



PROJECT REPORT

BLOCKCHAIN-BASED E-VOTING FOR INDONESIA: INTEGRATING ZKP AND PARALLEL DIFFERENTIAL PRIVACY FOR ENHANCED SECURITY AND SCALABILITY

HAIKAL HAIDAR PUTRA
22.K1.0038

Faculty of Computer Science
Soegijapranata Catholic University
2026

ABSTRACT

This research addresses critical privacy, scalability, and trust issues in Indonesia's traditional and blockchain-based e-voting systems, as identified in previous studies such as BP-Vot and Ethereum-based prototypes. Existing solutions often suffer from vulnerabilities like privacy leakage due to single-pivot differential privacy and dependence on third-party authentication tools that risk voter anonymity. To overcome these limitations, this project proposes a new blockchain-based e-voting system. It integrates Zero-Knowledge Proofs (ZKP) for anonymous authentication and parallel differential privacy to protect voting patterns. The entire architecture is implemented on a permissioned Hyperledger Fabric network. The system design includes smart contracts for automating election processes, a ZKP module for eligibility verification without revealing identity, and a parallel differential privacy algorithm that distributes Laplace noise across two pivot candidates (Double Pivot) to significantly increase resistance against reconstruction attacks. The system was evaluated using 10,000 synthetic voter records across multiple testing repetitions with varying privacy budgets ($\epsilon = 0.5, 0.3, \text{ and } 0.1$). The results demonstrate that the proposed approach maintains a highly stable vote count accuracy ranging from 99.38% to 99.87%, while consistently achieving 100% Rank Accuracy. These findings prove that combining ZKP and parallel differential privacy in a permissioned blockchain framework provides a practical, mathematically secure, and highly reliable solution for future e-voting in Indonesia.

Keywords: blockchain e-voting, zero knowledge proof, differential privacy, double pivot, hyperledger fabric, Indonesia