# Blockchain-enhanced electronic voting machine using fingerprint authentication

Vasudha Kulkarni[1], Sheetal Pawar[2], Sakshi Pawar[3], Dr. S B Dhonde Professor[4]
*Department of electronics and telecommunication AISSMS COE, Pune*

***Abstract*—Electronic voting (e-voting) systems are convenient and efficient but tend to have security and integrity issues. This paper introduces a blockchain-based electronic voting system with fingerprint authentication to improve security, transparency, and reliability. The system utilises a bespoke blockchain implemented through a Java library, an Arduino-based fingerprint module for voter verification, and a decentralised architecture to guarantee data integrity. Using a distributed ledger and a consensus algorithm, the system avoids risks of tampering and facilitates automatic recovery from an attack. The research discusses the methodology, design of hardware and software, security analysis, comparative performance analysis, and results obtained upon implementing this system.**

***Index Terms*—Blockchain, decentralized, distributed ledger, electronic voting)**

## I. INTRODUCTION

The fast development of technology has created the digitalization of numerous processes, such as electoral voting processes. Paper-based electoral voting processes, as widespread as theses process of counting votes and vulnerability to fraud or tampering. In a move to computerize electoral voting procedures, electronic voting (e-voting) systems have been conceived to accelerate the voting process and make it convenient. The systems, however, come with their own set of security issues, from vulnerability to hacking, leakage of data, and vote manipulation.

Among the most significant concerns with classical electronic voting systems is that they are built on centralized databases, single points of failure. Hacking of these databases can potentially breach the integrity of the election and confidence of people. In addition, threats to unauthorized disclosure of the information of the voters and manipulation of election results are enormous challenges. Therefore, the necessity for a secure, open, and auditable voting system, but maintaining the integrity of the election and secrecy of the voters, is compelling.In order to combat these attacks, we propose a blockchain-based e-voting system based on fingerprint verification for voter identification. Blockchain technology provides a decentralized and tamper-proof ledger for securely storing transactions and thus is most appropriate for the use of e-voting. With the integration of blockchain with fingerprint verification, we can guarantee that only the recorded voters can vote and the vote is held securely in a tamper-free space. Contrary to traditional systems that place the votes and authenticate them through a central body, our system places the voting information across several nodes, rejecting centralization threats.

With the growing popularity of blockchain technology among different industries, its use in electronic voting can be a potentially revolutionary step forward in securing and making electoral processes tamper-evident. This study examines the conceptualization and development of the proposed e-voting platform based on blockchain, giving a general overview of its structural model, constituent parts, and security features. By combining decentralized computing and biometric authentication, this platform raises the bar for holding elections more securely and transparently.

What is Blockchain and How It is Used in E-Voting?

Blockchain is a distributed and decentralized ledger technology that stores transactions in a secure and tamper-evident way. Each transaction is held in a block, which is connected to the previous block by cryptographic hashes, creating a chain of records.

This format provides once a vote has been cast that it cannot be changed or removed, with very high levels of security and transparency. For e-voting, blockchain does away with the requirement for a central authority,

safeguarding against election fraud and maintaining confidentiality and immutability of votes.

The voting algorithm checks each vote prior to its inclusion in the blockchain, maintaining the integrity of the electoral process. Furthermore, blockchain provides the capability of real-time tracking and auditing of votes, which permits stakeholders to check the correctness of electoral outcomes while not violating the anonymity of voters.

Through the use of blockchain, our e-voting system provides a secure, tamper-evident, and transparent voting process that increases voter confidence and trust in electronic elections.

## II. LITERATURE REVIEW

1. Blockchain-Based E-Voting Systems

Blockchain's fundamental properties decentralisation, transparency, and immutability make it a viable ground for safe e-voting systems. A critical review by Sharma and Sharma (2024) points out that blockchain has the ability to mitigate essential issues of electronic voting, including data integrity, transparency, and verifiability. The research underlines that though blockchain improves security components, scalability and privacy are concerns that need extensive study.

2. Biometric Authentication in Voting System

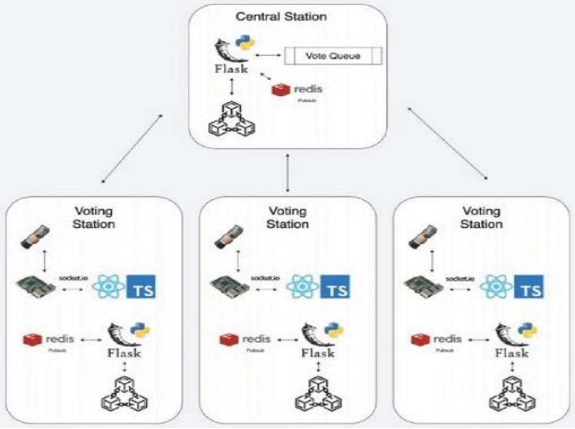
Biometric techniques, especially fingerprint verification, have been investigated to guarantee that only qualified voters vote and that every voter votes once. Sreejith et al. (2025) suggest a voting system that integrates blockchain with fingerprint verification to improve voter authentication and deter fraud. The use of these technologies is meant to simplify the voting process while ensuring high security levels.

3. Integration of Blockchain and Fingerprint Authentication

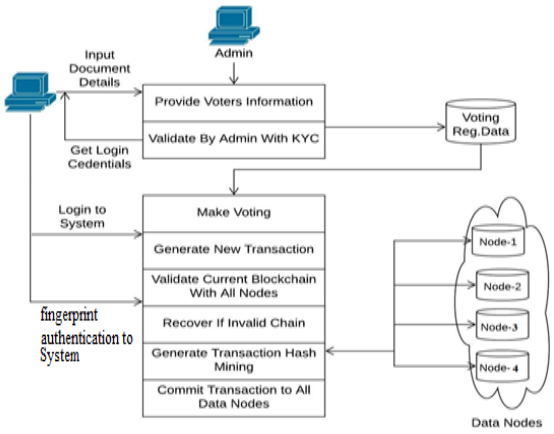
The amalgamation of blockchain technology with fingerprint verification aims to develop a secure e-voting system. For example, research in the International Journal of Advanced Research in Science, Communication, and Technology highlights an e-voting system that uses blockchain for safe vote recording and fingerprint biometrics for authenticating voters. This amalgamation has the potential to resolve matters regarding voter manipulation and data tampering, making votes both safely recorded and properly credited

Election Block

Election Block is designed to be a practical implementation demonstrating the usability of a centralized and permission-based blockchain system, It takes the assumption that the desired architecture is that of a centralized system, and trust is granted to the governing body for the use of the blockchain. As biometrics are also being collected and used for the method of authentication, it is assumed that all parties using the software are in agreement with the collection of this biometric data, In the brainstorming process and decision to use the fingerprint sensor, it did not present itself to be a large issue as many modern-day mobile devices also use fingerprint authentication and face recognition as authentication methods.




## III. PROPOSED SYSTEM




The proposed system integrates blockchain technology with biometric fingerprint authentication to create a decentralized and secure voting mechanism. Unlike traditional voting systems that rely on a central database, our system stores voting records in a distributed ledger to ensure transparency and prevent tampering.

The blockchain framework is implemented using Java, providing a robust and scalable solution. Voter authentication is performed through an arduino-based fingerprint sensor, which ensures that each voter is unique and can only cast a single vote. The system employs cryptographic hashing techniques to secure voting transactions, and a consensus algorithm validates each vote before it is permanently recorded. Additionally, real-time monitoring mechanisms are incorporated to detect and mitigate potential cyber threats. The combination of biometric authentication and blockchain technology enhances election security, eliminates voter fraud, and ensures a transparent and verifiable voting process.

Project Methodology

Login and Registration: Users or voters can Register for the application and maintain the profile. Where the admin can only log in and manage the other users. The fingerprint authentication system aims to automate the authentication procedure of a voting system using biometric technology.

User**:** A voter can register into the application and login in the application, after login users can view the parties and vote for their candidate, and also voters can view the live winner as election results. It is the user module where voters can see their listed elections and parties as per the election so they can vote, which is analyzed by the admin user. Fingerprint capture and matching algorithms. Voters register by providing fingerprint data.

Admin (Voting Result analysis): Admin can add, edit, delete and view the voters and parties. Also, the admin can view the elections list and manage their profile. Admin will view the complete voting list and find the winner. That is manual verification because the application uses an internal algorithm to find the election winner. Parties are another indirect user of the application that the admin will manage.

Block Generation: In this data is processed in multiple servers so the transactions are processed in a sequencing P2P distributed network. This illuminates the quality of service issue and time limits. The consensus model(s) help preserve the sanctity of data recorded on blockchain. The Blockchain is the distributed ledger used to represent the current state of delegated access rights in the system. Permissions to interact with the Blockchain are handled by the Root Authority and the Attribute Authorities

Results Generation**:** E-voting will be done successfully.
If attacker attacks the system, then the system will automatically recover the blocks using blockchain technology.

System Components

Operating System (Windows): Provides a stable and widely supported environment for running the e-voting software. Windows offers compatibility with essential development tools, database management systems, and blockchain frameworks. It ensures seamless communication between different hardware and software components, allowing smooth execution of Java-based blockchain operations and database queries.

Database (MySQL)**:** Serves as the backend storage system for user credentials, voter registrations, and election metadata. MySQL provides high performance, security, and scalability, ensuring that voter data and transaction logs are securely maintained. It acts as a supplementary storage system to manage registered users and interfaces with the blockchain for recording voting transactions.

Development Tools (Eclipse, Heidi SQL, JDK 1.7) Streamline the coding, debugging, and database management processes. Eclipse provides an integrated development environment for Java, enabling efficient coding and testing of blockchain algorithms. Heidi SQL facilitates seamless database management and query execution, while JDK 1.7 or higher ensures compatibility with advanced Java functionalities required for blockchain execution.

Fingerprint Module (R307) **:** Fingerprint is used to narrow sense is an impression left by the friction ridges of a human finger. The fingerprints recovery from a crime scene is an important method of forensic science purpose and the Fingerprints are easily deposited on suitable surfaces (such as glass or metal or polished stone) by the natural secretions of sweat from the eccrine glands that are present in epidermal ridges.

Optical fingerprint imaging involves capturing a digital image of the print using visible light rays. In this type of sensor is essence in a specialized digital camera. Where top layer of the sensor are used to place the finger which is known as the touch surface. Down of this layer is a light- emitting phosphor layer which illuminates the surface of the finger.

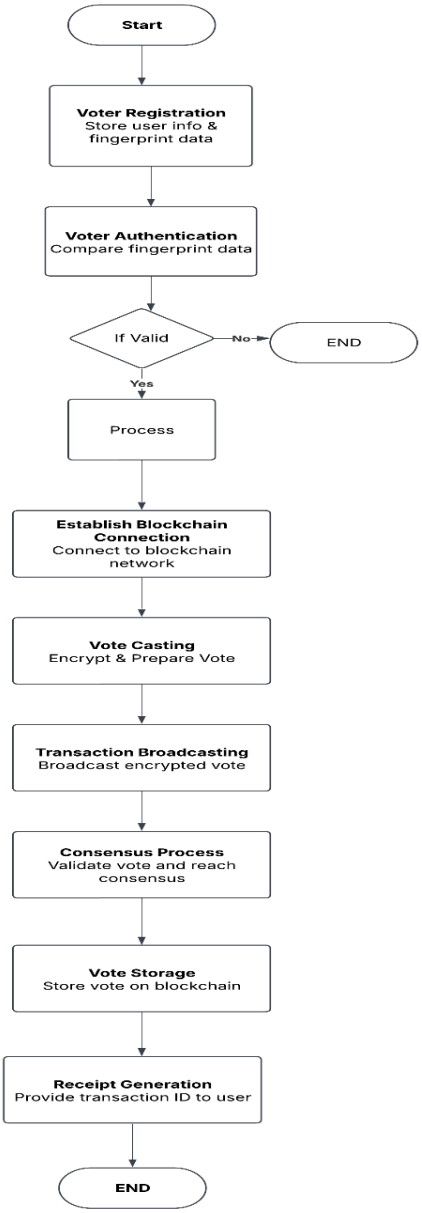
Then the light is reflected from the finger passes through the phosphor layer to an array of solid state pixels (a charge- coupled device) which captures a visual image of the fingerprint which is used for authentication. But a scratched or dirty touch surface can cause a bad image of the fingerprint

Arduino Uno: Acts as the central microcontroller that interfaces with the fingerprint module and other peripheral components. It processes fingerprint authentication requests, communicates with the database, and initiates the voting process upon successful verification. The Arduino board is responsible for ensuring seamless interaction between the biometric scanner and the software interface.

USB Cable**:** USB Cable is used to establish communication between the Arduino Uno and the computer running the e-voting system. It enables data transmission, power supply, and programming of the microcontroller, ensuring a reliable connection for executing authentication and voting tasks.

Decentralized Nodes: It forms the peer-to-peer blockchain network, ensuring that the voting process is secure, tamper-proof, and distributed. Each laptop acts as a node in the blockchain, validating transactions and maintaining a copy of the distributed ledger. This decentralized approach prevents single points of failure, making the system more resilient to attacks and ensuring election transparency.

System Flowchart




This flowchart represents a Blockchain-Based Voting System with Fingerprint Authentication.

1. Start: The process begins when a voter decides to cast their vote.
2. Voter Registration: Before voting, the voter needs to register by providing their personal details and fingerprint data. This ensures that only authorized voters can participate.
3. Voter Authentication: When the voter wants to vote, their fingerprint is scanned and compared with the stored data to verify their identity.

4. Validation Check: If the fingerprint does not match, the process stops, and the voter is denied access.
If the fingerprint matches, the process continues.
5. Establish Blockchain Connection: Once authenticated, the system connects to the blockchain network, ensuring a secure and tamper-proof voting process.
6. Vote Casting: The voter selects their choice, and their vote is encrypted to maintain privacy before being prepared for submission.
7. Transaction Broadcasting: The encrypted vote is then broadcasted to the blockchain network, just like a transaction in cryptocurrency.
8. Consensus Process: Blockchain nodes validate the vote and ensure that there is a consensus before adding it to the blockchain. This step ensures that no duplicate or fraudulent votes are recorded.
9. Vote Storage: Once validated, the vote is stored securely on the blockchain, preventing any modifications or tampering.
10. Receipt Generation: After the vote is recorded, a transaction ID (receipt) is generated and given to the voter. This allows them to verify that their vote has been successfully recorded.
11. End: The voting process is now complete.

## IV. EVALUATION RESULTS

In the results, we evaluate both sections for performance evaluation, blockchain execution and fake news detection accuracy using the proposed classification technique. The device runs with an INTEL 2.8 GHz i3 machine and 4 GB RAM in a distributed manner on the Java 3-tier analytics platform.
The Liar dataset is used for partial implementation of which is taken from www.kaggle.com. The Figure 2 below shows the time required for a consensus with Proof of Work (PoW) to authenticate the blockchain in a minimum of 3 nodes. For the validation of results, we have demonstrated first experiment analysis on blockchain implementation.

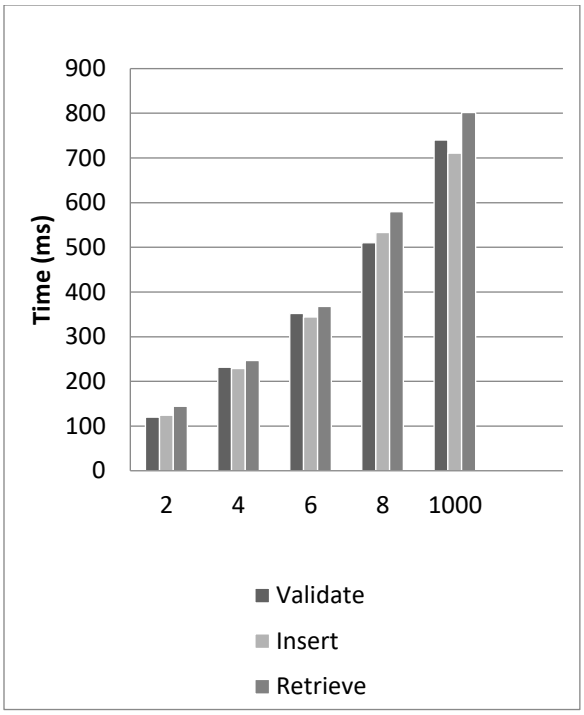



Figure 1: Time required for transaction with no. of transactions with blockchain

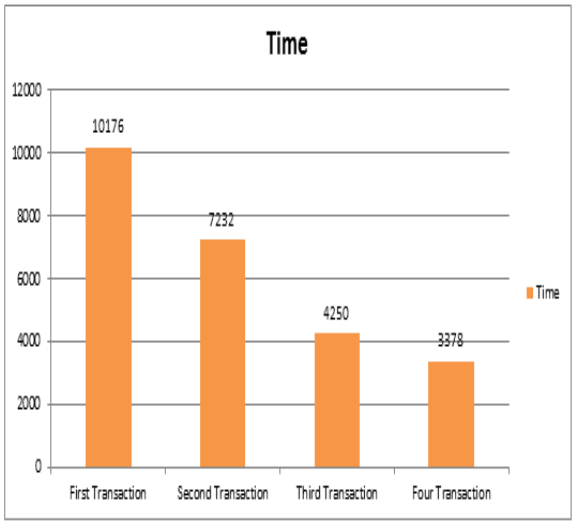



Fig. 2. Time required (in milliseconds) for complete transaction using 4 data nodes

## V. FUTURE SCOPE

The use of blockchain electronic voting systems is very much promising in terms of future growth and broader implementation. With the growth of technology, the system can be upgraded in order to address the challenges related to scalability, security,

and user friendliness. One such domain for future improvement is the incorporation of multi-modal biometric verification mechanisms such as facial scanning and iris scanning along with fingerprint scanning to enhance the verification of voters. In addition, artificial intelligence (AI) technologies to mark anomalies in real-time can be utilized to detect and stop fraudulent activities during the whole election process.

One of the most important research areas in the future is the construction of blockchain consensus algorithms for more scalability and efficiency. Old blockchain designs like Proof of Work (PoW) will have more computational overhead and bad performance. Future projects can use less bloated and power-hungry consensus protocols like Proof of Stake (PoS) or Delegated Proof of Stake (DPoS) to provide faster and cheaper transactions with no loss of security integrity.

Cross-platform voting is another area of advancement, which would enable the voters to cast their votes securely using diverse devices such as mobile phones and tablets, with extremely high-security measures in place. This feature would facilitate increased participation, particularly in elections held in geographically remote locations or abroad. Additionally, ongoing work in quantum-resistant cryptographic algorithms will also be a key factor in protecting the system against looming cybersecurity attacks resulting from advancements in quantum computing.

The application of smart contracts can additionally be used for automating additional aspects of elections such as candidate verification, registration of voters, and vote counting. Secure and auditable aspects of smart contracts will also help minimize human input and increase election process trust levels. Complying with legal frameworks and regulators will also become of utmost necessity in real application, requiring compliance with governments and election commissions.

The potential applications of this project include the use of decentralized autonomous organizations (DAOs) to control electoral processes and therefore the creation of fully open and self-controlling electoral systems. With increased global usage of blockchain technology, the integration of this technology with secure cloud-based systems and government databases can enhance the resilience, scalability, and performance of e-voting systems.

## VI. CONCLUSION

Blockchain technology introduces a futuristic approach to electronic voting, forestalling the most significant security challenges while ensuring transparency and voter authentication. Combining fingerprint authentication with an application-specific blockchain design, the system introduced here introduces an open, tamper-evident vote casting process and vote counting process. This new approach effectively counteracts the inherent weaknesses found in centralized databases as well as the conventional hand-counting process of vote tabulation, providing radically high levels of security, reliability, and transparency in voting. Future research can center on enhancing the performance of blockchain networks, enhancing consensus protocols for better efficiency, examining other biometric-based verification methods, and enhancing the overall scalability of such systems for national elections. The development and advancement of blockchain-based e voting systems are an achievement and major achievement
towards making transparent, secure, and accessible elections to the citizens of the world.

## REFERENCES

[1] 2021 IEEE 18th International Conference on Software Architecture Companion (ICSA-C) Election Block: An Electronic Voting System using Blockchain and Fingerprint Authentication

[2] IEEE Sponsored 2nd International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)2015 Secured Electronic Voting Machine using Biometrics.