



# ELECTRONIC VOTING SYSTEM USING BLOCKCHAIN

<sup>1</sup>A.S.Dhana Lakshmi, <sup>2</sup>M. Sreenivasu, <sup>3</sup>M.Sri Ramya, <sup>4</sup>K.V.D.Charan, <sup>5</sup>P.J.V.D.Uday Kumar, <sup>6</sup>K.Vasanth,

<sup>1</sup>Assistant Professor, <sup>2</sup>Associate Professor, <sup>3,4,5,6</sup>UG Students  
Information Technology,  
GIET Engineering College,Rajahmundry,Andhra pradesh,India

**Abstract :** Voter mistrust, security flaws, and transparency issues plague traditional voting systems frequently. This proposal suggests using blockchain technology to create an electronic voting system as a solution. The goal is to transform elections by utilizing blockchain ledgers' decentralized, immutable, and auditable properties. The main priorities are dealing with the widespread problems of vote tampering and guaranteeing voter anonymity, which are both critical to preserving the integrity of elections. By using cryptographic methods built into the blockchain architecture, the system seeks to prevent any efforts at fraud. Additionally, because blockchain technology is decentralized, no one party can manipulate the voting process, increasing voter trust and transparency. The potential of blockchain-based electronic voting to offer a transparent and verifiable record of every transaction is one of its main features. Every vote is cast and stored on the blockchain in an immutable format that cannot be changed or removed. This makes it easier to audit and verify election results in addition to preventing illegal vote manipulation. Further enhancing security and integrity, the system makes sure that any modifications to the ledger require consent from the majority of participants by utilizing consensus procedures like proof of labor or proof of stake. All things considered, blockchain-based electronic voting has great potential to overcome the drawbacks of conventional voting methods and provide a more safe, transparent, and reliable electoral process.

**Keywords:** *Electronic Voting, Blockchain, Security, Transparency, Immutability, Cryptography.*

## 1. INTRODUCTION

Any thriving democracy is built on the foundation of elections that are fair and credible. But traditional voting procedures, whether paper-based or dependent on centralized technological systems, frequently face problems including manipulation susceptibility, mistakes, and a conspicuous lack of transparency. These flaws seriously jeopardize public confidence in election results and, by extension, the democratic process itself. Blockchain technology presents itself as a game-changing answer to these problems, one that has the ability to completely transform voting procedures. Due to its intrinsic qualities such as immutability, decentralization, and cryptographic security, blockchain appears to be a viable option for revolutionizing electoral procedures. Regardless of their format, traditional voting techniques usually fail to maintain the integrity of elections. Election results are questioned because of their vulnerability to fraud, inaccuracies, and a lack of transparency, regardless of the method used paper-based ballots or centralized electronic systems. These weaknesses provide room for suspicions to grow, undermining public confidence in the democratic process. With its immutable record, decentralized structure, and cryptographic security, blockchain technology stands out as a ground-breaking remedy ready to tackle and resolve these fundamental problems. In the context of elections, blockchain's decentralized structure is a vital strength. Blockchain reduces the possibility of manipulation by doing away with single points of failure and spreading the process over a network of nodes. Election security and integrity are improved overall since this decentralized method makes sure that no one party controls the entire voting process.

Another essential component of blockchain technology that directly enhances the validity of election results is immutability. Votes that are registered on the blockchain are added to an irreversible and unchangeable ledger. Election data is guaranteed to remain unmodified and undamaged due to its immutability, offering a clear and verifiable record of the voting process.

Election security is further strengthened by the blockchain framework's use of cryptographic techniques. These methods help to increase public trust in the political process while simultaneously protecting the privacy and anonymity of individual voters. A crucial component of election integrity is addressed by blockchain technology, which guarantees the confidentiality and security of votes. Essentially, by offering a safe, transparent, and reliable framework for holding elections, blockchain technology has the ability to protect democracy. A strong foundation for democratic elections is provided by its decentralized structure, which reduces the possibility of manipulation, immutability, which ensures the integrity of the voting process, and cryptographic mechanisms,

which protect voters' privacy and anonymity. An electronic voting system built on the blockchain is an actual example of these ideas in action. Votes are guaranteed to be auditable, impenetrable to tampering, and shielded from unwanted access by such a system. This novel approach to elections is based on the protection of voter confidentiality and the concurrent facilitation of verifiable outcomes. This project uses the revolutionary potential of blockchain technology to set out on the big task of creating a transparent and safe electronic voting system. The main objective is to build a voting platform that will, in the end, promote a more effective and convenient voting experience for all residents while simultaneously enhancing and restoring voter confidence and reducing the likelihood of election fraud. Through exploring the nuances of blockchain technology and its application to the electoral process, this project aims to make a substantial contribution to the advancement of democratic norms in the digital era.

## 2. Literature Survey

The emergence of online voting offers a contemporary response to persistent issues with electoral procedures. Online voting is growing more and more popular in today's society because of its ability to save organizational costs and boost voter turnout. Online voting provides voters with the convenience of casting their ballots from any location with an Internet connection by doing away with the requirement for polling places and paper ballots. Nevertheless, despite these benefits, the introduction further risks to election integrity makes the deployment of online voting alternatives extremely cautious. Of fact, there is cause for concern regarding the possibility of widespread vote manipulation due to the inherent weaknesses of online voting systems. If one vulnerability is taken advantage of, it could seriously jeopardize the democratic process by casting doubt on the veracity and precision of election outcomes. Therefore, in order to maintain election integrity, electronic voting systems must place a high priority on legitimacy, accuracy, safety, and convenience. The apparent difficulties in implementing electronic voting systems could possibly be impeding their acceptance. To foster confidence in the dependability of electronic voting platforms, significant obstacles such voter fraud, technological malfunctions, and cybersecurity risks must be resolved. To guarantee fair participation in the political process, worries regarding the accessibility and inclusivity of online voting platforms also need to be properly taken into account. Blockchain technology has surfaced as a potential remedy to improve the reliability and security of electronic voting systems in response to these issues. Blockchain has special benefits in guaranteeing the openness and integrity of the voting process by utilizing decentralized nodes and cryptographic concepts. Blockchain Technology reduces the possibility of fraud and manipulation by enabling end-to-end vote verification in electronic voting systems. Therefore, there is a great chance that blockchain-based electronic voting systems will be able to overcome the drawbacks of conventional online voting systems and open the door to more dependable and safe electoral procedures. Online voting is increasingly recognized as a promising avenue to modernize electoral processes and potentially boost voter engagement. By enabling individuals to cast their votes remotely via the internet, online voting has the capacity to significantly reduce administrative costs associated with traditional paper-based voting methods. Additionally, the convenience factor cannot be understated, as voters can participate in elections from the comfort of their homes or any location with an internet connection, eliminating the need for physical polling stations and the logistical challenges they entail. Moreover, online voting holds promise for increasing voter turnout by removing barriers such as geographic distance, mobility issues, or time constraints that may prevent individuals from participating in traditional in-person voting.

The introduction of digital platforms and the reliance on internet connectivity create new avenues for potential vulnerabilities and cyber threats. A single weakness in the system could lead to widespread manipulation or tampering of votes, undermining the integrity and legitimacy of election outcomes. As such, there is a critical need for electronic voting systems to not only be efficient and convenient but also to prioritize legitimacy, accuracy, and security. In response to these challenges, blockchain technology has emerged as a promising solution to enhance the security and integrity of electronic voting systems. By leveraging the decentralized nature of blockchain networks, electronic voting platforms can distribute voting data across a network of nodes, significantly reducing the risk of centralized points of failure or manipulation. Research and development efforts have long been focused on creating a safe electronic voting system that maintains the privacy and fairness found in conventional voting systems while utilizing the transparency and adaptability of electronic systems. The use of blockchain technology as a service is investigated in this continuing study as a potential solution to this persistent problem. The reviewed paper describes a new blockchain-based electronic voting system that aims to address shortcomings in current systems. The assessment of different blockchain frameworks to determine their feasibility for building a reliable blockchain-based electronic voting system is central to the paper's goals. The paper explores distributed ledger technology in detail before diving into a case study that shows how an application based on blockchain is implemented and how elections are conducted. In the context of electoral procedures, this case study provides a useful illustration of the possible advantages provided by distributed ledger technologies. The suggested electronic voting system seeks to lower the expenses related to conducting national elections while also improving security measures by utilizing blockchain technology. A crucial part of the paper's approach is the assessment of well-known blockchain frameworks, which offers information on the viability and scalability of putting in place a blockchain-based electronic voting system. The goal of the study is to determine which framework is most suited for implementing the intended electronic voting solution by methodically evaluating different frameworks. The study also provides a thorough examination of the possible benefits that blockchain technology may provide for electronic voting. These benefits include higher resistance to fraudulent operations, increased transparency, and increased confidence in the validity of election results. In the end, the paper hopes to provide creative answers to the problems with conventional voting methods, opening the door to more reliable and efficient election procedures by investigating the use of blockchain technology in this context.

### 3. OVERVIEW OF THE SYSTEM

#### 3.1 Existing system

The introduction of Centralized Electronic Voting Machines (EVMs) as a contemporary substitute for conventional paper ballots aims to improve efficiency and streamline the voting process. Even while these devices do away with the necessity for actual paper ballots, they nevertheless rely on a centralized method for counting votes, in which every vote is totaled and handled in one place. Even though electronic voting machines (EVMs) have certain benefits, such as quicker results tabulation and less administrative work, they also have serious security flaws that compromise the integrity of the electoral process. The vulnerability of centralized EVMs to software flaws and vulnerabilities is one of the main worries. These devices frequently use proprietary software, which might not be thoroughly tested or examined for any potential flaws. They are therefore open to abuse by unscrupulous parties who might use software flaws to tamper with the voting process or influence votes. In addition, the closed-source nature of proprietary software poses challenges for impartial specialists performing comprehensive security evaluations, hence raising the likelihood of undiscovered vulnerabilities. Another serious risk to the security of centralized EVMs is tampering. Even with physical security features like lockable enclosures and tamper-evident seals, insiders or anybody with access to the hardware can still tamper with these computers. Modifying memory chips or implementing malicious hardware implants are examples of manipulating an EVM's internal components, which can jeopardize election results' accuracy and voting process integrity. Furthermore, it is difficult to identify and successfully counteract efforts at manipulation due to the centralized style of vote counting, which raises the probability of successful attacks. Online voting is an option offered by certain centralized EVM systems, which adds complexity and security risks. Due to their inherent vulnerabilities, online voting platforms are susceptible to a variety of cyber threats, such as voter privacy breaches, denial-of-service (DoS) attacks, and vote manipulation. Votes sent over the internet run the risk of being intercepted or manipulated by nefarious parties, jeopardizing the secrecy and integrity of the electoral process. DoS attacks on online voting platforms can also interfere with voting operations by blocking voters from accessing the platform or casting their ballots, which compromises the election's legitimacy and impartiality. Another major issue with centralized electronic voting machines (EVMs) is voter privacy, especially when it comes to internet voting. Voter anonymity is protected by the implementation of cryptographic protocols and anonymization techniques; yet, weaknesses in the system may allow unauthorized parties to access sensitive voter data. Since all votes are kept and processed in one place, making them vulnerable to manipulation or illegal access, the centralized form of vote processing also raises questions regarding the security and confidentiality of voter data. In summary, while centralized electronic voting machines provide considerable benefits in terms of comfort and efficiency, there are serious security dangers associated with them that compromise the legitimacy and integrity of the election process. Voter privacy can be compromised, elections can be disrupted, and votes can be manipulated by taking advantage of vulnerabilities such as software defects, manipulation, and insider threats. These concerns are made worse by the advent of internet voting, which exposes the electoral system to a variety of cyberthreats. In order to ensure the integrity of electronic voting systems and preserve democratic values, it is essential to implement strong security measures, such as stringent software testing, improved physical security controls, and cryptographic

#### 3.2 Proposed system

Blockchain technology is used in the suggested electronic voting system to overcome the drawbacks of online voting platforms and conventional centralized systems. Unprecedented levels of security, transparency, and auditability are ensured by the system by having votes recorded on a distributed ledger across several nodes. Due to the permanent recording of every vote on the blockchain, it is very impossible for malevolent actors to change or remove votes once they have been cast. Because the ledger is dispersed, there are no single points of failure and there is a far lower chance of manipulation or tampering, which improves the voting process's dependability and integrity. The integrity of the suggested electronic voting method is further strengthened by the fundamental property of blockchain technology immutability. Votes that are registered on the blockchain are part of an immutable historical record that cannot be tampered with or changed. By providing an auditable and transparent record of every vote cast, this unchangeable ledger improves election transparency and auditability. The blockchain guarantees the integrity of election results by offering a permanent and unchangeable record of voting data, which can be independently validated by stakeholders such as auditors, election officials, and voters. In order to secure each vote and maintain the integrity of the voting process, the proposed electronic voting system also places a high priority on security through the use of cryptographic techniques. Digital signatures and encryption are two examples of cryptographic approaches used to safeguard the integrity, confidentiality, and validity of voting data. Prior to being entered into the blockchain, every vote is encrypted to guarantee that the information can only be accessed and decrypted by those who are permitted. Digital signatures are also utilized to confirm each vote's legitimacy and make sure it wasn't altered during transmission or storage. By offering strong defense against illegal access, alteration, or tampering, these cryptographic techniques improve the voting system's overall security. A further important component of the suggested electronic

voting system is protecting voter anonymity. In order to verify that only qualified voters cast ballots, sophisticated measures are used to protect voter identities during the election. Through the use of cryptographic protocols like homomorphic encryption and zero-knowledge proofs, the system enables voters to cast anonymous ballots without disclosing their names or voting preferences. Cryptographic proofs are created concurrently to confirm each voter's eligibility and legitimacy, guaranteeing that only valid votes are counted while protecting each voter's anonymity. By striking a compromise between verifiability and privacy, these sophisticated anonymity approaches guarantee that voter secrecy is protected while maintaining the integrity of the voting process. In conclusion, the planned electronic voting system will transform elections by utilizing blockchain technology. The system provides unmatched levels of security, transparency, and integrity by utilizing distributed ledgers, immutability, cryptographic security, and sophisticated anonymity mechanisms. The suggested solution strives to restore faith in the political process by solving the limitations of both online voting platforms and traditional centralized systems. It also ensures that every vote counts and every voice is heard in a true democratic manner. Online voting platforms introduce additional security risks, as they rely on internet connectivity and digital transmission of votes, which are susceptible to various cyber threats such as hacking, malware, and denial-of-service attacks. Moreover, ensuring the dissociation of voter identities from their votes presents a significant challenge in online voting, as vulnerabilities in the system can potentially expose sensitive voter information to unauthorized parties, compromising voter privacy and anonymity. These inherent security vulnerabilities and privacy concerns associated with centralized electronic voting machines and online voting platforms underscore the urgent need for a more secure, transparent, and trustworthy alternative to safeguard the integrity of the electoral process and uphold the principles of democracy.

### 3.3 Software Requirements:

- Ethereum
- Solidity - 0.8.24
- Ganache - 2.71
- Node.js - V20
- Web Browsers - Google Chrome, Mozilla Firefox, Microsoft Edge (latest versions)

### 3.4 Hardware Requirements:

- Processor - Dual-core or higher
- RAM - 4GB or more
- Storage - At least 128GB
- Display - Minimum 1024 x 768 resolution
- Network - Integrated Ethernet or Wi-Fi
- Mouse - Min USB
- Keyboard - Min USB

## 4. Technologies Used

### 4.1 Node.js

Node.js is a powerful and versatile runtime environment for executing JavaScript code outside of a web browser. Initially released in 2009 by Ryan Dahl, Node.js has since gained immense popularity in the software development community due to its efficiency, scalability, and extensive ecosystem of libraries and frameworks. At its core, Node.js is built on the V8 JavaScript engine, developed by Google for their Chrome browser. This engine compiles JavaScript code into machine code, enabling faster execution compared to traditional interpreted languages. Node.js extends this capability to server-side development, allowing developers to write backend code using JavaScript. One of the key features of Node.js is its event-driven, non-blocking I/O model. This means that Node.js can handle a large number of concurrent connections without blocking the execution of other code. This is achieved through the use of event loops and callbacks, where asynchronous tasks are queued and executed when their respective I/O operations complete. As a result, Node.js applications can handle high levels of traffic and perform tasks efficiently, making it well-suited for building real-time applications, APIs, and microservices.

### 4.2 Ethereum

Ethereum is a decentralized platform that enables developers to build and deploy smart contracts and decentralized applications (dApps) on its blockchain. Launched in 2015 by Vitalik Buterin and a team of developers, Ethereum has become one of the most prominent blockchain platforms, offering a wide range of functionalities beyond simple cryptocurrency transactions. At the core of Ethereum's capabilities is its Turing-complete scripting language called Solidity, which allows developers to create complex smart contracts that can automate various processes and execute code on the blockchain. One of Ethereum's primary innovations is its ability to support smart contracts, which are self-executing contracts with predefined rules and conditions written in Solidity. These contracts are deployed on the Ethereum blockchain and can automatically enforce agreements, transfer digital assets (such as Ether,



Ethereum's native cryptocurrency), and execute code based on predefined conditions. Smart contracts eliminate the need for intermediaries or trusted third parties, as their execution is transparent, verifiable, and immutable on the blockchain. This feature has opened up a wide range of use cases across industries, including finance, supply chain management, gaming, identity verification, and more.

### 4.3 Solidity

Solidity is a high-level, statically-typed programming language specifically designed for writing smart contracts on blockchain platforms like Ethereum. Developed by Ethereum's co-founder Gavin Wood, Solidity aims to provide developers with a simple yet powerful language for creating and deploying smart contracts that run on the Ethereum Virtual Machine (EVM). With its syntax inspired by languages like JavaScript, Python, and C++, Solidity enables developers to express complex logic and business rules within smart contracts, facilitating the automation and execution of decentralized applications (dApps) on the Ethereum blockchain. One of Solidity's key features is its support for object-oriented programming (OOP) concepts such as inheritance, polymorphism, and encapsulation. This allows developers to organize and structure their smart contract code into reusable components, making it easier to manage and maintain complex applications. For example, developers can define multiple contracts with separate functionalities and then inherit or extend these contracts to reuse code and enhance modularity. Solidity's OOP capabilities contribute to code readability, scalability, and maintainability, essential factors for building robust and efficient smart contracts.

### 4.4 Vscode

Visual Studio Code (VS Code) is a widely used integrated development environment (IDE) developed by Microsoft. It has gained immense popularity among developers due to its lightweight yet powerful features, extensive customization options, and support for a wide range of programming languages and frameworks. VS Code is designed to enhance developers' productivity and streamline the coding experience across various platforms and projects. One of the key strengths of VS Code is its versatility and cross-platform compatibility. It runs seamlessly on Windows, macOS, and Linux operating systems, providing a consistent user experience regardless of the development environment. This flexibility allows developers to work on their preferred operating system and collaborate seamlessly with team members using different platforms.

### 4.5 Ganache

Ganache is a popular and powerful development tool used in blockchain and Ethereum development. It provides a local Ethereum blockchain environment that developers can use for testing, debugging, and deploying smart contracts without interacting with the main Ethereum network. Ganache is part of the Truffle Suite, which is a collection of tools designed to make Ethereum development more efficient and accessible. One of the key features of Ganache is its ability to create a local blockchain network that operates similarly to the Ethereum mainnet but is isolated and private.

## 5. Architecture

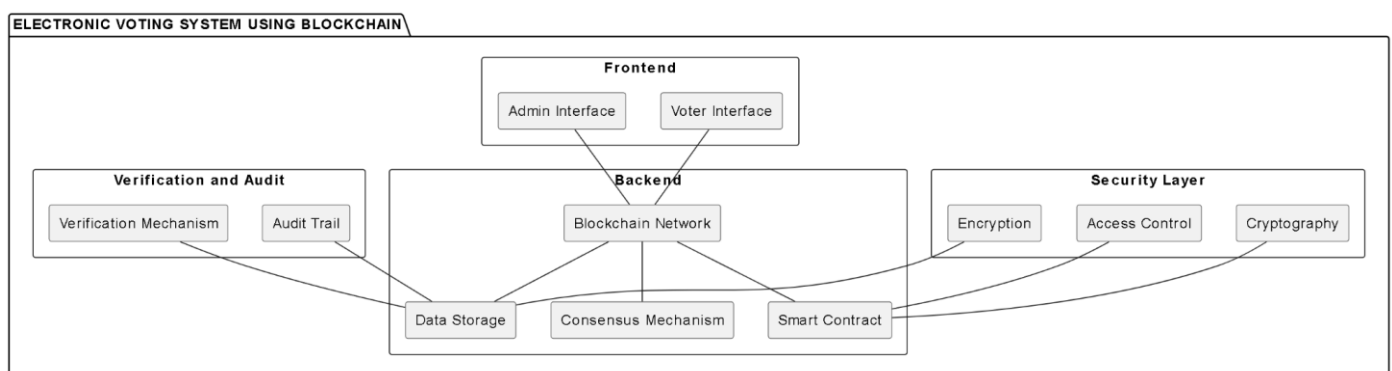


Fig 1: System Architecture

### *Economical Feasibility:*

The Economic Feasibility of developing a blockchain-based electronic voting system is evident through various advantages. Firstly, it offers cost savings by automating processes like ballot distribution, polling station management, and vote counting, reducing operational expenses over time. Secondly, efficiency gains are realized by enabling remote voting, minimizing the need for physical infrastructure and personnel. Thirdly, the system's ability to prevent fraud and tampering saves costs associated with legal challenges or recounts, ensuring the integrity of elections. Additionally, increased voter participation leads to a more representative democratic process, fostering stable governance and policy continuity.

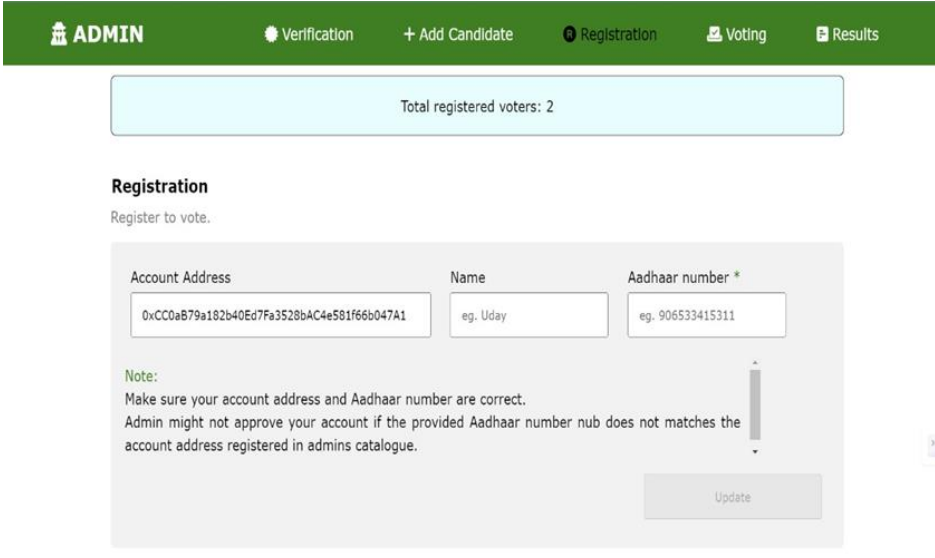
### Technical Feasibility:

The Technical Feasibility of a blockchain-based electronic voting system is underpinned by its core features and functionalities. Blockchain technology offers a decentralized and immutable ledger, which ensures that once votes are recorded, they cannot be altered or tampered with. This aspect enhances the security and integrity of the voting process, addressing key vulnerabilities present in traditional voting systems. Additionally, cryptographic techniques such as digital signatures and encryption play a crucial role in the system's technical feasibility. These techniques are used to verify voter identities securely, protect ballot secrecy, and ensure the authenticity of votes. By leveraging cryptographic mechanisms, the system can maintain voter anonymity while preventing unauthorized access to the voting system, ensuring a high level of security and trust.

### Social Feasibility:

The Social Feasibility of implementing a blockchain-based electronic voting system encompasses various aspects that are crucial for its acceptance and adoption by stakeholders and the general public. One of the key factors contributing to social feasibility is the system's ability to enhance trust and confidence in the electoral process. By leveraging blockchain technology's transparency and immutability, voters can have greater assurance that their votes are accurately recorded and securely stored, reducing concerns about fraud or manipulation. Moreover, the system's emphasis on voter anonymity ensures that individuals can cast their votes without fear of reprisal or coercion, thereby safeguarding the democratic principle of secret balloting. This aspect is particularly important in societies where political intimidation or discrimination may deter voter participation. Additionally, the accessibility and inclusivity of a blockchain-based voting system contribute to its social feasibility. By enabling remote voting options and providing user-friendly interfaces, the system can cater to a broader demographic of voters, including those with mobility issues or living in remote areas. This promotes greater participation in the electoral process and fosters a sense of inclusiveness and equal representation. The transparency and auditability of the voting process facilitated by blockchain technology can help mitigate concerns about electoral fraud or disputes. Citizens and stakeholders can independently verify election results and audit the integrity of the voting system, enhancing overall confidence in the democratic process.

## 6. RESULTS SCREENSHOTS



The screenshot displays the ADMIN interface with a navigation bar containing 'ADMIN', 'Verification', '+ Add Candidate', 'Registration', 'Voting', and 'Results'. Below the navigation bar, a light blue box indicates 'Total registered voters: 2'. The main content area is titled 'Registration' and includes the instruction 'Register to vote.'. The registration form has three input fields: 'Account Address' (containing '0xCC0aB79a182b40Ed7Fa3528bAC4e581f66b047A1'), 'Name' (containing 'eg. Uday'), and 'Aadhaar number \*' (containing 'eg. 906533415311'). A 'Note' section below the form states: 'Make sure your account address and Aadhaar number are correct. Admin might not approve your account if the provided Aadhaar number does not match the account address registered in admin's catalogue.' An 'Update' button is located at the bottom right of the form.

Fig 2: Registration of voter

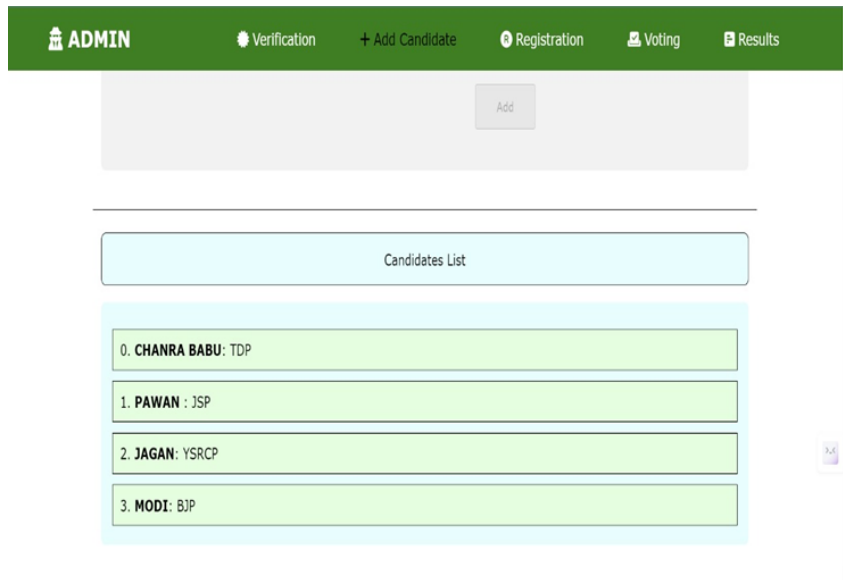


Fig 3: Candidate List

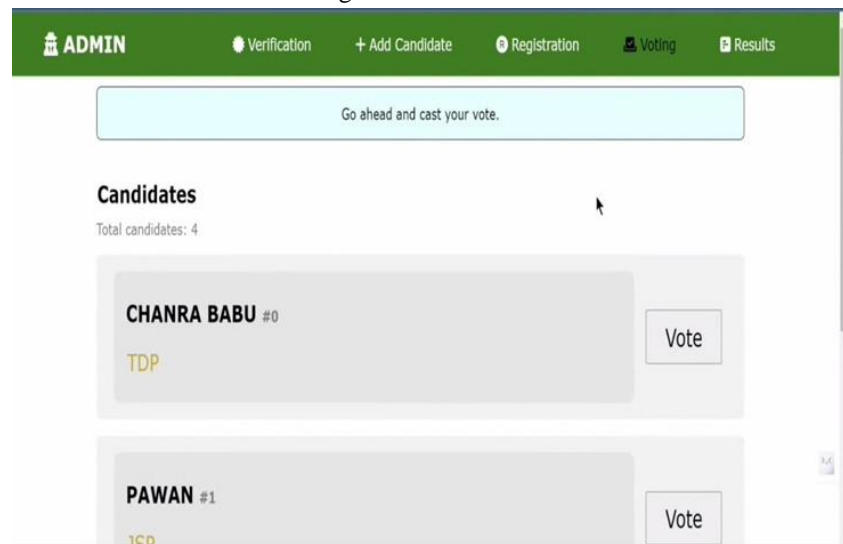


Fig 4: Voting Page



Fig5: Result Page

## 7. CONCLUSION

The creation of an electronic voting system built on blockchain technology is a big step forward in resolving the issues with traditional voting methods. The foundation for a more secure, transparent, and dependable voting process has been established by this project, which makes use of the decentralized, immutable, and auditable ledger offered by blockchain technology. Over the course of the project, a number of significant objectives have been met. First off, by utilizing a decentralized ledger, votes are recorded across numerous nodes, thereby guarding against vote manipulation and maintaining the credibility of the electoral process. This system preserves the integrity of the election result by ensuring that a vote cannot be changed or manipulated once it has been cast. Additionally, the project has placed a high priority on protecting voter confidentiality while upholding auditability and transparency. The system protects the privacy and confidentiality of individual votes while allowing public verification of election outcomes through the use of cryptographic techniques and consensus mechanisms. This careful balancing makes sure that the voting procedure stays open and answerable to all parties.

## 8. FUTURE ENHANCEMENT

The future scope of blockchain-based voting systems encompasses several advanced features and strategies that can significantly enhance the security, privacy, and functionality of electoral processes. Integration with advanced identity verification solutions is a key aspect, as combining blockchain voting with robust digital identity technologies such as biometrics and decentralized identity systems can substantially improve voter authentication and prevent fraud. Biometric authentication, such as fingerprint scanning or facial recognition, adds an extra layer of security by linking each vote to a unique biometric identifier, ensuring that only legitimate voters can participate in the electoral process. Decentralized identity systems further enhance security and privacy by providing individuals with control over their identity information and enabling secure, verifiable authentication without relying on central authorities. Zero-knowledge proofs offer another promising avenue for enhancing voter privacy while maintaining verification of voter eligibility and vote validity. Blockchain smart contracts play a crucial role in enabling more complex voting systems, such as ranked-choice voting, within blockchain-based electoral frameworks. Ranked-choice voting allows voters to rank candidates in order of preference, offering greater expressiveness and representation in electoral outcomes. Smart contracts can automate the processing of ranked-choice votes, ensuring accurate tabulation and allocation of preferences according to predefined rules. This not only enhances the functionality of voting systems but also fosters inclusivity and democratic representation by accommodating diverse voter preferences. Another area of future scope is the exploration of hybrid voting models, where blockchain technology is securely integrated with existing voting infrastructure to build trust gradually and enable phased adoption. Hybrid voting combines the strengths of blockchain, such as transparency, immutability, and security, with traditional voting methods to transition towards fully blockchain-based systems at a manageable pace.

## 9. REFERENCES

- [1] Anita A. Lahane, Junaid Patel, Talif Pathan and Prathmesh Potdar, "Blockchain technology based e-voting system", ITM Web of Conferences, vol. 32, pp. 03001, 2020.
- [2] Schinckus C. The good, the bad and the ugly: An overview of the sustainability of blockchain technology. Energy Res. Soc. Sci. 2020.
- [3] Kim T., Ochoa J., Faika T., Mantooth A., Di J., Li Q., Lee Y. An overview of cyber-physical security of battery management systems and adoption of blockchain technology. IEEE J. Emerg. Sel. Top. Power Electron. 2020.
- [4] Chang V., Baudier P., Zhang H., Xu Q., Zhang J., Arami M. How Blockchain can impact financial services—The overview, challenges and recommendations from expert interviewees. Technol. Forecast. Soc. Chang. 2020.
- [5] Ometov A., Bardinova Y., Afanasyeva A., Masek P., Zhidanov K., Vanurin S., Sayfullin M., Shubina V., Komarov M., Bezzateev S. An Overview on Blockchain for Smartphones: State-of-the-Art, Consensus, Implementation, Challenges and Future Trends. IEEE Access. 2020.
- [6] Hakak S., Khan W.Z., Gilkar G.A., Imran M., Guizani N. Securing smart cities through blockchain technology: Architecture, requirements, and challenges. IEEE Netw. 2020.
- [7] Çabuk U.C., Adiguzel E., Karaarslan E. A survey on feasibility and suitability of blockchain techniques for the e-voting systems. arXiv. 2020.



- [8] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. [(accessed on 28 July 2020)]; Available online: <https://bitcoin.org/bitcoin.pdf>.
- [9] Garg K., Saraswat P., Bisht S., Aggarwal S.K., Kothuri S.K., Gupta S. A Comparative Analysis on E- Voting System Using Blockchain; Proceedings of April 2019.
- [10] Hang L., Kim D.-H. Design and implementation of an integrated iot blockchain platform for sensing data integrity. Sensors. 2019.
- [11] Raesko P. Blockchain and Democracy. Soc. Econ. 2019.
- [12] Yaga D., Mell P., Roby N., Scarfone K. Blockchain technology overview. arXiv. 2019.
- [13] Wang B., Sun J., He Y., Pang D., Lu N. Large-scale election based on blockchain. Procedia Comput. Sci. 2018.  
Available online: <https://infographics.economist.com/2018/DemocracyIndex/>
- [15] Wood G. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Proj. Yellow Pap. 2014.
- [16] Cullen R., Houghton C. Democracy online: An assessment of New Zealand web sites. Gov. Inf. Q. 2000.
- [17] Szabo N. Formalizing and securing relationships on public networks. First Monday. 1997.