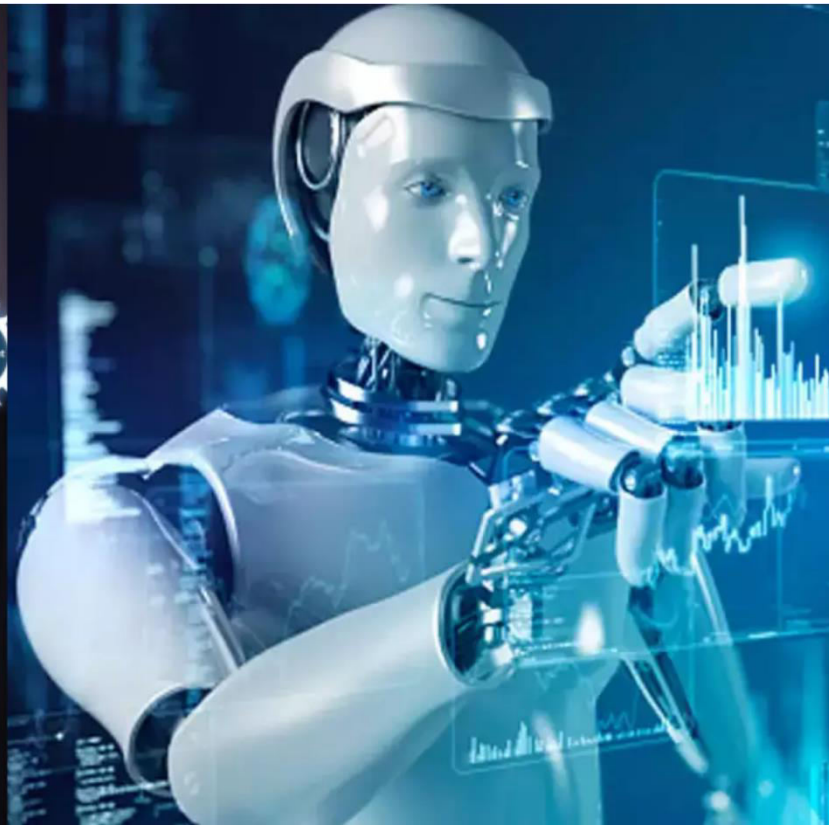
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 7, July 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 7, July 2025

|DOI: 10.15680/IJIRSET.2025.1407119|

DigiPoll: Blockchain-Powered E-Voting with Advanced Authentication

Hafiyya R M, Jitha K, Mufleh Mohamed Pulikuth, Muhammed Dishan V, Muhammed Muhsin P, Muhammed Shammas C K

Assistant Professor, Department of Computer Science & Engineering, MEA Engineering College, Kerala, India

Assistant Professor, Department of Computer Science & Engineering, MEA Engineering College, Kerala, India

Department of Computer Science & Engineering, MEA Engineering College, Kerala, India

Department of Computer Science & Engineering, MEA Engineering College, Kerala, India

Department of Computer Science & Engineering, MEA Engineering College, Kerala, India

Department of Computer Science & Engineering, MEA Engineering College, Kerala, India

ABSTRACT: Electronic voting is an essential element of modern democracies, yet it remains vulnerable to vote tampering, voter fraud, and inefficient vote handling. This paper proposes a novel blockchain-based solution aimed at enhancing the security, integrity, and efficiency of electoral processes. By leveraging blockchain's immutable and tamper-proof ledger, the system ensures that all votes are securely recorded and protected from manipulation. Voter eligibility is strictly verified, allowing only qualified voters to cast their ballots in person. The system supports voting through secure physical kiosks, making the process straightforward and reliable. Additionally, smart contract technology automates voter registration and vote counting, elim-inating human errors and enabling the immediate publication of election results as soon as voting concludes. Overall, this approach harnesses the power of blockchain to provide a secure, transparent, and efficient voting experience.

KEYWORDS: Blockchain Technology, E-Voting Systems, Ad-vanced Authentication, Smart Contracts, Electoral Security, On-line Voting, Vote Tampering Prevention, Ethereum Blockchain, Decentralized Systems.

I. INTRODUCTION

This undermines the confidence of the people in democratic institutions, for voting systems are becoming very susceptible to tampering and fraud and lack transparency. There are other issues, including vote manipulation, inaccessible polling op-tions, and inefficiencies in manual vote counting that require a secure and reliable solution. Blockchain-based voting systems are claimed to be transformative on this issue in that they provide a vote recording facility safely on an immutable ledger. This system takes advantage of the decentralised nature of blockchain, which is characterized by its openness, so as to improve election security, maintain privacy, and tally every vote cast. The employment of smart contracts also allows for the automation of some tasks like voter registration checks and vote counting to reduce possible human errors and increase productivity. This paper introduces a blockchain-based voting system that is secure, transparent, and accessible; that is, the platform allows in-person voting while preserving the integrity of the outcome.

A. Background and Motivation

As digital transformation changes the landscape of most industries, traditional voting systems find it hard to deal with increased demands for higher security, transparency, and ac-cess. Complications related to tampering, fraud, and a lack of remote or disabled voters still taint the integrity and inclusion of democratic processes. Even more often, cumbersome vote-counting processes and inefficiencies in logistics have helped create distrust and undermine public confidence in elections. Here, blockchain will be used to provide a secure voting solution that is transparent and trackable. The utilization of blockchain's permanent ledger along with the implementation of smart contract-driven verifications aims at making sure that only authorized voters are participating and that no vote cast was altered after

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 7, July 2025

|DOI: 10.15680/IJIRSET.2025.1407119|

casting. The aim is that it becomes a robust and effective in-person and online voting mechanism that eases and makes all administrative processes more accessible, as required by modern democracies.

B. Problem Statement

An effective decision aimed at addressing the problem under consideration should necessarily begin with a precise formu-lation of the problem at hand. Nevertheless, traditional voting systems have numerous deficiencies that cause influence and openness of elections. For instance, in such integrated systems, malfeasance or electoral fraud is achievable and the outcome leads to loss of people's confidence in the election results. Furthermore, when it comes to vote auditing, it is not very easy since there is no block-chain based, immutable ledger that would provide confirmation on the authenticity of the results as well as whether they tally with the human. Also, vote auditing is not made easy since there is no safe, unalterable record through which accuracy of the final results can be verified and questioned for their originality. The mobility is still one of the biggest issues, and current systems do not have many variants for safe remote voting. The same applies to vote management, with a high rate of error margin due to manual operations, which further extends the period of expectation of results and reduces the reliability level. These problems demand an end-to-end, blockchain-based voting solution in order to provide all relevant stakeholders with a safe, immutable, and convenient voting process.

II. LITERATURE SURVEY

One of the best potentials of blockchain technology in voting system changes is to solve security, transparency, and accessibility-related issues at its core. Several studies on blockchain-based voting systems have revealed many of the important benefits, which include integrity, tamper resistance, and auditability of the data.

1. M. Farhan et al., in their work titled Disrupting the Ballot Box: Blockchain as a Catalyst for Innovation in Electoral Pro-cesses [1], proposed a blockchain-based election framework that aims to ensure secure, transparent, and efficient elections.
2. Reineir S. Duran et al., in their paper EASY E-VOTE: An Ethereum-Based Voting System Using IPFS and MetaMask for Student Government Election [2], introduced a user-friendly system leveraging Ethereum, IPFS, and MetaMask to provide decentralized storage and enhance the voting experience.
3. Shekh Minhaz Uddin Deep et al., in E-Voting System Improvised by Blockchain Technology: A Case Study [3], demonstrated a secure and tamper-resistant e-voting system featuring remote access, using Ethereum, Quorum, and SHA-256 encryption.
4. Sushma S.A and Keerthan Kumar T.G presented E-voting System Using Public Blockchain [4], emphasizing lower costs and an irreversible voting process by utilizing public blockchain, JSON, and REST API.
5. Kingsley C. Nwosu and Musbah Abdulgader, in their work titled LegitVote: A Blockchain-Based System to Facilitate E-Voting Process [5], proposed a system to reduce fraud and increase transparency using blockchain, smart contracts, and a four-layer architecture.
6. Md Jobair Hossain Faruk et al., in BieVote: A Biometric Identification Enabled Blockchain-Based Secure and Trans-parent Voting Framework [6], integrated Hyperledger with facial and fingerprint biometrics to enhance security in voting systems.
7. The study Development of Blockchain-Based E-Voting System: Requirements, Design, and Security Perspective [7], by Md Jobair Hossain Faruk et al., discussed improved identity verification and transparency using Hyperledger, biometrics, and smart contracts.
8. Mohammad Malkawi, Luma Almasri, and Khalid Buqrais, in their work Secure Voting System for Jordan Par-liament Elections Using Blockchain Technology [8], proposed a private blockchain solution featuring SHA-256 encryption to enhance transparency and security.
9. Prasetya Cahya S. and Inayatulloh, in their paper Blockchain Model for Regional Elections in Indonesia [9], highlighted a blockchain model leveraging SDLC and SHA-256 to improve precision and transparency in elections.
10. Yamuna Rosasooria et al., in E-voting on Blockchain Using Solidity Language [10], introduced a system that detects fraud and reduces cost and time by utilizing Solidity and the Ethereum blockchain.

A. Research Gap

Current blockchain-based voting platforms have shown promise by incorporating greater security and transparency into such a system, yet there is still the challenge of scala-bility and infrastructure. Many proposed solutions, including biometric authentication, face concerns in the privacy domain and moral considerations of processing sensitive data.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 7, July 2025

|DOI: 10.15680/IJIRSET.2025.1407119|

Above all, they do not tend to change to electoral circumstances and settings. Our DigiPoll is proposed to overcome these loopholes by an enhanced blockchain hybrid framework designed with increased scalability but maintaining access across heteroge-neous populations while supporting confidentiality over a voter and thus a much more secure and inclusive process.

III. METHODOLOGY

The proposed blockchain-based e-voting system follows a structured workflow comprising several key stages: voter authentication, vote casting, blockchain transaction processing, vote counting and result verification, and audit finalization. These steps collectively ensure a secure, transparent, and efficient election process.

A. Voter Authentication
Users verify their identity using a secure authentication mechanism based on One-Time Passwords (OTP). The system cross-checks the credentials against a pre-registered voter database to ensure that only eligible voters gain access to the voting platform.

B. Vote Casting Process
Once authenticated, voters access an intuitive user interface that enables them to cast their vote easily. Each vote is encrypted with cryptographic techniques to maintain confiden-tiality and is securely transmitted to the blockchain network.

C. Blockchain Transaction Process
Every vote is recorded as an individual transaction on the blockchain ledger. Smart contracts deployed on the blockchain validate each vote, preventing duplication, ensuring eligibility, and blocking unauthorized access.

D. Vote Counting and Result Verification
Votes are automatically tallied by smart contracts imme-diately after the voting period ends, minimizing human in-tervention and errors. The election results are published on the blockchain, making them publicly verifiable and ensuring complete transparency.

E. Audit and Finalization
A tamper-proof election report is generated and published for audit and public verification. This immutable record guar-antees the integrity of the election and provides a trustworthy source for stakeholders.

F. Security Measures
The system incorporates multiple security layers including:
- End-to-End Encryption: Maintains vote integrity during transmission.
- Immutable Ledger: Prevents tampering or unauthorized modifications of recorded votes.
- Multi-Layer Authentication: Enhances voter security and mitigates fraudulent access.
- Consensus Mechanism: Validates votes via a secure and distributed blockchain network.

IV. SYSTEM DESIGN

The blockchain-driven e-voting system proposed is expected to provide election processes that are secure, transparent, and scalable. Each vote is treated as a transaction on the blockchain such that any tampering or modifying is not possible, thereby maintaining secrecy. This system architecture serves as the basis for the core constituent components such as the blockchain layer, smart contracts, the interface for the voters, the interface for the administrators, and many other very robust security measures orchestrated together for an efficient voting mechanism. It designates the real-time voter interaction, system integrity, and scalability in terms of accommodating elections of all sizes.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 7, July 2025

|DOI: 10.15680/IJIRSET.2025.1407119|

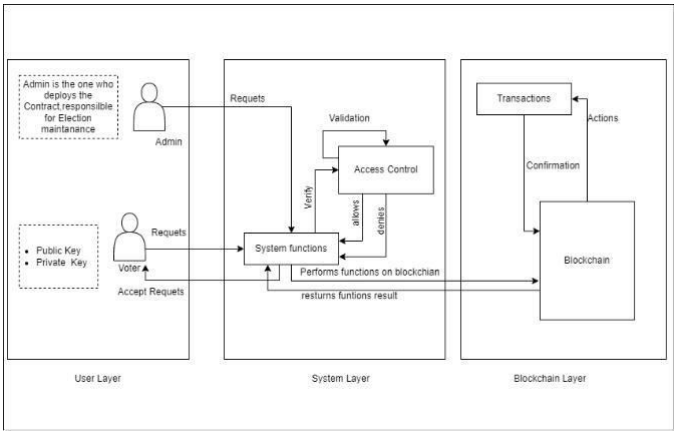


Fig. 1: System Design

The system design diagram represents the architecture and workflow of the blockchain e-voting system. All of these components synergize toward the secure registration process of voters, voting processes, and counting of results in order to ensure a transparent and accountable election process. All these work together as important parts that make a whole solution of the problem through the inherent features of the blockchain.

A. Blockchain Layer (Voting Ledger)

This is the heart of the e-voting system in which distributed technological-layer like Ethereum or Hyperledger is used. Every vote taken will be recorded as a transaction in a blockchain that is assured to be immutable and secure.

- Consensus Mechanism: It relies on a Proof of Stake or Proof of Authority consensus to confirm transactions, such that valid votes are added to the ledger but only authorized changes are made to it.
- Decentralization: The decentralized approach lowers the risk of being vulnerable to single points of control or failure, as the system is more robust-meaning requiring consensus among multiple nodes in recording each vote.
- Transparency and Trust: Accordingly, blockchain tech-nology makes the votes transparent. Voters can easily verify the counts against available blockchain records.

B. Smart Contracts for Vote Validation

The implementation of smart contracts automates important processes in the elections, such as voter eligibility verification and vote counting. The system streamlines operations and improves reliability.

- Voter Registration: Smart contracts track and verify voter eligibility so that only registered individuals are able to vote in the election.
- Vote Casting: Smart contracts cross-check existing vot-ing records with that of the voter and authenticate the voter's identity before recording the vote, should the voter be eligible to vote.
- Result Tallying: Once the voting is complete, smart contracts automatically calculate the votes and post the outcome on the blockchain, therefore making the election results open and accurate.

1) Voter Interface: The Voter Interface is designed to be simple, intuitive, and user-friendly, supporting seamless access via both web and mobile platforms. The system implements Multi-Factor Authentication (MFA), specifically OTP-based verification, to ensure secure registration, login, and voting processes. After casting a vote, the voter receives an instant, real-time receipt confirming that their vote has been success-fully recorded on the blockchain. This enhances transparency and trust in the system by allowing voters to verify that their submission was securely logged and cannot be altered.

2) Admin Interface: The Admin Interface is the one that monitors and manages the voting process in real time but does not allow voters to vote. It is decentralized and supports auditing through cryptographic proofs on the blockchain. In case of any discrepancy, administrators can review transactions and make corrections using the immutable ledger. It also does voter registration, updating voter information, and validating eligibility.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 7, July 2025

|DOI: 10.15680/IJIRSET.2025.1407119|

C. Security and Anonymity

The platform under consideration is a voting system based on a blockchain technology and provides reliable protection of participants' identities while raising highly protective mea-sures. All the communication needs to go through end-to-end encrypted connections like SSL/TLS so that information can be gotten or changed only by those people, it was sent to.

1) Encryption: AES-256 is one such advanced encryption used with data both at rest and in motion. The following data by the system are encrypted: voter information, voting preference, as well as admin information. No unprivileged individual is allowed to view this kind of information nor change it without authorization.

2) Authentication: This adds a critical layer of security with multi-factor authentication, which would require proving identity by password and one time passwords (OTP)-but in this way, even the possibility of unauthorized participation is highly reduced, for only eligible voters participate.

3) Anonymity with Zero-Knowledge Proofs: The process by which vote legitimacy may be verified without exposing the identity of the voter is Zero-Knowledge Proof (ZKP), and this enhances the anonymity. Thus, it preserves the voters' identity but keeps the record that will allow for unlimited auditing of the results of the voting without making a link between a voter and the specific vote cast by this voter.

D. System Workflow

With streamlined workflow, it enhances participation of the voter and ensuring the election process is done accordingly. The step is then controlled by the smart contract, and with this the processes get automated, decreasing possible human errors and manipulation at large.

- Voter Registration: From it, there is secured registration of voters – identity data verification data are provided. These data will then be validated by the system, verified, and in return will record a voter on blockchain.
- Authentication and Vote Casting: During the day of the election, voters first pay with MFA, secondly select candidates of their choice and thirdly vote. The system encrypts votes and submits them to the blockchain, which records those votes immutably.

- Vote Validation: Smart contracts along with the Blockchain technology guarantee validity and no repe-tition of the votes. Only then will the vote be recorded on the blockchain.
- Real-Time Tallying: The electronic voting system en-ables real-time tallying of votes through the use of smart contracts. As soon as the voting period concludes, votes are automatically counted and results are immediately available, eliminating delays and reducing the risk of human error.
- Auditing and Reporting: Using the blockchain trans-action record in the vault, the election process becomes fully auditable, allowing authorized parties to verify each vote without compromising voter anonymity. This ensures transparency, prevents tampering, and provides a perma-nent, tamper-proof record of all electoral activities.

This system design effectively incorporates security, trans-parency, and efficiency and offers a modern solution that is tamper-proof with regard to challenges associated with traditional electoral processes.

V. IMPLEMENTATION

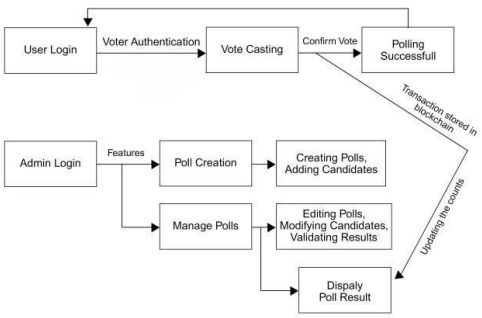


Fig. 2: Implementation Architecture

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 7, July 2025

|DOI: 10.15680/IJIRSET.2025.1407119|

The components in the blockchain-based e-voting system are divided into subsections, each integrated to provide high security alongside operational simplicity. The system includes front-end development, blockchain integration, backend sup-port, and comprehensive testing to ensure robustness and resistance to corruption.

A. User Interface (UI) Design

The e-voting system is developed using React.js and de-ployed on dedicated kiosks at voting counters for in-person voting. This setup guarantees a secure, consistent user expe-rience in a controlled environment. The interface is intuitive and straightforward, enabling voters to complete registration, authentication, and voting with minimal assistance, making the system accessible to users with varying technical skills.

B. User Experience (UX) Design

UX is central to the front-end design. The interface guides voters through the voting process with minimal steps, sup-ported by clear instructions and recognizable icons to reduce errors and confusion. It also adheres to basic accessibility standards, including screen reader compatibility and keyboard navigation, enabling independent and secure participation by voters with disabilities.

C. Blockchain Integration

The backend leverages blockchain technology, implemented using Ethereum. Blockchain ensures that votes are recorded as irreversible transactions that cannot be manipulated.

1) Smart Contract Deployment: Two smart contracts, de-veloped in Solidity and deployed on Ethereum, modularly handle system functions:

- Roles Contract: Manages user roles (e.g., admin, voter) and restricts access to sensitive functions.
- Voting Contract: Automates election setup, candidate registration, vote casting, and result tallying, ensuring immutable vote records on the blockchain.

2) Real-Time Vote Recording: Votes are captured live on the Voting Dashboard and recorded as blockchain transac-tions, allowing election officials and stakeholders to track vote counts in real time, thus enhancing transparency. The blockchain's distributed ledger guarantees that no third party can alter or delete votes.

3) Data Privacy: Data security is ensured through encryp-tion of voter identities and vote choices before storage on the blockchain. Anonymity techniques protect voter identities while enabling public and administrative verification of vote integrity.

D. Backend Development with Node.js and MySQL

The backend services are developed using Node.js, which handles API endpoints, business logic, and communication between the front-end and blockchain. Node.js facilitates effi-cient management of user requests and transaction submissions while ensuring scalability and responsiveness.

The system uses MySQL as the relational database man-agement system to securely store essential election data:

- Voter Data: Registration details and authentication cre-dentials of voters.
- Constituency Details: Information defining electoral dis-tricts and voter assignments.
- Elections and Candidates: Metadata about election events, candidates running, and their status.

MySQL supports robust querying and data integrity, provid-ing a reliable storage layer that complements the blockchain's immutable ledger for election transactions.

E. Smart Contract Development

Smart contracts are the system's backbone, rigorously tested to ensure security and reliability.

- Roles Contract: Enforces role-based access, defining admin and voter roles, restricting sensitive functions accordingly.
- Voter Verification: Validates voter eligibility based on registration data, ensuring only legitimate voters partici-pate.
- Vote Recording: Securely and automatically records each verified vote on the blockchain, preventing manip-ulation or errors.
- Result Tallying: Automatically tallies votes post-election and publishes results on the public blockchain to enhance transparency.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 7, July 2025

|DOI: 10.15680/IJIRSET.2025.1407119|

VI. RESULTS AND DISCUSSION

The proposed blockchain-based e-voting system was com-prehensively evaluated using key metrics such as security, transparency, performance, user accessibility, and feedback, demonstrating its effectiveness as a secure and user-friendly electoral platform.

A. Secure and Transparent Voting Process

The system successfully leveraged blockchain's immutabil-ity and tamper-resistance to secure votes. Every vote was recorded as an immutable transaction, preventing alteration or deletion. The decentralized nature enabled transparent, real-time vote verification while preserving voter anonymity by revealing only vote counts and confirmations.

B. Improved Voter Authentication

We successfully implemented a two-step OTP-based authen-tication mechanism, effectively preventing unauthorized vot-ing. Only verified voters, confirmed against the pre-registered database, were able to cast ballots, minimizing impersonation and fraudulent activity.

C. Efficient Vote Counting and Management

Smart contracts fully automated vote tallying, eliminating manual errors. Votes were instantly tallied after polls closed, enabling near real-time results and seamless election manage-ment through the blockchain interface without delays.

D. Enhanced Accessibility and Reliability

The React.js interface integrated with MetaMask provided a consistent user experience across desktops, tablets, and smartphones. The system demonstrated high reliability with zero downtime during testing, ensuring continuous access and maintaining voter trust across diverse user groups.

E. System Performance Evaluation

Our performance evaluation confirmed:

- Security: No vote tampering or unauthorized access occurred during rigorous testing.
- Transparency: Voters and auditors successfully moni-tored transactions live on the blockchain.
- Efficiency: Vote processing and tallying were completed within seconds after polling ended.
- User Feedback: Test participants reported a secure, intuitive, and user-friendly voting experience.
- Testing Scale: The system was tested with over 10 voters using test wallets created on the Ganache emulator. This simulation allowed thorough evaluation of the entire vot-ing workflow under realistic conditions. It helped verify the robustness of smart contract functions, authentication mechanisms, and the transaction processing pipeline. The testing confirmed the system's ability to handle multiple users concurrently without errors or performance degra-dation.

F. Interface and Functional Testing

Testing verified:

- Successful voter registration and verification ensuring eligibility.
- Admins efficiently created elections and managed candi-date lists.
- Vote casting integrated smoothly with MetaMask confir-mations.
- Real-time vote validation and immediate result displays functioned correctly.
- Automatic alerts effectively prevented double voting at-tempts.
- Comprehensive reports and ledger inspections confirmed data integrity.

TABLE I: Testing Summary of Blockchain-Based E-Voting System

Testing Aspect	Details
Number of Test Voters	10+ (using Ganache test wallets)
Purpose	Evaluate voting workflow, authentica-tion, and smart contracts

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 7, July 2025

|DOI: 10.15680/IJIRSET.2025.1407119|

Environment	Ganache blockchain emulator
Key Verifications	• Smart contract robustness • Authentication accuracy • Transaction processing reliability
Outcome	Successful multi-user handling without errors or delays

These results demonstrate that the system successfully meets core e-voting requirements, providing a secure, transparent, and accessible solution for electoral processes.

VII. FUTURE DIRECTION

Additional innovations on blockchain-based e-voting would be gathering data on the activities of the voters and demographic data to further fine-tune the model, with an enhance-ment on adaptability. Application of ensemble and transfer learning would improve pattern recognition, but having low latency would further advance the experience of clients. The real-time interaction with clients through a Flutter app, coupled with performance testing in simulated environments, will help in optimising the code. Crowdsourced validation will ensure user feedback and thus enhance transparency, security, and adaptability to changing electoral challenges.

VIII. CONCLUSION

Blockchain-based e-voting system developed here provides a huge advancement in safe and transparent voting. With real-time detection, ethical integration, and robust dataset handling, it promises to bring about safe and efficient voting experiences. Further work will be on dataset collection, web-application integration, and the testing of the system for real-time performance as the need grows with time. The project also stresses the importance of developing technologies that fight fake news and ensure democratic integrity.

REFERENCES

[1] M. Farhan, R. B. Sulaiman, A. H. Nur, and A. Salih, “Disrupting the bal-lot box: Blockchain as a catalyst for innovation in electoral processes,” Blockchain-based election framework, promotes secure, transparent, and efficient election processes; Implementation challenges and scalability concerns for broader applications.

[2] R. S. Duran, C. B. Balbon, J. Z. E. Balmes, P. B. G. Castro, U. G. Lopez, M. E. A. Noriega, and O. D. Tubola, “Easy e-vote: An ethereum-based voting system using ipfs and metamask for student government election,” Ethereum blockchain, IPFS for storage, MetaMask for authentication in a student election system, user-friendly MetaMask interface; decentral-ized data storage with IPFS; Requires technical setup; incurs gas fees for transactions on Ethereum.

[3] S. M. U. Deep, M. M. Hosen, M. Nisa, M. G. Hussain, and Y. Shiren, “E-voting system improvised by blockchain technology: A case study,” Ethereum and Quorum for secure e-voting, dual blockchain interaction, provides secure, tamper-resistant voting; SHA-256 encryption supports remote voting; High costs, scalability issues with large user adoption.

[4] S. S.A and K. K. T. G, “E-voting system using public blockchain,” Public blockchain for secure voting; JSON database and REST API integration; Ethereum blockchain with Ganache testing, irreversible voting process; lower costs with simplified, secure process; Limited scalability; requires technical infrastructure and expertise.

[5] K. C. Nwosu and M. Abdulgader, “Legitvote: A blockchain-based system to facilitate e-voting process,” Blockchain with smart contracts; four-layer architecture: Registration, Verification, Migration, Voting, reduces election fraud; increases transparency and efficiency; Requires internet access and blockchain infrastructure; setup complexity.

[6] M. J. H. Faruk, M. Islam, F. Alam, H. Shahriar, and A. Rahman, “Bievote: A biometric identification enabled blockchain-based secure and transparent voting framework,” Blockchain system using Hyper-ledger Fabric; facial and fingerprint biometric authentication, RESTful API, enhanced security with biometrics; improved trust and transparency; Requires advanced infrastructure for biometrics; concerns about biometric data security.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 7, July 2025

|DOI: 10.15680/IJIRSET.2025.1407119|

[7] M. J. H. F. et al., "Development of blockchain-based e-voting system: Requirements, design, and security perspective," Hyperledger Fabric with biometrics (facial and fingerprint recognition); smart contracts, increased transparency and security; enhances voter identity verification; Biometrics mandatory for participation; complex implementation for large-scale elections.

[8] M. Malkawi, M. B. Yassein, and A. Bataineh, "Blockchain-based voting system for jordan parliament elections," Private, centralized blockchain; hierarchical voting for group and candidate levels; SHA256 for security, ensures transparency and security; customized for regional use; Limited to a Jordan-specific case; requires high computational power for signa-ture verification.

[9] P. C. S. and Inayatulloh, "Block chain model for regional elections in indonesia," Blockchain system for regional elections; SDLC and SHA256 cryptographic hash for security, improves data accuracy and election transparency; tailored for regional elections; Internet access limits in remote regions; high IT infrastructure needs.

[10] Y. Rosasooria, M. A. M. Isa, A. K. Mahamad, S. Yamaguchi, S. Saon, and M. A. Ahmadon, "E-voting on blockchain using solidity language," Solidity smart contracts on Ethereum; designed for student council elections, detects voting fraud; reduces cost and time by eliminating paper ballots; Requires computational resources for smart contracts; internet and blockchain infrastructure dependency.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details