

Bucharest University of Economic Studies

The Faculty of Economic Cybernetics, Statistics and Informatics

IT&C Security Master

DISSERTATION THESIS

Coordinator

Ph. D. Cristian TOMA

Graduate

Mihail Rareș NEDELCU

Bucharest

2025



Bucharest University of Economic Studies

The Faculty of Economic Cybernetics, Statistics and Informatics

IT&C Security Master

E-VOTING APP BASED ON BLOCKCHAIN

DISSERTATION THESIS

Coordinator

Ph. D. Cristian TOMA

Graduate

Mihail Rareș NEDELCU

Bucharest

2025

Statement regarding the originality of the content

I hereby declare that the results presented in this paper are entirely the result of my own creation unless reference is made to the results of the other authors. I confirm that any material used from other sources (magazines, books, articles, and Internet sites) is clearly referenced in the paper and is indicated in the bibliographic reference list.

Table of Contents

[1. Introduction 5](#_Toc194142656)

# Introduction

Since we were kids, we all wanted to grow and take part to the voting process. It was such a mature action, it seemed like it involved a lot of knowledge and that its power was immense. Now, that we’ve grown, we can clearly see that a vote has immense pressure on us, voters, but also on those who are in charge of the entire organization of the process. Entire institutions must be organized in a way that is as efficient as possible and allows for a seamless voting process. Each voter must be identified and verified for their right to vote, then receive their ballot and stamp so they can go to the booth to choose their favorites. It is a complicated process that requires a lot of organizational skills, time, and human resources.

In contemporary democracies, the public trust in electoral outcomes decreases and people start to really question the existing infrastructure and its credibility. Even though we live in such a digitalized world, the vote counting process has lagged behind. We rely on a lot of people to put in a considerable effort to provide the population with statistics following their votes.

This dissertation investigates the design and implementation of a voter authentication architecture, focusing on how emerging technologies can strengthen democratic processes by mitigating identity fraud end enhancing trust in digital voting.

Blockchain technology has emerged as a viable option for transparent and safe electronic voting systems. E-voting systems can enhance voter anonymity, reduce fraud and manipulation and boost election process trust by utilizing blockchain technology’s decentralization, immutability and transparency. Furthermore, compared to traditional voting methods, blockchain-based electronic voting systems can save money and time.

Conventional voting methods sometimes depend on centralized organizations, which can create weaknesses like election fraud or result manipulation. A potential remedy for the shortcomings of conventional and other e-voting methods is provided by the decentralized and unchangeable characteristics of blockchain technology. It can provide a transparent and impenetrable platform for electronic voting. By combining consensus protocols and cryptographic techniques, blockchain-based electronic voting systems offer safe, verifiable and auditable voting processes.

Traditional paper-based voting procedures are still prone to fraud, human error and inefficiency in many electoral systems, which is why governments and corporate groups are looking into digital alternatives. However, there has been doubt about the reliability of these digital endeavors, especially in the wake of high-profile data integrity problems and cybersecurity attacks. This mistrust emphasizes how important it is to have an electronic voting system that strengthens security measures while also guaranteeing user accessibility. A hopeful remedy for this lack of confidence is blockchain technology, which consists of a series of blocks that use consensus algorithms to permanently record every transaction.

The distributed and append-only features of blockchain are what make it so effective in the electoral setting. Vote tampering is reduced since votes recorded on a blockchain are nearly impossible to change after the fact. Alongside this immutability, blockchain-based systems frequently use cryptographic methods to ensure the secrecy and authenticity of voter data, including hashing and public/private key encryption. However, there are still issues regarding the most effective way to confirm voter IDs prior to allowing people to vote on the blockchain. Thus, authentication becomes a crucial element that guarantees every vote is cast by a legitimate, registered vote. E-voting systems may guarantee that only authorized voters participate in the election process by utilizing sophisticated identity verification and biometric matching techniques.

The urgent necessity to balance the potential of blockchain’s security features with the real-world difficulty of certifying a frequently sizable and diverse electorate is what motivates this research. By automating voter verification, blockchain technology combined with trustworthy authentication can lower administrative expenses, increase public trust in electronic voting and lessen the possibility of fraudulent ballots or duplicate voting. Furthermore, by allowing independent auditors and election officials to confirm results using cryptographic proofs rather that proprietary, opaque software, such a system can promote transparency and traceability.

The inherent benefits of blockchain technology for safe data processing support the choice to base electronic voting on it. Because blockchain is a ledger, the votes that are recorded are protected from tampering, making it impossible for bad actors to change, remove, or falsify records without being discovered. Because it provides an auditable ballot trail that is consistent throughout the network of participating nodes, this feature is essential for maintaining election integrity.

Importantly, the importance of strong authentication techniques is also emphasized in this research. Blockchain can offer consensus-driven validation and maintain data integrity, but it is unable to independently verify a voter’s identity. The validity of blockchain’s unchangeable record is rendered irrelevant if an unauthorized user manages to access the system; the ledger will still record an invalid vote. In order to bridge this gap, the study looks into how blockchain technology can be integrated with biometric or multi-factor authentication systems, providing a comprehensive defense against impersonation and unwanted access. The suggested solution aims to strike a balance between user-friendliness and strict security techniques, such as facial matching and government-issued ID card analysis.

The dissertation uses interdisciplinary insights from identity verification, distributed computing and cryptography in choosing this strategy. The foundation of an electronic voting application might theoretically be other technologies, but blockchain is the only one that combines distributed consensus, transparency and cryptographic security in a way that satisfies the fundamental needs of a democratic election. The strategy aims to provide a reliable system where stakeholders may verify the procedure and the outcomes without depending on the internal records of a central authority when combined with stringent authentication.

This dissertation’s focus is on a thorough analysis of the efficacy and security of a blockchain-based electronic voting system that uses strong user authentication. Although this study’s foundation is informed by earlier research on blockchain applications and digital identity verification, the current study focuses on a single area: maintaining vote integrity in a safe online setting. Thus, the following primary areas are examined in this dissertation.

It begins by examining the theoretical underpinnings and real-world applications of blockchain technology in e-voting contexts, with a focus on the system’s capacity to uphold integrity, transparency and auditability. Second, it discusses how sophisticated user authentication techniques, especially those that use biometric information, might confirm voters’ identities prior to granting them access to the blockchain, reducing the possibility of multiple votes or impersonation by the same person. The study looks into the cryptographic safeguards for identity data as well as the effects incorporating such safeguards into an election process has on user experience.

The dissertation also assesses the system’s performance under normal election loads, emphasizing the ways in which network latency, blockchain throughput and cryptographic calculations affect the viability of widespread deployments. A key component of this work includes security issues, such as handling anonymized data and resilience of denial-of-service assaults. The study evaluates how well a blockchain-based electronic voting system with strict authentication procedures functions in real-world operational scenarios by putting these factors into practice in test or simulated situations.

While nothing that real-world adoption also depends on policy, legal frameworks and public acceptance, the dissertation focuses on conceptual and technical validations of blockchain security and authentication efficacy in defining its limitations. Despite note being the main focus, these social and legal aspects are acknowledged as having a significant impact on future scalability and useful implementation. The ultimate goal of this work is to clarify how e-voting may advance the goal of safe, transparent and reliable elections in the digital age by examining the complexities of blockchain protocols and cutting-edge authentication methods.