Digital Voting System Using Blockchain Technology

Prof. Jayshree Patil
Information Technology
Dr. J.J.Magdum college of Engineering, Jaysingpur
jayshree.patil@jjmcoe.ac

Sainath Mohite
Information Technology
Dr. J.J.Magdum college of Engineering, Jaysingpur
mohitesai2713@gmail.c

Sanket Kumbhar
Information Technology
Dr. J.J.Magdum college of Engineering, Jaysingpur
Jaysingpur

Bhushan Dandavate
Information Technology
Dr. J.J.Magdum college of Engineering, Jaysingpur
Jaysingpur
.in

Hrishikesh Kamble
Information Technology
Dr. J.J.Magdum college of Engineering, Jaysingpur
Jaysingpur

Abstract **-** A digital voting system with Aadhar authentication is an electronic voting mechanism that makes use of India's Aadhar system for safe and efficient voter identification. Voters authenticate themselves with their Aadhar cards, which are linked to personal and biometric data. This technology aims to reduce voter fraud, ensure accurate voter identification, and speed up the voting process while protecting data security and privacy.

Keyword:-
Blockchain,Aadhar,Application,Biometric,Machine Learning.

I INTRODUCTION

Democracy is not an exception in a world where technology has changed almost every element of our existence. A new era of secure, effective, and inclusive election procedures might be ushered in by the innovative combination of technology with the time-honored institution of voting. Leading the charge in this innovation is the Digital Voting System with Aadhar authentication, which has the potential to revolutionize how we exercise our democratic rights. This comprehensive study essay aims to explore the various aspects of this revolutionary idea, from its advantages and claims to the significant issues and ramifications it poses for contemporary democracies.

Aadhar, India's pioneering biometric identification system, has been praised as one of the world's most ambitious digital endeavours. It was launched in 2009 and has quickly expanded to over a billion registered users, radically changing the way people identify their identities. Aadhar provides each individual a unique 12-digit identity number and secures it with a variety of biometric data, such as fingerprints and iris scans. This large library of personal information is the foundation of Aadhar authentication. There are a number of possible benefits to an Aadhar-authenticated digital voting system. They include increased voter turnout, faster administration, increased security, and more accurate voter identification. However, there are a number of barriers to implementing such a system, such as concerns about data privacy, cybersecurity, and equitable access for all locals.

As we work through this paper, we want to make sure that we are taking current Aadhar authentication-based digital voting systems seriously. To shed light on the revolutionary potential of this unique technique in electoral processes and its wider implications for democratic administration, this research attempts to provide a comprehensive analysis of its benefits and drawbacks.Digital voting technologies have the power to completely transform elections in contemporary democracies, making them more reliable, inclusive, and efficient. Their significance resides in their ability to preserve the fundamentals of free and fair elections while modifying democratic procedures to the demands of the digital age.

Electronic Voting Machines (EVMs):

During elections, electronic voting machines, or EVMs, are used in polling places to cast and count votes. They are meant to replace manual vote counting and conventional paper ballots. Many countries have come to embrace EVMs, the most prominent being Brazil, the United States, and India.Digital voting technologies have been developed in order to modernize the electoral process and make it easier, more accessible, and efficient. Three widely used types of digital voting technologies include electronic voting machines (EVMs), online voting platforms, and mobile voting apps.

Online Voting System:

Residents can vote online through online voting technologies, also referred to as internet voting, which eliminates the need for them to physically visit polling sites. Voting online has become more and more common in many countries and regions, especially among international and rural voters. Machines (EVMs), online voting platforms, and mobile voting apps.

Mobile voting system:

Mobile voting apps are smartphone applications that allow people to vote via their mobile devices. While mobile voting applications are still in the experimental stage in many places,

They offer the potential to boost voter accessibility and engagement

II. RELEVANCE OF WORK

[8] This paper is an attempt to develop an efficient electronic voting system using blockchain features like encryption and transparency principles. The particulars of the proposed electronic voting plan were implemented using the multichain platform. With a web-based application written in Java EE and running on the NetBeans platform with a Glassfish server native, the system is constructed in a controlled environment. The database that the software uses is MySQL. The multichain platform was chosen by the researchers because it was suitable for cryptocurrency.

[9] In order to provide authentication and non-repudiation for the user's encoded data, the researchers in this study developed a synchronous model based on distributed ledger techniques. Additionally, they developed a model that allowed voters to modify their votes prior to a predetermined deadline. Ubuntu, a Linux operating system, was used to build the system. Voter ID, vote, new voter signature, timestamp, and hash of the previous block are all included in each block. When paired with other voting methods, it is more secure and anonymous since decentralization occurs without the help of a third party and users utilize identifications rather than their true identities. The results indicate that the approach is safe and useful, and that it tackles.

[10] In this study, voter anonymity is provided by the ring structure, and integrity and transparency are ensured by blockchain technology. The user must input the public keys of the other ring members into the input algorithm and utilize his private key securely in order to generate the signature. The number of keys selected depends on the voter's level of anonymity. The likelihood of masking the voter's identity rises sharply if the selected group is small. Some advantages of this method include the opportunity to review the voter's rights and anonymity as well as the voter's ability to verify the validity of his vote.

[11] In this research, the concepts of block creation and block sealing are presented. It serves the purpose of increasing the blockchain's customizability; using the consortium blockchain was advised

[12] The entire electoral process is supervised by the election commission. Election Commission is what EC stands for. The election is created, activated, and closed by the EC within a predetermined time frame. The Election Commission (EC) oversees the entire voting process and makes the results public following the election. Prior to the election, the EC is tasked with running a voter registration drive in order to produce a voter list. Vi's personal data is kept on file by EC. Within the suggested framework, EC is regarded as a reliable source that guarantees the integrity of the information in the The EC employs a variety of workers from the polling place to the constituency (such as the presiding officer, assistant returning officer, and returning officer). Voters in the system have the option of casting their ballots online or in person at a polling place. Voting online requires users to first authenticate themselves, load ballots, cast their ballots, and then examine the results after the election. To vote at a polling place, however, a voter must provide their National Identity (NID) Card and successfully complete the verification process before they may cast their ballot.

The proposed method surreptitiously introduces the vis into the V U. In the voting system, there are two different units: the authentication unit and the V U. Vis walks entirely incognito into the V U. After authentication, one is granted permission to build a block. The hash value from the previous block's hash value is produced, and this new block is generated using the vi NID number. No one can identify the person who built the block after the vote was inserted inside of it.before they may cast their ballot. The vi manages every aspect of our system, from building blocks to adding votes; no other parties, such as the returning officer, agent, or presiding officer, are engaged.

[13] An electronic voting program implemented using blockchain technology. The blockchain code on Ethereum is shared and immutable, while the data stored on the network is safe and decentralized. Code that can be added to the blockchain and run by network nodes is made possible by the Ethereum Blockchain. Using the smart contract protocol of the Ethereum blockchain, the code in this application publishes to the decentralized application. Ethereum's virtual computer, known as smart contracts, enable you to write code and have it run.

[14] The program stores voter accounts, votes, and candidate data using Ethereum Blockchain technology, which functions as a decentralized database and network. Due to the decentralized nature of blockchain, the network is stable, safe, adaptable, and able to provide real-time services. The voter understands that there is only one vote available to him due to the program's inability to support multiple ballots, and that it will go to the appropriate candidate. This approach could make computerized voting more dependable.

III. LITERATURE REVIEW

The loss of forests and the effects of climate change may be exacerbated by conventional article-based voting systems. Sophisticated e-voting procedures are replacing article-based systems to overcome this problem. Therefore, in order to provide a safe voting procedure.

[10:48 AM, 4/3/2024] Bhushan Dandavate IT JJ: [1] They offered a rank choice electronic voting procedure by eliminating built-in limitations. To maintain its confidentiality, each vote is encrypted using the EL Gamal process. Moreover, proofs are produced at the time each vote is stored, confirming the counting process without requiring the data to be decrypted. The proposed mechanism is verified by contrasting experimental results with established mechanisms. The computational and communication overhead of the network may increase due to the encryption and decryption of data at each node. Additionally, candidates who submit information and cast ballots in an electronic voting system need to be safeguarded.

[2] have introduced a crypto-biometric approach to online voting. The authors proposed two primary crypto-biometric methods—the palm vein and palmprint—and used a threshold measure in their gabor filter. Furthermore, the transmitted data is encrypted with a random key after being embedded in a biometric vector using a fuzzy commitment approach.

[3] have illustrated the openness and structural integrity of nationwide electronic voting in light of security concerns and requirements. The writers gave an example of how, more than 20 years ago, voting was adopted nationwide in Brazil. While the article-less voting procedure makes voting easier and more accessible for customers in remote areas. Nevertheless, there are serious security problems with article-less electronic voting systems, including voter un likability, integrity, and verifiability. Moreover, vote manipulation and authenticity are the two main security issues with e-voting systems that need to be addressed in order to verify the legitimacy of voters throughout the election process. A number of researchers have created secure electronic voting systems, but because computing devices are so small, none of the methods are workable.

[4] The term "smart contracts" and its notion are attributed to computer science and law graduate Nick Szabo. His stated goal with smart contracts is to build Internet-based electronic commerce protocols between strangers by applying extremely sophisticated legal procedures. An open-source blockchain platform called Ethereum is offered for the implementation of smart contracts. Ethereum created a new programming language called Solidity (similar to JavaScript) to be used in the development of these contracts. We use a permissioned blockchain smart contract mechanism to implement our electronic voting system. The functions will be covered in detail in Section III. Election administrators use the Admin dApp to instantiate a set of smart contracts on the Ethereum blockchain, which represent each election in Netvote.

A single ballot is referred to by each ballot smart contract. A voter pool smart contract can be used to list several ballots simultaneously; for example, each voter pool smart contract could represent a polling place. Consequently, a voter registers at the voting place and uses the voter dAapp to communicate with the voter pool smart contract. In order to provide voters with privacy during a private election, Netvote uses a Vote Gateway. Through the voter dApp, each voter sends a cryptographically signed vote token to the Vote Gateway for verification.[4] Similar to the AV-net protocol, the new protocol does not require a private channel or a third party to be trusted.

IV. PROPOSED SYSTEM

Praposing Up a Digital Voting Scheme Using blockchain technology and Aadhar, India's biometric identity system, to create a safe and transparent election process is known as "Using Blockchain with Aadhar Card Integration." This is a thorough description of how the suggested system would operate:

- Voter registration: To use the digital voting system, eligible voters must connect their Aadhar cards. This will entail authenticating their Aadhar details, which comprise biometric information such as fingerprint and iris scans, their personal identity.
- Creation of Digital Identity: Following verification, the voter would have a distinct digital identity that was directly connected to their Aadhar information.After training, the machine learning model should be tested on a hold-out set to determine its effectiveness. This will help to determine any areas in which the model requires, The blockchain would provide safe storage for this digital identity, guaranteeing its immutability and resistance to tampering.
- 3. Authentication: Voters would have to use their digital identities to authenticate themselves on election day,To ensure that only eligible voters may cast ballots, this authentication would entail a biometric scan, such as fingerprint or iris recognition.
- Ballot Creation: A digital ballot featuring the candidates' lists and election-specific topics would be created by the electoral authorities. In order to guard against manipulation, this ballot would be safely recorded on the blockchain and encrypted.
- Voting: Following successful authentication, voters would have access to the digital ballot via a secure website or mobile application. They would electronically cast their ballots, and the blockchain would verify their digital identities along with the votes they made.
- Blockchain Infrastructure: A transparent, tamper-proof record of each vote would be provided by the blockchain ledger. To ensure data security, it would be a permissioned blockchain that is only accessible by those who are permitted.
- Verification: Following the voting process, voters may independently check their selections on the blockchain, promoting openness and guaranteeing the validity of their ballots.
- Vote Counting and Outcomes: Using blockchain smart contracts, the votes would be automatically tallied as they are cast,Transparency would be improved by making election results available to the public and authorized authorities.
- Privacy and Security: In order to allay worries about privacy, the system will make sure that Aadhar data is kept private and safe and that only the vote itself is recorded on the blockchain. Robust encryption and cryptography methods would safeguard the information.
- Prevention of Double Voting: By cross-referencing digital identities, the blockchain would ensure that every voter can cast only one vote.
- Audit Trail: To improve the system's overall accountability and transparency, an audit trail would be kept up to date so that election officials could monitor and confirm each vote.
- Inclusivity and Accessibility: The system's digital format and Aadhar integration would enable it to be used by a

wider spectrum of voters, including those who are isolated or have impairments.

- Scalability and Reliability: In order to provide scalability during periods of high demand for elections, the technological infrastructure would be built to manage a sizable amount of transactions safely and consistently.
- Legal and Regulatory Compliance: To guarantee the system's validity and compliance, it would abide by all pertinent legal and regulatory standards, such as election and data protection regulations.The goal of the proposed Digital Voting System Using Blockchain with Aadhar Card Integration is to protect voters' privacy while improving election security, accessibility, and transparency. To guarantee successful implementation and broad acceptance, nevertheless, meticulous planning, stringent security measures, cooperation with governmental organizations, and public awareness campaigns would be required.

V. OBJECTIVES

Objective 1: There are fake voters in various elections so that's why we design this application.
Objective 2: Designing the graphical user interface for the application.
Objective 3: Utilize a reliable database management system, such as Firebase, to securely store and manage voter information.
Objective 4: The system is expected to facilitate real-time updates, ensuring timely and accurate election results
Objective 5: We are using blockchain technology for storing the data of voters and voting result so that's why it is temper proof, SHA256 hashing for storing and verifying votes.

VI. METHODOLOGY

The process of constructing Problem Solving Methods is assumption based. During this process assumptions are added that facilitate efficient operationalization of the desired functionality.
Establish strict data privacy controls to protect voters' personal information.
Implement data anonymization techniques to prevent the identification of individual votes.
Continuously assess and improve the system based on user feedback and evolving security threats.
Launch campaigns to inform the public about the new digital voting system and its benefits.

1. Open Block Chain.
2. Record transactions in a permanent way.
3. Closed Block Chain
4. A private network that maintains a shared record of transactions.
5. Those who have permission only they can access network.
6. Cryptography.
7. Symmetric Cryptography Asymmetric Cryptography.
8. Proof of Work
9. Start >> Transaction >> Minors >> Block >> Block puzzle >> Proof of Work >> Broadcasted new block to n/w>> Verification of minors

VII. RESULTS

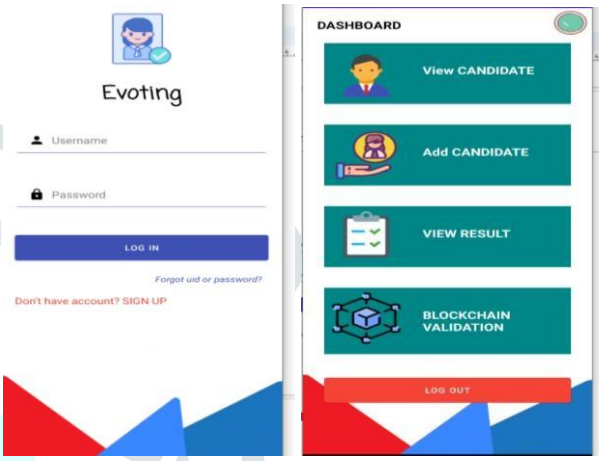

Fig. 1

First is the login page where only admin can login by using login credentials such as username and password.

Dashboard :-

1. View Candidate :- Here We can see the candidates those who are participate in Election.
2. Add Candidate :- Here we can the candidates those who are want to stand for election.
3. View Result :- Here we can display the election result.
4. Blockchain Validation :- Here we see the election participants hash value.

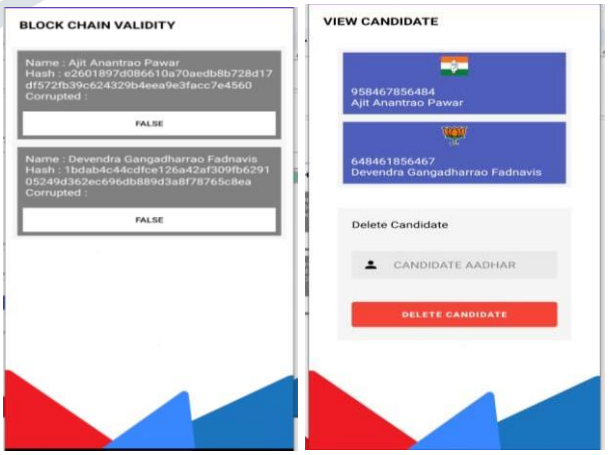

Fig. 2

VIII. CONCLUSION

The experiments in our research highlight the advantages and disadvantages of both conventional and blockchain electronic voting methods. Our study's research and conclusions demonstrate that key election stakeholders and government decision-makers do not have the information needed to hold an effective electronic voting system during national elections. This research looks at the experiences of several national elections in numerous significant countries and how problems and misguided attempts marred the process. Then came blockchain technology, which offers a unique way around the problems with electronic voting methods. Researchers are now conducting a number of experiments on blockchain technology both nationally and privately and last, a digital voting system that makes use of Aadhar identification might enhance voting process security and accessibility. However, it raises important questions about technology, privacy, and legal difficulties. A multidisciplinary strategy and a dedication to overcoming these challenges will be needed for the implementation to be effective. This is a dynamic subject of study that is open to ongoing inquiry and advancement as society and technology progress.

REFERENCES:

[1] X. Yang, X. Yi, S. Nepal, A. Kelarev, and F. Han, ``A secure veri_able ranked choice online voting system based on homomorphic encryption,"IEEE Access, vol. 6, pp. 20506_20519, 2018.

[2] A. Meraoumia, H. Bendjenna, M. Amroune, and Y. Dris, ``Towards asecure online E-voting protocol based on palmprint features," in Proc. 3rd Int. Conf. Pattern Anal. Intell. Syst. (PAIS), Oct. 2018, pp. 1_6.

[3] D. F. Aranha and J. van de Graaf, ``The good, the bad, and the ugly:Two decades of E-voting in Brazil," IEEE Secur. Privacy, vol. 16, no. 6,pp. 22_30, Nov. 2018.

[4] Blockchain-Based E-Voting System Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson School of Computer Science Reykjavik University, Iceland {fridrik14, gunnlaugur15}@ru.is of Science and Mathematics University of Minnesota, Morris Morris, Minnesota, USA 56267 schu4276@morris.umn.edu

[5] Electronic Voting System Implementation Through BitcoinBlockchain Technology Cassandra Schultz Division

[6] Secure Digital Voting System based on Blockchain Technology Kashif Mehboob Khan1, Junaid Arshad2, Muhammad Mubashir Khan1 1 NED University of Engineering and Technology, Pakistan 2 University of West London, UK.

[7] Secure Electronic Voting (E-voting) System Based on Blockchain on Various Platforms K. Varaprasada Rao and Sandeep Kumar Panda

[8] Khan, K. M., Arshad, J., and Khan, M. M. "Secure digital voting system based on blockchain technology" (Khan et al., 2018).

[9] Haibo Yi, "Securing e-voting based on blockchain in p2p network "(Yi, 2019)

[10] Oleksandr Kurbatov, Pavel Kravchenko, Oleksiy Shapoval, Nikolay Poluyanenko, Mariana Malchyk, Alina Sakun and Vladyslav Kovtun "Anonymous Decentralized E voting system" (Kurbatov et al., 2019).

[11] P. Raghava, P. Uday Kiran, Vimali. J.S, "Trustworthy Electronic Voting using Adjusted Blockchain Technology" (Shahzad & Crowcroft, 2019).

[12] Towards A Privacy-Preserving Voting SystemThrough Blockchain Technologies Rabeya Bosri, Abdur Razzak Uzzal, Abdullah Al Omar, and A S M Touhidul Hasan Department of Computer Science and Engineering University of Asia Pacific Dhaka, Bangladesh, Md. Zakirul Alam Bhuiyan Department of Computer and Information Sciences Fordham University New York, NY 10458, USA