ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

AN EFFICIENT VOTE CASTING SYSTEM WITH AADHAR VERIFICATION THROUGH BLOCKCHAIN

Mr. E. PRAVEEN[1], Mr. SK. ANJANEYULU[2]

#1 postgraduate student pursuing an MCA in the Department of Master of Computer Applications

#2 Associate Professor in the Department of Master of Computer Applications

QIS College of Engineering and Technology, Ongole, Andhra Pradesh.

ABSTRACT

The **Efficient Vote Casting System with Aadhaar Verification through Blockchain** is a secure and transparent electronic voting system designed to improve the reliability, efficiency, and integrity of the voting process. Traditional voting systems may face challenges such as identity verification issues, duplicate voting, unauthorized access, data manipulation, and delays in vote counting. The proposed system integrates **Aadhaar-based voter verification** with **blockchain technology** to provide a trusted voting environment. During registration and voting, the system verifies the voter's identity using Aadhaar-related information and ensures that only eligible and authenticated voters can cast their votes. After successful verification, the vote is recorded as a blockchain transaction, where decentralized and tamper-resistant storage helps prevent unauthorized modification of voting records. Cryptographic techniques and blockchain-based validation provide transparency while maintaining the integrity of the election data. The system also maintains voter eligibility and voting status to prevent multiple voting attempts. An administrative module can monitor registered voters, manage candidates, verify voting records, and perform vote counting after the election process. The proposed approach reduces manual effort, improves the speed of vote processing, and provides a more secure and auditable voting mechanism. The system is intended as an **academic prototype** demonstrating blockchain-based electronic voting and identity verification concepts.

Keywords: Blockchain, Electronic Voting, Aadhaar Verification, Voter Authentication, Smart Contracts, Cryptography, Secure Voting, Decentralized System, Vote Integrity, Election Management.

INTRODUCTION

Voting is a fundamental process in a democratic society, as it enables citizens to participate in the selection of their representatives and influence important decisions. Traditional voting systems generally depend on centralized authorities for voter registration, identity verification, vote collection, and result management. Although electronic voting systems have improved the speed and efficiency of elections, challenges such as voter impersonation, duplicate voting, unauthorized access, data manipulation, and lack of transparency can still affect the reliability of the election process. Therefore, there is a need for a secure, efficient, and transparent voting mechanism that can protect voter identity while maintaining the integrity of the votes.

The Efficient Vote Casting System with Aadhaar Verification through Blockchain is proposed to address these challenges by integrating Aadhaar-based identity verification with blockchain technology. Aadhaar verification can be used to authenticate eligible voters before they are permitted to cast their vote. Once the voter's identity is successfully

verified, the system can allow the voter to securely participate in the election while preventing multiple voting attempts. Appropriate privacy controls are required so that Aadhaar information is not unnecessarily exposed or stored directly on the blockchain.

Blockchain technology provides a decentralized and tamper-resistant environment for maintaining voting records. Instead of depending entirely on a single centralized database, vote-related records can be maintained using blockchain transactions, making unauthorized modification considerably more difficult. Cryptographic techniques can be used to protect the integrity of voting records, while smart contracts can automate important election operations such as voter eligibility validation, vote submission, and vote counting according to predefined rules.

The proposed system aims to provide a simple and efficient platform where a voter can register, undergo identity verification, authenticate securely, and cast a vote electronically. After successful voting, the system records the transaction on the blockchain without revealing sensitive voter information publicly. The election administrator can monitor eligible voters, manage candidates and elections, and obtain reliable results from the recorded transactions. By combining identity verification, cryptographic security, blockchain-based record management, and controlled access, the system seeks to improve the security, transparency, and efficiency of the voting process.

Overall, the proposed system demonstrates how blockchain and digital identity verification can be integrated to develop a more trustworthy electronic voting framework. It is particularly suitable as an academic-level prototype for studying secure e-voting concepts, although a real-world election system would require compliance with election laws, Aadhaar usage restrictions, privacy requirements, accessibility standards, independent security audits, and rigorous certification.

LITERATURE SURVEY

The development of secure electronic voting systems has attracted significant research attention because traditional and centralized voting mechanisms face challenges related to voter authentication, vote integrity, privacy, transparency, and result verification. Researchers have explored electronic voting, biometric authentication, blockchain, cryptographic techniques, and decentralized architectures to overcome these limitations. The following literature survey summarizes important research directions relevant to the proposed “An Efficient Vote Casting System with Aadhaar Verification through Blockchain.”

1. Blockchain-Based Electronic Voting Systems

Several researchers have investigated blockchain as a foundation for electronic voting because of its decentralized structure and tamper-resistant transaction records. Blockchain can maintain voting transactions in a distributed ledger, making unauthorized modification of recorded votes difficult. Smart contracts can also be used to automate voter validation, vote submission, and counting processes. These approaches improve transparency and reduce dependence on a single centralized authority. However, blockchain-based voting systems still need to address voter privacy, scalability, transaction costs, and secure integration with identity-management systems.

2. Biometric-Based Voter Authentication

Biometric authentication has been studied as a method for reducing voter impersonation and duplicate voting. Fingerprints, facial recognition, iris recognition, and other biometric characteristics can be used to verify whether a person is an authorized voter. Compared with traditional username-and-password authentication, biometric verification provides a stronger association between the voter and their registered identity. However, biometric systems require reliable hardware, accurate recognition algorithms, and appropriate protection of biometric

information. Privacy concerns also arise when sensitive biometric data is stored or transmitted without adequate security.

3. Aadhaar-Based Identity Verification

Aadhaar provides a digital identity framework that can potentially support identity verification in applications requiring authentication of individuals in India. Researchers have explored Aadhaar-based authentication for different digital services, including identity validation and access control. In an e-voting application, identity verification can be used as a preliminary step to establish voter eligibility before allowing the user to cast a vote. However, Aadhaar should not be treated as a public voting identifier, and sensitive Aadhaar information should not be stored directly on a blockchain. A practical system should use authorized authentication mechanisms and store only the minimum information necessary for the voting process.

4. Cryptography in Electronic Voting

Cryptographic techniques are widely used in secure e-voting research to protect voter information and voting records. Encryption can protect data during transmission and storage, while hashing can help detect unauthorized modification of records. Digital signatures can provide authentication and integrity, and advanced cryptographic approaches such as zero-knowledge proofs and homomorphic encryption have been investigated for achieving voter privacy and verifiable elections. Although these techniques provide strong security properties, they can increase system complexity and computational requirements, especially for academic-level implementations.

5. Smart Contracts for Vote Management

Smart contracts have been proposed for automating election procedures on blockchain networks. A smart contract can maintain candidate information, validate whether an eligible voter has already voted, record a valid vote, and calculate or support election results according to predefined rules. Since the contract logic is executed according to predefined conditions, it can reduce manual intervention and improve transparency. Nevertheless, smart-contract-based voting requires careful design because vulnerabilities in contract logic can affect the entire election process.

EXISTING SYSTEM

Traditional voting systems and conventional electronic voting systems generally depend on centralized authorities and databases for voter registration, identity verification, vote casting, and result management. In a typical system, voter information is maintained in a centralized database, and voters are verified using identification documents, voter IDs, passwords, or manual verification procedures. Electronic voting machines can reduce the time required for vote counting, but they still depend on trusted infrastructure and administrative processes to maintain the integrity of election data.

Some existing electronic voting systems use online databases for storing voter and election information. Although these systems provide faster processing and easier management, a centralized database can become a potential single point of failure. If the database or server is compromised, unauthorized users may potentially modify, delete, or manipulate sensitive election information. Furthermore, voters may have limited ability to independently verify that their votes have been recorded correctly.

Disadvantages of the Existing System

1. Centralized Architecture: Most conventional systems depend on a central server or database, creating a single point of failure.
2. Risk of Data Manipulation: Election records stored in centralized databases may be vulnerable to unauthorized modification if adequate security controls are not implemented.
3. Limited Transparency: Voters generally cannot independently verify the complete lifecycle of their votes

because the underlying election database is controlled by an authority.

4. Voter Impersonation: Conventional authentication methods may not provide sufficiently strong identity verification, potentially allowing unauthorized individuals to attempt voting.
5. Duplicate Voting: Preventing multiple voting attempts requires effective voter-status tracking and authentication mechanisms.
6. Manual Verification: Systems involving manual document or identity verification can increase processing time and administrative workload.
7. Privacy Concerns: Storing voter identity information together with election records can create privacy and data-protection risks.
8. Single Point of Failure: Failure or compromise of the central server can interrupt election services or affect access to election information.
9. Limited Auditability: Traditional systems may make independent verification of voting records more difficult because users must rely heavily on the central election authority.
10. Dependence on Trusted Administrators: The security and correctness of the system largely depend on administrators properly managing databases, authentication, and election records.

PROPOSED SYSTEM

The proposed Efficient Vote Casting System with Aadhaar Verification through Blockchain is designed to provide a secure, transparent, and efficient electronic voting environment. The system combines Aadhaar-based voter verification, secure authentication, blockchain technology, cryptographic techniques, and smart contracts to improve the reliability of the voting process.

In the proposed system, voters first register with the required information and undergo identity verification through an authorized Aadhaar authentication mechanism. After successful verification, the voter is permitted to access the election interface. The system ensures that an eligible voter can cast only one vote for a particular election. Once the voter selects a candidate and confirms the vote, the voting transaction is securely recorded on the blockchain.

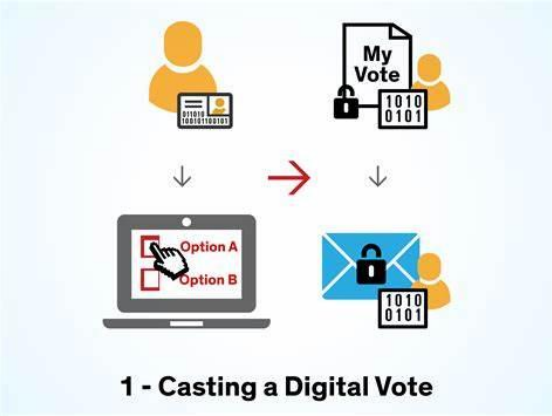
Blockchain provides a tamper-resistant ledger for maintaining voting transactions. Instead of storing sensitive Aadhaar information directly on the blockchain, the system can store only appropriate identifiers, transaction information, or cryptographic references. Smart contracts can be used to implement predefined rules such as voter eligibility, prevention of duplicate voting, vote recording, and election management. The administrator can manage elections, candidates, and authorized voters while monitoring the overall voting process.

Advantages of the Proposed System

1. Secure Voter Verification: Aadhaar-based authentication provides a stronger mechanism for confirming voter identity when implemented through authorized services.
2. Prevention of Duplicate Voting: The system maintains the voting status of each eligible voter and prevents multiple votes in the same election.
3. Blockchain-Based Security: Votes recorded on the blockchain are cryptographically linked, making unauthorized modification significantly more difficult.
4. Improved Transparency: Blockchain transactions provide a verifiable record of voting activity without exposing unnecessary voter information.

5. Data Integrity: Cryptographic techniques help protect voting records against unauthorized alteration.
6. Reduced Centralized Dependency: Distributed blockchain architecture can reduce dependence on a single database for maintaining vote records.
7. Smart Contract Automation: Election rules such as vote validation and transaction recording can be automated through smart contracts.
8. Privacy Protection: Sensitive Aadhaar information does not need to be stored directly on the public blockchain; only necessary cryptographic references or verification results can be maintained.
9. Faster Vote Processing: Electronic vote recording and automated processing can reduce the time required for managing and counting votes.
10. Improved Auditability: Blockchain transaction records can support auditing and verification of election activities.

SYSTEM ARCHITECTURE



METHODOLOGY

The methodology of the "An Efficient Vote Casting System with Aadhaar Verification through Blockchain" is designed to provide secure voter authentication, prevent duplicate voting, protect voter privacy, and maintain the integrity of voting records. The system follows a sequence of voter registration, identity verification, election access, vote casting, blockchain transaction creation, and result management.

1. Voter Registration

The process begins with voter registration. The voter provides the required basic information and Aadhaar-related verification details through the authorized verification mechanism. The system validates the submitted information and creates a voter profile after successful registration. Sensitive Aadhaar information is not directly exposed or stored on the blockchain.

2. Aadhaar-Based Verification

After registration, the system performs identity verification using an authorized Aadhaar authentication service. The purpose of this stage is to confirm that the voter is a valid and eligible individual. The system receives an appropriate verification response and does not need to place the complete Aadhaar number or other sensitive identity information on the blockchain.

3. Secure Voter Authentication

Once identity verification is completed, the voter authenticates into the voting system using the credentials or authentication mechanism provided by the application. The system checks the voter's eligibility and voting status before providing access to an active election.

4. Election and Candidate Management

The administrator creates and manages elections and candidate information. Details such as election name, candidate list, election start time, and closing time are maintained by the system. Only authorized administrators can perform election-management operations.

5. Vote Casting

After successful authentication, the voter can view the available candidates and select one candidate. Before submission, the system displays the selected choice for confirmation. Once the voter confirms the selection, the system generates a secure voting transaction.

6. Vote Validation

The system validates the voting transaction before recording it. It checks whether the voter is authenticated, eligible for the election, and has not already voted. Invalid or duplicate voting attempts are rejected. This stage helps maintain the uniqueness and correctness of the voting process.

7. Blockchain Transaction

After successful validation, the vote transaction is submitted to the blockchain network. The transaction contains only the information necessary for securely recording the vote and should avoid exposing sensitive personal or Aadhaar information. Cryptographic mechanisms are used to maintain the integrity of the transaction.

8. Smart Contract Execution

A smart contract can implement the predefined rules of the election. It can verify voting conditions, record the vote, update the voter's voting status, and support vote counting. Because the rules are executed according to predefined logic, manual intervention during individual vote processing can be minimized.

9. Blockchain-Based Vote Storage

The validated voting transaction is added to the blockchain ledger. Blockchain maintains transactions in a linked and tamper-resistant structure. Any attempt to modify an already recorded transaction can be detected through the cryptographic relationships between blockchain records.

10. Result Generation

After the election period ends, the recorded votes are processed according to the election rules. The system calculates the number of votes received by each candidate and generates the final result. The administrator can access the result through the authorized management interface.

11. Audit and Verification

The blockchain records can be used to support auditing of election transactions. Authorized personnel can verify that transactions were recorded according to the defined process. The system maintains a separation between voter identity information and voting records as far as technically and legally appropriate.

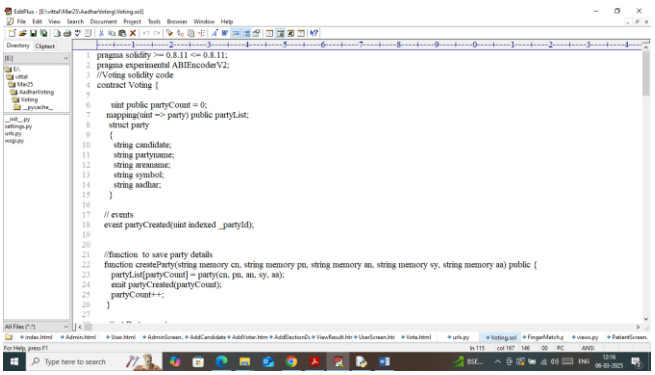
RESULTS AND DISCUSSIONS

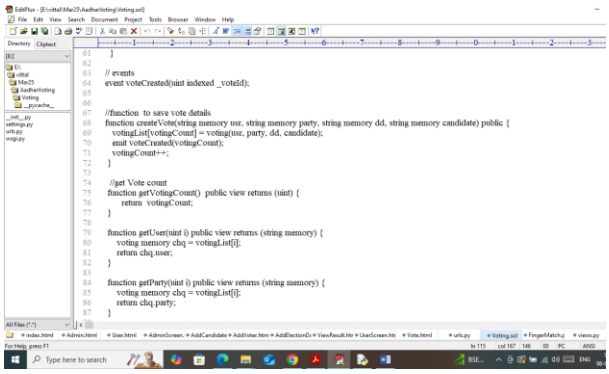
An Efficient Vote Casting System with Aadhar Verification through Blockchain

Traditional voting system in India often fall prey to bogus voting and to combat against this bogus voting EVM has been deployed but EVM database can be easily tamper. In propose paper author employing Blockchain along with IOT cloud connection to avoid EVM tampering.

Blockchain has inbuilt support for secured (encrypted) and tamper proof data storage which can be utilize to capture voter fingerprint and then matched with Aadhar fingerprint cloud database, if user fingerprint authenticated then only EVM will accept user vote. EVM will utilize IOT network to forward voting count details to centralized cloud server. IOT network cannot be easily hack so fully security will be provided to avoid any type of network attack.

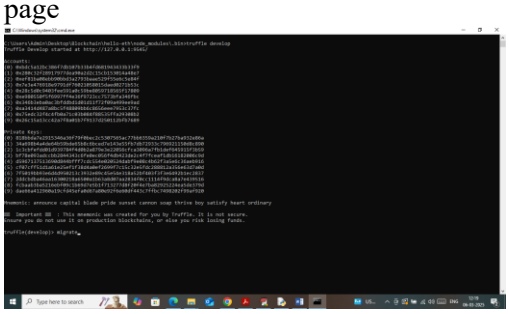
Blockchain can store and retrieve data with the help of Smart Contracts which can be designed using Solidity programming. Smart contract contains functions which can be called with any programming language. To manage candidate and voter details we have designed following contract



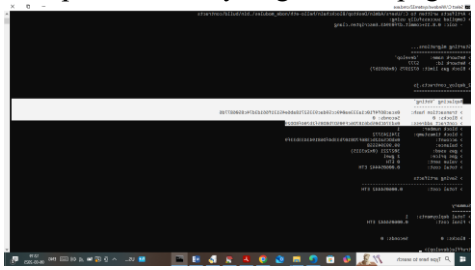


In above smart contract code we have defined required functions to manage candidate, voter and verification or tally functions. Now we need to deploy above contract to Blockchain Ethereum using below steps

1) First go inside 'hello-eth/node-modules/bin' folder and then look and double click on 'runBlockchain.bat' file to start Ethereum and get below page



2) In above screen Ethereum started with default accounts and private keys and now type command as 'migrate' and then press enter key to get below page



3)
4) In above screen in white colour text can see 'Voting' contract deployed and running successfully. Let the above console running till you executed code. All candidates and voter data will be saved in above EVM Blockchain memory.

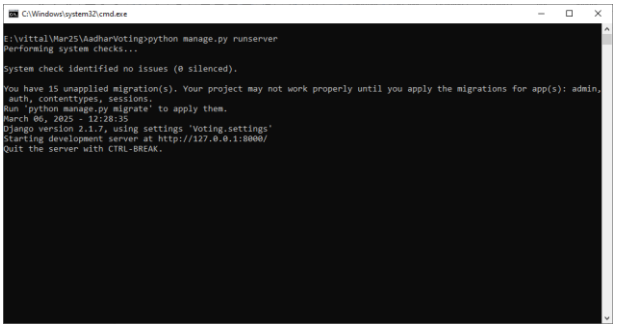
Modules Information

To implement this project we have designed two modules which consists of two different users such as 'Admin and Voter'.

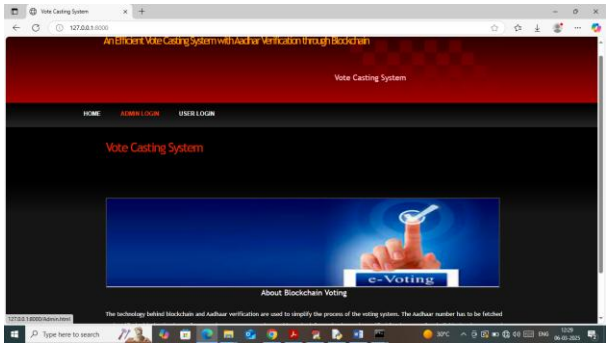
1) Admin Login: admin can login to system using username and password as admin and admin
2) Candidate Registration: after login admin will add candidate details
3) Voter Registration: using this module admin will add voter details by taking finger and Aadhar details and this data will be saved in Cloud Blockchain server
4) Add Election Date: using this module admin will add election date
5) View Vote Count: using this module admin can view number of voted secured by each candidate
6) User Login: whenever voter comes to cast vote then EVM will display Login page along with fingerprint image to upload. EVM will tally/matched user finger with Cloud Aadhar finger database. Once fingerprint authenticated EVM will forward user to cast vote. Each user allowed to cast vote only one time
7) View Result: voter can view number of votes secured by each candidate
8) Latency Graph: using this module will plot Blockchain Latency graph which take time to verify voters.

SCREEN SHOTS

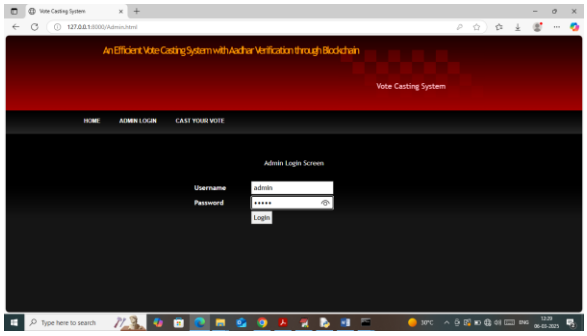
To run project double click on 'run.bat' file to get below page



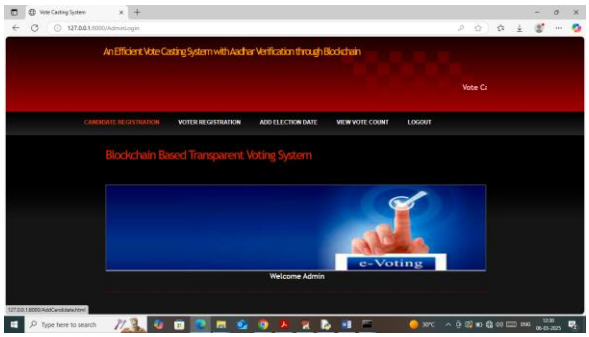
In above screen python web server started and now open browser and enter URL as http://127.0.0.1:5000 and then press enter key to get below page



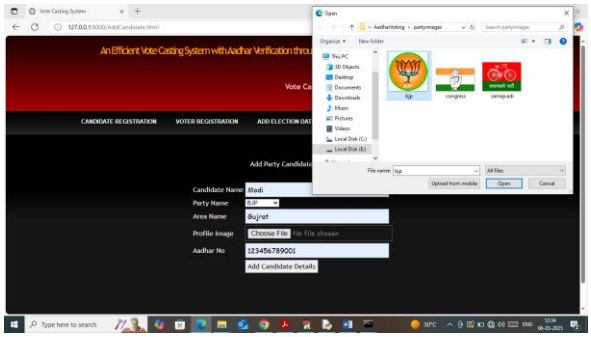
In above screen click on 'Admin Login' link to get below page



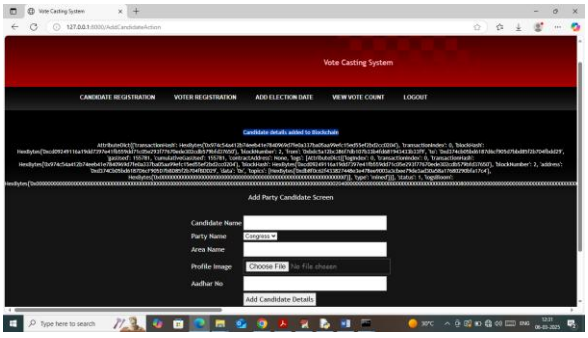
In above screen admin is login and after login will get below page



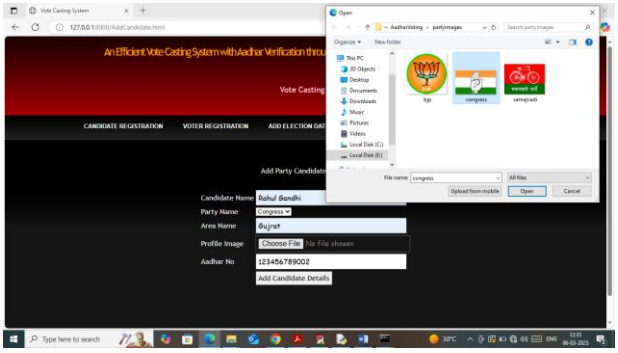
In above screen admin can click on 'Candidate Registration' link to add candidate details



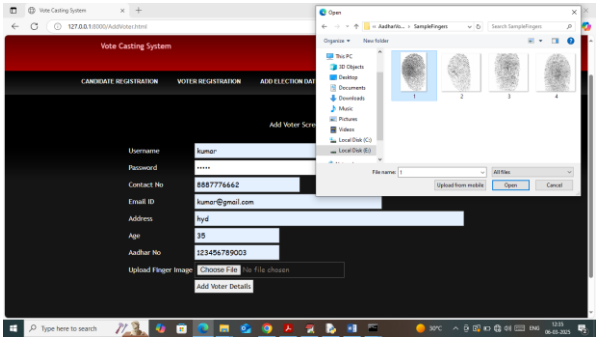
In above screen add candidate details along with party symbols and then press button to get below page



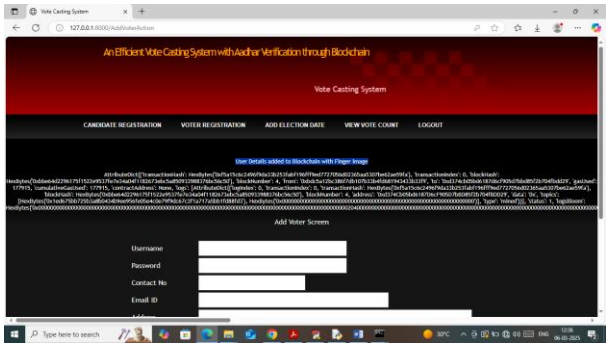
In above screen candidate details added to Blockchain and then in am displaying entire log obtained from Blockchain after data storage. In above log can see details like Transaction no, Block no, block hashcode and many other details. Similarly you can add as many candidates as you want



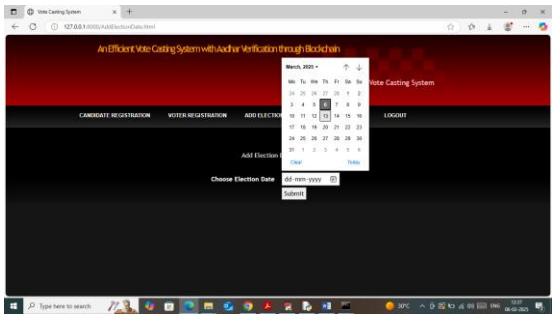
In above screen adding another candidate and now click on 'Voter Registration' link to get below page



In above screen adding voter details along with Aadhar no and fingerprint and then press button to get below page. (Note we don't have Aadhar database or fingerprint scanner so we are uploading as image).

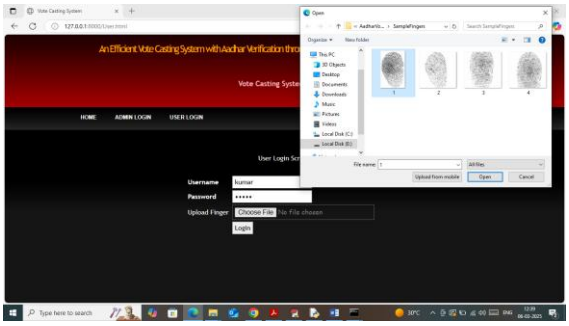


In above screen user details along with fingerprint added to Blockchain and similarly you can add as many voters as you want. Now click on 'Add Election Date' link to get below page



In above screen selecting and adding election date. You can choose any date but today only we have to run all modules so select today date only so voter can login and cast votes. Now click on 'View Vote Count' link to get below page

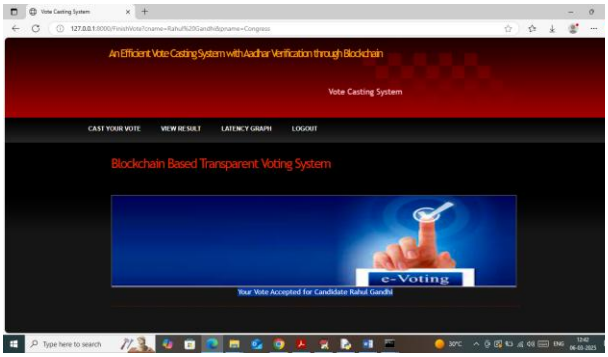
In above screen all candidates has 0 votes as no voter cast any votes yet. Now logout and login as voter to cast vote



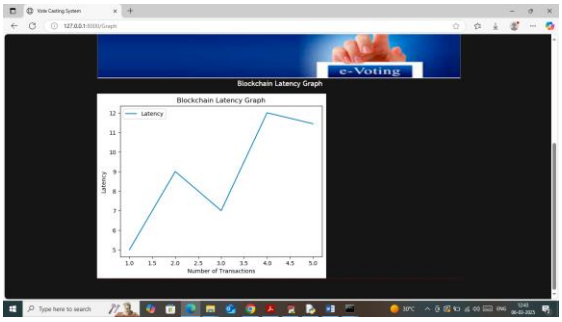
In above screen voter is login along with fingerprint and then Blockchain will authenticate voter finger with cloud database finger and upon successful verification will get below page

In above screen in blue text can see voter successfully verified and now click on 'Cast Your Vote' link to get below page

In above screen Voter can see list of candidates and can click on 'Click Here' link to cast vote and then will get below page



In above screen in blue text can see Voter votes successfully casted to selected candidate. Now click on 'Latency Graph' link to get below page



In above graph x-axis represents number of Blockchain transaction an dy-axis represents latency to execute transaction. Now click on 'View Result' link to get below page

In above screen user can view which candidate got how many number of votes.

Similarly by following above screens you can run project and manage all voting details in Blockchain.

CONCLUSION

The "An Efficient Vote Casting System with Aadhaar Verification through Blockchain" provides a secure and efficient approach to electronic voting by integrating identity verification with blockchain technology. The proposed system addresses major limitations of conventional voting systems, such as voter impersonation, duplicate voting, centralized data management, lack of transparency, and the possibility of unauthorized modification of voting records.

Aadhaar-based verification provides an additional layer for establishing voter eligibility, while blockchain technology helps maintain voting transactions in a tamper-resistant and auditable manner. Smart contracts can automate important operations such as voter validation, vote recording, and vote counting, thereby reducing manual intervention and improving system efficiency. The proposed approach also emphasizes privacy by avoiding unnecessary storage of sensitive Aadhaar information on the blockchain.

Overall, the system demonstrates the potential of combining secure authentication, cryptography, blockchain, and smart contracts to develop a more trustworthy electronic voting framework. The proposed model can serve as an academic prototype for studying blockchain-based e-voting systems. In the future, it can be enhanced with advanced privacy-preserving techniques, stronger multi-factor authentication, improved scalability, independent security auditing, and integration with officially authorized identity and election infrastructure.

REFERENCE

- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available as the foundational work describing blockchain and decentralized transaction management.
- Adida, B. (2008). *Helios: Web-based Open-Audit Voting*. Proceedings of the 17th USENIX Security Symposium.
- Chaum, D. (2004). *Secret-Ballot Receipts: True Voter-Verifiable Elections*. IEEE Security & Privacy, 2(1), 38–47.
- Benaloh, J., Rivest, R. L., Ryan, P. Y. A., Stark, P. B., Teague, V., & Vora, P. L. (2014). *End-to-End Verifiability*. In *Towards Trustworthy Elections*, 1–18. Springer.

- McCorry, P., Shahandashti, S. F., & Hao, F. (2017). *A Smart Contract for Boardroom Voting with Maximum Voter Privacy*. In *Financial Cryptography and Data Security*, Springer.
- Yavuz, E., Kalkan, K., & Çaglar, M. (2018). *Towards Secure E-Voting Using Blockchain Technology*. In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, IEEE.
- Ayed, A. B. (2017). *A Conceptual Secure Blockchain-Based Electronic Voting System*. International Journal of Network Security & Its Applications, 9(3), 1–9.
- Pawlak, M., Poniszewska-Marańda, A., & Kryvinska, N. (2018). *Towards the Intelligent Agents for Blockchain e-Voting System*. Procedia Computer Science, 141, 239–246.
- Hardwick, F. S., Akram, R. N., & Markantonakis, K. (2018). *E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy*. In *2018 IEEE International Conference on Internet of Things, Blockchain and Cyber Security (ICITBC)*, IEEE.
- Kshetri, N., & Loukoianova, E. (2019). *Blockchain Technology for Protecting Elections in Emerging Economies*. *Brookings Institution*.
- Election Commission of India. *Election Commission of India – Official Portal*. Information related to electoral processes, voter services, and election administration.
- Unique Identification Authority of India (UIDAI). *Aadhaar – Official Website*. Information related to Aadhaar enrolment, authentication, identity services, and associated policies.
- Wood, G. (2014). *Ethereum: A Secure Decentralised Generalised Transaction Ledger*. Ethereum Yellow Paper.
- Antonopoulos, A. M., & Wood, G. (2018). *Mastering Ethereum: Building Smart Contracts and DApps*. O'Reilly Media.
- Zyskind, G., Nathan, O., & Pentland, A. (2015). *Decentralizing Privacy: Using Blockchain to Protect Personal Data*. Proceedings of the 2015 IEEE Security and Privacy Workshops, 180–184.

Mr. E.PRAVEEN is a postgraduate student pursuing an MCA in the Department of Master of Computer Applications at QIS College of Engineering & Technology, Ongole an Autonomous college in Prakasam dist. He completed his undergraduate degree in BCA (Computers) from Acharya Nagarjuna University. With a keen interest in research and practical learning, he is actively involved in academic

Mr. SK. ANJANEYULU BABU is an Associate Professor in the Department of Master of Computer Applications at QIS College of Engineering and Technology, Ongole, Andhra Pradesh.