A Mobile Blockchain-Based E-Voting System

[1]Sourav Gogoi, [2]Chaitanya Garud, [3]Rutuj Khalane, [4]Mitesh Wagh, [5]Prof. Yogesh Gite,

Department of Computer Engineering,
Sandip Institute of Engineering and Management
Nashik, Maharashtra

***Abstract*- Our country India, being the largest democratic country in the world organizes the largest elections in the world. Voting is a fundamental democratic activity it is essential to make sure that the governing body is elected through a fair election. India makes use of the Electronic Voting Machines (EVMs) to conduct major elections in an offline manner, which in itself is rather ineffective and not up to the mark. It requires large manpower and time to process and publish the results. Therefore, to be made effective, the system needs a change to overcome these disadvantages. Many nations utilize digital voting methods to solve the difficulties of paper balloting. It does not force the person's physical appearance to vote, which makes things easier, but this method is not void of any faults and abuse either. A single flaw in the digital voting system may lead to massive vote-rigging, which is concerning. Voting methods for elections must be legal, accurate, safe, and convenient. However, any discrepancies with the digital voting methods may restrict acceptance. That being said, India suffers from a flawed electoral system making it vulnerable to ballot rigging, hacking of the EVM (Electronic voting machine), election manipulation, and polling booth capturing. These dilemmas need to be addressed in order to make the voting process fair. Blockchain, due to its end-to-end verification capabilities is just the right technology to address these problems. Numerous countries are experimenting with blockchain-based voting systems as we speak. We have used blockchain technology in our proposed system for the anonymity, privacy, verifiability, mobility, integrity, security, and fairness it provides in voting. By using blockchain, our proposed system ensures security and provides voter-verifiability by keeping the voter information as a hash in the blockchain thereby providing protection against fraudulent activities. We analyzed our system's performance based on its security and gas costs. It improves in terms of security characteristics and the related cost of the necessary infrastructure.**

***Key words*- E-voting, Blockchain, Hashing, Verification, Integrity, and Security.**

Published in IJIRMPS (E-ISSN: 2349-7300), Volume 11, Issue 3, May-June 2023

Introduction:

In the current era, the utilization of technology plays a vital role in meeting human needs. As technology usage increases, it poses new challenges to the democratic process, primarily due to widespread distrust in governments among the majority of people. Consequently, elections have gained immense importance in modern democracies. They serve as decisive events that determine the fate of nations and organizations by selecting their leaders. However, a major concern in democratic systems worldwide is the lack of trust in the electoral process, even in prominent democracies like India and the United States, where flaws exist. Issues such as vote rigging, EVM hacking, election manipulation, and polling booth capturing raise significant doubts about the integrity of the current voting system.Blockchain, a revolutionary decentralized and distributed technology, has the potential to address various challenges across numerous industries. By expanding e-voting using blockchain technology, the existing issues with the electronic voting system can be effectively resolved. It is worth noting that blockchain extends beyond just cryptocurrencies like Bitcoin, as it has opened the doors to a new era of online services and the Internet. The absolute nature of blockchain

makes it possible to migrate numerous administrative and fintech operations to the online realm, ensuring their security and reliability. The power of blockchain lies in its smart contracts and various features that surpass traditional systems. Smart contracts are segments of code integrated into the blockchain, which are executed according to a predetermined plan during each stage of updating the blockchain. In the realm of online services, e-voting is an important and trending topic. Blockchain, with its smart contracts, emerges as a strong candidate for the development of cost-effective, secure, transparent, and user-friendly e-voting systems.

PURPOSE

The Indian government has granted citizens the right to choose their desired leader through the process of elections. To oversee and manage this electoral process, an independent body called the Election Commission of India has been established. This commission is impartial and operates according to the laws and regulations governing elections. In order to facilitate voting, the Election Commission employs Electronic Voting Machines (EVMs), which require voters to present their election ID cards issued by the commission. These cards are verified against the official database before allowing the voter to cast their ballot. This method ensures efficiency by saving time and reducing the need for extensive manpower. Additionally, it is considered a secure alternative to previous voting procedures. However, the EVMs have certain drawbacks, such as delays in the counting and display of results, as well as the requirement for voters to cast their votes at designated locations, which may lead to inaccuracies. In contrast, our project enables candidates to cast their votes from any location, including their workplace, ensuring 100% accuracy in the voting process while minimizing manual effort and time consumption.

EXISTING SYSTEM

1. The use of computerized machines and equipment for voting has been a prominent subject of research for several years, aiming to facilitate accurate and reliable results that align with the preferences of the voters involved.
2. In its early stages, the voting process involved paper-based ballots that were subsequently counted by computer systems.
3. By ensuring that voters have a clear understanding of the voting system, its usability can be significantly enhanced.

PROBLEM DEFINITION

The traditional voting system poses significant challenges when managed by a single organization with complete control over the system and its database, making it susceptible to potential manipulation and the erasure of any evidence of changes made. To overcome these challenges, an effective solution involves adopting a public database that is collectively owned by multiple users. This approach enables data comparison to identify inconsistencies and discrepancies. Utilizing blockchain technology is an ideal solution for electronic voting systems, as it ensures the secure execution of voting applications. In a blockchain-based system, each voter's ballot can be treated as a transaction that is recorded on the blockchain, ensuring transparency in the vote-counting process. The transparency provided by the blockchain's audit trail allows all parties involved to verify the integrity of the data, preventing unauthorized alterations, deletions, or entries into the blockchain. This enhances the trust and reliability of the voting system, as the openness of the blockchain enables a transparent and verifiable process.

LITERATURE REVIEW & RELATED WORKS

[1] Proposes a novel online voting system based on hash graph technology, which overs superior encryption compared to traditional block chain methods. The system ensures participant's anonymity while allowing for public inspection. Voter authentication is conducted through a multi-factor verification process, encompassing the use of the voter's Voter ID, Aadhaar Card Number, and facial recognition. This comprehensive approach ensures the accurate identification of voters, enhancing the security and integrity of the online voting system. To enhance security, they implemented JWT Authentication in the login portal. The system generates a highly encrypted unique ID that allows voters to verify their cast vote. Voter data is stored securely in a protected database, and homomorphic encryption is used for vote storage and secure vote

counting. Additionally, a chatbot is incorporated to provide support to voters. In conclusion, it provides a comprehensive evaluation of their scheme, demonstrating its electiveness in establishing an end-to-end verifiable online voting system.

[2] Proposes the development of a secure Electronic Voting Machine (EVM) that instils trust in the voting process and eliminates malpractice. The project aims to leverage fingerprint identification technology and utilize the AADHAR card database for secure access. During elections, the EVM authenticates voters using finger vein sensing, allowing them to cast their votes electronically. The system also facilitates the transmission of voting data and voter details to the nearby Database Administration unit via Wi-Fi systems. Fingerprint scanning ensures security by preventing fake or repeated voting, enhancing the accuracy and speed of the process. The primary objective is to ensure that only legitimate users can exercise their voting rights. When a voter participates in an election, their thumb impression is captured as input for the system. The fingerprint pattern is then compared with the records in the database. If a match is found, the voter is granted access to cast their vote. However, if there is no match or if the fingerprint has been used previously, access to vote is denied or the vote is rejected.

The primary goal of [3] is to establish a secure and reliable voting system that addresses common misconceptions and challenges encountered during elections. It utilizes fingerprint recognition technology as input. The MATLAB platform stores a comprehensive voter database containing information such as fingerprints, photos, and mobile numbers. During voting, the voter's fingerprint is matched against the database. If a match is found, the voter is allowed to cast their vote. If the fingerprint does not match, the system will prohibit further progress. Notably, this voting system provides flexibility for voters to cast their votes from their preferred location. Additionally, the database administration unit is continuously updated with the number of votes cast. The implementation of this smart voting system ensures enhanced accuracy and high-speed processing. It aims to overcome the limitations associated with traditional electronic voting systems.

The purpose of [4] is to enhance the election process by preventing electoral fraud and ensuring the safety, security, reliability, and seamless conduct of elections in the country. The paper introduces an innovative approach to the voting process, where the device interacts with an RFID tag embedded in the voter's ID card. When a voter scans their card, the controller verifies the ID, and if it matches, the result is displayed on the LCD screen. This system aims to streamline the voting process and improve the overall integrity of elections.

[5] Describes an advanced voting machine that incorporates face recognition technology to establish a secure and reliable voting system. The primary objective is to enhance the safety and security of the voting process. During a voting session, the system verifies the person's identity by matching their face with the image stored in the database. Based on the results of the image recognition process, the system determines whether the person is eligible to vote or not. This systematic verification helps prevent the participation of fake voters. In the event of any fraudulent attempts, the original voter is notified through a GSM message, providing an additional layer of security and ensuring the integrity of the voting process. The use of face recognition technology in this voting machine aims to minimize impersonation and safeguard the fairness and authenticity of elections.

[6] Proposes the design and development of a novel tamper-resistant electronic voting system to overcome the flaws of existing voting machines. The system incorporates multiple layers of verification, including fingerprint recognition and Near Field Communication (NFC) smart card authentication, to verify the identity of potential voters. Once verified, the voter can cast their vote by pressing a button corresponding to their preferred candidate. The vote is recorded in the system and visually confirmed to the voter. Furthermore, the final vote is automatically printed onto a ballot box using a Point of Sales (POS) printer for added validation. This system aims to prevent multiple voting instances and eliminate discrepancies where individuals claim they haven't voted despite their name appearing in the list of vote casters. The project builds upon previous research and presents an incremental extension to address the shortcomings of existing voting systems.

[7] Proposes the implementation of a biometric system using fingerprint scanning. By utilizing fingerprint scanning, the system aims to enhance security and prevent fake and repeated voting. It also improves the accuracy and speed of the voting process. The system identifies voters based on their unique thumb impressions, providing an advantage over conventional voting systems. Its purpose is to ensure that only legitimate users can access their voting rights.

[8] Implements face recognition technology and adopting robust verification mechanisms. The project aims to provide a safer and more secure voting system. This contributes to the overall integrity of the electoral process and promotes a fair democratic system.
[9] Implements an Authenticated Voting Machine during college elections, aiming to streamline the process and enhance transparency. The model incorporates radiofrequency and fingerprint recognition technologies to ensure security. While the concept of the advanced voting system shows promise, further research is needed to strengthen its stability and theoretical foundation. The protection of votes is prioritized in the model, leveraging radiofrequency and fingerprint recognition to enhance security measures. Continued exploration and development of the model will contribute to the advancement of secure and transparent voting systems.
[10] Proposes a radical online voting system based on hash graph technology as an alternative. This system addresses numerous flaws found in blockchain through the utilization of hash graph encryption, an enhanced version of blockchain encryption. It maintains the anonymity of participants while allowing public scrutiny. To verify voters, we employ the use of Voter ID, Aadhaar card numbers, and facial recognition. Furthermore, JWT Authentication is implemented to fortify the security of the login portal. Additionally, our system generates highly encrypted unique IDs, allowing voters to verify their cast votes. A highly secure database is also utilized to safeguard voter data. Moreover, homomorphic encryption is employed to securely store and facilitate the vote count. Lastly, the system incorporates a Chatbot feature that assists voters. This paper thoroughly evaluates the scheme, demonstrating its electiveness in creating an end-to-end verifiable online voting system.
[11] Explores the concept of online voting as a viable alternative to traditional paper ballot systems and electronic voting machines (EVMs). The primary objective of an electronic voting portal is to ensure the security, integrity, transparency of votes, and privacy of voters. The implementation presented in the paper is specifically designed for small scale elections within corporate houses or boardrooms. Ethereum's smart contracts are utilized, and the development, testing, and deployment of these smart contracts are facilitated by the True framework. For testing purposes, Ganache is employed as the Ethereum client, while Meta-mask serves as the browser wallet component in this particular context.
The primary objective of [12] is to develop a voting system that leverages Blockchain technology to deliver transparency and security. For this purpose, the Ganache tool is employed to establish a local blockchain network, while the Metamask tool is utilized for account verification.
[13] Presents a novel approach to electronic voting. Voting serves as the preferred method for making democratic decisions. The paper thoroughly addresses the considerations taken during the development and implementation of the centralized and independent blockchain network, specifically tailored for use as a voting platform. Additionally, it explores the integration of biometrics to enhance user security throughout the voting process.
[14] Proposes a prototype blockchain-based electronic voting system specifically tailored for the political election process in the United Arab Emirates (UAE). A blockchain system is characterized by its distributed, decentralized, and immutable nature, allowing data to be shared and distributed among all participants in a network. The utilization of blockchain technology offers numerous advantages applicable to various use cases, including electronic voting systems. The paper examines the effectiveness of adopting blockchain technology specifically for political elections in the UAE, considering its potential benefits and implications.
[15] Aims to ensure data integrity, transparency, and privacy while enforcing the rule of one vote per mobile phone number for each poll. To achieve this, they leveraged the Ethereum Virtual Machine (EVM) as the Blockchain runtime environment. Organizers deploy transparent, consistent, and deterministic smart contracts on the EVM for each voting event to govern the voting rules. User authentication is facilitated through mobile phone numbers, eliminating the need for a third-party server. Experimental results demonstrate the feasibility of the proposed system, highlighting its potential to establish ideal environments for secure and trustworthy voting experiences. By leveraging Blockchain technology, this decentralized approach aims to address the trust concerns inherent in centralized voting systems and pave the way for more transparent and reliable voting processes.
[16] Discusses the concept of a smart city, which involves the intelligent integration of available resources and cutting-edge technologies. The proposed mechanism is validated through analysis against multiple security parameters, including message alteration, Denial of Service (DoS) attacks, Distributed Denial of

Service (DDoS) attacks, and authentication delays. By leveraging IoT and Blockchain, the proposed e-voting system provides enhanced security and transparency, addressing the inherent vulnerabilities in traditional e-voting systems.

[17] Explores the utilization of ring signatures to achieve anonymity in a decentralized e-voting system. Unlike conventional signature algorithms that uniquely authenticate the author of a signature, a ring signature conceals the true public key for verification purposes among the public keys of other participants within the system. Simultaneously, the incorporation of blockchain technology enables the verification of vote integrity, authentication of votes (through binding with valid public keys), and ensures transparency in the vote calculation process, as well as verification of accurate vote accounting for individual users.

The proposed system in [18] leverages blockchain to ensure security, privacy, and integrity. By storing voter information as a hash on the blockchain, it maintains voter anonymity. Additionally, to ensure fairness, the casted vote remains encrypted until the end of the election. Once the election concludes, voters can verify their casted vote, thus ensuring verifiability. To assess the efficacy of the protocol, it was implemented on Ethereum 2.0, a blockchain platform that utilizes Solidity as the programming language for developing smart contracts. The integration of smart contracts offers a secure method for voter verification, safeguards the accuracy of voting results, enables transparency in the counting process, and protects against fraudulent activities. The system's performance was analyzed, considering security aspects and gas costs. This approach demonstrates improvements in terms of security features and the associated expenses for the required infrastructure.

OBJECTIVES

1. To develop a secure E-Voting System
2. To develop a system which will be easy to use and more user friendly for our client.
3. To obtain a centralized management system.
4. Building an online system would enable voters to cast their votes on chosen candidates.
5. Study and implement a security method to be used to ensure that votes being cast in the system will not be compromised and any outside intrusion attacks.
6. To ensure the legitimacy of voters and restrict voting to authorized individuals only.
7. To ensure the protection of voter anonymity, the proposed system focuses on establishing an unlinkability between the voter and their submitted vote.
8. To minimize election expenses in comparison to current systems.

PROPOSED METHODOLOGY

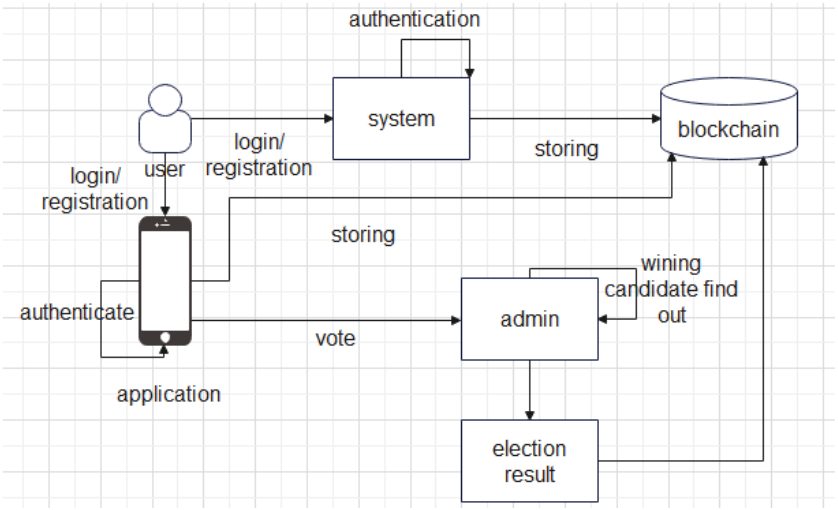

Fig. 1. Architecture of the Proposed System

The architecture of the proposed methodology is shown in Fig. 1. We have used blockchain technology in our system. There are also some external entities present in our system which are:

- **Election Commission (EC)/Admin-** The election commission is in charge of overseeing the whole election process. The election commission is denoted as EC. The Election Commission (EC) commences an

election, initiates its proceedings, and subsequently concludes it after a designated duration has elapsed. EC notices the entire voting process and publishes the result just after the election has been over. Another crucial duty of the EC is to create a roster of eligible voters ahead of the election through the implementation of a voter registration process.

- **Voter-** Voters refer to individuals who possess the right to vote and are duly registered within their respective local election districts. Each voter is entitled to cast a vote for a single candidate.
- **Blockchain-** It is essential to prohibit illegal access to the votes to maintain privacy. Each vote must be encrypted before being sent to the database in order to do this. For this purpose, a blockchain-based on SHA256 is used here for storing the voter's information. The voter registration system implemented by the EC does not retain any voting data, and it is not accessible to individual voters. This Blockchain is responsible for verifying whether the voter is a legitimate part of the blockchain and whether voting permissions should be given to him/her or not.

Voters may use their smartphones to cast their votes in the proposed Digital Voting System. The Election Commission (EC) is responsible for creating and closing the election by interacting with the admin panel from within the app. By using the blockchain, the voter's registration process, voter authentication, and voting are done directly between the voter and the database

At first, the hash value of the voter's information is stored by the blockchain during the registration process to secure the voter's information and provide anonymity to the voter. Hash values are also utilized to authenticate voters during the process of casting their votes. After the election starts, voters perform the voter authentication process and then choose one of the candidates from the list of candidates provided by the EC and cast a vote using a vote coin. In this context, the term "vote coin" symbolizes the voting status of the individual. When the balance of the vote coin is 1, it indicates that the voter has not yet cast their vote. If the balance of the vote coin is 0, that means the voter has already cast their vote and they are barred from casting any more votes. In our system, for every n vote, there will be n voting blocks created to represent each individual vote.

The proposed voting System includes four phases:

1. **Registration Phase:** The First phase of the voting system consists of the Registration unit where the Voters register using their Name, E-mail, Password, and Aadhar Number. We have also used the device's biometric system for authentication of the voter during login.
2. **Voting Setup Phase: T**he election is created by the EC. The EC creates the election through the Admin side login and also lists all the eligible election candidates.
3. **Voting Phase:** During the voting phase, the voter is required to provide their credentials for authentication purposes. Once the credentials are provided, a hash value is generated from these credentials and compared with the existing hash values stored in the blockchain. If a match is found, the voter is deemed valid and eligible to cast their ballot. After successful authentication, the voter is presented with a ballot containing a list of candidates along with their respective party symbols. Voters can make their candidate selections from the list and cast their votes using the designated vote coin.
4. **Result Phase:** Following the completion of the voting process, each vote is transformed into a block and added to the blockchain. As a result, the counting of votes happens instantly once they are submitted, with minimal risk of tampering or manipulation.

IMPLEMENTATION

To develop a decentralized application that can effectively substitute a traditional voting system, a mobile application is developed that provides the voting environment. Also, people who cannot go to their polling locations for various reasons may vote by using a user-friendly application displaying their city's election ballot. First and foremost, to implement a blockchain-based voting system, we must first create the necessary environment. Components used for the implementation of our system include:

1. **Android Studio:** In our system, we have utilized Android Studio as an essential tool for development purposes. It serves as a crucial tool for the development and implementation of our Android-based solution. Android Studio, an integrated development environment (IDE), offers a comprehensive set of features and functionalities specifically designed for building Android applications. By leveraging the capabilities of

Android Studio, we were able to efficiently develop, test, and debug our mobile application. The IDE provides a user-friendly interface, extensive libraries, and robust tools that simplify the development process and enhance productivity. With Android Studio, we could seamlessly design the user interface, write and organize code using Kotlin or Java, and utilize various debugging and profiling tools to optimize performance. Additionally, Android Studio's integration with the Android Software Development Kit (SDK) allowed us to access a wide range of APIs and platform-specific features, ensuring compatibility and enhancing the functionality of our application. Overall, Android Studio played a pivotal role in enabling us to create a robust and feature-rich Android application for our project.

2. **Google Firebase:** In our proposed system, we have incorporated Google Firebase as a crucial component to support various functionalities and enhance the overall performance. Google Firebase is a comprehensive mobile and web development platform that offers a suite of cloud-based services and tools. We have leveraged Firebase to handle multiple aspects of our system, including data storage, user authentication, and real-time communication. With Firebase's Realtime Database, we were able to securely store and synchronize data in real-time, ensuring that the latest information is accessible to all users. The Firebase Authentication feature provided a robust and seamless authentication mechanism, allowing users to securely log in and access the system's features. Additionally, Firebase Cloud Messaging facilitated efficient and reliable communication between the system and the users by enabling push notifications. Moreover, we utilized Firebase Analytics to gain valuable insights into user behavior and system performance, enabling us to make data-driven decisions for system improvements. By integrating Google Firebase into our proposed system, we were able to enhance its functionality, scalability, and reliability.

3. **SHA256:** In our proposed e-voting system, we have implemented SHA256 (Secure Hash Algorithm 256-bit) as a critical component to ensure the integrity and security of the voting process. SHA256 is a widely used cryptographic hash function that generates a fixed-size hash value (256 bits) from any input data. In our system, SHA256 is employed to hash the voter's information, providing a secure and irreversible representation of their identity. By storing the hashed voter information on the blockchain, we establish a link between the voter and their casted vote without compromising their anonymity. Furthermore, SHA256 is used to generate a unique hash for each casted vote, which helps in detecting any tampering or alteration of the vote during transmission or storage. The use of SHA256 in our e-voting system adds an additional layer of security and ensures the integrity of both the voter's identity and the casted votes, enhancing trust and reliability in the electoral process.

First and foremost, a genesis block is created and added to the blockchain. The genesis block is the first block in the chain and serves as the initial starting point. Following that, we have three functions: **addBlock**, **calculateHash**, and **isChainValid**.

- The "**addBlock**" function is responsible for adding a new block to the blockchain. It takes a Block object as input.
- Within the "**addBlock**" function, the previous hash of the new block is set to the hash of the last block in the chain (**blockchain[blockchain.size - 1].hash**).
- The "**calculateHash**" function is used to generate the hash for a given block. It concatenates the block's data, previous hash, and timestamp, and then applies the SHA-256 hash algorithm to generate a hash value represented as a string.
- The "**isChainValid**" property is a Boolean value that checks the validity of the blockchain. It iterates through each block in the chain, comparing the hash of each block with the recalculated hash based on its data, previous hash, and timestamp. It also ensures that the previous hash of each block matches the hash of the preceding block. If any inconsistency is detected during the validity check, the function returns "false", indicating that the blockchain is invalid. Otherwise, it returns "true", indicating a valid blockchain.

ADVANTAGES OF THE PROPOSED SYSTEM

- Offering a voting prevention system to ensure secure voting procedures.
- Eliminates the possibility of invalid votes.
- Its usage results in the reduction of polling time.
- Results in fewer issues with election planning and expenditures on law and order candidates.

- It has the potential to save money on printing supplies and the transportation of massive amounts of election materials.

APPLICATIONS

Our developed system can be used wherever there is a need for an election. This includes corporate-level elections among employees, general elections held in a school/university, or even major state-level elections.

RESULTS

Fig. 2. Splash Art

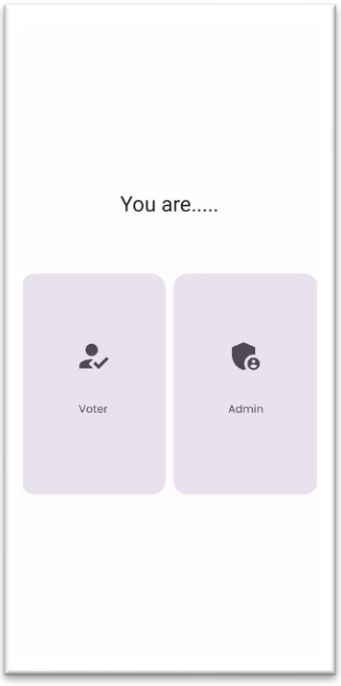

Fig. 3. App Home Screen

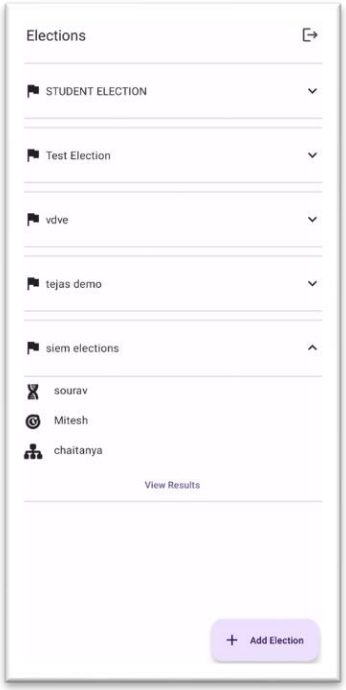

Fig. 4. Admin Home Screen

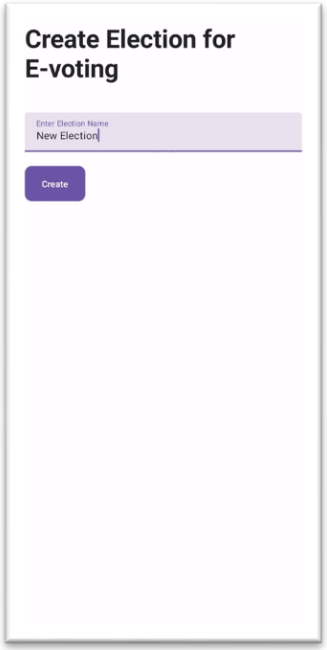

Fig. 5. Creating New Elections

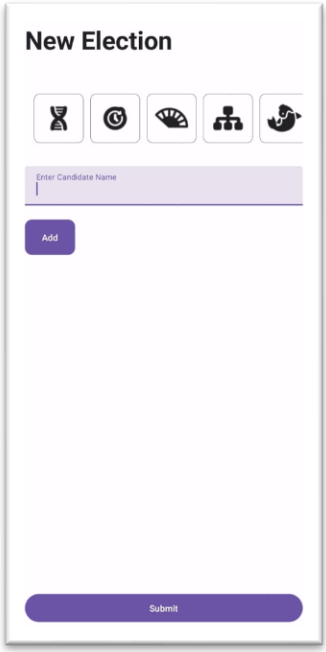

Fig. 6. Candidate Name and Logo

Fig. 7. New User Registration

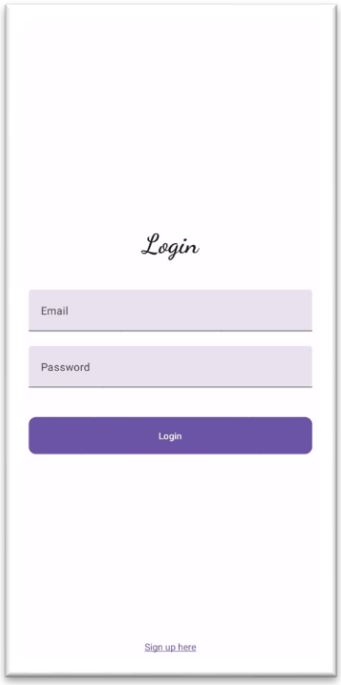

Fig. 8. User Login

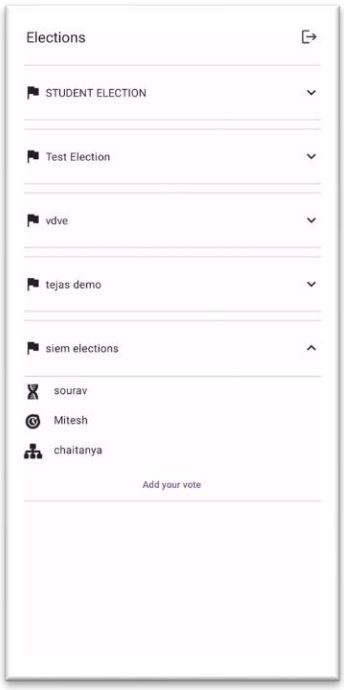

Fig. 9. User Home Screen

Fig. 10. Vote Casting

Fig. 11. Voting Results displayed on the Admin side

CONCLUSION AND FUTURE SCOPE

The proposed system offers several advantages, including reduced costs, faster tabulation of results, improved accessibility, enhanced accuracy, and decreased risks of human and mechanical errors. This implementation has undergone through its paces on a virtual client. It may be tested in the future on the Ethereum test net with many accounts. The possibility of a blockchain-based online voting System for large scale elections should be investigated in further research. The System can be employed for a particular use case, with the ability to assess the accuracy of calculations through measurements. To enhance speed and security, synchronization and consensus methods can be subject to discussion and continuous improvement.

REFERENCES:

1. Blockchain-Based E-Voting System, May 2021 International Journal of Scientific Research in Science and Technology, Prof. Mrunal Pathak, Amol Suradkar, Ajinkya Kadam, Akansha Ghodeswar
2. E-voting systems: A tool for e-democracy, January 2010Knowledge Management Research Practice 2(3):264-274, Emad Abu-Shanab, Michael B. Knight
3. Science and Information Conference 2015 July 28-30, 2015 — London, UK 1365 — P a g e www.conference.thesai.org, A Secure e-Government's e-Voting System, Mohammad Hosam Sedky, Essam M. Ramzy Hamed
4. E-Voting System Based on Blockchain Technology: A Survey, Sarah Al-Maaitah; Mohammad Qatawneh; Abdullah Quzmar, 2021 International Conference on Information Technology (ICIT)IEEE 2021
5. International Journal of Trend in Research and Development, Volume 2(5), ISSN 2394-9333 www.ijtrd.com IJTRD — Sep - Oct 2015 Available Online@www.ijtrd.com 438, Student Online Voting System, Raja Lakshmi, Meenakshi Nivya and K S Selvanayaki.
6. Hasan, S. M., Rashid, M. T., Chowdhury, M. S. S., & Rhaman, M. K, 2016, Development of a credible and integrated electronic voting machine based on contactless IC cards, biometrie fingerprint credentials and POS printer. Canadian Conference on Electrical and Computer Engineering (CCECE), Vancouver, BC, 2016, 1-5
7. M, D. K., A, S., N S, A., & D, P. K, 2016, Embedded System Based Voting Machine System using Wireless Technology. International Journal of innovative research in electrical, electronics, instrumentation and control engineering, February 2016, 4(2), 127–130.
8. 'Advanced Voting Machine Using Face Recognition', A Samundeeswari , P Parthasarathy, K Ragul, K Raguram , International Journal of Creative Research Thoughts (IJCRT) www.ijcrt.org, 2020. [Accessed 13 10 2019].
9. 'Arduino Based Authenticated Voting Machine (AVM) using RFID and Fingerprint for the Student Elections', Vinayachandra, K Geetha Poornima, M Rajeshwari and K Krishna Prasad, Journal of Physics: Conference Series, 2020.
10. Sroa, Rohit and Sinha, Priyanshu and Sharma, Ritwik and Rustagi, Parth and Sharma, Moolchand, A Visionary Approach to Smart Voting System (July 12, 2021). Proceedings of the International Conference on Innovative Computing & Communication (ICICC) 2021
11. K. Patidar and S. Jain, "Decentralized E-Voting Portal Using Blockchain," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019, pp. 1-4, doi: 10.1109/ICCCNT45670.2019.8944820.
12. T. Vairam, S. Sarathambekai and R. Balaji, "Blockchain based Voting system in Local Network," 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), 2021, pp. 363-366, doi: 10.1109/ICACCS51430.2021.9441912.
13. M. Ibrahim, K. Ravindran, H. Lee, O. Farooqui and Q. H. Mahmoud, "ElectionBlock: An Electronic Voting System using Blockchain and Fingerprint Authentication," 2021 IEEE 18th International Conference on Software Architecture Companion (ICSA-C), 2021, pp. 123-129, doi: 10.1109/ICSA-C52384.2021.00033.
14. N. B. Al Barghuthi et al., "An Analytical View on Political Voting System using Blockchain Technology - UAE Case Study," 2019 Sixth HCT Information Technology Trends (ITT), 2019, pp. 132-137, doi: 10.1109/ITT48889.2019.9075074.

15. D. Khoury, E. F. Kfoury, A. Kassem and H. Harb, "Decentralized Voting Platform Based on Ethereum Blockchain," 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), 2018, pp. 1-6, doi: 10.1109/IMCET.2018.8603050.
16. G. Rathee, R. Iqbal, O. Waqar and A. K. Bashir, "On the Design and Implementation of a Blockchain Enabled E-Voting Application Within IoT-Oriented Smart Cities," in IEEE Access, vol. 9, pp. 34165-34176, 2021, doi: 10.1109/ACCESS.2021.3061411.
17. O. Kurbatov, P. Kravchenko, N. Poluyanenko, O. Shapoval and T. Kuznetsova, "Using Ring Signatures For An Anonymous E-Voting System," 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), 2019, pp. 187-190, doi: 10.1109/ATIT49449.2019.9030447.
18. Syada Tasmia Alvi, Mohammed Nasir Uddin, Linta Islam, Sajib Ahamed, "DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system", Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 9, 2022, Pages 6855-6871, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2022.06.014.