Statement of Purpose & Research Proposal: Blockchain-Based on the E-Voting System

Najib Mahfuj 22-48248-2 Section :K

1. Statement of Purpose

Electoral integrity faces unprecedented challenges in the digital age, with documented cases of vote manipulation, fake voting, and cyber interference threatening democratic processes globally. This research is project-based, involving the practical development and simulation of a blockchain-based e-voting system to address real-world challenges in electoral integrity, security, and voter anonymity

The proposed research will systematically study how blockchain can stop electoral fraud while meeting strict voting system requirements. The main focus areas include developing strong identity verification to eliminate fake votes, using zero-knowledge proofs for anonymous but verifiable ballots, and creating consensus mechanisms that prevent vote tampering. The system will include smart contracts for automatic vote counting and blockchain's built-in features for clear auditing.

The importance of this research goes beyond just technical innovation; it has wider effects on democracy. By developing a framework that stops vote theft while maintaining electoral secrecy, this work could help rebuild public trust in digital voting systems. Possible uses include national elections and organizational decision-making. It provides a plan for secure and verifiable voting in the digital age.

This research highlights the important link between technology and democracy. It offers practical solutions to protect a key process in society. The suggested blockchain-based system aims to set new standards for electoral integrity. It combines innovative cryptography with a focus on user needs to fight fraud while supporting democratic values.

2. Introduction

In recent years, electronic voting (e-voting) has become a possible way to modernize electoral processes, improve accessibility, and lower costs tied to traditional paper-based voting. However, current e-voting systems encounter serious challenges, such as security weaknesses, a lack of transparency, and risks of tampering or manipulation. Centralized e-voting systems are especially vulnerable to cyberattacks, insider threats, and single points of failure. These issues weaken public trust in electoral results.

With its decentralization, cryptographic security, and immutability, blockchain technology provides a practical option for electronic voting systems. Unlike traditional databases, blockchain spreads voting records across a network of nodes. Without consent, this configuration makes it nearly impossible to make unauthorized changes. Moreover, blockchain enables credible, clear, and auditable voting methods while preserving voter anonymity through homomorphic encryption and zero-knowledge proofs.

This study explores how blockchain could improve the efficiency, transparency, and security of e-voting systems. It explores especially:

1. How practicable is a dispersed, tampering-proof e-voting system.
2. Processes for maintaining auditability while guaranteeing voter privacy.
3. Scalability issues and possible solutions for massive elections.

By addressing these questions, this study contributes to the growing discourse on digital democracy and secure electoral systems.

3. Literature Review

Centralized electronic voting systems still have major problems like data breaches, manipulation, and lack of openness, which erode voter trust. Ainur et al. [1] underline these flaws, observing that centralized systems are still susceptible to trust issues and single points of failure. Emerging as a hopeful substitute, blockchain technology overcomes these difficulties by allowing decentralization, immutability, and cryptographic security.

Many research have shown blockchain's ability to increase transparency and improve e-voting security. Hjalmarsson et al. [12], for instance, proposed a blockchain-based system using smart contracts to automatically count votes while guaranteeing verifiable public ledgers. González et al. [9] also created an enterprise blockchain paradigm using consensus processes to enable safe vote recording and validation, hence lowering possibilities of tampering.

As the public character of blockchains might reveal voter identities, privacy protection continues to be a major issue in blockchain e-voting systems. Employing cryptographic methods, Alshehri et al. [2] and Bendjemaa et al. [4] suggested privacy-aware systems to safeguard voter anonymity without thereby compromising verifiability. As discussed by Benabdallah et al. [3], however, these techniques can introduce computational overhead that might influence real-time usability and scalability.

High transaction volumes in national elections cause ongoing scalability problems. Jayakumar et al. [13] investigated hybrid blockchain designs using cloud infrastructure to boost system throughput and latency. Although not entirely developed, emerging layer-2 technologies and sharding techniques show potential in balancing decentralization, speed, and security [5][6].

Practical deployment challenges exist notwithstanding these advancements. Ohize et al. [18] point out that many blockchain e-voting systems are untested extensively in actual settings like cyberattacks and network failures. Moreover, Mahmood et al. [17] advise integrating intelligent gesture recognition to improve accessibility and security, highlighting the possibility for interdisciplinary developments.

The literature generally shows increasing agreement on blockchain's transformational function in ensuring electronic voting. Still, there are discrepancies in getting completely scalable, privacy-protecting, and user-friendly solutions that resist challenging conditions. To create reliable and inclusive digital democracies, future studies must tackle these obstacles.

4. Research Objective

Main objectives

To develop and assess a blockchain-based e-voting system that increases security, transparency, and scalability while yet protecting voter privacy.

Sub-Objectives

1. To analyze existing blockchain e-voting models and identify their limitations.
2. To develop a hybrid blockchain architecture (public-private) for secure and scalable voting.
3. To integrate privacy-preserving techniques (ZKPs, ring signatures) for anonymous yet verifiable
4. To simulate and test the proposed system's performance under high transaction loads.

5. Research Questions

Primary Research Question

How can blockchain technology be optimized to create a secure, transparent, and scalable e-voting system while ensuring voter privacy?

Sub-Questions

1. What major security weaknesses exist in modern e-voting systems, and how does blockchain help to alleviate them?
2. Will a hybrid blockchain design (combining public and private chains) help national elections scale?
3. How do zero-knowledge proofs (ZKPs) and homomorphic encryption improve voter anonymity without sacrificing auditability?
4. What trade-offs between decentralization, speed, and security exist in blockchain-based e-voting?

6. Proposed Research Methodology

This study will employ a mixed-methods approach combining theoretical modeling, computational simulations, and expert consultations to develop and evaluate a decentralized blockchain-based e-voting system. The methodology is structured to address three core research questions regarding scalability, security, and implementation challenges of partitioned blockchain voting architectures.

For Research Question 1 on scalability improvements, we will design a hierarchical blockchain architecture where the electoral jurisdiction is divided into administrative sub-regions (states/provinces → districts → local polling areas). Each polling area will host a lightweight blockchain node responsible for local vote collection and validation. These nodes will form localized consensus groups using a modified Practical Byzantine Fault Tolerance (PBFT) algorithm optimized for faster block confirmation. To evaluate performance, we will develop discrete-event simulations comparing: (1) traditional centralized e-voting, (2) conventional blockchain voting, and (3) our partitioned model. Key metrics will include transaction throughput (votes processed per second), confirmation latency, and resource utilization under varying voter loads (1,000 to 10 million simulated voters).

To address Research Question 2 concerning security and integrity, we will implement a three-layer cryptographic framework: (1) Zero-Knowledge Proofs for anonymous voter authentication, (2) threshold signatures for distributed key management among election authorities, and (3) Merkle Patricia Tries for efficient vote verification. Security testing will involve: (a) penetration testing using OWASP methodologies, (b) Byzantine node simulations (30% malicious actors), and (c) formal verification of smart contracts using tools like Certora. We will particularly examine resistance to Sybil

attacks through stake-based node identity mechanisms and protection against coercion through time-locked vote re-encryption.

For Research Question 3 on implementation challenges, we will consult three stakeholder groups using the Delphi method: (1) blockchain architects (n=15), (2) election commission officials (n=10), and (3) cybersecurity experts (n=12). The multi-round survey will assess technical feasibility, regulatory compliance, and risk factors with Likert-scale questionnaires and open-ended responses. We will examine physical infrastructure needs through case studies of three areas (urban, semi-urban, rural), looking at factors such as internet access (5G, satellite, or mesh networks) and hardware costs (Raspberry Pi clusters or cloud nodes).

The validation process will use a phased approach. Lab testing with Hyperledger Fabric and Ethereum testnets will be part of phase 1. Pilot distribution will be included in Phase 2 in controlled municipal elections. Phase 3 will concentrate on stress testing with up to one million synthetic voters. Every experiment will use artificial voter databases retaining demographic distributions yet omitting actual personal information. Ethical problems include gaining institutional review board approval, employing GDPR-compliant data handling techniques, and creating an independent audit committee to guarantee the veracity of the results.

This method offers a thorough framework for creating and assessing a workable blockchain e-voting system that takes into consideration real-world execution constraints and addresses the trilemma of scalability, security, and decentralization. With repetitive changes based on simulation findings and expert input, the mixed-methods approach guarantees both technical dependability and operational feasibility.

Ethical Considerations

Developing a blockchain-based e-voting system, this study places top priority on data privacy, confidentiality, and anonymity to uphold ethical integrity. As the study involves simulations, expert conferences, and possibly pilot testing, the following precautions will be taken:

data protection

- **Synthetic Datasets:** There will be no authentic voter information used. Rather, generated datasets will duplicate demographic distributions without revealing any personally identifiable information.
- **Encryption & Secure Storage:** All test data will be encrypted (AES-256) and housed on access-controlled servers. Blockchain testnets will use dummy wallet addresses to prevent traceability.
- **GDPR & Compliance:** Research plans will follow institutional review board (IRB) rules and the General Data Protection Regulation (GDPR). Should pilot testing take place, explicit permission will be sought from subjects.

Confidentiality

- **Role-Based Access Control (RBAC):** Sensitive simulation information will be handled only by authorized researchers. If talking about proprietary systems, election officials and experts consulted will sign non-disclosure agreements (NDAs).
- **Secure Communication:** To stop unwanted interception, expert interviews will employ end-to-end encrypted platforms (Signal, ProtonMail).
- **Anonymized Expert Feedback:** Before analysis to avoid identification, stakeholder responses from surveys will be compiled and anonymized.

Anonymity

- **Zero-Knowledge Proofs (ZKPs)**: Stakeholder reactions from polls will be gathered and anonymized before analysis to prevent detection.
- **Decentralized Identity (DID):** Self-sovereign identity (SSI) models will be applied in test scenarios for voter authentication, thereby removing need for centralized biometric databases.
- **No On-Chain Personal Data:** Ensuring no personally identifiable information (PII) is kept, blockchain records will include just hashed voter IDs and encrypted vote choices.
- Using these methods guarantees privacy-by-design while upholding scientific rigor.

Reference

Ainur, J., Elmira, A., Asset, T., Gulzhan, M., Amangul, T., & Shekerbek, A. (2024). Analysis of research on the implementation of Blockchain technologies in regional electoral processes. *International Journal of Electrical and Computer Engineering (IJECE)*, *14*(3), 2854–2867. https://doi.org/10.11591/ijece.v14i3.pp2854-2867

Alshehri, A., Baza, M., Srivastava, G., Rajeh, W., Alrowaily, M., & Almusali, M. (2023). Privacy-preserving e-voting system supporting score voting using blockchain. *Applied Sciences*, *13*(2), 1096. https://doi.org/10.3390/app13021096

Benabdallah, A., Audras, A., Coudert, L., El Madhoun, N., & Badra, M. (2022). Analysis of blockchain solutions for e-voting: A systematic literature review. *IEEE Access*, *10*, 70746–70759. https://doi.org/10.1109/ACCESS.2022.3187688

Bendjemaa, I., Cherifi, K. I., Benarous, L., & Boudjit, S. (2024). Blockchain-based privacy-aware voting system. *SN Computer Science*, *5*(8). https://doi.org/10.1007/s42979-024-03434-8

Chafiq, T., Azmi, R., & Mohammed, O. (2024). Blockchain-based electronic voting systems: A case study in Morocco. *International Journal of Intelligent Networks*, *5*, 38–48. https://doi.org/10.1016/j.ijin.2024.01.004

Cohen, J. D., & Fischer, M. J. (1985). Robust and verifiable cryptographically secure election scheme. *Annual Symposium on Foundations of Computer Science (Proceedings)*, 372–382. https://doi.org/10.1109/SFCS.1985.2

El Kafhali, S. (2024a). Blockchain-based electronic voting system: Significance and requirements. *Mathematical Problems in Engineering*, *2024*, 1–17. https://doi.org/10.1155/2024/5591147

El Kafhali, S. (2024b). Blockchain-based electronic voting system: Significance and requirements. *Mathematical Problems in Engineering*, *2024*(1), 5591147. https://doi.org/10.1155/2024/5591147

González, C. D., Mena, D. F., Muñoz, A. M., Rojas, O., & Sosa-Gómez, G. (2022). Electronic voting system using an enterprise blockchain. *Applied Sciences*, *12*(2), 531. https://doi.org/10.3390/app12020531

Hajian Berenjestanaki, M., Barzegar, H. R., El Ioini, N., & Pahl, C. (2024a). Blockchain-based e-voting systems: A technology review. *Electronics (Switzerland)*, *13*(1). https://doi.org/10.3390/electronics13010017

Hajian Berenjestanaki, M., Barzegar, H. R., El Ioini, N., & Pahl, C. (2024b). Blockchain-based e-voting systems: A technology review. *Electronics (Switzerland)*, *13*(1). https://doi.org/10.3390/electronics13010017

Hjalmarsson, F. P., Hreioarsson, G. K., Hamdaqa, M., & Hjalmtysson, G. (2018a). Blockchain-based e-voting system. *IEEE International Conference on Cloud Computing (CLOUD)*, *2018*-July, 983–986. https://doi.org/10.1109/CLOUD.2018.00151

Hjalmarsson, F. P., Hreioarsson, G. K., Hamdaqa, M., & Hjalmtysson, G. (2018b). Blockchain-based e-voting system. *IEEE International Conference on Cloud Computing (CLOUD)*, *2018*-July, 983–986. https://doi.org/10.1109/CLOUD.2018.00151

IEEE Xplore. (n.d.). *Full-text PDF*. Retrieved June 27, 2025, from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10061373&utm_source=mendeley&getft_integrator=mendeley

Jafar, U., Aziz, M. J. A., & Shukur, Z. (2021). Blockchain for electronic voting system—Review and open research challenges. *Sensors (Basel, Switzerland)*, *21*(17), 5874. https://doi.org/10.3390/s21175874

Jayakumari, B., Sheeba, S. L., Eapen, M., Anbarasi, J., Ravi, V., Suganya, A., & Jawahar, M. (2024). E-voting system using cloud-based hybrid blockchain technology. *Journal of Safety Science and Resilience*, *5*(1), 102–109. https://doi.org/10.1016/j.jnlssr.2024.01.002

Kranthi Kiran Reddy, G., Vijay Kumar, G., Sirimulla, S. S., Singh, C., Kumar Reddy, C., & Reddy, P. P. S. (2024). Decentralized voting system using blockchain. *International Journal of Scientific Research in Science, Engineering and Technology*, *11*(2), 211–219. https://doi.org/10.32628/IJSRSET2310216

Kshetri, N., & Voas, J. (2019). Supply chain trust. https://doi.org/10.1109/MITP.2019.2895423

Mahmood, W. A., Waleed, J., Abbas, A. R., Alaskar, H., Altulyan, M., & Hussain, A. J. (2024). Intelligent gesture-enhanced blockchain voting: A new era of secure and accessible e-voting. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3468338

Ohize, H. O., Onumanyi, A. J., Umar, B. U., Ajao, L. A., Isah, R. O., Dogo, E. M., Nuhu, B. K., Olaniyi, O. M., Ambafi, J. G., Sheidu, V. B., & Ibrahim, M. M. (2024). Blockchain for securing electronic voting systems: A survey of architectures, trends, solutions, and challenges. *Cluster Computing*, *28*(2), 1–39. https://doi.org/10.1007/s10586-024-04709-8

Peelam, M. S., Kumar, G., Shah, K., & Chamola, V. (2024). DemocracyGuard: Blockchain-based secure voting framework for digital democracy. *Expert Systems*. https://doi.org/10.1111/exsy.13694