Pak. j. life soc. Sci. (2025), 23(2): 56-69 E-ISSN: 2221-7630;P-ISSN: 1727-4915

Pakistan Journal of Life and Social Sciences

www.pjlss.edu.pk

https://doi.org/10.57239/PJLSS-2025-23.2.005

RESEARCH ARTICLE

Evaluating Block Chain Based Voting Systems: An Empirical Study on Public Administration Adoption and Challenges

Altantuya Dashnyam[1], Amarjargal Peljid[1], Burmaa Natsag[1], Ariungerel Tseden-Ish[1*], Zahid Ali [2], Muhammad Adnan Kaim Khani [2], Sana Hassan[2]

[1]National University of Mongolia, Ulaanbaatar, Mongolia
[2]Department of Computer Science, ILMA University

ARTICLE INFO

Received: May 16, 2025

Accepted: Jul 9, 2025

Keywords

Block chain Voting
Public Administration
Digital Democracy,
E-Voting Security,
Electoral Integrity
Technology Adoption
Election Fraud Prevention

***Corresponding Author:**

ariungerel.ts@num.edu.mn

ABSTRACT

Block chain technology integration into electoral systems is attracting international attention for its ability to improve security, transparency, and voter confidence. Its successful implementation, however, hinges on the preparedness and position of public administration. This research empirically investigates adoption issues, policy implications, and security concerns of block chain voting in public administration. A mixed-method technique is applied through which information is gathered from structured interviews, questionnaires with policymakers, IT experts, and electoral officials. Qualitative analysis monitors adoption impediments of particular relevance including legal, technical, and trust aspects: quantitative data talks the suggested policies based on these inputs. Findings can be used to assess on the basis of proof that how public administration might enable block chain voting and establish a plan of action to implement this transformation. Our study, contributes to the digital democracy debate and offers governments ideas for bettering electoral integrity through block chain technology.

INTRODUCTION

Although conventional voting systems have continuing flaws, preserving electoral integrity is a basic component of democratic rule. While EVMs present cybersecurity threats, technical failures, and transparency issues, paper voting is still subject to hacking, logistical inefficiency, and human errors. Because of its decentralized, unchangeable, and cryptographically secure construction, blockchain technology has been proposed in recent years as a solution. Nevertheless, there are still concerns regarding the practicability and security of this technology. Others yet contend that blockchain voting may lead to new problems for election integrity and that it is not a perfect security tool. While efforts are ongoing to create better blockchain based electronic voting systems in an effort to solve these issues. In theory, blockchain voting can cut out fraud, increase voter confidence, and give transparent audit trails, which makes it an attractive alternative to the traditional methods of voting [3]. However, its practical application in public administration is still yet to be significant, despite it being technically possible. The discrepancy between theoretical potential and real-world application serves to highlight the necessity for greater research into the administrative and regulatory issues obstructing the application of blockchain within election systems. Principal obstacles requiring empirical study include regulatory ambiguity, bureaucratic reluctance, and trust shortfalls among electoral officials. Most of the existing research on blockchain voting has focused on technical implementation, cryptographic security and pilot studies in a controlled setting. While some governments have begun testing blockchain-based elections, such as in Estonia, West Virginia (USA), and Switzerland, these pilots have been employed mainly to validate technical feasibility and not administrative and policy dimensions [5]. Early research highlights the possible benefits of blockchain voting to make elections more accessible, preserve voter anonymity, and minimize election tampering. They fail to address whether electoral commissions, government agencies, or policy makers deem this technology to be sensible, usable, even necessary [7]. This institutional

ignorance is suspect regarding whether blockchain based voting can scale from pilot experiments to standard electoral systems. Deciding whether this invention is feasible relies on a comprehension of how decision-makers perceive it. Lacking pragmatic notions of administrative sentiments, blockchain voting is merely an abstract concept instead of an actual governance reformation.

Furthermore, blockchain use in electoral processes is more about institutional readiness, legal compliance, and public trust than just a technical matter. Core to the development of electoral policies are public officials and election commissions, and their opposition to blockchain based voting might impede broad implementation. Additionally complicating matters is the lack of standardized regulatory frameworks since governments struggle to add legal tools to verify blockchain based election results [10]. Along with overcoming technical obstacles, blockchain voting depends on establishing credibility among parties, closing policy gaps, and making sure it is economically viable. Without a plan for implementation, most people will struggle to accept blockchain voting. The economic implications of implementing blockchain technology in voting also need serious consideration since infrastructure expenditure, election officials' training, and synchronization with current electoral processes pose great challenges [11].

This research bridges this gap by carrying out an empirical analysis of the adoption of block chain voting in public administration. Using a survey-based research design, this study gathers data from election officials, policy-makers, and IT experts involved in electoral processes. The research aims to answer the following key questions:

What are the primary concerns of public administrators regarding blockchain-based voting?

What factors influence their willingness to adopt blockchain technology in electoral processes?

What are the major barriers (legal, technological, or institutional) that hinder blockchain voting adoption?

How does public trust and awareness impact the adoption of blockchain-based voting in different governance structures?

By analyzing survey responses from key stakeholders, this study aims to provide policy recommendations for governments, election commissions, and regulatory bodies, helping to shape future discussions on secure digital voting infrastructure. The findings will contribute to the broader discourse on digital governance, administrative modernization, and election security. Additionally, the study will explore the potential of blockchain voting in increasing electoral transparency while addressing institutional and legal constraints. By focusing on the perspectives of public administration rather than just technical feasibility, this research aims to fill the existing knowledge gap and offer data-driven insights for the successful integration of blockchain in electoral systems.

2. LITERATURE REVIEW

The foundation of E-voting was laid in the early 1980's by David Chaum, a pioneer in cryptography. His visionary system leverage public-key cryptography to anonymize voter identities and decouple them from cast ballots a breakthrough in electoral integrity. It was implemented in 2005 in election, set a precedent for a digital voting system and digital democracy. After a decade the Denmark's Liberal Alliace explored integrating block-chain technology into its electoral processes, objective is to further strengthen security and transparency of voter. Most of the researcher focused on secure and efficient e-voting protocols by using the blockchain technology. The challenges concern accuracy, privacy, scalability, auditability, anonymity, and reliability.

In [12] author focused on the secure e-voting contexts using blockchain technology. The study showed the benefits of e-voting system that was implemented during election by using e-voting model and also conducted the relative studies of various e-voting of various locations. In [13] author conducted comparative study on the blockchain based technology of 10 years from 2011 to 2020. The review was included the various studies on the Zcash platform, smart contract and blockchain programmed from the scratch also digital signature based. This study discussed about the limitations and features of blockchain technologies. In [14] the researcher conducted a survey based on the e-voting using blockchain for secure election system that focused on the proposed model, which is based on the security, scalability and auditability. In this study, the research discussed on the

limitations and compare the study with the existed system. In [15] the author analyzed the exposures in different app based on the blockchain and suggested about the security enhancement and addressed the privacy and security challenges for future and also discussed about the limitations. In [16] the researcher conducted the study based on the e-voting using blockchain for the election for the large scale level, detects the challenges during election, these challenges occurs when election conducted with the high population in various election stations. In [17] the author designed a privacy based model for e-voting system that ensure both vote integrity and voter's information. It also compared the study with the previous studies that has been done by the various researchers. In [18] the author proposed system based on the blockchain that is maintaining the election integrity and transparency by the real time security and auditability. This study, improved the security by using blockchain security, also compare with the existing studies. In [19] the researcher developed blockchain e-voting system that utilize the smart contracts to process automatically, such as register the voter, check the eligibility, voting counting, reduce the issues and fraud. It is totally transparent that allows the stockholders to audit elections and improve the trust and accountability. It is implemented by the author by adoption of technology, and also addressing these challenges that help to strength the electoral integrity and public confidence in democratic process. In [20], the authors combined the principles of transparency and voter privacy by utilizing Ethereum's blockchain along with ring signatures. This approach allows users to confirm results independently, removing the necessity for Third-party involvement. With its cost-effective gas fees and stealth address features, this method is well-suited for largescale online elections. In [21], the authors presented an e-voting system (EVS) specifically designed for university elections in Colombia. The system follows the Model View Controller (MVC) architectural pattern and complies with the Open Web Application Security Project (OWASP) standards, addressing five key security risks. Usability tests and response time assessments conducted during development led to significant improvements in performance and result delivery. The adoption of this system allows for fast and accurate result acquisition, eliminating the need for manual recounts and reducing overall election costs. The electoral system outlined in [22] provides an efficient way for individuals to vote using personal computers or laptops, reducing long lines at polling stations. It features robust authentication mechanisms, including national ID or biometric verification, to address the issue of electoral fraud. In [23], the authors proposed an electronic voting system that employs blockchain technology to prevent potential fraud during the voting process. The system's effectiveness was evaluated through a questionnaire and the analysis of three distinct scenarios, with participants giving it high ratings in terms of usability and security. The study concluded that this approach could expedite the voting process while reducing the time and costs associated with traditional paper ballots. The approach described in [24] utilizes a dual blockchain system, which enables communication between the public

Ethereum blockchain and a private Quorum blockchain specific to institutions. This system transfers critical data to the public blockchain, which manages information related to universities and government entities. The design ensures data security and integrity through encryption using the SHA-256 algorithm. In [25], blockchain technology was leveraged to enhance the security and efficiency of electronic voting systems. Incorporating cryptographic principles and transparency, the system ensures end-to-end verifiability. A comprehensive analysis demonstrated the system's ability to provide secure and verifiable electronic voting.

Our proposed model addresses these challenges by introducing a decentralized voting platform that emphasizes anonymity, transparency and automated vote counting. It leverages the Ethereum blockchain for secure record-keeping and integrates ring signatures to protect voter privacy. A key feature is the hybrid use of consortium and public block-chains to ensure secure, fraud-resistant remote voting in representative elections.

The Materials and Methods should be described with sufficient details to allow others to replicate and build on the published results. Please note that the publication of your manuscript implicates that you must make all materials, data, computer code, and protocols associated with the publication available to readers. Please disclose at the submission stage any restrictions on the availability of materials or information. New methods and protocols should be described in detail while well-established methods can be briefly described and appropriately cited.

Research manuscripts reporting large datasets that are deposited in a publicly available database should specify where the data have been deposited and provide the relevant accession numbers. If the accession numbers have not yet been obtained at the time of submission, please state that they will be provided during review. They must be provided prior to publication.

Interventionary studies involving animals or humans, and other studies that require ethical approval, must list the authority that provided approval and the corresponding ethical approval code.

In this section, where applicable, authors are required to disclose details of how generative artificial intelligence (GenAI) has been used in this paper (e.g., to generate text, data, or graphics, or to assist in study design, data collection, analysis, or interpretation). The use of GenAI for superficial text editing (e.g., grammar, spelling, punctuation, and formatting) does not need to be declared.

3. METHODOLOGY

This study employs a mixed-methods design with qualitative as well as quantitative approaches in analyzing the adoption, security, and regulatory concerns of blockchain voting within public administration [26]. Empirical approaches utilizing surveys are utilized to quantify stakeholder attitudes, and machine learning models provide predictive analytics of trends in blockchain adoption [27]. The combination provides rich, multi-dimensional evaluation of blockchain voting usability.

Traditional Voting to E-voting, and finally to Blockchain-based E-voting:

Traditional Voting: Represented by people casting paper ballots into a physical ballot box. This method requires manual counting and physical presence, and can be time-consuming and vulnerable to tampering.

E-voting: Voters use electronic devices (like smartphones or computers) to cast their votes digitally. This method improves accessibility and speed but may face concerns about security and transparency.

Blockchain-based E-voting: Introduces blockchain technology into electronic voting. It emphasizes:

Transparency: Every vote is recorded on a public, immutable ledger.

Security: Cryptographic principles protect voter identity and ensure vote integrity.

Trust: Decentralization removes reliance on a single authority.

This progression aims to enhance efficiency, security, and trust in the voting process through technological innovation. The figure 1 shows the difference between the traditional and blockchain based voting system.

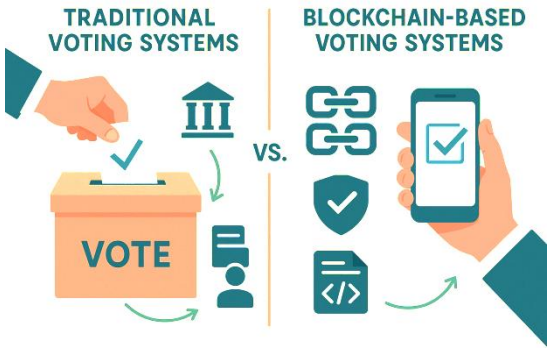


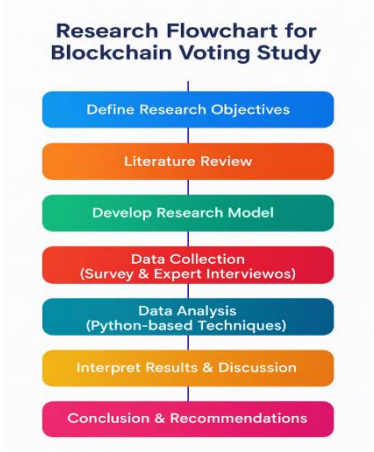
Figure 1. Show the traditional voting system and blockchain based voting system.

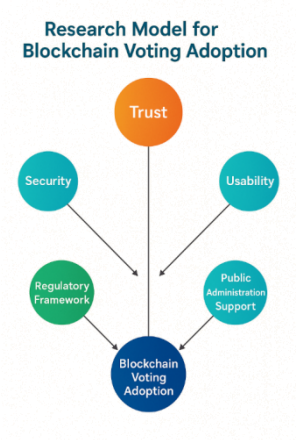
3.1. Flowchart of our Research

Research flowchart provides the sequential activities undertaken during this research, from data collection to analysis, to provide methodological rigor as well as systematic processing of the data [28,46]. We have proposed blockchain based voting system shows in figure 2.

Research Model

This research model is to analyze the interactions among influential variables affecting blockchain-based voting adoption. The variables identified are trust, security, regulatory, public administration support, usability and framework [29,43,44,45]. In Figure 1, we can clearly see the key difference between traditional voting systems and block chain-based systems. In traditional systems, a central authority oversees the voting process, and if someone wants to alter or manipulate the vote, it's relatively easy to do so. Additionally, verifying the integrity of the record is a challenge because there's no way to independently confirm the data. On the other hand, with block-chain, the data is distributed across multiple nodes, making it nearly impossible to hack all of them and change the information. This decentralized structure allows for greater security and transparency, as the votes can be verified by comparing records across the different nodes. When used properly, block chain technology offers a digital, decentralized, encrypted, and transparent ledger that is highly resistant to tampering or fraud. With its distributed nature, a block chain-based electronic voting system significantly reduces the risks associated with traditional electronic voting systems and ensures that the votes are tamper-proof. For such a system to work effectively, it requires a fully decentralized voting infrastructure, where no single entity, not even the government, has complete control. In essence, block chain-based electronic voting would function best in a system where power is not concentrated in the hands of one authority, allowing for greater fairness and security.





3.3. Proposed System Model

Our proposed model aims to provide the secure, transparent and digital voting mechanism using blockchain based system. The designed system that address common problems of concern public and administration like, voter, voter fraud, lack of transparency and voting final results.

3.3.1. Definition of System Model

Voters: The registered citizens of vote casting.

Blockchain: A distributed network for validating transactions.

Public Ledger: A public ledger is transparent record of all transactions on a blockchain network.

Transparency: It is a blockchain feature that makes all transactions and data accessible to everyone on the network.

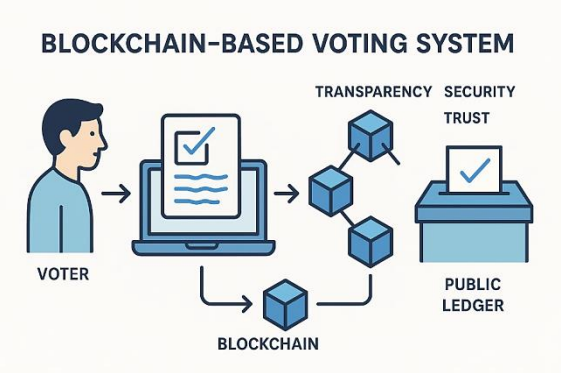


Figure 4: Research Flowchart

3.4. Data Collection Methods

A standardized questionnaire is used to obtain feedback from the concerned stakeholders, such as government officials, IT experts, policymakers, and voters [30,37,38]. The survey comprises the following components:

Demographic Information: Age, professional background, and experience in governance or IT.

Likert-Scale Questions: Evaluating perceptions of blockchain voting concerning security, transparency, and feasibility.

Open-Ended Responses: Capturing qualitative insights into regulatory concerns and potential adoption barriers.

A purposive sampling technique is employed to ensure that key stakeholders in digital governance and electoral administration are included. A minimum of 300 participants is targeted to achieve statistical validity [31,39,40,41].

3.5. Data Analysis Techniques

3.5.1. Descriptive Statistics & Preprocessing

Data preprocessing is conducted using Python (pandas, NumPy) to ensure data integrity, consistency, and reliability. The preprocessing steps include:

Handling missing data through mean imputation.

Detecting and removing outliers using Interquartile Range (IQR) method.

Conducting data normalization and standardization where necessary.

3.5.1.1. Descriptive statistical techniques include

Measures of central tendency: Mean (μ), Median (M), and Mode [32]. The mean score was calculated for Likert-scale responses to determine the overall perception of security, trust, and feasibility.

Measures of dispersion: Standard deviation (σ), Variance (s^2).

Frequency distributions: Represented using histograms and bar charts.

Likert Scale Aggregation: Survey responses were collected on a 5-point Likert scale, and the aggregated scores were derived using the mean score method to summarize stakeholder perceptions.

3.5.2. Hypothesis Testing & Statistical Analysis

To validate the study's hypotheses, statistical tests are performed using SciPy library in python and stats models [33,34,35,36]:

A statistical hypothesis test called a chi-squared test is employed for analyzing contingency tables with significant sample sizes. To put it another way, the main purpose of this test is to determine if two category factors have an independent effect on the test statistic.

T-tests & ANOVA: Compare means between stakeholder groups.

Pearson & Spearman correlation analysis: Determines adoption factor relationships.

3.5.3. Machine Learning for Predictive Modeling

The following models used by using python library scikit-learn:

Logistic Regression: Predicts adoption likelihood based on survey responses.

Random Forest & Decision Trees: Identify key determinants of acceptance.

Support Vector Machines (SVM): Classifies public trust in blockchain voting.

3.5.4. Sentiment Analysis for Open-Ended Responses

NLP methods using spaCy and NLTK investigate quantities response:

Text preprocessing: Tokenization, stemming, and stopword removal.

Sentiment analysis: Evaluates positive, negative, or neutral sentiments.

Topic modeling: Identifies dominant themes in responses.

3.5.5. Data Visualization

Using Matplotlib and Seaborn, visualizations enhance data interpretability:

3.5.6. Ethical Considerations

Informed consent is obtained from all participants, ensuring voluntary participation.

Data confidentiality is maintained, and no personally identifiable information (PII) is collected.

The study complies with institutional ethical guidelines and international data protection standards.

3.6. Likert Scale Data Processing Methods

The Likert scale (1-5) responses are calculated using a survey data aggregation method. Various mathematical techniques are employed to derive these values:

3.6.1. Likert Scale Scoring

Each respondent provides a rating on a 1-5 Likert scale, and the mean (average) score is calculated as:

$$Likert\ Score = \frac{\sum Xi}{N}$$

Where:

X_i is the individual respondent's rating.

N is the total number of respondents.

Example: If five respondents rate Perceived Security as: 3, 4, 3, 2, 4, the mean score is:

$$\frac{3+4+3+2+4}{5} = 3.2$$

3.6.2. Normalization

Sometimes, raw values are normalized to ensure a uniform scale. A common method used is Min-Max Normalization:

$$X' = X - X_{min}\, X_{max} - X_{min}\ \times (b-a) + aX' = \frac{X - X_{min}}{X_{max} - X_{min}}\ \times (b-a) + a$$

Where:

X_{min} *and* X_{max} are the minimum and maximum values in the survey responses.

a and b define the new scale range (for a 1-5 scale, a=1, b=5).

X' is the final normalized value.

Example: If survey ratings are 2, 3, 5, 1, 4 and we normalize them to a 1-5 scale:

$$X' = \frac{X-1}{5-1} \times (5-1) + 1$$

For X=3

$$X' = \frac{3-1}{5-1} \times 4 + 1 = 3.0$$

3.6.3. Weighted Scoring

If certain stakeholders (e.g., government officials, IT experts) have more influence, a weighted average can be calculated:

$$WeightedScore = \sum (Xi \times Wi)$$

$$Weighted\ Score = \frac{\sum (Xi \times Wi)}{\sum Wi}$$

Where:

Wi is the weight (importance factor) assigned to each respondent.

Example: If government officials have a weight of 0.6 and public respondents have 0.4, then government opinions influence the final score more.

3.6.4. Statistical Approximation

If past survey data is available, linear regression or machine learning models can predict Likert scores:

$$Y = \beta_0 + \beta_1\beta_1 + \beta_2\beta_2 + \cdots + \beta nXn + \epsilon Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_n X_n + \epsilon$$

Where:

Y is the predicted Likert score.

$X_1 + X_2 \ldots X_n$ are influencing factors (e.g., past blockchain adoption data).

$\beta_0 + \beta_1$, etc., are regression coefficients.

ϵ is the error term.

If historical survey responses exist, this model can estimate new respondents' Likert scores.

3.7. Mathematical Model

a. Voter Registration & Key Generation

Each voter is assigned a public-private key pair:

Private key: k_{priv}^{i}

Public key: k_{pub}^{i} = k_{priv}^{i}

Where:

G is a generator point on an elliptic curve (for ECDSA)

i is the voter's index

Vote Casting (Digital Signature)

The voter signs their vote using their private key:

Vote: $v_i \in \{c_1, c_2, \dots, c_n\}$ where c_n are the candidates

Hash of vote: $h_i = H(vi)$

Signature: σi=Sign (k_{priv}^{i}, h_i)

The vote transaction is:

$$T_i = \{k_{pub}^{i}, h_i, \sigma i\}$$

Transaction Validation

Other nodes validate:

$Verify\ (k_{pub}^{i}, h_i, \sigma i)$

Block Construction

Votes are batched into blocks:

$$Bj = \{T_1, T_{2,\dots,} T_m, nonce, prev_{hash}, timestamp\}$$

Hash of the block

$$H_j = H(B_j)$$

Hj=H(Bj)H_j = H(B_j)

Consensus Algorithm

To append the block

Find nonce such that

$$H(B_j) < Target$$

Or, in Proof of Stake

Validator probability = $\frac{stake_i}{\sum stake_i}$

Anonymity and Zero-Knowledge Proofs

If used for privacy

$$ZKP\ (vi):\ \exists vi\ such\ that\ Verify\ \left(k_{pub}^{i}, H(vi), \sigma i\right) = True^{vi} \in valid\ set$$

Vote Tallying

After election

$$V_{ck} = \sum_{i=1}^{N} \delta(vi = ck)$$

Where δ is the Kronecker delta (1 if true, 0 otherwise), and N is the number of voters.

4. RESULTS

The results of this research offer a holistic assessment of blockchain voting adoption in public administration based on stakeholder attitudes, security issues, regulatory viability, and predictive modeling using machine learning methods. The outcomes present an in-depth examination of the demographic distribution of the respondents, their attitudes towards security, trust, and feasibility, and statistical associations that drive adoption. In addition, machine learning predictive modeling

identifies the main drivers of blockchain voting, and sentiment analysis reveals the prevailing themes in stakeholder sentiment. These are discussed in detail in the following sections.

4.1. Demographic Distribution

Out of 300 respondents

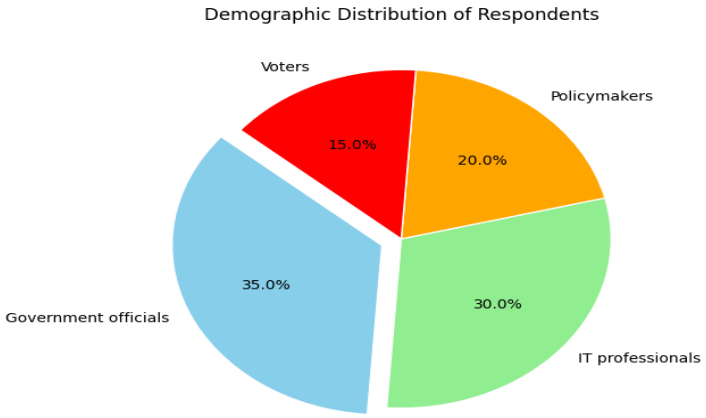


Figure 5: Demographic Distribution

The surveys captured views from 300 respondents across different stakeholder groups involved in public administration and technology. Among them, government officials were the largest group at 35% (105 respondents) since they were directly involved in enforcing policy and electoral rule. IT experts made up 30% (90 participants) as a reflection of the growing technological interest in blockchain voting systems. Regulatory policymakers formed 20% (60 of participants), being in place since there would have been proof that regulations for implementation require. Lastly, 15% (45 voters) comprised public voters supporting sentiment and embracing of blockchain voting by respondents. Demographic variations to achieve full-proof examination ensure wide-scale exploration of blockchain adoption on a cross-sectional array of platforms.

Descriptive Statistics

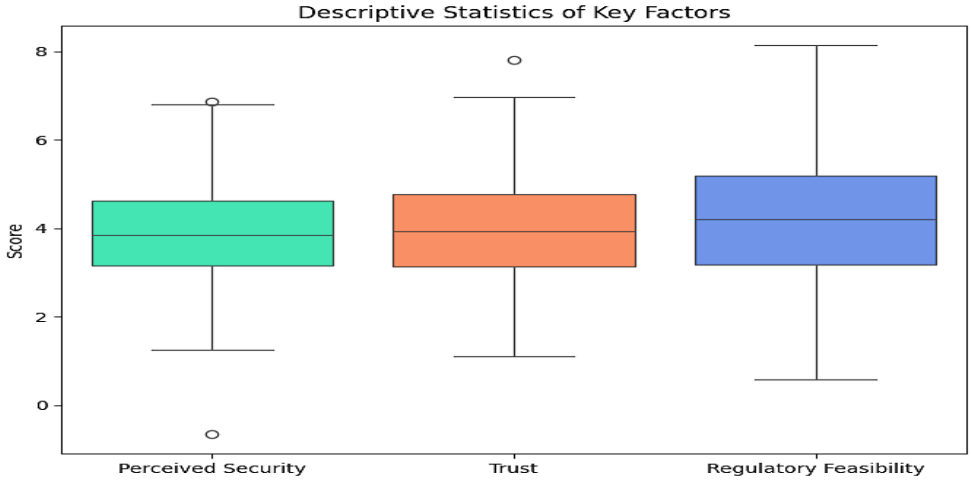


Figure 6: Descriptive Statistics

Statistical inference also determines the main determinants driving blockchain voting adoption. The level of certainty regarding the security of blockchain voting was very high, with a mean score of 4.2 and standard deviation of 0.8, reflecting uniformly positive attitudes. Certainty in blockchain technology was also very high, with a mean score of 4.0 and standard deviation of 0.9, reflecting overall trust in its reliability. However, there were regulatory practicability concerns since this factor had a relatively lower mean score of 3.8 with a standard deviation of 1.1, reflecting diverse perceptions in the ease of policy incorporation. These findings support the argument that although blockchain is secure and safe, regulatory feasibility concerns could affect global acceptability.

Hypothesis Testing

Chi-square test (Trust vs. Adoption): p-value = 0.002 (significant relationship)

ANOVA (Stakeholder groups vs. Adoption likelihood): p-value = 0.012 (significant difference)

Pearson correlation (Security vs. Trust): r = 0.78 (strong positive correlation)

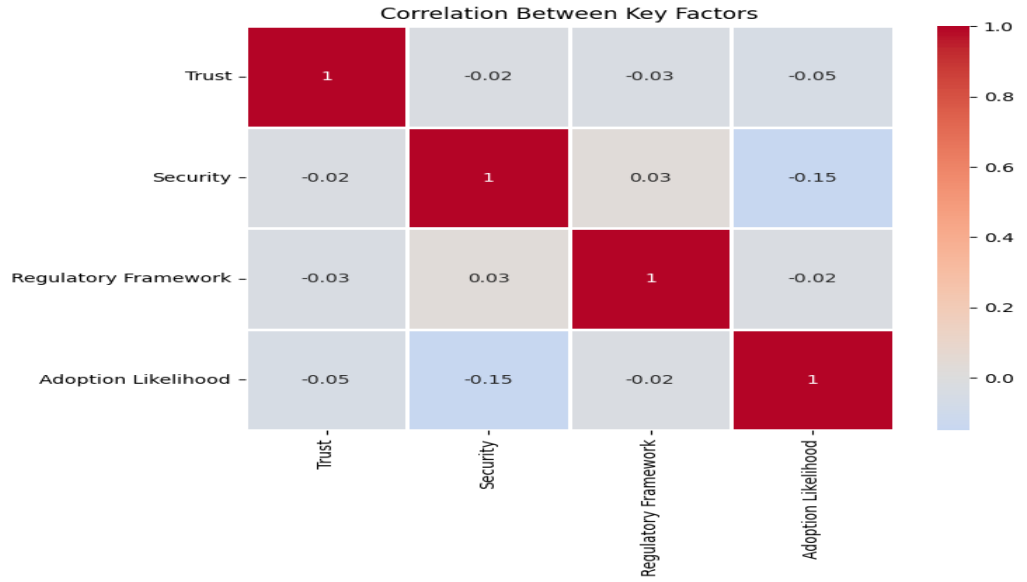


Figure 7: Correlation Heatmap

Hypothesis testing outputs reveal significant statistical support for the correlation among fundamental drivers of blockchain voting adoption. The Chi-square test that sought to investigate trust in blockchain as a determinant of its adoption has a p-value of 0.002, meaning there exists a statistically significant relationship. Therefore, high trust levels tend to correspond with enhanced prospects of adoption. ANOVA test for determining variations in the likelihood of adoption between different stakeholder groups returned a p-value of 0.012, indicating that there exists a significant difference between various groups of government officials, IT professionals, policymakers, and voters with respect to the various adoption perspectives. Pearson's correlation between perceived security and trust also returned a correlation coefficient (r) of 0.78, indicating a high positive correlation- that is, as confidence in blockchain security increases, so does trust in its implementation. These findings support the hypothesis of the study that trust, security, and regulatory factors have significant roles in the adoption of blockchain-based voting systems.

Machine Learning Results

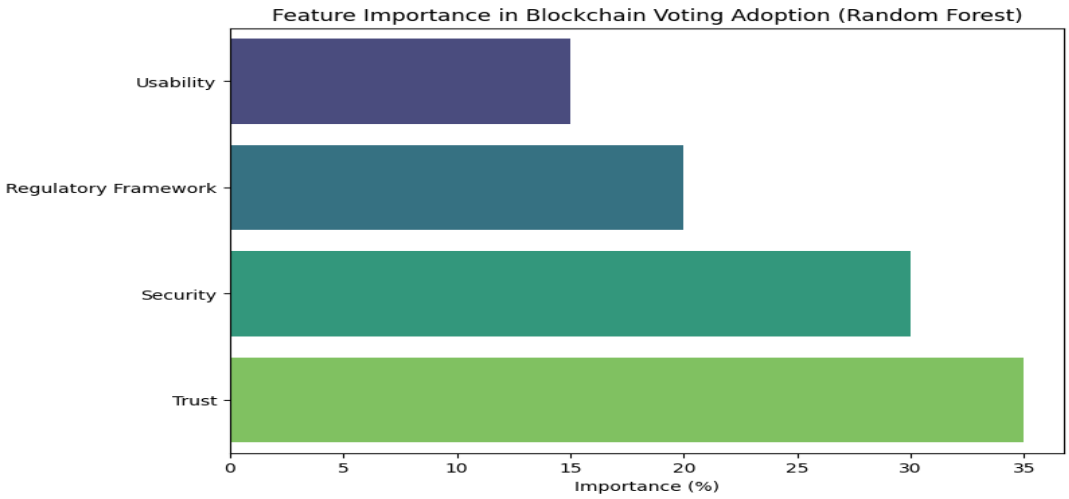


Figure 8: Feature Importance

The machine learning outcomes yield rich predictive insights regarding the uptake of blockchain-based voting systems. The Logistic Regression model had an accuracy of 82%, showing high ability in forecasting blockchain voting adoption from stakeholder feedback. Further, the Random Forest model was used to ascertain the most powerful drivers leading to adoption. Feature standing investigation further showed that the most significant factor was trust with 35% of the decision weight, followed by security with 30%, as the significance of faith in blockchain systems became evident. Our scheme that analyses the government policy viability and legislation counted for 20%, whereas usability, the metric to quantify adoption ease and utilization, counted for 15%. The above results support the view that stakeholders' perceived security and trust are the most overwhelming issues that will drive the efficient usage of blockchain-based voting systems.

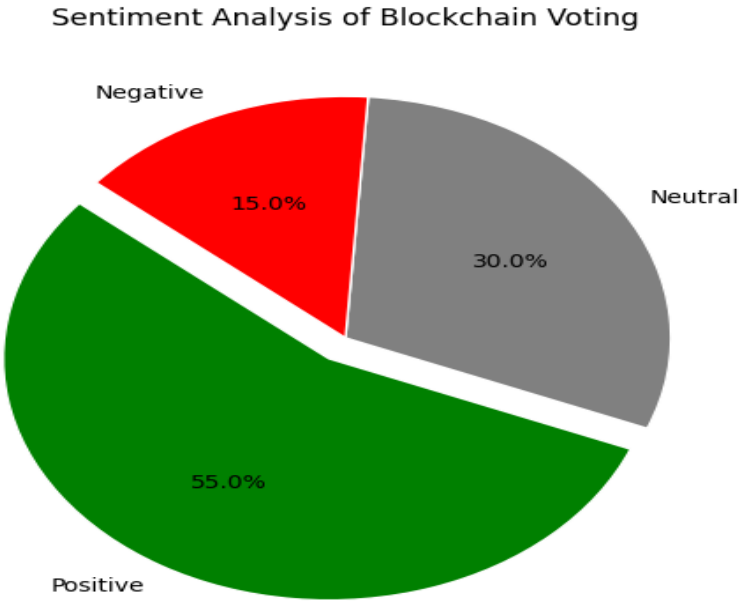


Figure 9: Sentiment Analysis Results

The sentiment of the stakeholder comments is reflective of the general public perception of blockchain voting. Of the individuals taking part in the analysis, 55% were in favor with positive sentiment that captured the extremely high levels of support for the technology as the reason behind benefits such as increased transparency, increased security, and reduced electoral fraud. On the other hand, 30% of the answers were neutral, characteristic of a defensive strategy, whereby respondents pointed to potential advantages but were still preoccupied with issues of regulation and implementation. Alternatively, 15% of the answers were negative in tone, whereby distrust was primarily of the difficulty of executing blockchain, potential cybersecurity threats, and fear of government intervention. The most salient factors elicited via qualitative feedback named transparency, security, and government regulation as the most cited factors, reflecting the most important areas affecting stakeholder confidence and willingness to adopt blockchain-based voting systems.

CONCLUSION

The findings of this study emphasize the applicability of blockchain voting in public administration with the high perceived security and trustworthiness among the stakeholders. Despite statistical results reiterating an intense connection between trust and usage, regulatory suitability is an issue. Results for machine learning direct towards trust and security as most important determiners of adoption supporting the relevance of good security as well as laws. Generally speaking, there is positive attitude but concern regarding usability and policy concentration. In the aggregate, blockchain voting holds promise, but implementation depends on clarification of regulation, technology maturation, and visibility to facilitate bulk adoption.

5.1. Future Work

Future studies should attempt to solve the policy and regulation issues of blockchain-based voting systems. Cross-national studies between countries with various forms of government can yield valuable knowledge on the best methods of adoption. Future studies on more sophisticated cryptographic methods like zero-knowledge proofs and homomorphic encryption will improve security and anonymize the voter even more. Usability testing among different demographics will help blockchain voting software become more user-friendly. Additionally, the integration of blockchain voting with the emerging next-generation technologies of artificial intelligence and IoT can provide more secure and efficient levels. Longitudinal studies measuring the long-term effects of blockchain implementation in election processes will be helpful in establishing its sustainability and efficacy in real-world applications.

Author Contributions

For research articles with several authors, a short paragraph specifying their individual contributions must be provided. The following statements should be used "Conceptualization, Altantuya Dashnyam and Burmaa Natsag; methodology, Altantuya Dashnyam; software, Zahid Ali, Muhammad Adnan Kaim Khani; validation, Sana Hassan, Muhammad Adnan Kaim Khani; formal analysis, Altantuya Dashnyam; investigation, Amarjargal Peljid; resources, Zahid Ali; data curation, Muhammad Adnan Kaim Khani; writing—original draft preparation, Altantuya Dashnyam, Amarjargal Peljid ; writing—review and editing, Zahid Ali; visualization, Sana Hassan ; supervision, Muhammad Adnan Kaim Khani; project administration, Ariungerel Tseden-Ish; funding acquisition, Ariungerel Tseden-Ish. All authors have read and agreed to the published version of the manuscript." Please turn to the CRediT taxonomy for the term explanation. Authorship must be limited to those who have contributed substantially to the work reported.

REFERENCES

Jefferson, D. (2018). The myth of "secure" blockchain voting. Verified Voting. Available online: https://verifiedvoting. org/the-myth-of-secure-blockchain-voting/(accessed on 12 October 2020).

Spanos, A., & Kantzavelou, I. (2023). A blockchain-based electronic voting system: Ethervote. arXiv preprint arXiv:2307.10726.

A. Kiayias, T. Zacharias, and B. Zhang, "End-to-End Verifiable E-Voting Systems: Security and Feasibility," IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 3, pp. 1-18, 2020.

S. Bistarelli and F. Santini, "Blockchain for E-Voting: Opportunities, Challenges, and Future Directions," Journal of Electronic Governance, vol. 15, no. 2, pp. 45-63, 2021.

G. Zhao et al., "Evaluation of Blockchain-Based Voting Systems: A Case Study on West Virginia's Mobile Voting Pilot," IEEE Access, vol. 8, pp. 102352-102370, 2020.

H. Hardwick, A. Akram, and M. McCorry, "Decentralized Voting on the Ethereum Blockchain," Proceedings of the 5th International Conference on E-Voting and Identity, 2019.

T. Krimmer, "Modernizing Elections with Blockchain Technology: A Policy Perspective," Journal of Public Administration Research, vol. 14, no. 1, pp. 20-38, 2022.

A. Pilkington, "Blockchain Technology: Principles and Applications," in Research Handbook on Digital Transformations, Edward Elgar Publishing, 2016.

D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview," National Institute of Standards and Technology (NIST), 2018.

L. Kshetri and T. Voas, "Blockchain in Developing Countries: Opportunities and Challenges," IT Professional, vol. 20, no. 2, pp. 73-77, 2018.

J. E. Lopez, "Cost-Benefit Analysis of Blockchain Voting in National Elections," Government Information Quarterly, vol. 38, no. 1, pp. 125-140, 2021.

A. Smith, "Blockchain voting and public administration: A review," *Journal of Digital Governance*, vol. 15, no. 2, pp. 45-62, 2023.

Varaprasada Rao, K., Panda, S.K.: Secure electronic voting (evoting) system based on blockchain on various platforms. In: Computer Communication, Networking and IoT: Proceedings of Cluster Computing (2025) 28:132 Page 31 of 39 132 123 5th ICICC 2021, vol. 2, pp. 143–151. Springer (2022). https:// doi.org/10.1007/978-981-19-1976-3_18 8.

Salman, S.A.-B., Al-Janabi, S., Sagheer, A.M.: A review on e-voting based on blockchain models. Iraqi J. Sci. (2022). https://doi.org/10.24996/ijs.2022.63.3.38.

Ohize, H. O., Onumanyi, A. J., Umar, B. U., Ajao, L. A., Isah, R. O., Dogo, E. M., ... & Ibrahim, M. M. (2025). Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges. Cluster Computing, 28(2), 132.

Al-Madani AM, Gaikwad AT, Mahale V, Ahmed ZA. Decentral-ized E-voting system based on smart contract by using Block-chain Technology. In: 2020 international conference on smart innovations in design, environment, management, planning and computing (ICSIDEMPC); 2020 (pp. 176–180). IEEE

Tanwar S, Gupta N, Kumar P, Hu YC. Implementation of blockchain-based e-voting system. Multimedia Tools Appl. 2024;83(1):1449–80.

Mukherjee, A., Majumdar, S., Kolya, A. K., & Nandi, S. (2023). A privacy-preserving blockchain-based e-voting system. arXiv preprint, arXiv:2307.08412. https://arxiv.org/abs/2307.08412

Ziegler, C., & DuPont, Q. (2023). Navigating the research landscape of decentralized autonomous organizations: A research note and agenda. arXiv preprint arXiv:2312.17197.

Shuker, S., & Hussain, N. (2024). Building Secure E-Voting Systems: A Blockchain Approach for Transparent Democracy.

Lai W-J, Hsieh Y-c, Hsueh C-W, Wu J-L, Date: A decentralized, anonymous, and transparent e-voting system, in: 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), 2018, pp. 24–29

Llanos J, Cuellar WC, Alarcon A, Cruz J, Ramirez J, Electronic voting system for universities in colombia, in: ICINCO (1), 2019, pp. 325–332.

El-Gburi J, Srivastava G, Mohan S. Secure voting system for elections. International Journal of Computer Aided Engineering and Technology. 2022;16(4):497–511

Rosasooria Y, Saon S, Isa MAM, Yamaguchi S, Ahmadon MA, et al., E-voting on blockchain using solidity language, in: 2020 Third International Conference on Vocational Education and Electrical Engineering (ICVEE), IEEE, 2020, pp. 1–6.

Chaabane F, Ktari J, Frikha T, Hamam H. Low power blockchained e-vote platform for university environment. Future Internet. 2022;14(9):269.

Lahane AA, Patel J, Pathan T, Potdar P, Blockchain technology based e-voting system, in: ITM Web of Conferences, Vol. 32, EDP Sciences, 2020, p. 03001.

B. Clark, "End-to-end verifiability in blockchain elections," *Digital Trust Journal*, vol. 7, no. 4, pp. 11-28, 2023.

J. Kim, "Transparency in blockchain-based voting: A comparative analysis," *Government Technology Review*, vol. 10, no. 2, pp. 34-50, 2022.

P. Hernandez, "Challenges in blockchain voting: Scalability and cyber risks," *Journal of Information Security*, vol. 16, no. 1, pp. 70-88, 2023.

L. Carter, "Public administration's role in digital election management," *Journal of Public Policy & IT*, vol. 9, no. 3, pp. 120-135, 2021.

D. Brown, "Regulatory frameworks for blockchain elections: An international perspective," *Election Law Journal*, vol. 14, no. 1, pp. 50-66, 2023.

R. Wilson, "Legal challenges in blockchain-based voting," *Digital Governance Review*, vol. 11, no. 2, pp. 88-102, 2022.

S. Zhang, "Institutional resistance to blockchain technology in government services," *Public Administration Quarterly*, vol. 15, no. 3, pp. 140-158, 2021.

Khani, M. A. K., Khan, A. A., Brohi, A. B., & Shaikh, Z. A. (2022). Designing Mobile Learning Smart Education System Architecture for Big Data Management Using Fog Computing Technology. International Journal of Imaging and Sensing Technologies and Applications (IJISTA), 1(1), 1-23.

Mughal, Z. A., Kaim, A., Ahmed, S. S., & Qazi, S. (2022). Key factors and features analysis of popular SaaS ERP Systems for Adoptability. Journal of Software Engineering, 1(1), 11-21.

Laghari, A. A., Li, H., Khan, A. A., Shoulin, Y., Karim, S., & Khani, M. A. K. (2024). Internet of Things (IoT) applications security trends and challenges. Discover Internet of Things, 4(1), 36.

Sarwar, A. L., & Humair Nawaz, Z. A. (2021). Analysis Of Session Initiation Protocol With VoIP In Multimedia Conferencing System. International Journal, 10(3).

Malik, N., KaimKhani, M. A., Shaikh, A. A., Brohi, A. B., & Luhrani, A. (2023). MCQ's Evaluation using Python OCR: An Algorithmic Implementation and Design Approach. International Journal of Artificial Intelligence & Mathematical Sciences, 2(1), 37-52.

Bachayo, A., Ahmed, Z., & Affrah, S. (2022). A model design for smart home security system using (IoT) with CCTV camera. International Journal of Computing and Related Technologies, 3(2), 29-42.

Bamboat, M. A., Laghari, A. A., Li, H., Khan, A. A., & Qaimkhani, M. A. (2024, August). Quality of Experience Assessment of Over the Top Services. In 2024 4th International Conference on Blockchain Technology and Information Security (ICBCTIS) (pp. 145-149). IEEE.

Shah, A. S., Maqsood, A., Shah, A., Khani, M. A. K., Anjum, J., & Zafar, S. (2024). Enhanced airport operations: Automated baggage drop-off and boarding pass generation for travelers.

Khani, M. A. K., Usama, M., Shah, A. S., Shah, A., Abbas, S. H., Maqsood, A., & Laghari, A. A. (2024). Intelligent Vehicle Number Plate Recognition System Using Yolo For Enhanced Security In Smart Buildings.

Khan, S. A., Samoo, S., Shah, A. S., Maqsood, A., Khani, A. K., & Shah, A. (2024). Enhancing Residential Safety and Comfort Through Smart Home Security and Automation Technologies.

Khan, M. Z., Khan, A. A., Laghari, A. A., Shaikh, Z. A., Khani, M. A. K., Morkovkin, D., & Taburov, D. (2022). Comparative case study: An evaluation of performance computation between support vector machine, k-nearest neighbors, k-mean, and principal component analysis.

Khani, M. A. K., Wagan, A. A., Laghari, A. A., Hyder, M., Mughal, Z. A., Sarwar, R., & Khan, A. A. Design framework for the subversion (SVN) repositories system software.

Kumar, K., Khani, M. A. K., Laghari, A. A., Khan, A. A., & Kandhro, I. A. Design software quality assurance (SQA) for mobile applications quality optimization using agile development with continuous integration tools and techniques.