EdinBurg Peer Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 6||pp 70-89||August||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

Blockchain-Based Voting System for Transparent and Tamper-Proof Elections in Rwanda

Niyonsaba Alice[1*], Dr.KN Jonathan[2], Dr. Djuma Sumbiri[3]
[123]Faculty of Computing and Information Sciences, Department of Information Technology, University of Lay Adventist of Kigali (Unilak), Rwanda
Corresponding Author Email: allicy1@gmail.com, phialn1@gmail.com, sumbirdj@gmail.com

Accepted: 13 June 2025 || Published: 20 August 2025

Abstract

This paper presents a comprehensive framework for deploying a blockchain-based electronic voting system in Rwanda to address challenges of transparency, security, and public trust in electoral processes. Through detailed analysis of the current Rwandan electoral infrastructure and limitations, we propose a multilayered blockchain architecture that incorporates advanced cryptographic techniques, a national digital identity framework, and mobile accessibility features tailored to Rwanda's unique socio-economic landscape. Our proposed system leverages permissioned blockchain technology with a hybrid consensus mechanism to ensure the immutability of vote records while maintaining voter privacy through zero-knowledge proofs. The paper further discusses implementation challenges specific to Rwanda's context, including digital literacy (UNESCO, 2019), infrastructure limitations, and regulatory considerations. Our findings suggest that progressive, phased implementation of blockchain voting systems can significantly enhance electoral integrity while maintaining cultural and technological accessibility for Rwanda's diverse population.

Keywords: *Blockchain technology, electronic voting, cryptographic security, digital identity, Rwanda elections, democratic transparency, secure voting*

How to Cite: Niyonsaba, A., Jonathan, K. N., & Sumbiri, D. (2025). Blockchain-Based Voting System for Transparent and Tamper-Proof Elections in Rwanda. *Journal of Information and Technology, 5*(6), 70-89.

1. Introduction

Elections form the cornerstone of democratic governance, and their integrity is paramount to maintaining public trust in governmental institutions. In Rwanda, a nation with a complex political history and ongoing democratic development (UNDP, 2020; Human Rights Watch, 2022), ensuring transparent and tamper-proof electoral processes takes on particular significance. Traditional voting systems in Rwanda, as in many developing nations, face numerous challenges, including vulnerability to manipulation (NEC, 2022; Rights Watch 2022, 2022), limited transparency, and logistical difficulties in remote areas. The 2017, 2022, and 2024 elections (NEC, 2022; NEC, 2024 EU Election Observation Mission, 2018) in Rwanda highlighted several challenges in the current electoral system, including allegations of irregularities in voter registration, concerns about ballot security, and delays in result tabulation. These issues underscore the need for innovative solutions that can enhance the

transparency and security of the electoral process while accommodating the nation's specific socio-economic context.

Blockchain technology (Drescher, 2017; Swan, 2015), with its inherent characteristics of decentralization, immutability, and transparency, presents a promising solution to these challenges. By providing a tamper-resistant and transparent platform (Iansiti & Lakhani, 2017; Nakamoto, 2008) for recording and verifying votes, blockchain has the potential to revolutionize the way elections are conducted in Rwanda and restore public confidence in the democratic process. This paper explores the potential implementation of a blockchain-based voting system in Rwanda, addressing the unique challenges and opportunities presented by the country's context. The technical architecture, governance models, security measures, and accessibility considerations necessary for successful deployment are examined.

2. Literature Review

2.1. Evolution of Voting Systems in Rwanda.

Rwanda's electoral systems have evolved significantly since the country's independence. Following the 1994 genocide, Rwanda rebuilt its democratic institutions, initially relying on paper-based voting systems. In 2017, limited electronic components were introduced, such as electronic voter registration (NEC, 2018), though the core process remained manual. The National Electoral Commission (NEC) of Rwanda has shown a progressive shift in its electoral technology, transitioning from manual systems to semi-electronic methods between 2017 and 2024 (see Figure 1). This evolution sets the groundwork for integrating more advanced digital solutions like blockchain in further modernizing the electoral process, aligned with Rwanda's Vision 2050 (Government of Rwanda, 2020) strategy, emphasizing digital transformation. Rwanda

2.2. Blockchain Technology and Its Potential in Voting

Blockchain, originally for cryptocurrencies, is a distributed ledger technology. Key attributes include decentralization, immutability, transparency, and smart contracts. These make blockchain particularly suitable for secure, verifiable, and tamper-resistant voting systems.

2.3. Challenges in Implementing Electronic Voting in Developing Nations

Challenges include infrastructure limitations, digital literacy (UNESCO, 2019) gaps, high costs, trust and acceptance issues, and the need for robust regulatory frameworks.

EdinBurg Peer Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 6||pp 70-89||August||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

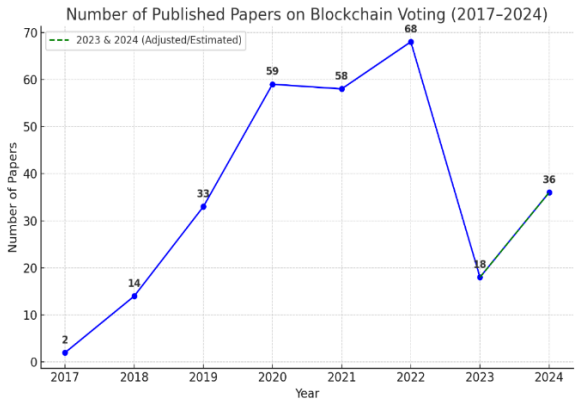

Figure 1: Blockchain-based voting systems between 2017 and 2024.

3. Current Electoral Challenges in Rwanda

Rwanda faces significant disparities in electricity and internet access between urban and rural areas, which presents a major challenge for the implementation of technology-driven electoral systems. In rural regions, limited digital infrastructure, unreliable power supply, and low digital literacy rates hinder equitable participation in modern voting processes. These issues exacerbate existing concerns regarding voter registration, including the risk of disenfranchisement due to data inaccuracy, limited outreach, and logistical difficulties in reaching remote communities. Additionally, ballot security remains a critical concern, with the need to prevent tampering, ensure the secrecy of votes, and maintain the integrity of the voting process.

Verifying election results transparently and credibly is also a persistent challenge, particularly in a context where public trust in institutional processes must be continually reinforced. Observation and access to the electoral process by independent entities, civil society, and international observers are often restricted, leading to doubts about the transparency and fairness of elections. Politically, Rwanda's tightly controlled landscape—with limited space for opposition parties and dissent—demands that any new voting system be perceived as impartial, secure, and inclusive. It must foster public confidence, safeguard democratic principles, and support Rwanda's long-term goals of national unity, reconciliation, and political stability.

4. Traditional Voting System Overview

In Rwanda, the traditional voting system follows a largely manual process that, while functional, is susceptible to a variety of operational and security challenges such as ballot tampering, vote miscounting, voter fraud, and significant delays in result tabulation and dissemination. The process comprises several sequential stages, beginning with manual voter registration, where eligible citizens are enrolled through local administrative offices using national ID cards. Although efforts have been made to digitize parts of this process, much of it remains paper-based, which increases the risk of errors and data inconsistencies.

Identity verification during elections is conducted by presenting a national identification card at the polling station, followed by cross-checking names against printed voter lists. After verification, voters issued paper ballots that they marked manually in privacy booths. The

completed ballots were then placed into sealed ballot boxes under the supervision of election officials and observers.

At the close of polling, the ballot boxes are opened, and designated officials manually count votes, a process that is often time-consuming and prone to human error. Counting may take place at local centers before results are transmitted—sometimes physically or via SMS—to district and national tallying centers. This process can lead to delays in announcing official results, creating room for mistrust, especially in tightly contested races.

Moreover, the lack of real-time monitoring mechanisms and transparent auditing systems adds to concerns about the credibility and integrity of the electoral outcomes. While Rwanda's National Electoral Commission (NEC) has taken steps to strengthen transparency, including involving local and international observers, the reliance on manual methods limits efficiency, scalability, and resilience against electoral malpractice.

5. Methodology and System Design

5.1 Comparative Analysis

To contextualize the benefits of the proposed blockchain-based voting system, Table 1 presents a comparative analysis with the existing traditional voting system used in Rwanda.

Table 1*:* Comparison of the current voting system with the proposed blockchain-based system

Criteria	**Traditional Voting System**	**Proposed Blockchain-Based System**
Transparency	Limited	Full auditability
Security	Susceptible to tampering	Cryptographically secured
Voter Privacy	Moderate	Strong anonymity with ZKPs
Result Accuracy	May be compromised by manual errors	Guaranteed by cryptographic tallying
Accessibility	Often limited in rural areas	Initial investment, long-term savings
Cost	Recurring logistical costs	Initial investment, long-term savings
Trust & Verifiability	Requires institutional trust	Verifiable by public and independent observers

EdinBurg Peer Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 6||pp 70-89||August||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

5.2. System Architecture

The proposed blockchain-based voting system comprises four layers: Application Layer, Blockchain Layer, Consensus Layer, and Infrastructure Layer, as shown in Figure 2.

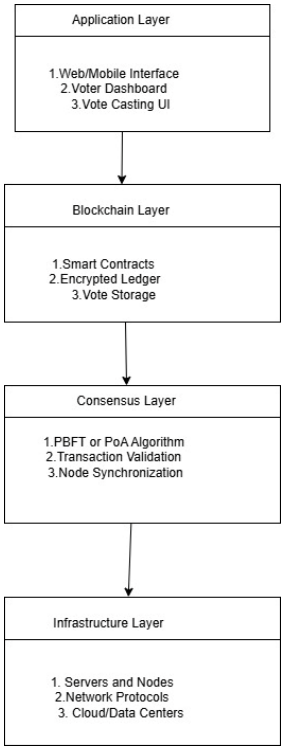

Figure 2: showing the relationships between the different layers and components.

The proposed blockchain-based voting system is designed with a layered architecture to ensure modularity, security, scalability, and ease of maintenance. The architecture comprises the following four primary layers:

5.2.1 Application Layer

The Application Layer is the topmost level of the voting system architecture and serves as the primary interface between end-users and the underlying technology. This layer includes intuitive and user-friendly web and mobile interfaces, voter dashboards, and secure voting modules, all designed to provide a seamless experience for various user groups. These users include voters, who need to register, authenticate, and cast their ballots; election administrators, who are responsible for setting up elections, managing participants, and overseeing the process; and observers, who monitor transparency and compliance.

Key functionalities provided at this layer include voter registration, identity verification through secure authentication mechanisms, the casting and confirmation of votes, and the ability to view real-time vote counts in a transparent and auditable manner. Additionally, administrators are equipped with tools for election configuration, system monitoring, and issue resolution. By combining accessibility, usability, and security, the application layer ensures that all participants can interact with the system confidently, regardless of their technical background.

5.2.2 Blockchain Layer

This layer is responsible for the secure storage and transparent management of voting records using blockchain technology. It ensures that every vote is stored in a tamper-proof manner, offering a reliable and auditable digital trail. Key components include the distributed ledger, smart contracts, and cryptographic mechanisms. Each vote is recorded as a transaction on the blockchain, which is then cryptographically linked to previous transactions, preventing any retroactive alterations or deletions.

Smart contracts play a vital role by automatically enforcing election rules—such as opening and closing polls, eligibility verification, and tally initiation—thereby eliminating the need for manual intervention and reducing the risk of human error or manipulation. The use of immutable storage guarantees that once a vote is cast, it remains permanently recorded. This architecture delivers several core benefits, including transparency**,** as all stakeholders can independently verify the process; auditability, due to the existence of a permanent and accessible vote ledger; and decentralization, which removes single points of failure and enhances the system's resilience against attacks or corrupt practices.

5.2.3 Consensus Layer

The consensus layer plays a critical role in maintaining the reliability and consistency of the blockchain-based voting system by ensuring that all participating nodes agree on the validity of each vote recorded. This layer leverages a consensus mechanism such as Proof of Authority **(**PoA) or Practical Byzantine Fault Tolerance (PBFT), both of which are well suited for permissioned networks where speed, efficiency, and trust among known validators prioritize over resource-intensive mining.

Through this mechanism, each vote submitted to the network undergoes a verification and validation process to confirm its authenticity and compliance with voting rules. The consensus layer also acts as a defense against double voting, vote tampering, and other fraudulent activities by rejecting any illegitimate transactions. By synchronizing the accepted vote records across all nodes in the network, this layer ensures data integrity and consistency, making it impossible for any single node to manipulate results without being detected. The result is a trustworthy, distributed system that strengthens the security and legitimacy of the entire election process.

5.2.4 Infrastructure Layer

The infrastructure layer serves as the backbone of the blockchain-based voting system, providing the hardware, networking, and deployment environment necessary for the platform to function securely and reliably. It includes critical components such as blockchain nodes (servers)**,** cloud-based or on-premises infrastructure, and supporting network protocols and APIs. These components collectively host the distributed ledger, enabling the system to store and share voting data across multiple nodes.

This layer also ensures high availability and continuous uptime, which is essential during elections when system accessibility is critical. To maintain robust security, the infrastructure layer incorporates features like data encryption**,** firewall protection**,** and network resilience mechanisms to guard against cyber threats and ensure system integrity. Deployment strategies must also take into account factors like the geographic distribution of nodes, which enhances fault tolerance and system redundancy in case of localized failures. Furthermore, deploying

infrastructure in government-regulated data centers ensures compliance with national data sovereignty laws and electoral regulations, thereby increasing trust in the system's legality and security.

6. Digital Identity and Voter Authentication

The proposed blockchain-based voting system leverages Rwanda's national ID system to provide a secure and verifiable digital identity framework for voter authentication. This mechanism enhances the integrity of the electoral process while preserving voter privacy.

Key Components:

1. Biometric Verification

Utilizes existing biometric data, such as fingerprints or facial recognition, stored in the national ID registry. Ensures that only eligible voters can access the system and prevents identity fraud or impersonation.

2. Integration with National ID System

Voter identity is verified in real-time against the centralized national ID database before allowing access to the voting interface. This approach enables cross-verification and eligibility checks without manual intervention.

3. Zero-Knowledge Proofs (Buterin, 2014; Ayed, 2019) (ZKPs)

A cryptographic protocol is implemented to prove the validity of a voter's identity without revealing their personal data. Ensures compliance with data privacy laws while maintaining trust and transparency in the process. Voters prove their eligibility (e.g., Rwandan citizen, registered voter, has not voted yet) without disclosing who they are.

4. Anonymity and Privacy

The system separates identity verification from the vote-casting process. Authenticated voters cast their votes anonymously, ensuring that no link exists between a voter's identity and their ballot.

7. Vote Casting and Verification

The proposed electronic voting system guarantees secure, transparent, and trustworthy vote casting and verification by leveraging advanced cryptographic techniques in combination with blockchain technology. When voters cast their ballots, the system immediately encrypts the votes with homomorphic encryption (Mattila et al., 2016), allowing it to be tallied later without ever revealing its contents. This ensures that voter privacy is preserved throughout the entire process. The encrypted vote is then submitted as a transaction to the blockchain, where it is immutably recorded and protected against tampering or deletion.

To enhance confidence in the process, the system provides receipt-based verification, allowing voters to confirm that their votes successfully recorded—without revealing whom they voted for; Additionally, cryptographic proofs and smart contracts ensure that every vote counted exactly once and that any attempt at fraud (such as double voting or vote substitution) becomes automatically detected and rejected. By combining transparent auditability, tamper-proof recording, and verifiable vote integrity, this system fosters a high degree of public trust in the electoral process.

EdinBurg Peer Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 6||pp 70-89||August||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

Algorithm 1: Smart Contract – Casting Vote in Blockchain-Based Voting System

The algorithm outlines the smart contract logic for secure vote casting and validation within the blockchain-based Voting Management System.

Input: Voter ID (VID), Candidate ID (CID)

Output: Confirmation of successful vote casting or error message

```
Function castVote(VID, CID)
    If!isRegisteredVoter(VID) then
        return "Error: Voter not registered"
    end if
    if hasVoted(VID) then
        return "Error: Vote already cast"
    end if
   if !isValidCandidate(CID) then
      return "Error: Invalid candidate"
   end if
   recordVote(VID, CID)
   markAsVoted(VID)
   emit VoteCast(VID, CID, timestamp)
   return "Success: Vote cast successfully"
end function;
```

Explanation of Key Functions:

isRegisteredVoter(VID): Checks if the voter is registered in the blockchain ledger.

hasVoted(VID): Ensures one vote per voter by verifying if the voter has already voted.

isValidCandidate(CID): Confirms the selected candidate is valid and eligible.

recordVote(VID, CID): Logs the vote in an immutable blockchain transaction.

markAsVoted(VID): Flags the voter to prevent multiple voting.

Emit VoteCast(...): Generates an event for blockchain transparency and auditing.

EdinBurg Peer Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 6||pp 70-89||August||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

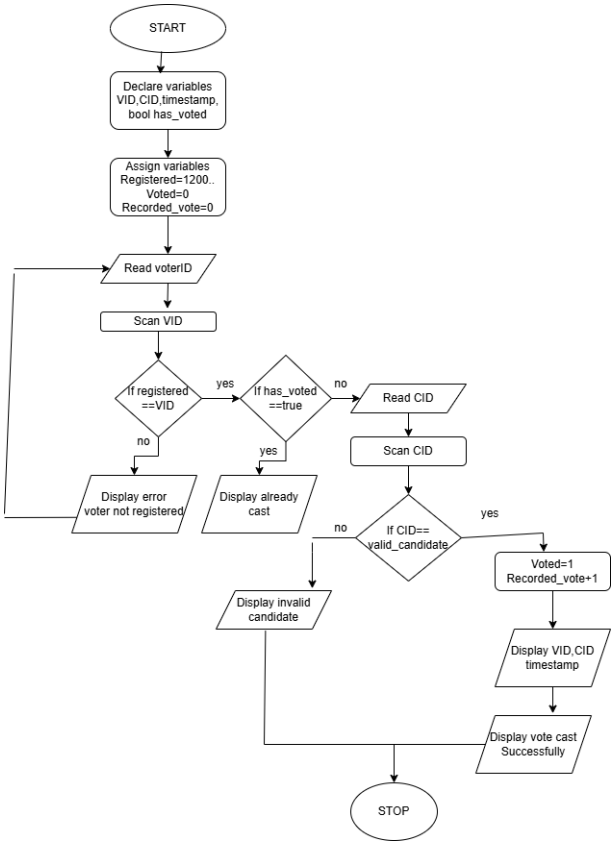

Figure 3: Flowchart of Smart Contract – Casting Vote in Blockchain-Based Voting System

8. Public Blockchain Bulletin Boards

The system employs public blockchain bulletin boards to enhance transparency, accountability, and public trust in the electoral process. In this model, all encrypted votes are published on a publicly accessible, decentralized ledger effectively functioning as a digital bulletin board. While the content of each vote remains confidential due to encryption, the publication of these records ensures that the voting process is fully visible and verifiable to anyone, without compromising voter privacy.

This tamper-proof ledger leverages the inherent immutability of blockchain, making it impossible to alter or remove votes once they are recorded. As a result, independent observers, civil society organizations, NGOs, and even members of the public can audit the election process in real-time or retrospectively, verifying that all votes are accounted for and that no irregularities occurred. By making the voting data openly accessible yet cryptographically protected, the system fosters a new level of transparency and democratic accountability never before possible in traditional voting systems.

9. Verifiability:

The proposed voting system incorporates both individual verifiability and universal verifiability**,** two foundational principles that enhance transparency and build trust without relying on a central authority. Individual verifiability allows voters to confirm that his or her specific vote has been recorded and included in the final tally, without revealing the content of

their vote. This is achieved through cryptographic mechanisms such as encrypted vote receipts or zero-knowledge proofs, which ensure privacy while providing personalized verification. On the other hand, universal verifiability enables third parties—such as observers, independent auditors, civil society organizations, and watchdog groups—to verify that every vote counted is legitimate, and that no fraudulent or duplicate votes have been introduced. These properties work together to create a transparent, tamper-evident system where the correctness of the election outcome can be independently confirmed by any interested party. Ultimately, this decentralization of trust helps eliminate reliance on central authorities, reducing the potential for manipulation and significantly increasing confidence in the electoral process.

D. Result Tabulation and Announcement

Utilizes homomorphic encryption (Mattila et al., 2016) for privacy-preserving tallying and blockchain for immutable result storage. The result tabulation and announcement process is designed to ensure accuracy, privacy, and transparency using homomorphic encryption (Mattila et al., 2016) and blockchain technology.

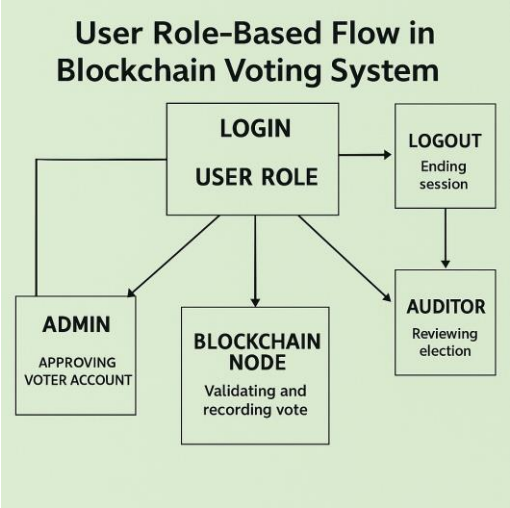

Figure 4 :User Role-Based Flow in the Proposed Blockchain Voting System

Privacy-Preserving Tallying and Transparent Result Publication – Ensuring Integrity without Compromising Privacy:

The proposed electronic voting system integrates multiple advanced technologies to deliver a secure, private, and transparent tallying process. Central to this is the use of Homomorphic Encryption, which allows mathematical operations—such as vote counting—to be performed directly on encrypted data. This means that individual ballots never need to be decrypted during tallying, preserving voter privacy while ensuring accurate computation. The result decrypts only after tallying, and even then, it requires the collaboration of multiple authorized entities through a distributed key-sharing scheme, preventing any single party from accessing or manipulating the outcome.

Moreover, the system ensures a verifiable and trustworthy tallying process by allowing all encrypted votes to be aggregated transparently. It provides cryptographic proofs that the results were correctly computed, enabling independent observers and third parties to verify the accuracy of the tally without compromising individual vote secrecy. Notably, even election

officials are prevented from accessing the contents of specific ballots, reinforcing the system's privacy-by-design principle.

To further enhance integrity and public trust, the results and associated cryptographic proofs are published on the blockchain, ensuring that the results are immutable, tamper-proof, and publicly auditable. This permanent ledger can serve as a historical reference for audits, dispute resolution, or legal verification, ensuring long-term accountability. Additionally, the system features real-time result access via a public dashboard (Transparency International, 2022), which enables all stakeholders—including citizens, observers, and the media—to view results as they are decrypted and confirmed, fostering openness and trust in the entire electoral process.

Benefits:

Privacy

Homomorphic encryption plays a crucial role in preserving the confidentiality of each vote cast in an electronic voting system. With this encryption technique, votes can be mathematically manipulated and counted without ever being decrypted, ensuring that the contents of individual ballots remain private even during the tallying process. This approach eliminates the risk of exposing voter choices to any third party, including system administrators or tallying authorities, thus reinforcing voter anonymity and protecting the democratic process from undue influence or coercion.

Integrity

Blockchain technology (Drescher, 2017; Swan, 2015) introduces a decentralized and tamper-resistant ledger that ensures the authenticity and immutability of all recorded votes. Once a vote is cast and stored on the blockchain, it becomes part of a permanent, time-stamped record that cannot be altered or deleted without consensus from the network. This inherent immutability prevents fraudulent activities such as vote tampering or result manipulation. Each transaction (vote) is cryptographically linked to the previous one, creating a verifiable audit trail that upholds the integrity of the election process.

Transparency and Trust:

The combination of public verifiability and cryptographic proofs in blockchain-based voting systems fosters greater transparency and public trust. Anyone can independently verify the correctness of the final tally without compromising the secrecy of individual votes. Cryptographic mechanisms such as zero-knowledge proofs and digital signatures enable voters and observers to confirm that the election was conducted fairly, that all legitimate votes were counted, and that no illegitimate votes were introduced. This openness reassures stakeholders, including voters, candidates, and election monitors, that the results are accurate and trustworthy, thereby strengthening confidence in democratic institutions.

Security and Privacy Considerations

The proposed blockchain-based voting system is designed with a multi-layered security and privacy architecture that leverages advanced cryptographic techniques and robust threat mitigation strategies. These safeguards ensure that the electoral process remains confidential, tamper-proof, and resilient against both present and emerging cyber threats.

EdinBurg Peer Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 6||pp 70-89||August||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

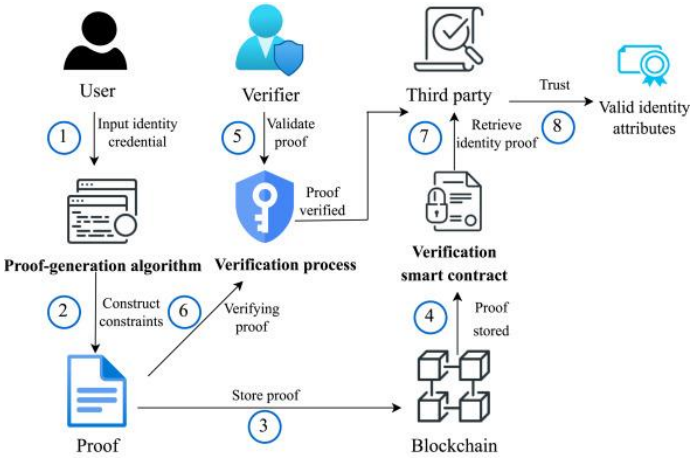

Figure 5: Security and Privacy Considerations

1. Privacy-Enhancing Cryptographic Techniques

Zero-Knowledge Proofs (Buterin, 2014; Ayed, 2019) (ZKPs), Voters can prove they are eligible and have cast a valid vote without revealing their identity or vote content. This ensures compliance with privacy laws while supporting transparent verification. Ring Signatures: Allow a voter's identity to be anonymously authenticated within a group. This provides plausible deniability and ensures that votes cannot traced back to individuals, even by system administrators. Mixing Techniques (Mixnets) Votes are shuffled through a series of cryptographic mix servers before being recorded on the blockchain. This breaks the link between the voter and their encrypted vote, enhancing anonymity and resisting traffic analysis attacks.

2. Infrastructure and Protocol Security

DDoS Mitigation The infrastructure is protected by distributed denial-of-service (DDoS) countermeasures, such as rate limiting, traffic filtering, and decentralized network architecture. These mechanisms maintain system availability during peak usage or targeted attacks. Smart Contract Security with Formal Verification. All critical smart contracts (e.g., for vote casting, tallying, and verification) are subjected to formal verification, a mathematical method used to prove correctness and eliminate logic vulnerabilities. This prevents exploits and ensures the contracts behave as intended.

3. Quantum-Resistant Cryptography

3.1. Post-Quantum Cryptography (PQC)

As quantum computing continues to evolve, traditional cryptographic methods—such as RSA and ECC—face the risk of becoming vulnerable to quantum-enabled attacks. In anticipation of these future threats, the proposed voting system is designed with Post-Quantum Cryptography (PQC) in mind. PQC involves the integration of quantum-resistant algorithms (ITU, 2019) that can withstand the computational power of quantum computers. These include lattice-based cryptography, hash-based signatures, code-based schemes, and multivariate polynomial cryptography—each offering robust alternatives to current standards. By embedding these algorithms into critical components such as vote encryption, digital signatures, and authentication protocols, the system ensures long-term data protection, even in a post-quantum era. This proactive approach not only enhances the durability and resilience of the system but

also demonstrates a commitment to future-proofing the electoral infrastructure against the next generation of cybersecurity threats.

Benefits:

The proposed blockchain-based electronic voting system delivers a robust security architecture that ensures end-to-end privacy for voters while maintaining full transparency and verifiability of the election process. By using advanced cryptographic techniques such as homomorphic encryption (Mattila et al., 2016), zero-knowledge proofs, and anonymous receipts—voter choices remain confidential, yet the system can publicly demonstrate the correctness of the tally. In addition, the platform is built to be resilient against both conventional cybersecurity threats, such as data breaches and malware, and emerging threats, including those posed by quantum computing. This resilience is reinforced through the integration of Post-Quantum Cryptography (PQC) and multi-layered security mechanisms. Furthermore, the system prioritizes trust in its software and protocol behavior by applying formal verification methods, which mathematically prove the correctness and security of critical code and cryptographic protocols. These practices not only safeguard elections today but also ensure long-term integrity and reliability, establishing a strong foundation of trust in digital democratic processes.

10. Implementation Strategy for Rwanda

The successful implementation of any national digital or technological initiative in Rwanda requires a well-structured and inclusive strategy. As Rwanda continues to position itself as a regional leader in digital transformation and innovation, a carefully planned implementation approach is critical to ensure efficiency, sustainability, and widespread impact. This strategy outlines a three-pronged framework: Phased Deployment, Infrastructure Development, and Training and Public Awareness. Phased deployment enables the government and stakeholders to gradually roll out initiatives, allowing for iterative learning, troubleshooting, and scaling. Infrastructure development ensures that the necessary physical and digital foundations are in place to support technological systems, particularly in underserved and rural areas. Lastly, training and public awareness are essential for building the human capacity and trust required to maximize adoption and long-term success. Together, these components form a comprehensive roadmap toward Rwanda's digital future.

A. Phased Deployment

Description:
Implement the project in clearly defined stages to manage resources efficiently, minimize risks, and allow for evaluation and adjustment at each phase.

Phases could include:

To ensure a smooth and effective transition to the proposed electronic voting system, a phased deployment strategy (NEC, 2021) is recommended. The process begins with a pilot phase in carefully selected regions or sectors, such as the Gasabo District, specifically within the Jabana Sector. This limited rollout allows stakeholders to test the system in a controlled environment, identify operational or technical challenges, and gather feedback from users, including voters, administrators, and observers. Insights from the pilot will guide the expansion phase, during which the system will be scaled up incrementally to cover additional regions, incorporating improvements and optimizations based on the pilot experience. Once confidence in the

system's performance, security, and user adoption is established, the final stage involves a full national rollout, making the system available across the country. This structured approach minimizes risk, builds trust, and ensures readiness at every level before committing to nationwide implementation.

B. Infrastructure Development

Description:

To support the successful implementation and operation of the proposed electronic voting system, it is essential to build and upgrade the necessary physical and technological infrastructure in alignment with the project's requirements. This includes ensuring the availability of high-speed and reliable internet connectivity, especially in remote or underserved areas, to facilitate smooth access to the system across all regions. The deployment of secure data centers and scalable cloud platforms is also critical to store, process, and safeguard electoral data. Additionally, a stable and uninterrupted power supply must be guaranteed, as any outages during voting or tallying could compromise system integrity and public trust. Finally, the procurement and setup of appropriate hardware and networking equipment, including servers, secure terminals, routers, and backup systems, will ensure that all technical components function seamlessly. Investing in robust infrastructure will not only support current needs but also provide the scalability and resilience required for future elections.

Focus Areas:

To maximize efficiency and reduce deployment costs, the project should leverage existing national infrastructure, such as Rwanda's fiber optic backbone (Rwanda Ministry of Infrastructure, 2020), which provides high-speed internet connectivity across much of the country. Tapping into this backbone ensures broader reach, faster data transmission, and minimal need for new groundwork. In addition, the project should prioritize collaboration with telecom companies and technology providers, both public and private, to supply essential services such as mobile access, cloud hosting, secure authentication, and technical support. These partnerships can accelerate implementation, enhance innovation, and ensure that the system adheres to global scalability and security standards. By integrating existing national assets and building strong collaborations, the system can achieve a sustainable, scalable, and secure digital election infrastructure that is both cost-effective and future-ready.

C. Training and Public Awareness

A critical component of the project's success is the implementation of a comprehensive capacity-building and public education strategy aimed at equipping both the workforce and the public with the knowledge and skills required to effectively operate and sustain the new electronic voting system. This initiative will include targeted training programs for government officials, IT personnel, election administrators, and end-users to ensure smooth system operation and maintenance. Simultaneously, public awareness campaigns will be launched to educate citizens on the system's benefits, usage, and safety measures, fostering trust and encouraging participation. To enhance outreach and impact, the project will establish strategic partnerships with educational institutions and community organizations, enabling localized training and broader civic engagement. The ultimate goals are to promote system adoption, reduce resistance to technological change, and empower citizens through improved digital literacy (UNESCO, 2019). Additionally, by fostering a culture of innovation and data-driven

EdinBurg Peer Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 6||pp 70-89||August||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

decision-making, this initiative will contribute to the long-term sustainability and advancement of Rwanda's digital governance landscape.

11. Results (Proposed architectural overview)

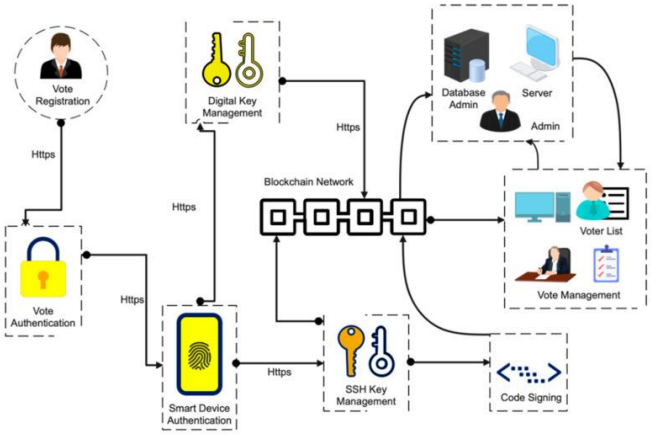

Figure 6: The resulting system architecture offers a secure, scalable, and inclusive blueprint for blockchain-based voting tailored to Rwanda.

The proposed system architecture delivers a secure, scalable, and inclusive blueprint for a blockchain-based voting system specifically tailored to Rwanda's unique social, technological, and regulatory environment. Key highlights include: Security, leveraging blockchain's immutable ledger and cryptographic protocols ensures voter data integrity, transparency, and fraud resistance. Scalability: The design supports expansion from local pilot projects to nationwide deployment without compromising performance. Inclusivity: The system accommodates diverse user groups, including those with limited digital literacy (UNESCO, 2019), by integrating accessible interfaces and multilingual support.

This framework sets a robust foundation for modernizing Rwanda's electoral process, fostering trust, transparency, and greater civic participation.

11.1. Software implementation

The software implementation of the blockchain-based voting system utilizes a modular architecture developed using a combination of front-end, back-end, and blockchain technologies. The front-end is built using web-based interfaces with support for mobile responsiveness, allowing accessibility for users in various environments. Technologies such as HTML5, CSS, and JavaScript frameworks (e.g., React or Vue.js) are employed for dynamic and intuitive interfaces.

The back-end is implemented using a secure and scalable framework like Node.js or Django, which handles interactions with the blockchain layer, user authentication, and admin functionalities. For blockchain integration, platforms like Hyperledger Fabric or Ethereum with smart contracts written in Solidity are used, depending on whether a permissioned or public system is adopted.

Security mechanisms such as SSL/TLS encryption, end-to-end encryption of votes, secure APIs, and smart contract auditing are integrated to ensure the platform is resilient against cyber threats.

This implementation ensures that the blockchain voting system is not only secure and transparent but also practical and adaptable to Rwanda's digital landscape.

11.2. System Integration

The integration phase ensures that all individual components of the blockchain-based voting system function cohesively to deliver a secure, transparent, and efficient voting process. This includes the front-end user interfaces, back-end logic, smart contracts, and blockchain nodes.

By completing this integration phase, the voting system becomes an operational and reliable digital platform, ready for pilot deployment and real-world elections in Rwanda.

11.3 Working Mechanism

The working mechanism of the blockchain-based voting system follows a structured process to ensure the secure, anonymous, and transparent casting and tallying of votes. The process consists of the following steps:

1. User Authentication: Voters first log in through a secure interface using multi-factor authentication tied to Rwanda's national ID database. This ensures only eligible voters can access the system.

2. Casting Vote: After authentication, the voter selects a candidate from the user-friendly interface. This vote is then encrypted and signed by the voter's private key to maintain confidentiality and authenticity.

3. Smart Contract Validation: The encrypted vote is sent to a smart contract, which validates whether the voter has already voted and whether the selected candidate is valid. If both conditions are met, the vote is accepted and added to the blockchain.

4. Vote Recording: Each validated vote is recorded as a transaction on the blockchain ledger. This immutable entry ensures that votes cannot be altered or deleted.

5. Receipt Generation: A cryptographic receipt is generated for the voter, containing a hash of the vote that allows them to verify its inclusion without revealing vote content.

6. Real-Time Tallying: Votes are tallied automatically through homomorphic encryption (Mattila et al., 2016) techniques, allowing aggregation without decrypting individual votes.

7. Result Announcement: Final encrypted tallies are decrypted using a secure multi-party computation scheme and published on a public blockchain bulletin board for transparency.

This mechanism ensures end-to-end security, voter privacy, and transparency, making the system trustworthy for all stakeholders, including voters, administrators, and observers.

EdinBurg Peer Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 6||pp 70-89||August||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

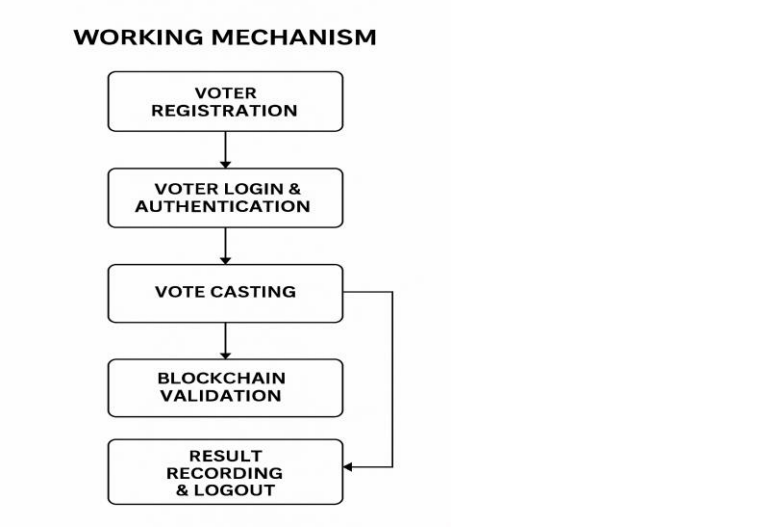

Figure 7: Flowchart Representing the Working Mechanism of the Blockchain-Based Voting System.

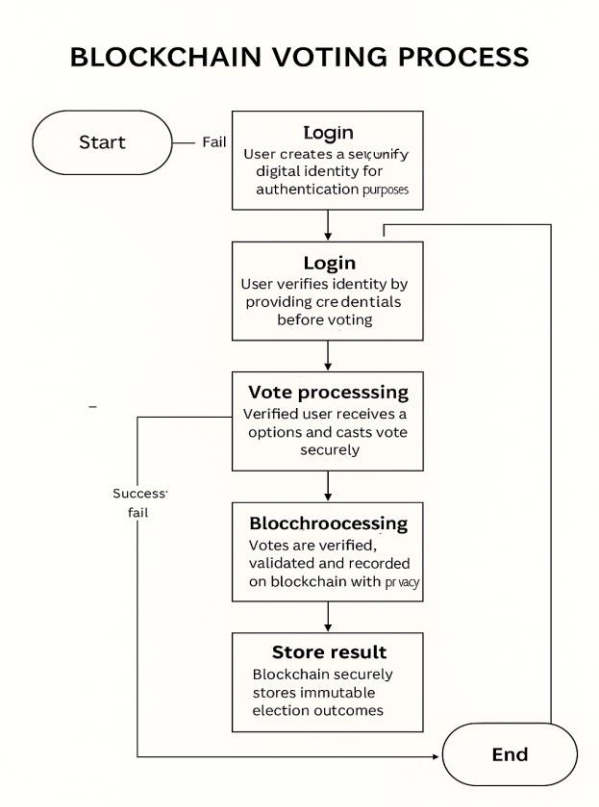

Figure 8: Flowchart Showing the Overall Blockchain Voting Process from Login to Result Storage.

12. Discussion

As digital technologies continue to reshape societies and economies, the successful implementation of innovative systems depends not only on technical capabilities but also on the broader ecosystem in which they operate. This includes a strong governance and regulatory framework, inclusive and equitable access to services, and the ability to anticipate and address implementation challenges.

Effective governance ensures that systems operate within legal and ethical boundaries, safeguarding the rights of all stakeholders while promoting accountability and transparency. Simultaneously, accessibility and inclusivity are essential to ensure that all segments of the population, regardless of geography, gender, disability, or socio-economic status, can benefit from technological advancements.

However, even the well-designed systems face practical challenges, ranging from infrastructure gaps and financial constraints to resistance from stakeholders. Therefore, identifying these challenges and developing strategic mitigation measures is critical to ensuring the sustainability and effectiveness of any initiative.

This discussion explores three key pillars essential for the success of any large-scale technological or policy-driven system: governance and regulatory frameworks, accessibility and inclusivity, and the challenges that must be addressed through targeted mitigation strategies.

12.1. Governance and Regulatory Framework

12.1.1. Importance: Effective governance and regulation are critical to ensuring the integrity, legality, and public trust in the blockchain voting system.

12.1.2. Key Considerations:

Establishing clear policies on data privacy, voter identification, and election oversight, defining roles and responsibilities of government bodies, election commissions, and technology providers, ensuring compliance with Rwanda's legal standards and international best practices, and creating mechanisms for dispute resolution and audit trails.

Strategies:

Designing user-friendly interfaces, including mobile platforms and multilingual support (e.g., Kinyarwanda, English, and French). Providing offline voting options or assisted voting centers for populations with limited internet access. Running targeted digital literacy (UNESCO, 2019) and awareness campaigns to educate and empower voters. Ensuring accessibility for persons with disabilities through assistive technologies

Challenges and Mitigation Strategies

While blockchain-based electronic voting systems offer numerous advantages, they also face significant challenges that must be carefully addressed for successful implementation. One key barrier is technological limitation, particularly in regions with limited internet penetration, unreliable electricity, or lack of access to suitable hardware, which can hinder voter participation. Additionally, there may be resistance to adoption driven by a lack of trust, limited technical literacy, or fear of unfamiliar systems. Cybersecurity threats, such as hacking attempts or malware, also pose a serious risk to the system's integrity. Moreover, legal and

procedural challenges, including outdated electoral laws (International IDEA, 2020) and bureaucratic resistance, can slow or obstruct implementation. To overcome these issues, a series of mitigation strategies should be employed. First, adopting an incremental and phased deployment approach, beginning with small-scale pilot programs, allows for controlled testing, feedback collection, and continuous improvement while gradually building public confidence. Second, the system must be reinforced with robust cybersecurity defenses, including advanced encryption, multi-factor authentication, secure coding practices, and regular independent security audits. Third, transparent public communication and stakeholder engagement are essential for dispelling misinformation, fostering understanding, and gaining trust from voters, political actors, and civil society. Finally, collaboration with legal experts and policymakers is critical to align the system with existing electoral frameworks or to facilitate necessary reforms. Together, these strategies help ensure the system is secure, inclusive, and legally viable.

13. Conclusion

This paper presents a blockchain-based voting system tailored to enhance transparency, security, and inclusivity within Rwanda's electoral processes. By adopting a phased deployment strategy (NEC, 2021), implementing robust security protocols, and prioritizing accessibility, the proposed framework offers a practical and sustainable path toward modernizing elections in Rwanda. Future research should emphasize conducting real-world pilot testing and a comprehensive evaluation of system performance to refine and validate the solution before full-scale implementation.

References

(IMF)., I. M. (2022). Rwanda: Article IV consultation.

(ITU)., I. T. (2019). Measuring digital development.

(NIDA)., N. I. (2023). National ID coverage report.

(NISR), N. I. (2022.). Rwanda census .

(RURA)., R. U. (2023). Electricity access report.

(RURA)., R. U. (2023). Internet penetration report.

(UNDP)., U. N. (2020). Governance in Rwanda: Progress and challenges.

Ayed, B. B.-b. (2019). In Proceedings of the 2019 Blockchain Conference (BLOCKCHAIN'19) . (pp. 233–238).

Bank., W. (2021). World development indicators.

Buterin, V. (2014). Ethereum white paper.

Center., P. R. (2018). Global attitudes toward technology.

Commission., E. (2018). Election cooperation networks.

Crosby, M. P. (2016). Blockchain technology (Drescher, 2017; Swan, 2015): Beyond bitcoin. Applied Innovation, . 2, 6–19.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly. 13(3), 319–340.

Drescher, D. (2017). Blockchain basics. Apress.

GSMA. (2021). Mobile economy Sub-Saharan Africa.

House., F. (2022). Freedom in the world: Rwanda.

Human Rights Watch (Human Rights Watch,). (2022-2017). The climate of fear.

Iansiti, M. &. (2017). The truth about blockchain. Harvard Business Review, 95(1),. 118–127.

IDEA)., I. I. (2020). Electoral integrity framework.

Infrastructure., R. M. (2020). Development report.

International, T. (2022). Corruption perception index 2022. *N/A*, N/A.

International., A. (2018). Case of Victoire Ingabire.

Mattila, J. S. (2016). The blockchain paradox. ETLA Brief, (45).

Mission., E. U. (2018). Final report.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

Reuters. (2017). Kagame wins with 99%. Reuters.

Rwanda., .. N. (2018). lectoral process report .

Rwanda., G. o. (2020). Vision 2050 (Government of Rwanda).

Rwanda., N. E. (2021-2016). Strategic plan .

Rwanda., N. E. (2022). Post-election report . *N/A*, N/A.

State., U. D. (2021). Human rights report.

Swan, M. (2015). Blockchain: Blueprint for a new economy. O'Reilly Media.

Times, T. N. (2017). Rwanda introduces electronic voting system in urban areas.

Times., T. N. (2017). Rwanda introduces electronic voting system in urban areas.

UNESCO. (2019). Global education monitoring report .

Union., A. (2017). Election observation report.

Watch, H. R. (2022). Rwanda events . *N/A*, N/A.

Wood, G. (2014). Ethereum white paper.