE

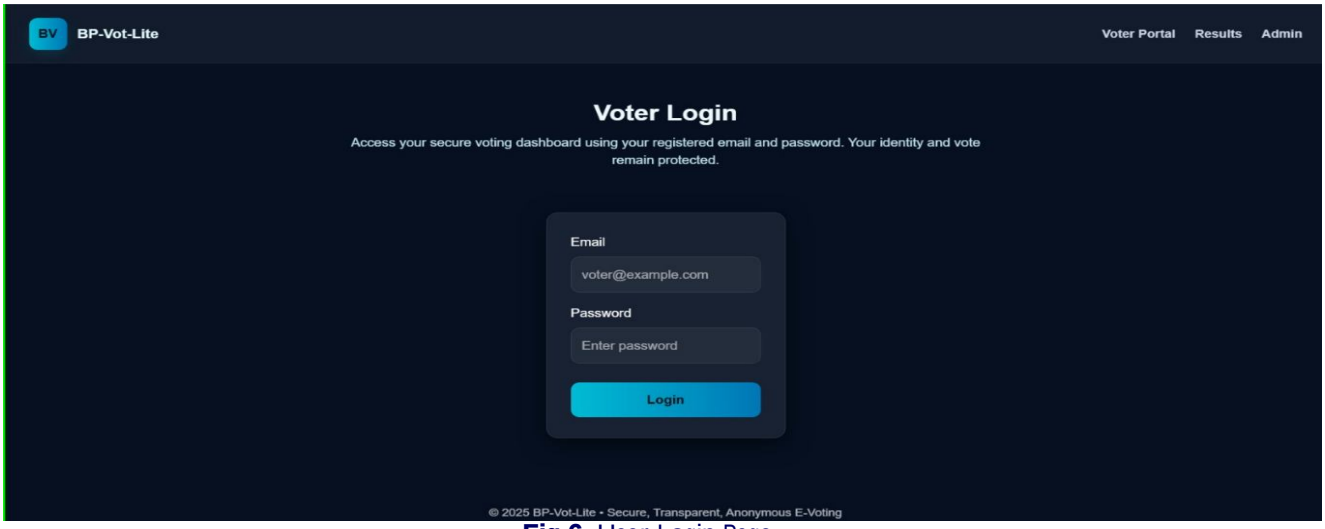

Fig 6: User Login Page

VOTE CASTING PAGE

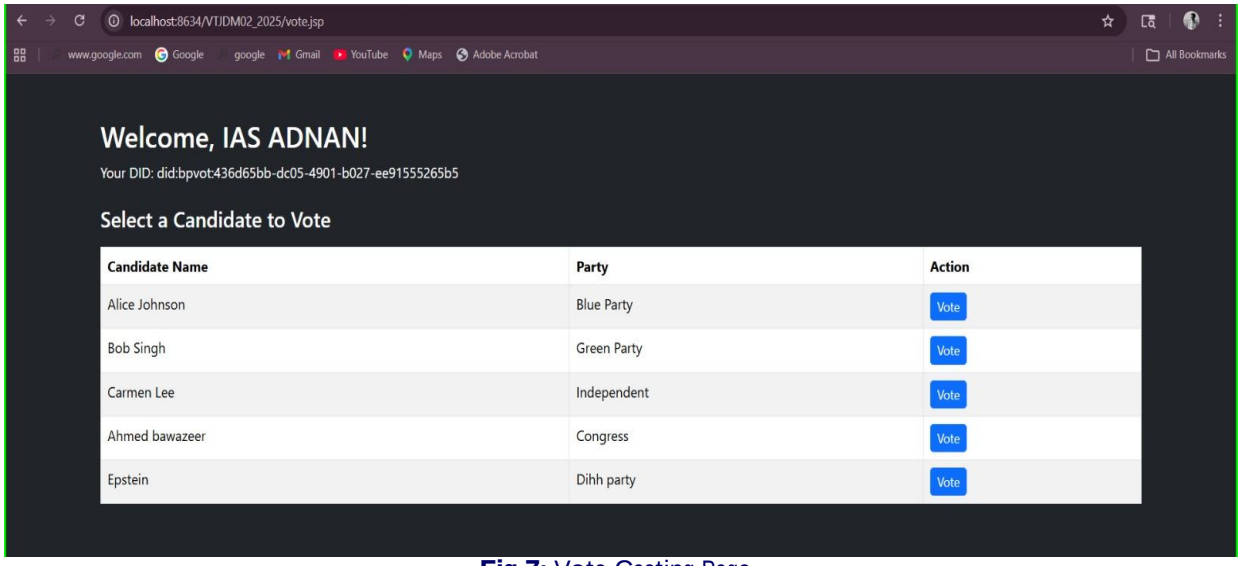

Fig 7: Vote Casting Page

VII. CONCLUSION

The proposed system for secure electronic voting using blockchain technology provides an effective and reliable solution for modern digital elections. By integrating decentralized storage, smart contracts, and privacy-preserving techniques, the system ensures transparency, security, and data integrity compared to traditional voting methods. The use of blockchain enables tamper-proof vote recording and prevents unauthorized modifications, while smart contracts automate key processes such as voter authentication, vote casting, and result computation.

VOTE CONFIRMATION PAGE

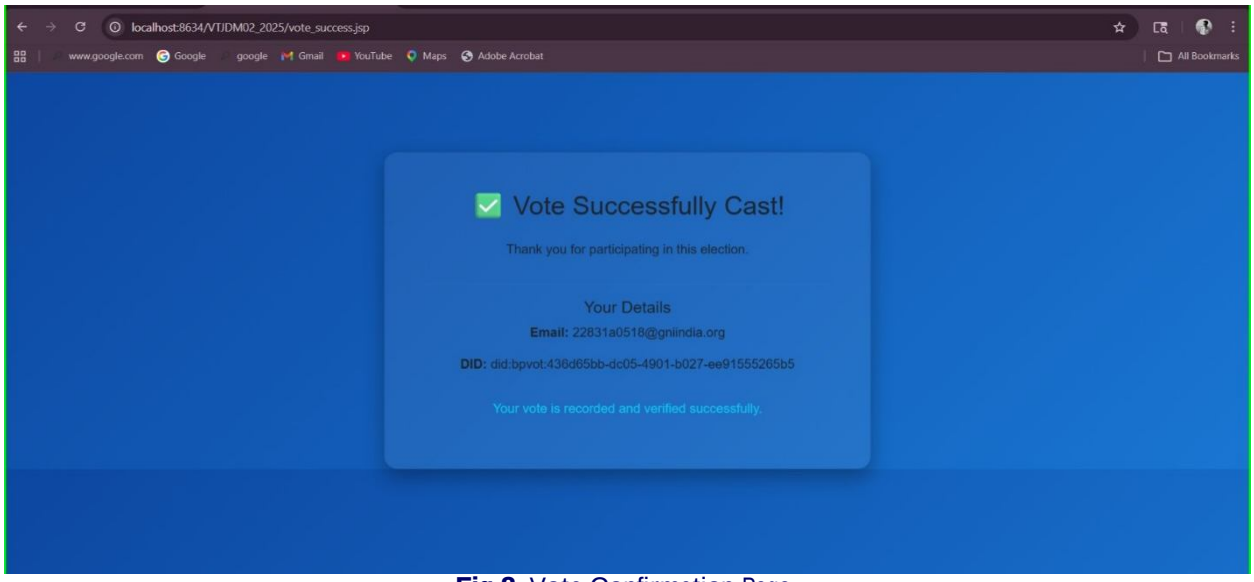

Fig 8: Vote Confirmation Page

The system also supports efficient handling of voting data, reducing manual efforts and time required for election management. Overall, this project demonstrates the potential of advanced technologies in improving the security and reliability of e-voting systems, enhancing trust among users, and contributing towards fair and transparent election processes.

VIII. FUTURE ENHANCEMENT

The next generation of the system will feature improved security and performance with the use of new technologies like blockchain scalability options and consensus protocols optimization. It is possible to upgrade the system for conducting elections on a national scale and integrate it with the governmental identity management system for better voter verification. Possible improvements will include more sophisticated user authentication tools such as biometric authentication, which will contribute to the system security. Furthermore, it is possible to develop cloud-based versions of the software as well as mobile applications for increased accessibility. The system can also be upgraded with analytical capabilities for monitoring and detecting voting fraud.

REFERENCES

1. Y.Liu, M.Li, and K.Chen, “Blockchain-Based E-Voting System with Distributed Consensus and Privacy Preservation,” IEEE Access, vol. 8, pp. 136–145, 2020.
2. A.Sharma and R.Kaur, “A Secure E-Voting Framework Using Smart Contracts on Ethereum Blockchain,” International Journal of Computer Applications, vol. 183, no. 45, pp. 25–31, 2021.
3. P.Zhang and L.Wang, “Integrating Differential Privacy for Secure and Anonymous Blockchain-Based Voting,” Journal of Information Security and Applications, vol. 67, 2022.
4. J.Park and H.Nguyen, “Self-Sovereign Identity and Verifiable Credentials for Decentralized Voting Systems,”. IEEE Transactions on Emerging Topics in Computing, vol. 11, no. 3, pp. 570–582, 2023.
5. S.Mehta and D.Patel, “Hybrid Blockchain-Based Secure and Transparent E-Voting with Multi-Factor Authentication,” International Journal of Advanced Computer Science and Applications (IJACSA), vol. 15, no. 4, 2024.
6. B.Wang, F.Guo, and Y. Liu, “An Efficient and Versatile E-Voting Scheme on Blockchain,” Cybersecurity, SpringerOpen, 2024.
7. I.Singh, A.Kaur, and P.Agarwal, “Enhancing Security and Transparency in Online Voting through Blockchain Decentralization,” SN Computer Science, Springer, 2024.
8. Y.Liang, X.Zhang, and C.Zhao, “Multi-Party Confidential Verifiable Electronic Voting Scheme Based on Blockchain and IPFS,” Journal of Cloud Computing, SpringerOpen, 2024.
9. Pathan Saifullah Khan et al., “Quantum-Resistant Blockchain-Based E-Voting System with Enhanced Voter Privacy and Real-Time Transparency,” International Journal of Computer Applications, vol. 27, no. 4, 2025.
10. M.Hossain and T.Alam, “Differential Privacy-Enabled Blockchain Voting System: Balancing Transparency and Anonymity,” IEEE Internet of Things Journal, vol. 12, no. 6, pp. 9552–9564, 2025.
11. Joshi, Y., Totad, S. G., Geeta, R. B., & Prasad Reddy, P. V. G. D. (2018). Mobile agent-based frequent pattern mining for distributed databases. In S. Bhalla, V. Bhateja, A. Chandavale, A. Hiwale, & S. Satapathy (Eds.), Intelligent computing and information and communication (Vol. 673). Springer. https://doi.org/10.1007/978-981-10-7245-1_9
12. Bharamagoudar, G. R., Totad, S. G., Prasad Reddy, P., &Shobha, R. B. (2015). Zealous leadership paradigms. International Journal of Globalisation and Small Business, 7(1), 92–106. https://doi.org/10.1504/IJGSB.2015.069033
13. Geeta, R. B., Totad, S. G., Prasad Reddy, P., &Shobha, R. B. (2015). Big data structure and usage mining coalition. International Journal of Services Technology and Management, 21(4/5/6), 252–271. https://doi.org/10.1504/IJSTM.2015.073930