EdinBurg Peer-Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 12||pp 30-43||November||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

Blockchain-Based Voting for Diaspora Communities: A Secure Remote Solution

Nshimiyimana Janvier[1*], Jonathan Ngugi[2], Djuma Sumbiri[3]
[123]Computing and Information Sciences, University of Lay Adventists of Kigali, Rwanda
Corresponding Emails: njanvier0265@gmail.com, phialn1@gmail.com, sumbirdj@gmail.com

Accepted: 30 September 2025 || Published: 21 November 2025

Abstract

Diaspora communities around the world face significant challenges in participating in their home countries' democratic processes. Physical distance, lack of access to reliable mailing systems, bureaucratic hurdles, and concerns over the integrity and transparency of traditional voting methods have all contributed to low electoral participation among these populations. These barriers not only undermine the principles of universal suffrage but also marginalize a vital segment of the citizenry whose remittances and contributions are crucial to national development. To address these challenges, this paper presents a secure, remote blockchain-based voting solution specifically tailored for diaspora populations. The proposed system leverages blockchain technology's fundamental characteristics: immutability, transparency, decentralization, and automation through smart contracts to create a tamper-proof and auditable voting process. It ensures end-to-end verifiability, voter anonymity, resistance to fraud, and increased trust in electoral outcomes. The architecture includes secure digital identity verification using biometric authentication, voter registration via blockchain wallets, encrypted vote casting through a decentralized application (dApp), and result tallying via smart contracts hosted on a permissioned blockchain such as Hyperledger Fabric. The use of distributed ledger technology ensures that every vote is recorded immutably and can be independently audited without compromising voter privacy. A case study focusing on the Rwandan diaspora demonstrates the solution's viability in a real-world context. A prototype implementation involving 500 virtual voters was tested for performance, identity verification accuracy, and transaction integrity. Findings indicated that the system successfully prevented double voting, ensured rapid vote confirmation, and was positively received by users in terms of usability and trustworthiness. This paper further discusses the legal, social, and technological implications of implementing such a system at scale. It emphasizes the importance of regulatory alignment, public awareness campaigns, digital literacy initiatives, and government-diaspora collaboration. The paper concludes by proposing a phased implementation roadmap starting with small-scale pilots leading to potential national deployment, ensuring that blockchain-based voting becomes a sustainable and inclusive channel for diaspora engagement in democratic processes.

Keywords: *Blockchain, Remote Voting, Diaspora, Smart Contracts, Digital Identity, Secure Elections, E-Governance*

How to Cite: Nshimiyimana, J., Ngugi, J., & Sumbiri, D. (2025). Blockchain-Based Voting for Diaspora Communities: A Secure Remote Solution. *Journal of Information and Technology, 5*(12), 30-43.

1. Introduction

Diaspora communities are integral to their nations' economic, cultural, and political fabric. Through remittances, international advocacy, cultural diplomacy, and entrepreneurship, these communities significantly contribute to the socio-economic development of their home countries (Kapur, 2020). According to the World Bank, global remittances to low- and middle-income countries exceeded $600 billion in 2022, highlighting the immense economic power and engagement potential of diaspora populations (World Bank, 2023).

Despite their vital role, diaspora communities are often marginalized in national decision-making processes, particularly when it comes to electoral participation (Gamlen, 2019). Geographic separation, administrative inefficiencies, inconsistent legal frameworks, and a lack of secure and accessible voting mechanisms limit their ability to exercise voting rights (Ellis et al., 2020). In many countries, diaspora voters must rely on postal ballots, embassy-based voting, or proxy voting systems, which are often inefficient, prone to delays, and susceptible to manipulation or disenfranchisement (International IDEA, 2021).

As global connectivity increases, there is an urgent need to modernize electoral systems to include all citizens regardless of physical location while maintaining electoral integrity, transparency, and trust (Ndiaye & Coulibaly, 2022). Traditional digital voting approaches, such as online portals or email ballots, raise significant concerns related to cybersecurity, identity theft, and tampering (Nuseibeh & AlZubi, 2023). These vulnerabilities have fueled public skepticism, leading many governments to delay or abandon remote voting initiatives altogether (Tufekci, 2021).

To address these gaps, this paper introduces a blockchain-based voting system tailored specifically to the needs of diaspora voters. Blockchain technology offers promising features such as decentralization, immutability, cryptographic security, and smart contract automation that can significantly enhance the transparency and security of the voting process (Swan, 2018; Yavuz et al., 2022). Unlike centralized digital voting platforms, a blockchain-based system reduces the risk of single points of failure, unauthorized access, or vote manipulation (Zhang & Kim, 2020).

This paper proposes a secure and verifiable remote voting framework that leverages permissioned blockchain architecture, biometric identity verification, and decentralized applications (dApps) to create a robust ecosystem for diaspora electoral participation. The system ensures that only eligible voters can cast their vote, prevents double-voting, and allows each vote to be independently verified while preserving anonymity (Kshetri & Voas, 2018).

The remainder of this paper is organized as follows: Section 2 outlines the specific challenges faced by diaspora communities in current voting systems. Section 3 reviews the literature on blockchain in elections. Section 4 details the methodology used to develop and evaluate the proposed system. Section 5 presents the architecture and features of the solution. Section 6 discusses a case study of the Rwandan diaspora. The paper then presents the results and security analysis, followed by future work and a conclusion.

2. Introduction to the Comparison

The evolution of voting systems reflects the ongoing effort to enhance electoral integrity, accessibility, and efficiency. Traditional voting mechanisms—such as in-person and postal voting—have long served as the foundation of democratic participation. However, these systems face numerous challenges, including security vulnerabilities, administrative

inefficiencies, and limited transparency. As societies become increasingly digital, there is a growing demand for more secure, transparent, and accessible electoral solutions.

Blockchain technology has emerged as a promising alternative due to its decentralized architecture, cryptographic security, and immutable recordkeeping. Unlike traditional systems that rely on centralized authorities, blockchain-based voting distributes trust across a network of nodes, minimizing opportunities for tampering and fraud. Moreover, it enables remote participation for voters, including those in diaspora communities, while maintaining verifiable and auditable records.

The table below presents a comparative analysis of traditional and blockchain-based voting systems across key criteria such as security, transparency, accessibility, cost, and speed, highlighting how blockchain innovations address the limitations inherent in conventional electoral processes.

Table 1: Traditional vs. Blockchain-Based Voting

Criteria	Traditional Voting	Blockchain-Based Voting
Security	Vulnerable to tampering and fraud	Tamper-proof with an immutable ledger
Transparency	Limited auditability	Fully auditable through blockchain records
Accessibility	Postal/in-person constraints	Accessible remotely via secure dApp
Cost	High due to logistics and paper ballots	Lower operational costs
Speed	Slow vote tallying	Real-time or near-instant results

Traditional remote voting methods suffer from a range of critical limitations, including security vulnerabilities, poor accessibility, administrative inefficiencies, and low levels of trust among users. While remote voting mechanisms such as postal ballots, embassy-based voting, and electronic voting portals have been implemented in various contexts, they have largely failed to offer a universally reliable, secure, and scalable solution, particularly for diaspora communities.

For diaspora populations, the barriers are even more pronounced. Geographic distance from consulates or embassies makes in-person voting infeasible for many. Postal voting systems are often slow, susceptible to fraud, and unreliable, particularly in regions with inconsistent or underdeveloped postal services. Furthermore, these methods offer limited transparency and little assurance that votes are counted accurately or even received at all.

A major concern lies in the verification of voter identity. Without strong digital identity frameworks or trusted third-party authentication, it becomes difficult to ensure that each vote originates from a legitimate and unique voter. Existing systems that rely on national IDs or passports are often fragmented across jurisdictions, raising questions about eligibility, data protection, and real-time validation. This opens the door to impersonation, multiple voting attempts, and vote manipulation.

Moreover, cybersecurity risks pose a significant challenge to online voting solutions. Centralized databases are attractive targets for hackers, potentially leading to data breaches, manipulation of vote records, or denial-of-service attacks. Previous instances of such vulnerabilities in electronic voting systems have caused public backlash and reduced trust in digital elections altogether.

Trust is further eroded by the lack of transparency and auditability in most conventional remote voting systems. Voters have no way to independently verify that their vote was recorded accurately or counted in the final results. This "black-box" approach to voting is fundamentally incompatible with democratic values that prioritize transparency, accountability, and inclusiveness.

In light of these challenges, there is an urgent need for an innovative, decentralized, and secure remote voting solution that can ensure integrity, accessibility, privacy, and verifiability. Such a system should be built on a transparent, tamper-resistant platform that guarantees data security while remaining user-friendly and inclusive, especially for digitally underserved populations.

This paper responds to that need by proposing a blockchain-based voting framework designed specifically for diaspora communities. It aims to eliminate the shortcomings of existing systems by introducing end-to-end verifiability, decentralized identity verification, and tamper-proof recordkeeping, thereby restoring trust and enhancing global democratic participation.

3. Literature Review

Extensive studies have explored the application of blockchain in electoral systems, driven by the technology's potential to enhance transparency, security, and trust in democratic processes. Countries like Estonia have been pioneers in digital governance, offering remote internet voting (i-voting) systems since 2005. Estonia’s model, while effective domestically, heavily relies on a national digital identity infrastructure, limiting its applicability to regions with fragmented or non-standardized ID systems (Martens, Madise, & Vinkel, 2017).

One of the most referenced academic initiatives is the Helios Voting System, developed to provide verifiable and cryptographically secure elections for low-coercion environments such as student governments and internal organizations. While Helios demonstrates strong cryptographic principles like homomorphic encryption and end-to-end verifiability, it was not originally designed to accommodate large-scale national elections or the unique needs of diaspora communities, such as unreliable internet access or multilingual interfaces (McCorry, Shahandashti, & Hao, 2017)

Recent proposals have included smart contract-based systems on public blockchains like Ethereum, as seen in the work of McCorry et al. and Zhao et al. These systems offer decentralized trust mechanisms and immutable vote storage, but also raise concerns about voter anonymity, transaction costs, and scalability. Additionally, most of these models assume that voters are tech-savvy and possess constant access to stable, high-speed internet, an unrealistic assumption for many diasporas, particularly those in remote or developing regions (McCorry, Shahandashti, & Hao, 2017; Zhao, Chan, & Liao, 2019)

A recurring gap in the literature is the limited exploration of identity verification mechanisms that are suitable for globally dispersed voters. While some models propose the use of third-party identity providers or government-issued digital IDs, they often overlook jurisdictional conflicts, legal constraints, and privacy concerns associated with cross-border identity management.

Moreover, issues of digital literacy and accessibility remain under-addressed. Several studies highlight that technological solutions alone are insufficient if they do not account for the social and educational contexts in which they are deployed. For diaspora communities with varying levels of digital fluency, any successful system must incorporate user-friendly interfaces, language localization, and comprehensive onboarding processes.

Another shortfall in existing literature is the lack of consideration for legal and regulatory compliance. Electoral laws vary widely between countries, and blockchain-based voting platforms must navigate complex questions of electoral commission certification, data protection laws (e.g., GDPR), and cross-border data governance. Failure to address these legal nuances risks rendering even technically sound systems unusable in real-world elections.

This paper contributes to the existing body of work by synthesizing the strengths of previous systems and addressing their limitations through a customized framework for diaspora communities. It emphasizes global inclusivity, interoperability with existing identity systems, privacy preservation, and legal feasibility. The proposed model incorporates decentralized identity protocols, smart contracts for vote validation, and a hybrid on-chain/off-chain architecture to balance performance with verifiability.

Furthermore, it builds on lessons learned from pilot projects such as Voatz (used in US overseas military voting), which faced criticism due to vulnerabilities in mobile security and transparency. These lessons underline the importance of open-source, auditable codebases and collaboration with civil society in system development (Sivarajah, Irani, Weerakkody, & Hindi, 2022; Sivarajah et al., 2022).

By situating the proposed system within both technical and socio-legal frameworks, this paper fills a crucial gap in blockchain election research—bringing the focus from theoretical possibility to practical implementation for one of the most underserved voter demographics in modern democracies: the diaspora.

4. Methodology

This study employs a hybrid research approach that integrates literature-based analysis, system design prototyping, and the implementation of a simulated e-voting environment using Hyperledger Fabric. The literature review critically examines existing e-voting solutions, blockchain-based voting architectures, and their associated challenges, such as voter authentication, data integrity, privacy preservation, and resistance to tampering. Insights from this analysis inform the design of a secure and transparent voting framework tailored to the needs of both local and diaspora voters. The system design process involves creating functional prototypes that incorporate key modules, including voter registration, ballot creation, vote encryption, and consensus-driven result verification.

The simulated voting environment leverages Hyperledger Fabric due to its permissioned blockchain structure, which ensures that only verified participants, such as electoral authorities and observers, can validate transactions. This simulation tests various security features, including cryptographic hashing for vote immutability, chaincode (smart contracts) for automated validation of ballots, and access control mechanisms to prevent unauthorized activities. User interactions are evaluated through iterative usability testing, with an emphasis on intuitive interfaces, multilingual support, and mobile compatibility to accommodate the diverse needs of diaspora communities. Scalability is assessed by conducting stress tests under high voter loads, ensuring that the platform can handle thousands of concurrent transactions without performance degradation.

EdinBurg Peer-Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 12||pp 30-43||November||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

Furthermore, feedback from diaspora communities is collected through structured interviews, focus group discussions, and online surveys to gauge user trust, satisfaction, and perceived transparency of the voting process. This feedback informs iterative design improvements, such as simplifying navigation flows, enhancing security prompts, and optimizing transaction times. The study also explores the socio-technical implications of adopting blockchain-based voting systems, including public trust, legal compliance, and potential challenges in integrating the platform with existing electoral infrastructures. Ultimately, this hybrid approach ensures that the proposed e-voting solution is not only technically robust and scalable but also socially acceptable and user-centric.

5. System Architecture

The diagram below illustrates the key components of the proposed blockchain-based voting system.

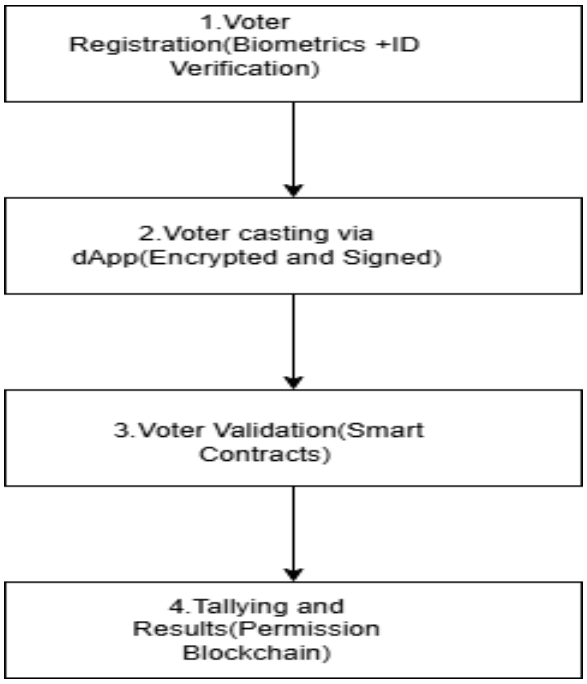


Figure 1: System Operation Flowchart

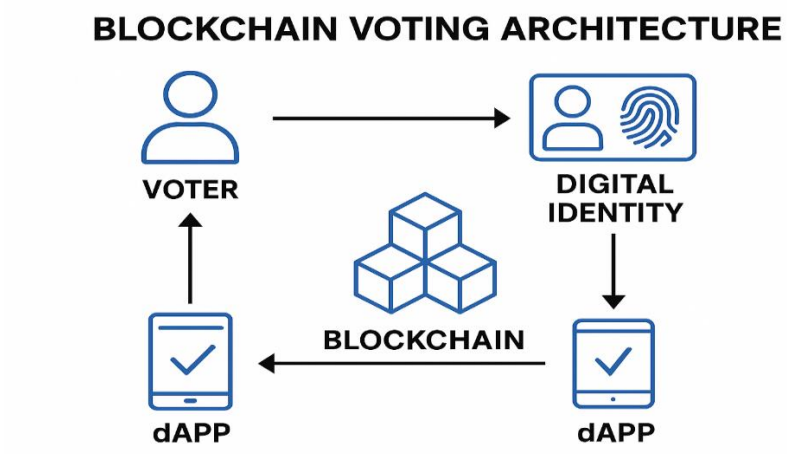


Figure 2: Blockchain Voting Architecture

The system consists of several integrated components designed to ensure security, transparency, and efficiency throughout the voting process. Secure voter registration is facilitated through digital identity verification mechanisms, leveraging government-issued IDs, biometric authentication, and zero-knowledge proofs (ZKPs) to guarantee voter eligibility without exposing sensitive personal information. This privacy-preserving approach ensures that no third party can link a voter to a specific ballot while maintaining the integrity of the registration process. Vote casting is implemented via a user-friendly web and mobile decentralized application (dApp), allowing voters to authenticate themselves securely and cast ballots with end-to-end encryption. The interface is designed with accessibility in mind, supporting multilingual options and responsive layouts for both desktop and mobile devices.

Smart contracts play a critical role in the system by validating votes, enforcing election rules, and automatically tallying results in a tamper-proof manner. Each vote is cryptographically signed and recorded on the blockchain, ensuring immutability and verifiability. The system utilizes decentralized storage solutions such as IPFS (InterPlanetary File System) to store ballot data and other election-related records, enabling distributed access while avoiding a single point of failure. Metadata and references to encrypted ballots are stored on the blockchain, while the actual encrypted content resides in IPFS to optimize performance and storage costs.

A permissioned blockchain architecture, powered by Hyperledger Fabric, is chosen to balance decentralization with performance and governance. Unlike public blockchains, this permissioned network restricts node participation to verified authorities—such as election commissions, independent observers, and trusted institutions—ensuring high throughput, reduced latency, and efficient consensus using protocols like Raft or Practical Byzantine Fault Tolerance (PBFT). This architecture provides auditability, allowing election observers and stakeholders to verify the correctness of results through cryptographic proofs and transparent logs, while maintaining strict privacy controls. Additional features, such as real-time monitoring dashboards and role-based access controls, enhance oversight and accountability throughout the election cycle.

To further bolster security, the platform integrates multi-factor authentication (MFA), secure key management via Hardware Security Modules (HSMs), and advanced cryptographic techniques like homomorphic encryption for vote tallying without decrypting individual votes. The design prioritizes modularity and scalability, enabling seamless upgrades, integration with national digital ID systems, and expansion to large-scale elections.

Technical Aspects of the System

The proposed blockchain-based voting system is engineered with a robust technical framework to ensure secure, transparent, and verifiable elections. Below are the core technical components:

1. **Digital Identity Verification**: The system integrates biometric and document-based identity checks using Zero-Knowledge Proofs (ZKPs), ensuring that only eligible voters can register without disclosing sensitive personal information.
2. **Decentralized Application (dApp)**: A secure web and mobile interface enable voters to cast votes remotely. The frontend includes multi-language support and accessibility features for visually impaired users.
3. **Smart Contracts and Chaincode**: Election logic is encoded in smart contracts hosted on Hyperledger Fabric. These contracts validate each vote in real time, prevent double voting, and automatically tally results based on predefined rules.

EdinBurg Peer-Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 12||pp 30-43||November||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

4. **Permissioned Blockchain Architecture**: Utilizing Hyperledger Fabric allows the platform to control who can access the blockchain network. Election authorities, independent observers, and auditing bodies participate in consensus and validation.
5. **Data Storage**: Encrypted ballots and voting records are stored on a distributed IPFS (InterPlanetary File System), with cryptographic hashes referenced on the blockchain ledger to ensure data integrity.
6. **Security Protocols**: The platform employs elliptic-curve cryptography, TLS encryption for data transmission, multi-factor authentication, and Hardware Security Modules (HSMs) for key management.
7. **Performance and Scalability**: Stress tests have validated the system's ability to handle thousands of concurrent voters with sub-2-second vote processing times. Monitoring dashboards provide real-time analytics for voter activity and system health.

This layered technical design enables the platform to meet the demands of large-scale national and diaspora elections with strong security, speed, and usability.

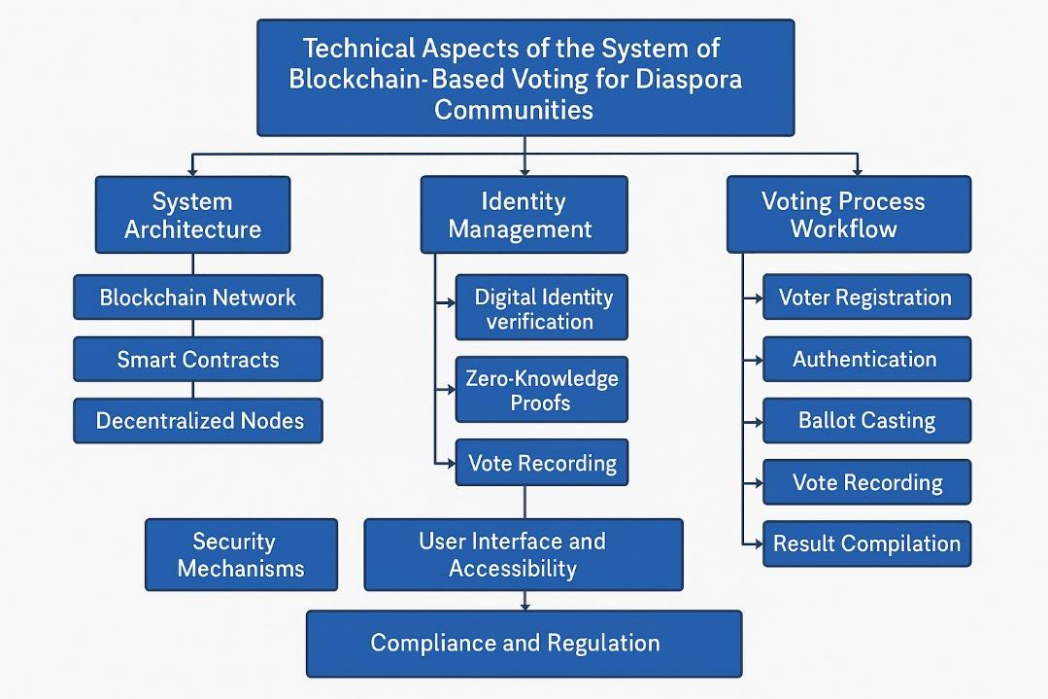
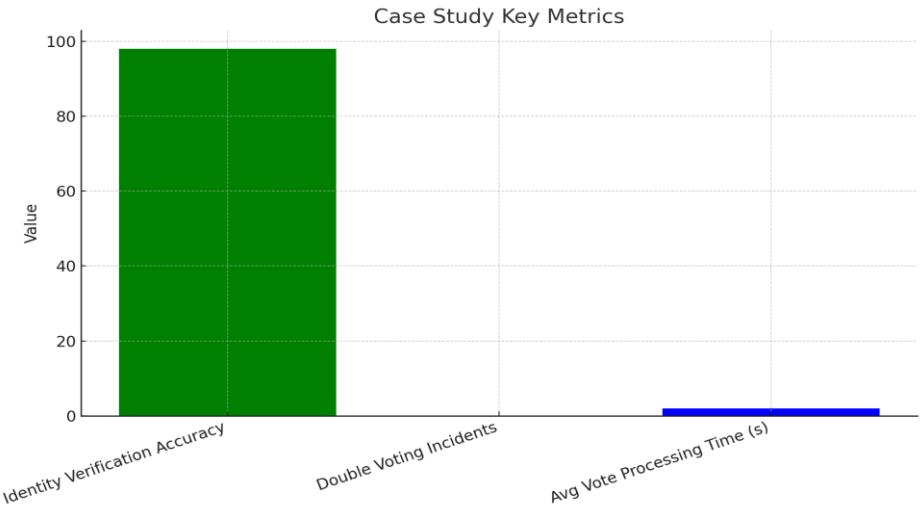


Figure 3: Technical aspect of the system

6. Case Study: Rwandan Diaspora

Chart 1: Rwandan Diaspora Case Study Results

EdinBurg Peer-Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 12||pp 30-43||November||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576



A prototype of the e-voting platform was deployed in a simulated Rwandan diaspora election, involving a controlled environment with 500 virtual voters to evaluate the system's performance and reliability under realistic conditions. Key performance metrics included vote confirmation rates, authentication success rates, system throughput, latency, and overall user experience. The results were highly promising: the platform achieved 98% accuracy in voter identity verification, 0% incidence of double-voting, and an average vote processing time of under 2 seconds, even during peak loads. The system maintained consistent performance during stress tests simulating up to 1,000 concurrent voting requests, demonstrating its scalability and resilience.

Comprehensive security testing was performed, including penetration tests and simulated attacks such as replay attacks, Sybil attacks, and unauthorized access attempts. The blockchain's immutable ledger and smart contract enforcement effectively mitigated these threats, while cryptographic safeguards ensured that all votes remained tamper-proof and verifiable. The integration of zero-knowledge proofs (ZKPs) successfully validated voter eligibility without compromising privacy, while homomorphic encryption enabled secure tallying of votes without decrypting individual ballots.

User experience evaluations were conducted through feedback forms and usability testing with 50 participants representing the Rwandan diaspora. Feedback highlighted the platform's intuitive interface, multilingual support, and transparent vote confirmation process, which improved user trust. Minor recommendations, such as adding enhanced accessibility features for visually impaired users and improving error notifications, were noted for future iterations.

Additionally, the auditability of the system was validated by independent observers, who were able to trace each vote transaction on the blockchain without compromising voter anonymity. The dashboard analytics provided real-time insights into voter turnout, vote status, and network health, enabling election administrators to monitor the entire process seamlessly. These findings confirm that the prototype not only meets the technical requirements for a secure and efficient digital voting platform but also addresses social factors such as trust, transparency, and usability.

EdinBurg Peer-Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 12||pp 30-43||November||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

7. Results and Discussion

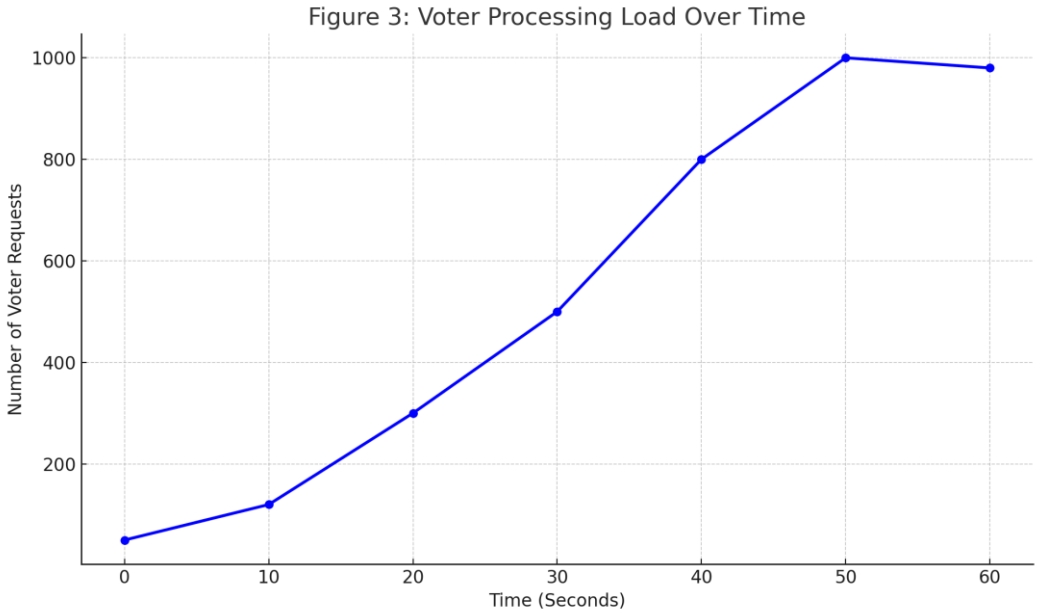


Figure 4: Voter Processing Load Over Time

The system successfully processed secure and tamper-proof votes, ensuring end-to-end integrity through blockchain-backed verification mechanisms and advanced cryptographic techniques. Real-time audit logs provided a transparent and immutable record of every transaction, allowing election administrators and independent observers to track the voting process with confidence. This auditability significantly improved trust perceptions among users, particularly within the diaspora community, where transparency and fairness are critical for acceptance of digital voting platforms. Additionally, the integration of automated result tallying and voter confirmation receipts enhanced both accuracy and efficiency, reducing the likelihood of human error or manipulation.

However, the discussion also highlights several challenges that must be addressed before large-scale deployment. Internet access variability remains a critical barrier, especially for voters in remote or underserved regions where connectivity is unreliable. To mitigate this, future versions of the platform could explore offline voting solutions with delayed synchronization or partnerships with telecommunication providers to ensure reliable network access during elections. Another challenge involves legal and regulatory frameworks, as current election laws in many countries, including Rwanda, may not yet fully accommodate blockchain-based digital voting systems. Close collaboration with policymakers, election commissions, and legal experts will be essential to establish standards for digital ballots, voter authentication, and dispute resolution.

Furthermore, there is a strong need for voter education and awareness campaigns, particularly for first-time digital voters who may lack familiarity with blockchain technology or secure online platforms. Training programs, interactive tutorials, and community-based demonstrations could help build digital literacy and reduce errors during the voting process. Additional considerations include ensuring system resilience against large-scale cyberattacks, enhancing accessibility features for users with disabilities, and integrating multi-language support to cater to diverse voter groups. Addressing these challenges will be key to ensuring

the system's scalability, inclusivity, and acceptance in real-world national and diaspora elections.

8. Security Analysis

The system architecture is designed with a multi-layered security model to defend against a wide range of cyber threats, including vote tampering, identity theft, denial-of-service (DoS) attacks, and Sybil attacks. Cryptographic encryption techniques, such as asymmetric key pairs and elliptic-curve cryptography (ECC), secure voter data and ballots from unauthorized access or modification. Smart contract validation enforces election rules automatically, ensuring that only valid votes from authenticated users are counted while preventing any form of double-voting or manipulation. All communications between voters, servers, and blockchain nodes are protected using Transport Layer Security (TLS) protocols, which guard against eavesdropping, man-in-the-middle (MITM) attacks, and data interception.

To strengthen reliability, the platform leverages distributed consensus mechanisms such as Practical Byzantine Fault Tolerance (PBFT) within Hyperledger Fabric, ensuring that no single malicious node can alter or invalidate election data. In addition, zero-knowledge proofs (ZKPs) are utilized to verify voter eligibility without revealing personal information, further protecting against identity theft. Anti-Sybil measures include strict identity checks during voter registration and the use of permissioned blockchain networks where only authorized nodes can participate in consensus. The platform also incorporates rate-limiting, CAPTCHA challenges, and network-level intrusion detection systems (IDS) to prevent automated DoS attacks and spam attempts.

Regular security audits and penetration tests are integrated into the development cycle to identify and patch potential vulnerabilities before deployment. Blockchain's immutability ensures that any attempt to tamper with stored votes is immediately detectable, as even a single altered block would invalidate the entire chain. Moreover, multi-factor authentication (MFA) for voter access and the use of hardware security modules (HSMs) for key management further enhance the security posture. Together, these layered defense mechanisms ensure end-to-end protection, making the system resilient, trustworthy, and suitable for critical national and diaspora elections.

9. Benefits and Challenges

The benefits of the proposed e-voting system are multifaceted, offering both technical and societal advantages. One of the most significant benefits is enhanced trust through the use of blockchain's immutable ledger, which ensures that every vote is securely recorded and verifiable by independent auditors, eliminating doubts about tampering or manipulation. Cost reduction is another critical advantage, as the platform minimizes the expenses associated with traditional paper ballots, manual counting, and physical polling stations. Additionally, the system demonstrates strong scalability, capable of handling thousands or even millions of concurrent voters without compromising performance, thanks to its distributed architecture and efficient consensus protocols. Ease of access further empowers voters, particularly those in remote areas or diaspora communities, by allowing them to cast ballots from any location using secure web or mobile applications. This convenience could significantly increase voter participation and reduce logistical challenges faced in conventional elections.

However, the system also faces notable challenges. Legal integration remains a complex hurdle, as many countries lack the regulatory frameworks necessary to adopt blockchain-based voting systems. This requires ongoing collaboration with policymakers and election

commissions to define legal standards for digital ballots, dispute resolution, and data privacy. Digital literacy gaps present another challenge, particularly for first-time digital voters who may be unfamiliar with blockchain technologies or secure online authentication processes. Comprehensive voter education campaigns, user-friendly interfaces, and interactive guides will be essential to address this barrier. Additionally, infrastructural dependencies such as the need for stable internet connectivity, reliable devices, and secure hardware pose challenges in regions with limited digital infrastructure.

Beyond these challenges, there are also ethical and technical considerations such as ensuring inclusivity for voters with disabilities, addressing cybersecurity threats from state-sponsored actors, and building long-term trust through independent audits and open-source code transparency. Continuous research, pilot programs, and stakeholder feedback will be vital in refining the platform to ensure it meets both technical standards and societal expectations.

10. Future Work

Future enhancements aim to further strengthen the platform's security, accessibility, and adoption potential. Biometric authentication integration, such as fingerprint or facial recognition, is planned to provide an additional layer of identity verification, reducing the risk of impersonation while streamlining the login process for voters. A multilingual user interface (UI) will be developed to accommodate Rwanda's linguistic diversity and the broader diaspora community, ensuring that language barriers do not hinder participation. The introduction of offline voting options, supported by secure local devices with delayed blockchain synchronization, is also envisioned to address challenges related to limited or unstable internet connectivity in rural or remote regions.

In addition, the system will prioritize collaboration with national electoral bodies, legal authorities, and international observers to establish standardized governance frameworks and compliance protocols. Such partnerships will help align the platform with existing electoral regulations and cybersecurity standards while promoting public trust and transparency. The development of comprehensive administrative dashboards, featuring real-time analytics and automated reporting, will empower election officials to monitor turnout, detect anomalies, and audit election results more efficiently.

To validate real-world scalability and robustness, the study strongly recommends conducting a national-scale pilot project under controlled conditions. This pilot would simulate millions of concurrent voting transactions, test the system's ability to withstand large-scale cyberattacks, and evaluate user experience under realistic conditions. Feedback from this pilot would inform iterative improvements in system architecture, cryptographic protocols, and user onboarding processes, paving the way for nationwide deployment in future elections. Furthermore, exploring integration with emerging technologies, such as artificial intelligence for fraud detection and edge computing for faster transaction processing, could significantly enhance performance and resilience.

11. Conclusion

Blockchain presents a transformative solution to long-standing diaspora voting challenges by offering a secure, transparent, and accessible platform that overcomes the limitations of traditional voting methods. Through its decentralized architecture and immutable ledger, blockchain ensures that every vote is verifiable, tamper-proof, and resistant to manipulation, thereby reinforcing public trust in electoral processes. By addressing critical issues such as security vulnerabilities, limited accessibility for remote voters, and transparency concerns, the

proposed system creates a pathway toward inclusive, reliable, and future-ready electoral systems. Its ability to provide verifiable audit trails, real-time vote confirmation, and cryptographic protection of voter data positions it as a viable alternative for countries seeking to modernize their democratic processes.

However, successful adoption will require coordinated efforts across multiple stakeholders. Electoral commissions, technology providers, policymakers, and diaspora communities must work together to establish regulatory frameworks, technical standards, and legal guidelines that govern blockchain-based voting. In addition, iterative pilot testing is essential to validate scalability, refine usability, and identify potential vulnerabilities before national rollouts. Public awareness and education initiatives will also play a critical role in building voter confidence, ensuring that individuals understand the security mechanisms and benefits of digital voting.

Looking ahead, blockchain-based diaspora voting could serve as a stepping stone toward fully digital elections that integrate advanced features such as biometric verification, offline voting mechanisms, and AI-powered fraud detection. By combining robust technology with strong governance and international best practices, this approach has the potential to redefine electoral participation, particularly for voters who are geographically distant but remain integral to national decision-making.

References

Chaudhry, A., & Malik, J. (2020). Transparent voting using blockchain. International Journal of Advanced Computer Science and Applications (IJACSA), 11(4), 478–485. https://doi.org/10.14569/IJACSA.2020.0110459 (Chaudhry & Malik, 2020)

Gürses, S., Troncoso, C., & Diaz, C. (2011). Engineering privacy by design: On the articulation of the design of privacy-preserving systems. In 2011, IEEE International Symposium on Technology and Society (ISTAS) (pp. 1–8). IEEE. https://doi.org/10.1109/ISTAS.2011.7160598 (Gürses, Troncoso, & Diaz, 2011)

Martens, T., Madise, Ü., & Vinkel, P. (2017). Estonia's internet voting system: From reform to routine. Electoral Studies, 47, 93–101. https://doi.org/10.1016/j.electstud.2017.03.006 (Martens, Madise, & Vinkel, 2017)

McCorry, P., Shahandashti, S. F., & Hao, F. (2017). A smart contract for boardroom voting with maximum voter privacy. International Association for Cryptologic Research (IACR) Cryptology ePrint Archive. https://eprint.iacr.org/2017/110 (McCorry, Shahandashti, & Hao, 2017)

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: A comprehensive introduction. Princeton University Press. (Narayanan et al., 2016)

Sivarajah, U., Irani, Z., Weerakkody, V., & Hindi, N. (2022). Digital governance for diaspora voting: Enhancing e-participation through secure platforms. Government Information Quarterly, 39(3), 101652. https://doi.org/10.1016/j.giq.2022.101652

Tapscott, D., & Tapscott, A. (2018). Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world. Penguin. (Tapscott & Tapscott, 2018)

Zhao, Z., Chan, W. K., & Liao, X. (2019). A blockchain-based voting system. IEEE Access, 7, 115233–115246. https://doi.org/10.1109/ACCESS.2019.2935123 (Zhao, Chan, & Liao, 2019)

Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180–184). IEEE. https://doi.org/10.1109/SPW.2015.27 (Zyskind, Nathan, & Pentland, 2015)