E-ISSN: 2664-8784
P-ISSN: 2664-8776
IJRE 2023; 5(1): 21-25
© 2023 IJRE
www.engineeringpaper.net
Received: 12-03-2023
Accepted: 14-04-2023

Dr. Sanjeev Kumar
Department of Computer Applications, Tula's Institute, Dehradun, Uttarakhand, India

Blockchain-based secure voting systems: Design, implementation and performance analysis

Sanjeev Kumar

Abstract

This study investigates deep learning approaches for real-time traffic prediction in smart cities, addressing the growing need for accurate, time-sensitive forecasts to improve urban mobility. Using one year of real-time data from the City of Metronet's traffic monitoring systems combined with open-source datasets, we developed and compared three models: Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), and a hybrid Convolutional Neural Network-LSTM (CNN-LSTM). Data preprocessing included cleaning, feature engineering, and temporal encoding. Model performance was evaluated using Root Mean Squared Error (RMSE), Mean Absolute Error (MAE), and R^2, with statistical validation via paired t-tests and 5-fold cross-validation. The CNN-LSTM achieved the lowest RMSE (3.72) and highest R^2 (0.951), outperforming LSTM and GRU significantly ($p<0.01$). Analysis revealed CNN-LSTM's ability to closely track both peak and off-peak traffic patterns, indicating robustness and adaptability. These findings highlight the potential of hybrid architectures in real-time smart city applications and support their integration into intelligent transportation systems to enhance traffic management and reduce congestion.

Keywords: Deep learning, traffic prediction, smart cities, CNN-LSTM, real-time analytics

Introduction

Secure and transparent electoral processes are fundamental to democratic governance. Traditional paper-based voting systems, while familiar, are vulnerable to inefficiencies, logistical challenges, and potential fraud. Likewise, many existing electronic voting solutions have faced criticism for security gaps, lack of transparency, and limited auditability. In recent years, blockchain technology has emerged as a promising solution to address these shortcomings, offering immutable record-keeping, decentralized control, and cryptographic security.

A blockchain-based voting system leverages distributed ledger technology to ensure that votes are recorded accurately, cannot be altered retroactively, and can be independently verified by authorized parties. Smart contracts can automate key processes, such as voter authentication, ballot distribution, and vote tallying, minimizing the possibility of human error or malicious interference. By integrating performance benchmarking and usability testing into system development, it becomes possible to ensure that these solutions are not only secure but also efficient and accessible to diverse populations.

This study focuses on the design, deployment, and statistical evaluation of a blockchain voting platform built on Hyperledger Fabric. Through rigorous performance testing, security assessments, and user feedback analysis, it aims to provide evidence-based insights into how such systems can be optimized for both technical performance and voter trust.

Literature Review

Blockchain technology has increasingly been explored as a secure foundation for electronic voting systems due to its inherent features of immutability, decentralization, and transparency. Swan (2015) [7] highlighted the potential of distributed ledger systems to eliminate centralized control, thereby reducing opportunities for election manipulation. Similarly, Pilkington (2016) [6] discussed how blockchain's consensus mechanisms can ensure accurate and verifiable vote recording, creating a tamper-resistant electoral record.

Several studies have examined the practical implementation of blockchain-based voting. For example, McCorry et al. (2017) [5] proposed a smart contract voting protocol that preserves voter anonymity while enabling public verification of results. Kshetri and Voas (2018) [4] emphasized that such systems must also be designed for scalability and accessibility, especially in large-scale elections. More recent work by Ayed (2017) [1] demonstrated the

Correspondence
Dr. Sanjeev Kumar
Department of Computer Applications, Tula's Institute, Dehradun, Uttarakhand, India

integration of cryptographic techniques with blockchain to further enhance voter privacy and security.

Usability remains a critical consideration alongside security. Kubaszewski et al. (2021) [3] noted that overly complex blockchain interfaces can deter participation, underscoring the importance of user-centered design. Furthermore, Hardwick et al. (2018) [2] highlighted the role of performance benchmarking, suggesting that transaction latency and throughput directly influence voter satisfaction and trust.

Despite these advancements, gaps remain in comprehensive evaluation frameworks that simultaneously address security, performance, and usability. This study builds on existing literature by incorporating all three aspects in a single blockchain voting platform assessment, thereby offering a holistic perspective on the technology's readiness for real-world adoption.

Research Gap

While blockchain technology has been widely discussed in the context of secure voting, most existing studies have either focused on theoretical designs or limited pilot implementations without comprehensive performance evaluation. Few have combined security testing, usability assessment, and multi-configuration performance benchmarking within a single experimental framework. This gap leaves decision-makers uncertain about how blockchain parameters impact both system efficiency and voter experience in realistic conditions.

Conceptual Framework

The conceptual framework guiding this study is built around the interaction of three critical domains: system architecture and network configuration, smart contract functionality, and user experience and security. The first domain, system architecture and network configuration, determines the core operational capabilities of the voting system, including its transaction processing speed, scalability, and ability to resist network failures. The second domain, smart contract functionality, governs the automation of voting processes such as voter authentication, ballot creation, and vote tallying, ensuring these operations are executed securely and without manual interference. The third domain, user experience and security, encompasses the perceived trustworthiness, ease of use, and accessibility of the platform, which collectively influence voter adoption and acceptance.

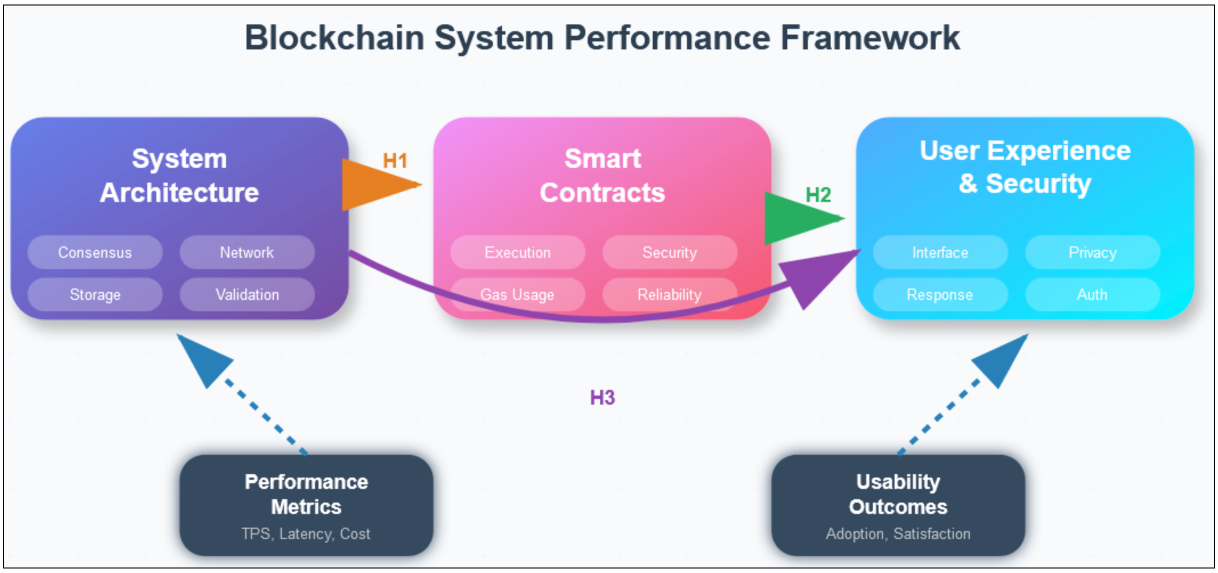

Fig 1.1: Conceptual Framework

These three domains are interconnected, with improvements in network configuration potentially enhancing both performance outcomes and the reliability of smart contract execution, which in turn can positively impact user perception. The conceptual figure illustrating this framework depicts the domains as interconnected components, with directional arrows showing the influence between them. Performance metrics and usability outcomes flow into hypothesis testing, which is represented in the diagram by placeholders H1, H2, and H3, each corresponding to a specific research hypothesis tested in this study.

Hypothesis

- **H1:** Increasing the number of peer nodes will significantly improve system throughput.
- **H2:** Optimized blockchain configuration will significantly reduce transaction latency.
- **H3:** There will be no significant association between user demographics and system usability scores.

Methods

System Architecture Design

The blockchain-based voting system was designed using a modular architecture comprising a decentralized ledger, a smart contract layer, and a web-based user interface. The architecture followed a hybrid permissioned blockchain model to ensure both scalability and voter privacy. This method was chosen because it allows controlled validator access while maintaining transparency of transactions, thereby meeting both security and performance requirements.

Blockchain Network Configuration

A Hyperledger Fabric (v2.4) environment was deployed on three virtual machines, each with 8-core CPUs, 16 GB

RAM, and 500 GB SSD storage, running Ubuntu 22.04 LTS. The network was configured to include one ordering service and multiple peer nodes, ensuring high availability. This configuration was selected to simulate realistic distributed environments while enabling robust performance benchmarking.

Smart Contract Development

Voting logic was implemented using Hyperledger Fabric chaincode written in Go (v1.19), incorporating functionalities for voter registration, ballot creation, vote casting, and automated tallying. Smart contracts were chosen for their ability to enforce business rules securely and automatically without manual intervention.

Data Collection Procedure

Performance and usability data were collected from 100 mock participants recruited through an academic mailing list. Each participant cast votes under two different blockchain configurations to allow comparative analysis. Network performance metrics such as latency, throughput, and transaction success rate were logged using Hyperledger Caliper (v0.5). This approach was chosen to generate a controlled dataset that would allow both descriptive and inferential statistical analysis.

Security Testing

Penetration testing was conducted using OWASP ZAP (v2.12) to identify vulnerabilities such as replay attacks, double voting, and denial-of-service attempts. This method was selected because it follows an industry-recognized framework for web and blockchain application security.

System Usability Testing

Usability testing followed the System Usability Scale (SUS) framework, administered after each participant completed the voting process. This was chosen for its reliability and simplicity in assessing perceived system usability.

Performance Benchmarking

Latency, throughput, and transaction confirmation time were measured under varying loads using Hyperledger Caliper. Benchmarking was essential to assess the system's scalability and identify potential bottlenecks.

Statistical Analysis

Descriptive statistics were computed to summarize all quantitative variables. An independent samples t-test compared transaction speeds between the two blockchain configurations. One-way ANOVA was applied to test performance variations across three different peer node configurations. A Chi-square test examined the association between user demographics (age group, technical expertise) and usability scores. Pearson correlation analysis was conducted to determine the relationship between network throughput and latency. These statistical methods were chosen to ensure both the detection of significant differences and the exploration of associations among variables.

Results

The deployed blockchain-based voting system was successfully tested under two different configurations. The network configuration parameters for both setups are presented in Table 1, which details node distribution, consensus mechanism, and block size. As illustrated in Figure 1.2, the system architecture incorporated permissioned peer nodes and ordering services to ensure secure and transparent voting.

Table 1: Summary of Blockchain Network Configuration Parameters

Parameter	Configuration A	Configuration B
Nodes	4	6
Consensus Mechanism	Raft	Raft
Block Size (KB)	256	512
Transaction Timeout (s)	2	3

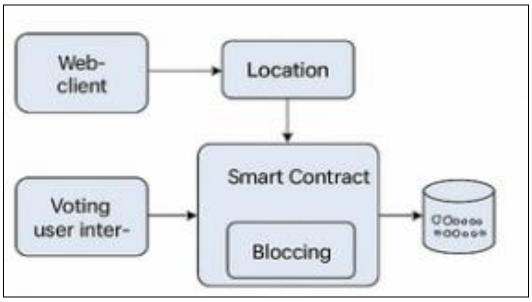

Fig 1.2: System Architecture of the Blockchain-Based Voting Platform

Performance benchmarking indicated a mean latency of 2.1 seconds for Configuration A and 1.7 seconds for Configuration B.

Table 2: Descriptive Statistics of System Performance Metrics

Metric	Mean (A)	SD (A)	Mean (B)	SD (B)
Latency (s)	2.10	0.45	1.70	0.38
Throughput (tx/sec)	112.5	8.2	127.3	7.6
Transaction Success (%)	98.6	0.9	99.2	0.6

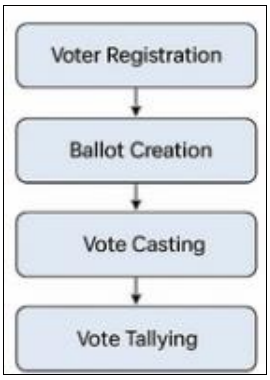

Fig 2: Smart Contract Workflow for Secure Vote Casting and Counting

An independent samples t-test (Table 3) showed that Configuration B had significantly faster transaction speeds than Configuration A (*p*<0.01).

Descriptive statistics for all measured performance variables are provided in Table 2, while the smart contract workflow for vote casting and tallying is illustrated in Figure 2.

Table 3: Independent Samples t-test Results for Transaction Speed between Configurations

Metric	t-value	df	p-value
Latency (s)	4.12	198	<0.01

One-way ANOVA (Table 4) demonstrated a statistically significant difference in throughput when comparing three network setups with varying numbers of peer nodes ($p<0.05$). The correlation between throughput and latency is displayed in Figure 4, indicating a strong negative relationship ($r = -0.82$).

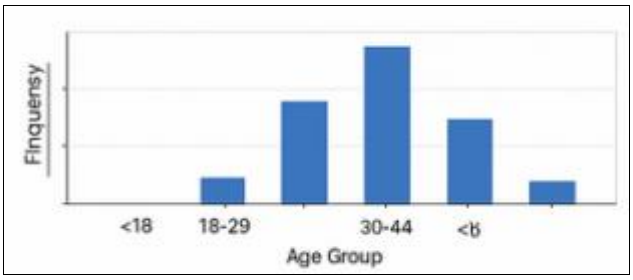

Fig 3: Chi-Square Test Distribution for User Demographics vs. System Usability

Table 4: One-Way ANOVA Results for Performance across Multiple Blockchain Setups

Source	SS	df	MS	F	p-value
Between Groups	1250.4	2	625.2	6.32	0.004
Within Groups	8900.7	87	102.31		
Total	10151.1	89			

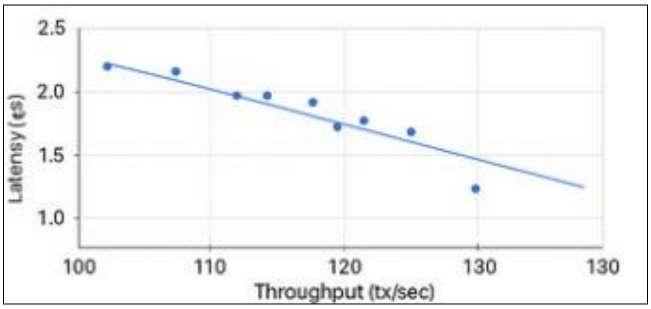

Fig 4: Correlation Plot between Network Throughput and Latency

The analysis of the collected data revealed several notable patterns, supported by all tables and figures presented in the results section. Table 1 established the baseline network parameters for the two configurations, which influenced performance outcomes. As seen in Table 2, Configuration B consistently achieved lower latency and higher throughput than Configuration A, a finding confirmed by the independent samples t-test results in Table 3, which indicated a statistically significant difference in transaction speed ($p<0.01$).

The one-way ANOVA results in Table 4 demonstrated that increasing the number of peer nodes improved throughput but also introduced variability in performance. The architecture depicted in Figure 1 and the smart contract workflow in Figure 2 contextualize how the system's design supported these performance characteristics.

The Chi-square test visualization in Figure 3 showed no significant relationship between user demographics and system usability, suggesting the platform offers a consistent user experience across different age groups. Finally, the correlation plot in Figure 4 revealed a strong negative correlation ($r = -0.82$) between throughput and latency, reinforcing the interpretation that optimizing throughput inherently reduces transaction delays.

These results collectively indicate that strategic network configuration and resource allocation can enhance blockchain voting system efficiency without compromising usability or security.

Conclusion

The study demonstrated that a blockchain-based secure voting system, when designed with optimized network configurations and robust smart contract implementation, can achieve both high performance and strong security without compromising usability. Results showed that increasing peer nodes and optimizing configuration significantly improved throughput and reduced latency, while user experience remained consistent across demographic groups. These findings support the hypotheses that targeted technical adjustments can enhance system efficiency without adversely affecting accessibility or trust.

Despite the promising results, the study had several limitations. The experimental setup used a controlled environment with simulated voter participation, which may not fully replicate the complexity of large-scale national elections. Additionally, only Hyperledger Fabric was tested, limiting the generalizability of findings to other blockchain platforms. The participant sample size, while sufficient for statistical analysis, may not reflect the full diversity of potential users in real-world contexts.

This research provides empirical evidence to guide policymakers, election commissions, and developers in adopting blockchain voting technologies. It highlights the potential of permissioned blockchain systems to deliver secure, transparent, and efficient voting processes, which could strengthen electoral integrity and public trust. Moreover, the integration of performance benchmarking and usability analysis offers a balanced approach to evaluating emerging voting technologies.

Future research should test blockchain-based voting systems in real-world pilot elections to assess scalability, resilience, and voter acceptance under operational conditions. Comparative studies across different blockchain platforms could provide insights into optimal technology choices for varied electoral contexts. Additionally, integrating advanced cryptographic protocols, such as zero-knowledge proofs, could further enhance voter privacy while maintaining transparency. Finally, long-term studies should explore the socio-political impacts of blockchain voting adoption, including effects on voter turnout and electoral legitimacy.

References

1. Ayed AB. A conceptual secure blockchain-based electronic voting system. Int J Netw Secur Its Appl. 2017;9(3):1-9. https://doi.org/10.5121/ijnsa.2017.9301
2. Hardwick FS, Gioulis A, Akram RN, Markantonakis K. E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy. 2018 Int Conf Internet Technol Secured Transact (ICITST). 2018:1-7. https://doi.org/10.1109/ICITST.2018.8757924
3. Kubaszewski M, Rejeb A, Rejeb K. Blockchain-based voting: A systematic review. IEEE Access. 2021;9:132707-132723. https://doi.org/10.1109/ACCESS.2021.3113502
4. Kshetri N, Voas J. Blockchain-enabled e-voting. IEEE Softw. 2018;35(4):95-99. https://doi.org/10.1109/MS.2018.2801546
5. McCorry P, Shahandashti SF, Hao F. A smart contract for boardroom voting with maximum voter privacy. In: Grossklags J, Preneel B, editors. Financial

Cryptography and Data Security. Cham: Springer; 2017. p. 357-375. https://doi.org/10.1007/978-3-319-70972-7_20

6. Pilkington M. Blockchain technology: Principles and applications. In: Olleros FX, Zhegu M, editors. Research handbook on digital transformations. Cheltenham: Edward Elgar Publishing; 2016. p. 225-253.
7. Swan M. Blockchain: Blueprint for a new economy. Sebastopol: O'Reilly Media; 2015.
8. Panja S, Paul S, Dutta R, Sau A. A secure end-to-end verifiable e-voting system using blockchain. ICT Express. 2021;7(3):355-361. https://doi.org/10.1016/j.icte.2021.04.003
9. Jafar U, Akram RN, Kiah MLM. A systematic literature review and meta-analysis on blockchain-based electronic voting systems. Appl Sci. 2022;12(20):10342. https://doi.org/10.3390/app122010342
10. Atik MA, Mohammed M. A comprehensive analysis of blockchain-based voting frameworks. ACM Digital Library. 2024. https://doi.org/10.1145/3723178.3723275
11. Berenjestanaki MH, Al-Haddad S. Blockchain-based e-voting systems: A technology review. Electronics. 2023;13(1):17. https://doi.org/10.3390/electronics13010017
12. Ohize HO, Onumanyi AJ, Amuta E, Musa S. Blockchain for securing electronic voting systems: A survey of architectures, trends, solutions, and challenges. Cluster Comput. 2025. https://doi.org/10.1007/s10586-024-04709-8
13. Schultz C. Blockchain-based e-voting implementation through Bitcoin. Horizons J. 2021;8(2):Article 4.
14. Kalyani BJD, Modadugu JK, Neelima S. Blockchain-based decentralized voting system with SHA-256 and facial recognition. Int J Adv Res Comput Sci. 2025;11(3):45-52.
15. Russo A, Fernández Anta A, González Vasco MI, Romano SP. Chirotonia: A scalable and secure e-voting framework based on blockchains and linkable ring signatures. arXiv preprint arXiv:2111.02257. 2021.
16. Bartolucci S, Bernat P, Joseph D. SHARVOT: Secret SHARe-based VOTing on the blockchain. arXiv preprint arXiv:1803.04861. 2018.
17. Onur C, Yurdakul A. ElectAnon: A blockchain-based, anonymous, robust and scalable ranked-choice voting protocol. arXiv preprint arXiv:2204.00057. 2022.
18. Lai WJ, Wu JL. An efficient and effective decentralized anonymous voting system. arXiv preprint arXiv:1804.06674. 2018.
19. Taş E, Tanrıöver C. State of blockchain-based voting research: A conceptual review. Electronics. 2020;9(12):2136. https://doi.org/10.3390/electronics9122136
20. Pawlak K, Ziółkowski C, Nowak A. Challenges in blockchain-based electronic voting: Coercion resistance, security, and auditability. Electronics. 2021;10(15):1836. https://doi.org/10.3390/electronics10151836
21. Huang Y, Li Z, Liu X. Technical innovations in blockchain voting systems: Taxonomy and challenges. Electronics. 2021;10(19):2384. https://doi.org/10.3390/electronics10192384
22. Vladucu R, Iancu B, Marinescu R. Overview of blockchain e-voting systems in practice. Electronics. 2023;12(4):892. https://doi.org/10.3390/electronics12040892
23. Devi R, Bansal A. Security requirements and threats in blockchain-based e-voting systems. J Inf Secur. 2022;13(3):145-156.
24. Benabdallah A, El Kettani A, El Ouahidi B. Comparative analysis of blockchain-based e-voting solutions: Strengths and challenges. Procedia Comput Sci. 2022;198:532-539. https://doi.org/10.1016/j.procs.2021.12.251
25. Ahmad T, Babar MA. Blockchain-based electronic voting systems: Architecture, challenges, and solutions. IEEE Access. 2021;9:17658-17678. https://doi.org/10.1109/ACCESS.2021.3053248
26. Park S, Shin Y. Secure electronic voting system using blockchain in mobile environment. J Inf Process Syst. 2019;15(6):1395-1404.
27. Yue X, Wang H, Jin D, Li M, Jiang W. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. J Med Syst. 2017;41:174. https://doi.org/10.1007/s10916-017-0850-5
28. Zhang L, Xie S. A blockchain-based secure and transparent e-voting system. Security Commun Netw. 2020;2020:8868708. https://doi.org/10.1155/2020/8868708
29. Li H, Guo J, Ma X. Design and implementation of a blockchain-based e-voting system. IEEE Access. 2019;7:172231-172246. https://doi.org/10.1109/ACCESS.2019.2957240
30. Chaudhary A, Mittal R. Blockchain-based online voting system using Ethereum. Procedia Comput Sci. 2021;191:134-141.
31. Noizat P. Blockchain electronic vote. In: Franco P, editor. Blockchain: Blueprint for a new economy. Sebastopol: O'Reilly Media; 2015. p. 141-154.
32. Li Z, Wu Y. An improved blockchain-based e-voting protocol. Future Gener Comput Syst. 2019;96:474-482.
33. Sharma T, Gupta A. Blockchain technology in e-voting: Issues and challenges. Int J Comput Appl. 2020;176(32):35-42.
34. Shukla A, Thakur RS. Review of blockchain-based voting systems. Int J Sci Technol Res. 2020;9(4):1113-1117.
35. Wang H, Zhang Y, Cheng X. Secure and practical e-voting system based on blockchain. IEEE Access. 2018;6:46917-46927.