IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 6, May 2025
Impact Factor: 7.67

Decentralized E-Voting System Using Blockchain Technology

Prof. Disha Nagpure, Hanuman Keskar, Krushna Khairnar, Jidnesh Shah, Abhay Sanap
Department of Artificial Intelligence and Machine Learning
Alard College of Engineering and Management, Marunji, Pune, Maharashtra, India

Abstract: *Elections form the foundation of contemporary democratic systems. Yet, traditional voting mechanisms often face issues related to trust and susceptibility to manipulation. This study investigates the capabilities of decentralized electronic voting systems enhanced by blockchain technology and Aadhaar-based OTP verification. By utilizing the security, transparency, and unchangeable nature of blockchain along with the strong identity validation provided by Aadhaar OTP, the proposed system seeks to transform the current voting process. It effectively tackles significant problems of conventional voting, such as electoral fraud and distrust, through the use of smart contracts, verified voter identities, and cryptographic safeguards.*

Keywords: Blockchain, Decentralized Voting, Electoral System, Aadhaar OTP, Distributed Technology, EVM

I. INTRODUCTION

The emergence of blockchain technology has paved the way for a new generation of decentralized applications, bringing transformative changes across multiple sectors. One domain with significant potential for innovation is the electoral system. Conventional voting methods are frequently challenged by issues like tampering, fraud, and public mistrust. In response, decentralized electronic voting systems are gaining attention as viable solutions. This study examines the practicality and advantages of deploying a blockchain-based e-voting system integrated with Aadhaar OTP (One-Time Password) verification. By combining blockchain's features—such as immutability, transparency, and security—with the strong user authentication provided by Aadhaar OTP, the proposed approach seeks to strengthen the reliability and effectiveness of the voting process.

Blockchain functions as a decentralized and distributed ledger that is inherently resistant to manipulation, ensuring that each vote is permanently and securely recorded. Its open and verifiable nature also promotes transparency, enabling public scrutiny of the entire voting procedure and thereby building greater voter trust and assurance.

A. Traditional E-Voting System

One of the prominent technical hurdles faced by modern e-voting systems is secure digital identity management. It is essential that eligible voters are registered within the system before the election takes place, and their data must be stored in a digitally compatible format. Moreover, protecting the confidentiality of their identity within any database is critical. Traditional electronic voting systems may encounter several challenges, including:

- **Anonymity in Vote Casting:** It is vital to maintain the anonymity of voters after their ballots are submitted.
- **Secure Ballot Representation:** Safely representing votes within web platforms or databases continues to be a significant challenge.
- **Vote Verification by Individuals:** There must be a method for voters to confirm that their vote has been accurately recorded.
- **High Deployment Costs:** The initial implementation of electronic voting infrastructure can incur substantial expenses.
- **Escalating Security Concerns:** The growing threat of cyber-attacks presents a major vulnerability for online voting platforms

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 6, May 2025
Impact Factor: 7.67

B. What is Blockchain technology?

Fig 1. Blocks of Blockchain

Blockchain is a decentralized and distributed ledger system designed to record transactions with a high level of security and transparency. It consists of a series of blocks, each holding a set of data or transaction records. Once a block is appended to the chain, its contents become permanent and tamper-proof, guaranteeing the immutability of the stored information. Due to its open- access nature, blockchain enables public verification, thereby enhancing transparency and building trust and confidence in processes like electronic voting.

C. Working Of E-Voting Using Blockchain

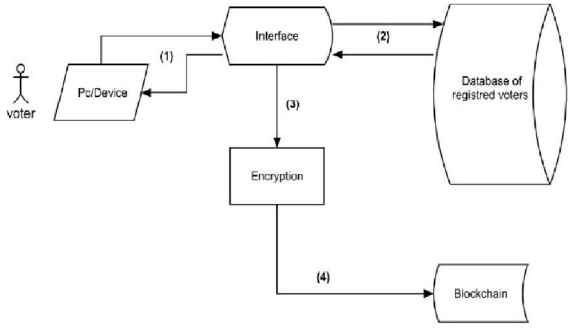


Fig 2. Working of E-Voting System

As per the above structure the working of e-voting system using blockchain is:

Requesting to Vote:

To initiate the voting process, users must log in using their credentials. In this e-voting system, authentication will rely on a combination of the voter's Social Security Number, residential address, and a voting confirmation code issued by local election authorities. The system verifies the submitted data and, if it matches a registered voter's record, grants access to vote. The system is designed to prevent users from self-generating identities or registering arbitrarily. Allowing random identity creation can lead to Sybil attacks, where malicious users submit multiple fake identities to manipulate the election outcome.

Casting a Vote:

Once verified, voters can either select a candidate or cast a protest vote through a user-friendly interface. Each verified voter receives a unique token (represented by Ethereum) with an initial Boolean value of 1. Upon casting a vote, the token's value changes to 0. A voter is permitted to vote only when the token value is 1, thereby eliminating the risk of multiple voting attempts.

Encrypting Votes:

After casting a vote, the system generates a unique input composed of the voter's identification number, full name, and a hash of the previous vote. This ensures that each vote has a distinct and verifiable encrypted output. The data is then stored in the block header of the newly cast vote. To secure this information, the SHA (Secure Hash Algorithm) one-way encryption is applied—making it practically impossible to reverse-engineer the hash. As a result, no personal voter information can be retrieved from the encrypted data.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 6, May 2025
Impact Factor: 7.67

Adding the Vote to the Blockchain:

Once a new vote block is generated, it is stored in the relevant blockchain based on the candidate selected. Each new block links back to the previous vote, maintaining the integrity and chronological order of the voting chain.

D. Consensus Algorithms

Consensus algorithms are fundamental to blockchain technology, playing a critical role in maintaining the integrity and security of the decentralized ledger. These protocols allow the distributed network's nodes to reach an agreement on the validity and sequencing of transactions, which helps prevent double spending, ensures data consistency, and reinforces the overall trustworthiness of the system. Consensus mechanisms are designed to keep all copies of the ledger across the blockchain nodes consistently synchronized.

This overview examines several consensus algorithms commonly utilized in blockchain-based e-voting systems, including Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof of Activity, Proof of Burn, Practical Byzantine Fault Tolerance (PBFT), Proof of Vote, and Parallel Proof of Vote. Among these, Proof of Work is perhaps the most widely known, being the foundation of blockchains like Bitcoin and Ethereum.

In PoW, nodes—referred to as miners or validators— compete to solve complex mathematical puzzles. The first to solve it successfully earns the right to append a new block to the chain, a process commonly known as "mining." This mechanism secures the blockchain but demands significant computational power.

On the other hand, Proof of Stake (PoS) aims to improve efficiency by removing the need for resource-intensive mining. In PoS, participants are known as forgers, and the block creation process is called forging. Forgers lock up a certain amount of cryptocurrency as a "stake," and the protocol uses this stake to determine which forger will produce the next block. Two main techniques are employed for selecting the next forger: coin-age selection and randomized block selection.

E. Aadhar

Img 1. Aadhar

Aadhaar is a 12-digit unique identification number assigned to residents of India, based on their biometric and demographic details. The Unique Identification Authority of India (UIDAI), a statutory body, is responsible for collecting and managing this data. As the world's largest biometric ID system, Aadhaar contains highly sensitive personal information. This data is critical, especially as many significant financial transactions are linked to Aadhaar details.

However, data breaches pose a serious threat. UIDAI has acknowledged that over 200 government websites had once publicly exposed private Aadhaar data. Though this information has since been removed, any data accessed by malicious actors remains potentially in circulation. All Aadhaar records are stored in a centralized database managed by UIDAI, which introduces a key vulnerability—centralized systems are more susceptible to security breaches.

Storing this information on a blockchain could significantly reduce such vulnerabilities. Blockchain functions as a cryptographically secured digital ledger, where transactions are grouped into blocks. Each block includes a cryptographic hash of the previous one, creating a secure and tamper-resistant chain. When a new block is added, the

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 6, May 2025
Impact Factor: 7.67

update is propagated to all copies of the ledger within the network. At its core, blockchain allows a community of users to maintain a shared and immutable transaction history, which cannot be altered once recorded.

F. Aadhar Verification

Aadhaar verification is a mechanism that allows individuals to verify and manage their identities, ensuring secure authentication, authorization, data protection, and controlled data sharing both within organizations and online platforms. Traditional systems currently in use are prone to issues such as single points of failure, lack of interoperability, and potential breaches of privacy. Blockchain-based verification systems offer a solution by enabling consensus-driven, transparent, and secure sharing of personal information via distributed ledger technology.

Aadhaar OTP (One-Time Password) verification is widely used across India as an added security layer for online transactions. It functions by sending a unique, time-bound code to the user's registered mobile number, which must be entered to confirm identity—thus helping to prevent unauthorized access and fraud.

In decentralized e-voting systems, Aadhaar OTP verification plays a crucial role in ensuring secure access and eliminating voter impersonation. When a voter registers on the platform, their Aadhaar number is linked to their account. At the time of voting, an OTP is sent to the voter's registered mobile device, and the vote can only be cast upon entering the correct code. This mechanism ensures that only the legitimate Aadhaar holder can access the system and participate in the voting process.

The proposed Aadhaar OTP-based verification approach supports self-sovereign identity, leveraging decentralized networks. It empowers users with full control over their identity data, ensuring that no third party can access or share their personal information without explicit consent.

G. Comparison of Hashing Algorithms

In the following table the comparison between the various cryptographic hash algorithms like SHA-1, SHA-2, and SHA-3 shows various parameters.

Properties	Name of Algorithms		
	SHA-1	SHA-2	SHA-3
Block size	512 bits	512/1024 bits	1088/576 bits
Word size	32 bits	32/64 bits	320/320 bits
Output size	160 bits	256/512 bits	1600/1600 bits
Rounds	80	64/80	24/24
Operations	ADD, XOR, OR, AND, NOT, ROTATE	ADD, XOR, OR, AND SHIFT, ROTATE	-
Constructions	Merkle-Damgard	Merkle-Damgard	Sponge

Table 1. Comparison of Hashing algorithm

Ethereum uses a consensus algorithm known as Ethash, which relies on the Keccak-256 hashing function. Keccak is a family of cryptographic hash functions that eventually became standardized as SHA-3. However, Ethereum continues to refer to it as Keccak because the implementation it uses has parameters that slightly differ from the official SHA-3 standard. In contrast, Bitcoin uses SHA-256, which is part of the SHA-2 family, for hashing its blockchain blocks—specifically applying a double SHA-256 operation (SHA-256(SHA- 256(TXN))).

Ethash, Ethereum's hashing mechanism, encrypts blockchain data using Keccak-256. Starting from Solidity version 0.4.3, the keccak256 function was introduced, which is functionally identical to sha3, but named differently to minimize confusion—especially for developers who are new to Ethereum development. As a result, developers are encouraged to use keccak256 over sha3 in their smart contract code.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 6, May 2025
Impact Factor: 7.67

Keccak is based on a unique method known as the sponge construction. This technique relies on a random permutation or pseudorandom function and allows an arbitrary amount of input data to be "absorbed." It can then "squeeze" out any amount of output data, acting like a pseudorandom function relative to all previous inputs. This flexible and efficient approach contributes to the robustness and adaptability of Keccak-based hashing functions.

H. Algorithm

1. The user begins by providing essential information such as their username, contact number, and email address to create a wallet.
2. A hash will be generated for the transaction that creates the user's wallet.
3. The user will upload their Aadhaar identity details along with a scanned copy of the Aadhaar card. This data will be stored on IPFS, with the corresponding hashed addresses saved on the blockchain.
4. A smart contract is used to digitally sign a transaction and generate a hash value, which is recorded in each block on the blockchain. Any alteration in the block will result in a drastic change in the hash value, ensuring the integrity of the data.
5. Third-party companies that request access to specific identity details for authentication purposes will trigger a notification to the individual whose identity is being queried.
6. Once the individual grants permission, third parties can use the provided identifiable information for authentication. Importantly, blockchain does not store the user's personal data. Instead, only the transactions between the identity holder and third- party companies are recorded on the blockchain, while Aadhaar details are securely encrypted and stored on IPFS.

II. LITERATURE SURVEY

Decentralized e-voting systems powered by blockchain technology have emerged as a promising alternative to traditional voting methods. The integration of Aadhaar verification adds an extra layer of security and authenticity to the process. This literature survey explores existing research and developments in this field.

Blockchain technology provides a secure, transparent, and immutable ledger for recording votes. Studies have demonstrated its potential to enhance the integrity and reliability of elections. Aadhaar, India's unique identification system, can be used to verify voter identity and prevent fraud. Integrating Aadhaar OTP verification adds an extra layer of security to the voting process.

Smart contracts can automate various aspects of the voting process, such as ballot creation, voting, and tallying, reducing the risk of human error and manipulation. Researchers have explored cryptographic techniques to protect voter privacy and ensure the security of the voting process. Addressing scalability challenges for large-scale elections is a key area of research. Techniques such as sharding and layer-2 solutions are being investigated. Ensuring interoperability between different blockchain-based e-voting systems is crucial for widespread adoption.

These studies have explored various aspects of decentralized e-voting systems, including system architecture, security measures, privacy protection, scalability, and interoperability. While significant progress has been made, further research is needed to address remaining challenges and ensure the widespread adoption of this technology.

III. METHODS AND MATERIAL

The suggested decentralized e-voting system is composed of the following key components:

- **Blockchain Network**: A permissioned blockchain network, such as Hyperledger Fabric or Ethereum, is implemented to securely store and manage voting data.
- **Smart Contracts:** Smart contracts are implemented on the blockchain to automate key voting processes, including the creation of ballots, the casting of votes, and the tallying of results.
- **Voter Registration Module:** A module designed for registering eligible voters, which includes identity verification through Aadhaar OTP.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 6, May 2025
Impact Factor: 7.67

- **Voting Interface:** A secure and user-friendly interface that allows voters to cast their votes in a safe and efficient manner.
- **Authentication Server:** An Aadhaar authentication server responsible for verifying voter identities using OTP.

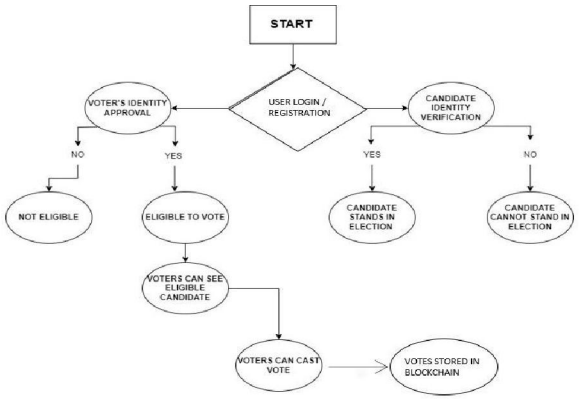


Fig 3. Flow Chart

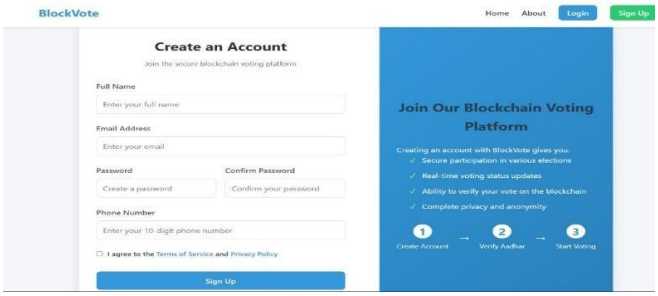
IV. WORKFLOW

- **Voter Registration:** Eligible voters enter their information into the system and provide their Aadhaar number. An OTP is sent to the registered mobile number for verification. After successful verification, the voter's details are securely stored on the blockchain.
- **Ballot Creation:** Smart contracts create unique, encrypted ballots for each registered voter. These ballots are stored on the blockchain, ensuring transparency and immutability.
- **Voting:** Voters log in to the voting interface using their credentials, select their preferred candidates, and cast their votes. Each vote is recorded as a transaction on the blockchain.
- **Tallying:** Smart contracts automatically tally the votes, ensuring the process is efficient and accurate, all within the blockchain.
- **Result Publication:** The results are published on the blockchain, providing a tamper-proof and auditable record of the election outcomes

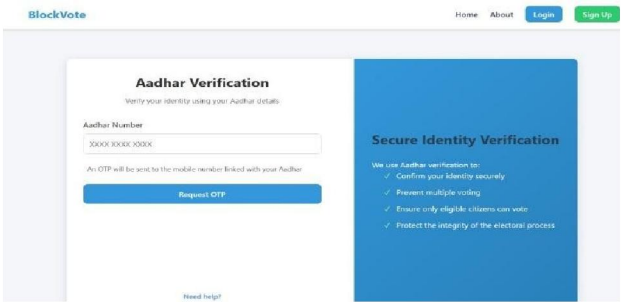
V. IMPLEMENTATION IMAGES

Img 1. Home page

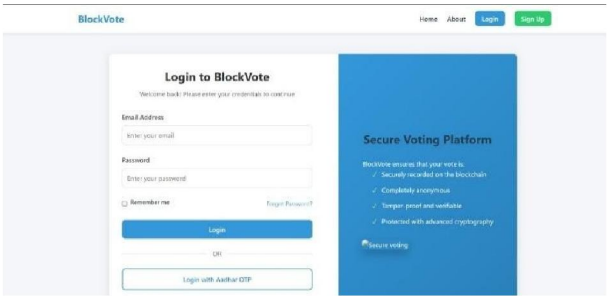
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 6, May 2025
Impact Factor: 7.67



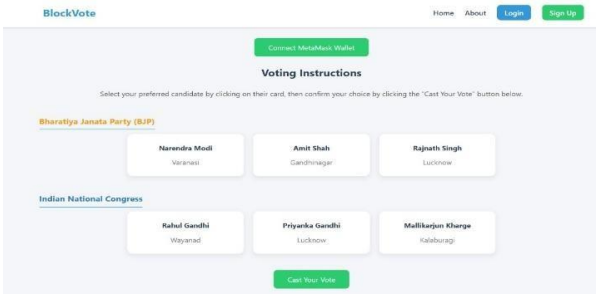
Img 2. Signup Page



Img 3. Adhar Verification Page



Img 4. Login Page



Img 5. Voting Interface

VI. CONCLUSION

Decentralized e-voting systems leveraging blockchain technology and Aadhaar verification present a promising alternative to the limitations of traditional voting methods. Although substantial advancements have been made, additional research is necessary to overcome challenges related to scalability, privacy, and regulatory issues. By tackling these obstacles, blockchain-based e- voting systems have the potential to improve the integrity and efficiency of democratic processes.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 6, May 2025
Impact Factor: 7.67

REFERENCES

[1]. A. Mandavkar and R. V. Agawane, "Mobile based facial recognition using OTP verification for voting system," 2015 IEEE International Advance Computing Conference (IACC), Banglore, India, 2015, pp. 644-649, doi: 10.1109/IADCC.2015.7154786.

[2]. N. Choudhary, S. Agarwal, G. Lavania, "Smart Voting System through Facial Recognition", April 2019, https://doi.org/10.26438/ijsrcse/v7i2.710. pp. 7-10, doi:

[3]. A Alvappillai, P. N. Barrin, "Face Recognition using MachineLearning",2017.doi:https://api.semanticscholar.org/CorpusID :43539771 .

[4]. H. Agarwal and G. N. Pandey, "Online voting system for India based on AADHAAR ID," 2013 Eleventh International Conference on ICT and Knowledge Engineering, Bangkok, Thailand, 2013, pp. 1-4, doi: 10.1109/ICTKE.2013.6756265

[5]. Ayesha Shaikh, Bhavika Oswal, Divya Parekh, Prof. B. Y. Jani, 2014, E-voting Using One Time Password and Face Detection and Recognition, Issue 02.

[6]. J. Liu, B. Li, L. Chen, M. Hou, F. Xiang and P. Wang, "A Data Storage Method Based on Blockchain for Decentralization DNS," 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), Guangzhou, China, 2018, pp. 189-196, doi: 10.1109/DSC.2018.00035.

[7]. Dagher, Gaby G.; Marella, Praneeth Babu; Milenkovic, Matea; and Mohler, Jordan. (2018). "Bronco Vote: Secure Voting System Using Ethereum's Blockchain". ICISSP 2018: Proceedings of the 4th International Conference on Information Systems Security and Privacy, 2018-January, http://dx.doi.org/10.5220/0006609700960107

[8]. Hanifa Tunisia, Rifa & Rahardjo, Budi. (2017). Blockchain based e voting recording system design. 1-6. 10.1109/TSSA.2017.8272896.

[9]. S. A. Adeshina and A. Ojo, "Maintaining Voting Integrity using Blockchain," 2019 15th International Conference on Electronics, Computer and Computation (ICECCO), Abuja, Nigeria, 2019, pp. 1-5, doi: 10.1109/ICECCO48375.2019.9043225.

[10]. F. Schroff, D. Kalenichenko and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Boston, MA, USA, 2015, pp. 815-823, doi: 10.1109/CVPR.2015.7298682