Smart and Secure E-Voting Application using Blockchain Technology

Prof. V. M. Khanapure[1], Joshi Mahi[2], Kadam Amruta[3], Patil Swarupa[4],
Swami Gayatri[5], Kambale Sakshi[6]
HOD, Department of Information Technology[1]
Students, Department of Information Technology[2,3,4,5,6]
Puranmal Lahoti Government Polytechnic, Latur, Maharashtra, India

Abstract*: The realm of electronic voting systems is experiencing a profound transformation propelled by technological advancements. In response to the demand for secure and transparent voting mechanisms,this project, supervised by Mrs. V.M. Khanapure, endeavors to develop a Smart and Secure E-Voting Application employing blockchain technology. Traditional voting methods often face challenges related to tampering and fraud, which the proposed system aims to mitigate through the decentralized and immutable nature of blockchain. By leveraging the strengths of blockchain, such as transparency and decentralization, the project seeks to establish a trustworthy and efficient electronic voting solution.*

A primary focus of the Smart and Secure E-Voting Application is the implementation of advanced security measures. Cryptographic techniques are incorporated to secure vote transmissions and protect voter privacy. The application employs end-to-end encryption and multi-factor authentication, fortifyingthe overall security posture of the system. Moreover, the user-friendly interface caters to both voters and election administrators, ensuring accessibility without compromising the high level of security. This project not only addresses current challenges in electronic voting but also lays the foundation for future innovations, setting a precedent for reliable and transparent electoral processes through the utilization of blockchain technology..

Keywords: blockchain technology

I. INTRODUCTION

The landscape of democratic processes and electoral systems has been undergoing a substantial evolution in recent years, prompted by the rapid advancements in information technology. Traditional voting methods, reliant on paper ballots and manual counting, have faced persistent challenges such aslogistical inefficiencies, susceptibility to fraud, and the need for extensive resources. In response to these limitations, electronic voting systems have emerged as a potential solution to streamline the voting process and enhance the overall integrity of elections.

However, the transition to electronic voting brings its own set of challenges, particularly in terms of security, transparency, and voter trust. Ensuring the confidentiality and accuracy of votes in an electronic environment has become a critical concern for electoral authorities and stakeholders. It is within this context that the project, under the guidance of Mrs. V.M. Khanapure, seeks to contribute tothe advancement of electronic voting systems. By focusing on the integration of blockchain technology, a decentralized and tamper-resistant ledger, the project aims to address the vulnerabilities inherent in traditional electronic voting systems and establish a foundation for a secure and transparent e-voting application. This general background sets the stage for understanding the necessity and relevance of the proposed Smart and Secure E-Voting Application.

II. LITERATURE SURVEY

In the digital era where hacking and bypassing a system is easy, tampering of data is always possible leading to bad situations. Blockchain is used to store data which is near impossible to change or tamper with as it is very secure in nature. Voting as a process in any nation is an essential event and if votes get miscalculated by any external source it will be harmful. To avoid such kinds of situations and making it more comfortable blockchain technology comes in

Copyright to IJARSCT
www.ijarsct.co.in

DOI: 10.48175/IJARSCT-15999

ISSN
2581-9429
IJARSCT

626

acknowledgment. This paper proposes a decentralized national e-voting system based on blockchain technology. It includes an admin panel to schedule the voting, manage candidates and declare the results. The web application will provide the users with an interface to enter their Aadhar card ID (text input) and a photo of themselves at the time of voting. The eligibility of the voter will be checked at the time they enter their Aadhar card ID. Eligible voter's phone numbers will be verified via One Time Password (OTP). After voter verification, individual voters will be considered eligible for voting. During voting, voters will be monitored through a webcam/front camera. The votes will be stored in a blockchain and any tampering would be detected easily. The address and the corresponding constituency will be checked in the backend.

III. PROPOSED IMPLEMENTATION

The proposed decentralized voting system using Ethereum blockchain aims to provide a transparent and tamper-proof solution for conducting elections. By leveraging smart contracts on the Ethereum network, the system enables secure and anonymous voting, while ensuring the integrity and immutability of the voting data. This would increase voter trust in the election process and reduce the risk of fraud or manipulation.
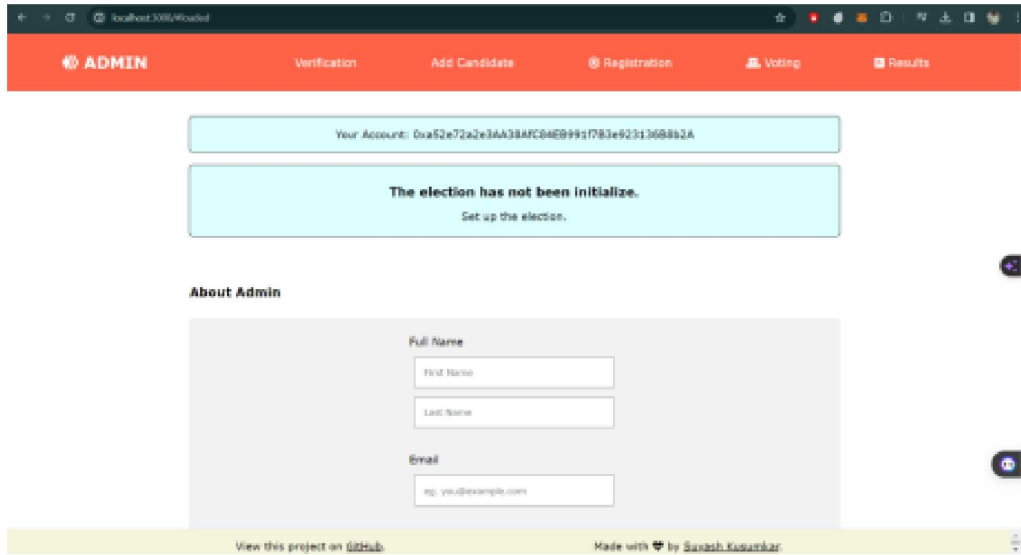
Objectives of Proposed Research:

1. Security: The proposed system aims to provide a secure platform for conducting elections, eliminating the possibility of tampering with votes, and ensuring that the election results are transparent and verifiable.

2. Transparency: The proposed system aims to provide complete transparency to the voters, allowing them to view the entire voting process, including the vote counting and results.

3. Accessibility: The proposed system aims to make the voting process more accessible to all eligible voters by eliminating the need for physical presence at a polling station, thus increasing voter turnout.

4. Efficiency: The system aims to increase the efficiency of the voting process by reducing the time and resources required to conduct elections. Since the system is automated and eliminates the need for intermediaries, it can significantly reduce the cost and time associated with traditional voting methods.

5. Trust: The proposed system aims to increase trust in the voting process by providing a transparent and tamper-proof mechanism for recording and tallying votes
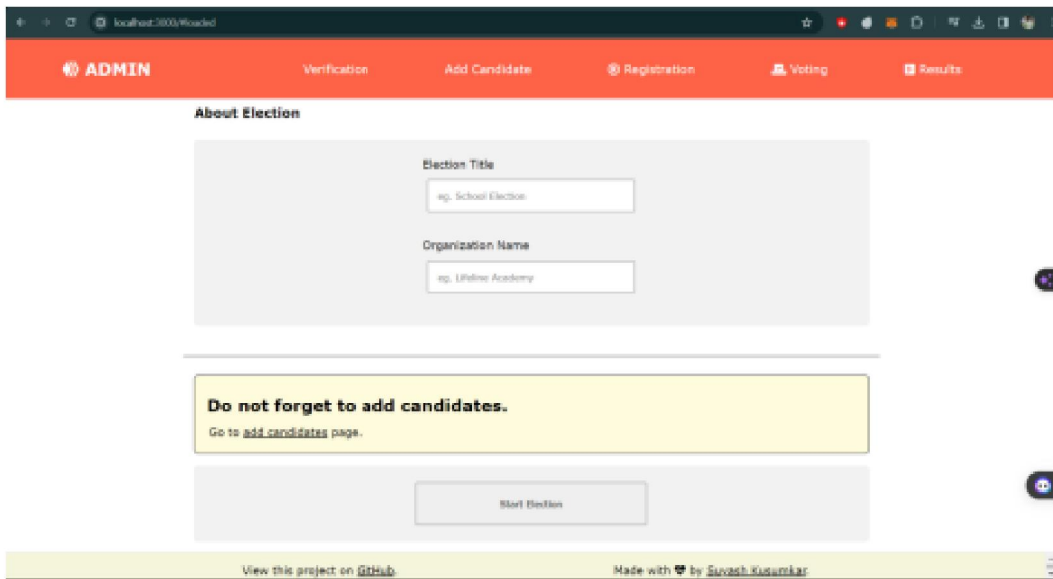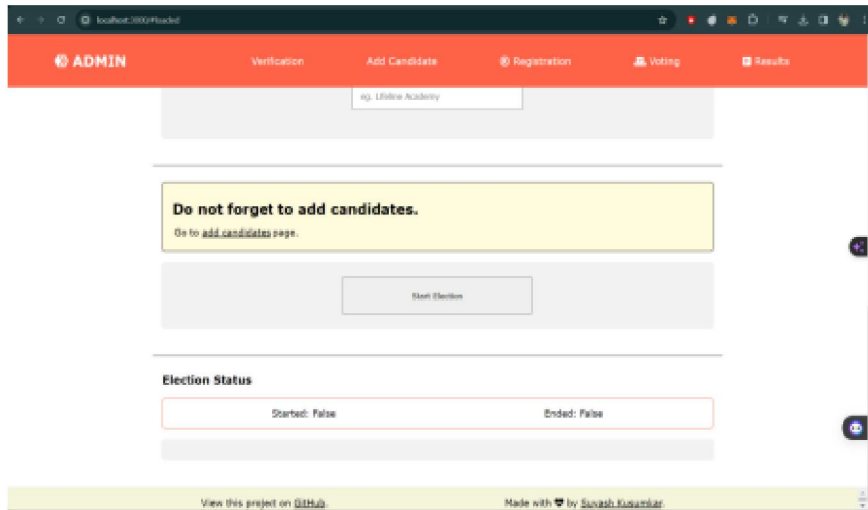
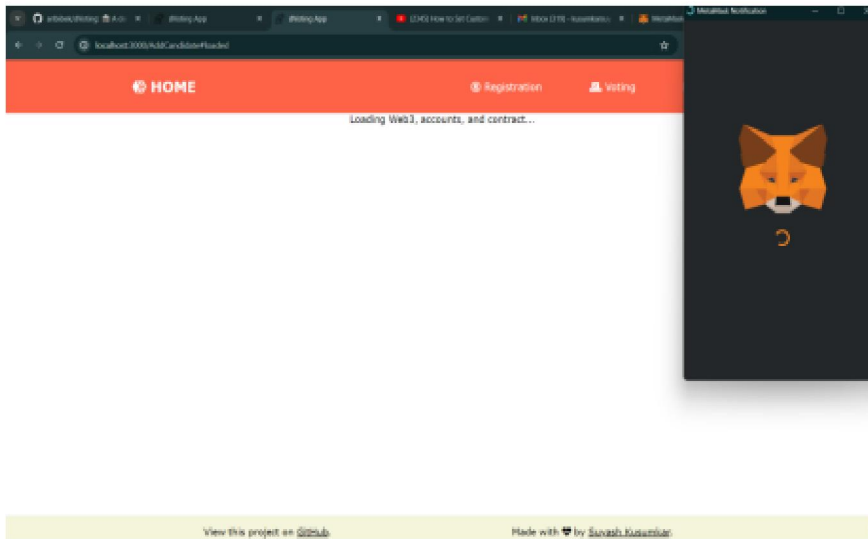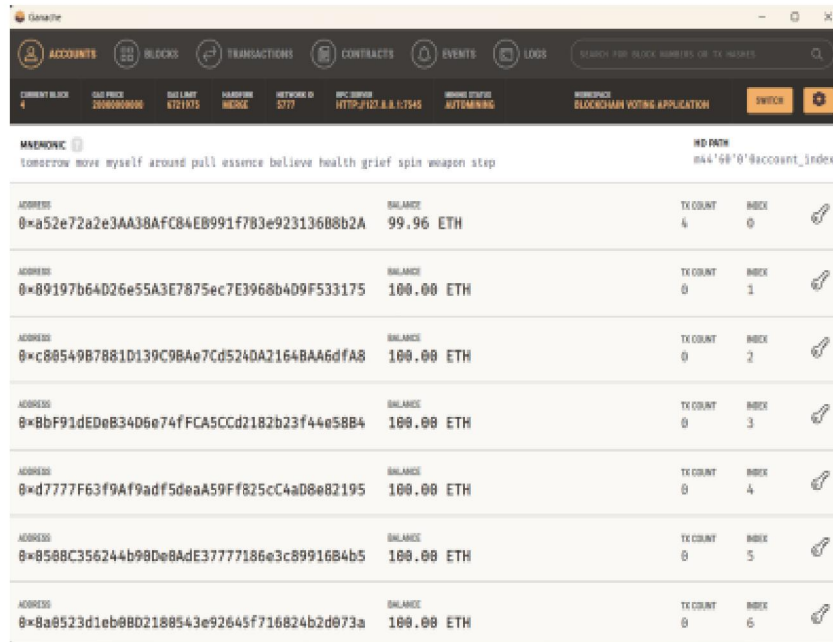## IV. FLOWCHART
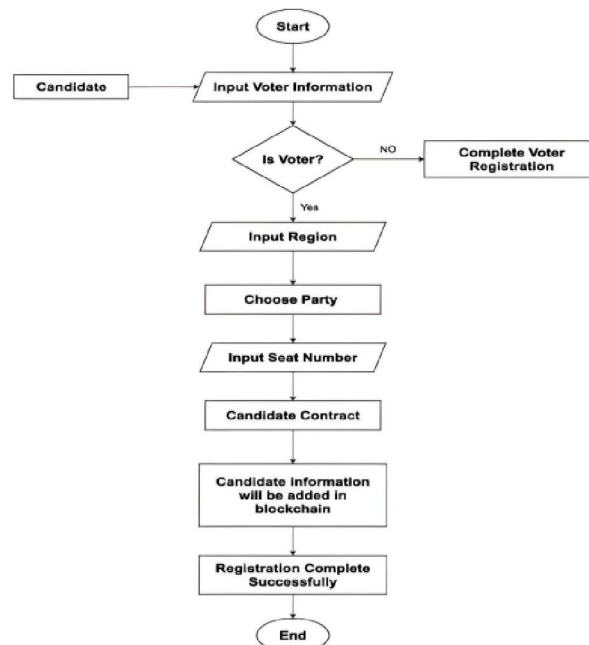
V. OUTPUT

Fig: Admin Panel

Fig: Admin Panel

Fig: Admin Panel

Fig: Adding Candidate with blockchain Security

Fig: Ganache Server to add ETH in Server for Authentication

Fig: Available Accounts and Private Keys will show in CMD

VI. CONCLUSION

Decentralized Voting with Ethereum Blockchain offers a robust and transparent solution for secure elections. By leveraging blockchain technology, it ensures the integrity of votes and provides a tamper-proof platform. With

continued enhancements, including improved user experience, scalability, and integration with other cutting-edge technologies, it has the potential to revolutionize the democratic process and empower citizens to participate in a trusted and efficient voting system. It represents a significant step towards building a more democratic and accountable society.

REFERENCES

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

[2] Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world. Penguin.

[3] Swan, M. (2015). Blockchain: Blueprint for a new economy. O'Reilly Media, Inc.

[4] Bhargava, R. B., &Ranchal, R. (2017). Blockchain for dummies. John Wiley & Sons.

[5] Antonopoulos, A. M. (2014). Mastering Bitcoin: Unlocking digital cryptocurrencies. O'Reilly Media, Inc.

[6] Zohar, A. (2015). Bitcoin: Under the hood. Communications of the ACM, 58(9), 104-113.

[7] Eyal, I., &Sirer, E. G. (2018). Majority is not enough: Bitcoin mining is vulnerable. Communications of the ACM, 61(7), 95-102.

[8] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. Future Generation Computer Systems, 1(5), 119-129.

[9] Kshetri, N. (2017). Can blockchain strengthen the internet of things? IT Professional, 19(4), 68-72.

[10] Merkle, R. C. (1987). A digital signature based on a conventional encryption function. Advances in Cryptology–CRYPTO'87, 369-378.