E-Voting App Based on Blockchain

# Abstract

The integrity, transparency, and verifiability of electronic voting (e-voting) systems are critical to the democratic process in digital societies. Traditional systems face numerous challenges including centralized trust models, data manipulation risks, and limited auditability. This paper proposes a secure, scalable e-voting solution grounded in blockchain technology, enhanced by biometric identity verification and public key infrastructure. Drawing on contemporary research, the system architecture ensures immutability, voter anonymity, and end-to-end verifiability. Solutions such as Hyperledger-based private ledgers (Khan et al., 2021), Ethereum smart contracts (Ahmed & Arain, 2020), and decentralized PKI protocols (Al-Bassam, 2017) provide foundational support for robust security and transparency. Furthermore, advances in biometric recognition (Tian et al., 2020) and voter authentication using zero-knowledge proofs (Xia et al., 2021) reinforce privacy-preserving identity validation. The paper reviews cryptographic models, evaluates implementation frameworks, and discusses the applicability of blockchain voting in real-world elections. Our findings advocate for a hybrid biometric-blockchain e-voting model that resists coercion, supports transparency, and strengthens trust in electoral technologies.

# Keywords

Blockchain, E-Voting, Identity Verification, Smart Contracts, Cryptographic Protocols

# 1 Introduction

The digitalization of electoral processes introduces both opportunities and challenges. As modern democracies seek more efficient, secure, and transparent voting systems, blockchain technology emerges as a compelling solution. Its decentralization, immutability, and verifiability directly address key limitations found in traditional electronic voting (e-voting) platforms [1], [2].  
Research has emphasized that existing e-voting systems often suffer from centralized control, vulnerability to manipulation, and a lack of voter-verifiable audit trails [3], [7], [36]. Blockchain technology, with its consensus-based integrity models [24], [17], and smart contracts [21], offers robust alternatives. Several proposals have explored using permissioned or public ledgers to create secure, tamper-resistant vote recording systems [1], [12], [14], [25], [31].  
Biometric authentication mechanisms, including facial recognition and gait analysis, have been proposed as effective means of verifying voter identity while maintaining usability and accessibility [4], [6], [26], [27], [28]. Deep learning and webcam-based solutions have been shown to enhance both security and voter convenience in remote settings [29], [30], [40]. These biometric techniques, when combined with blockchain, offer dual guarantees of authenticity and tamper-evidence [5], [32], [39].  
However, e-voting still faces significant challenges. Issues such as voter coercion, vote-buying prevention, and privacy preservation remain under active investigation [8], [16], [11], [23]. Cryptographic approaches—such as zero-knowledge proofs [9], mix-nets [8], and receipt-free protocols [36]—aim to mitigate these risks while preserving voter anonymity. The integration of decentralized public key infrastructures (PKI) via smart contracts also plays a pivotal role in eliminating centralized certificate authorities [10].  
From a system design perspective, usability and trust are crucial to adoption. Studies show that even well-secured platforms may fail without adequate attention to user interface, transparency, and end-user trust [34], [37], [35]. Estonia's real-world deployment of online voting demonstrates the viability of secure digital elections at national scale [38], although concerns over trust and verification mechanisms remain.  
Identity management and authentication frameworks are equally vital. Blockchain-based ID solutions, when aligned with privacy laws and standards, can support scalable and privacy-aware voting platforms [13], [15], [22]. Moreover, governance frameworks like "Votebook" [12] and platform-specific designs using Ethereum or Hyperledger [2], [25], [31] provide a foundation for secure implementation.  
Despite promising developments, real-world deployment of blockchain-based e-voting systems still requires resolving trade-offs between transparency, privacy, legal compliance, and technical scalability [14], [3], [20]. Furthermore, researchers have begun exploring the role of behavioral economics in shaping voter attitudes toward digital privacy and trust [34].