International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Secure and Decentralized Algerian E-Voting System Based on Blockchain and NFC

Hanane Echchaoui*[1], Rachid Boudour[1]

Submitted: 01/03/2025 **Revised:** 05/04/2025 **Accepted:** 15/04/2025

Abstract: The democratic process relies on credible and fair elections for decision-making, which are crucial within communities and in modern democratic countries like Algeria. In recent years, electronic voting systems have gained interest for their potential to minimize costs and enhance efficiency and participation. However, widespread adoption is hindered by security and reliability concerns. As smart cities become more prevalent, it is vital to integrate robust security measures within governmental systems to maintain public trust and safety. Incorporating new, reliable technologies such as blockchain, smart contracts, and NFC into the voting process has the potential to make it quicker, more effective, and less susceptible to security vulnerabilities. This paper introduces an innovative electronic voting system leveraging NFC and blockchain technologies to address these challenges. Our approach aims to ensure security, legitimacy, and trust while employing the Algerian biometric and electronic identity card, which has remained unexploited and underutilized since its launch. Preliminary results highlight the system's potential to revolutionize electronic voting, paving the way for more reliable and secure electoral processes.

Keywords: *Biometric Card, Blockchain, Electronic Voting, NFC, Smart Contract*

1. Introduction

The integrity of elections serves as the foundation for effective decision-making within communities and nations. The beginnings of voting trace back to ancient Greece, where it was conducted by counting raised hands and then progressed to punched cards and paper ballots, among other methods [1]. Surprisingly, most nations, including Algeria, still rely on the outdated traditional paper ballot voting system, a process known for its time and resource-intensive nature. It relies on centralized counting, has limited security measures, and depends on third parties. Additionally, it is susceptible to fraud, manipulation, and malfunctions [2]. These inherent drawbacks underscore the pressing need for modernization in the electoral process.

Over the years, electronic voting systems have emerged as a focal point of interest, promising to minimize costs, enhance efficiency, and increase overall voter participation [3]. However, they still face major vulnerabilities, as well as fraud and corruption allegations, due to their lack of transparency, which has prevented their widespread adoption.

To overcome these challenges, the integration of blockchain technology presents a promising solution. By leveraging blockchain, the voting process can become transparent, traceable, and more secure. Several countries have successfully integrated or are in the process of integrating blockchain into their voting systems. Estonia, for example, has successfully integrated blockchain into its voting system, making it verifiable and more secure [4]. Similarly, South Korea and Sierra Leone have made major advances in implementing blockchain-based voting systems, improving the integrity and inclusivity of their electoral processes [4]. These real-world examples demonstrate the viability and effectiveness of blockchain technology in transforming the way elections are conducted.

Another cutting-edge technology, NFC (short for near-field communication), stands out for its numerous advantages—it is user-friendly, secure, open, and standards-based [5]. These qualities position NFC as a compelling choice for integration into electronic voting systems.

In the pursuit of advancing the democratic process, this paper first explores the drawbacks specifically associated with Algeria's traditional elections and addresses issues such as the security and privacy of votes and voters, as well as the speed of the overall process. Then, it aims to combine the benefits and features of blockchain and NFC technologies to establish a secure e-voting system that does not require extensive equipment, infrastructure, or staff, unlike traditional voting systems. Voters will not need a separate electoral card, as the Algerian biometric and electronic identity card facilitates the process. The objective is to implement a strategic plan that enhances public confidence in the electoral process and increases voter participation.

The paper is structured as follows: First, we provide an overview of the two technologies used in the system. Next, we explain the current Algerian voting process and introduce the Algerian biometric and electronic identity card (CNIBE) along with its features. Then, we discuss several related works from the literature. Afterwards, we present the design and features of the proposed system and conclude with future research directions.

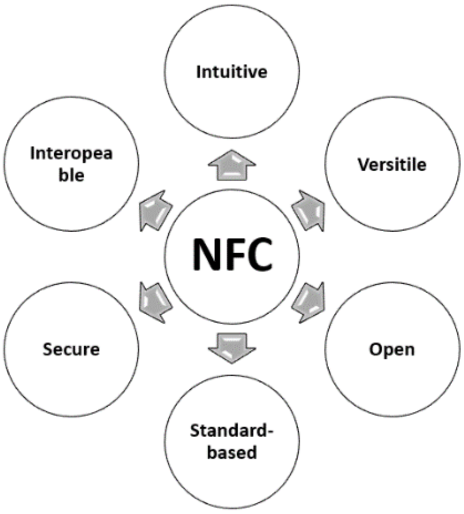
1 Embedded systems laboratory, Badji Mokhtar Annaba University, BO 12 Annaba 23000, Algeria
ORCID ID : 0009-0007-4946-8236
** Corresponding Author Email: hanane.echchaoui@univ-annaba.dz*

2. Background

2.1. NFC

Near-field communication (NFC) is a wireless connectivity technology that allows devices to communicate and transfer data when they are touched or brought within approximately 4 centimetres [6] using magnetic field induction. It is an upgrade to the proximity card standard (RFID), seamlessly combining the functionalities of a smart card and a reader into a single device. The effectiveness and security of NFC have been demonstrated in various applications, as highlighted in the literature [7],[8]. Fig. 1 summarizes the advantages and features of NFC technology.

Fig. 1. NFC features



2.2. Blockchain

The work of Stuart Haber and W. Scott Stornetta on blockchain technology in the early 1990s inspired Satoshi Nakamoto to create Bitcoin, establishing the first decentralized electronic currency system [9].

A blockchain is a chain of interconnected blocks, which gives rise to its name. It operates as a shared ledger across nodes, storing records in blocks where each block is linked to the previous one, forming a secure, immutable, and transparent chain of information. Each block is identified by a hash and contains key data, the previous hash, the current hash, a timestamp, and other information [10].

Aside from decentralization, blockchain technology offers numerous other advantages, such as transparency, immutability, verifiability, security, and reliability. These attributes have piqued the interest of organizations and researchers, leading to the implementation of a wide range of blockchain-based applications across various sectors.

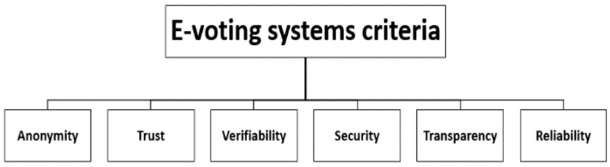
Smart contracts are, by definition, sets of computer code stored on the blockchain network and specify the terms to which all contract parties must agree. The terms of an agreement between two parties are explicitly encoded into a smart contract as lines of code, which then self-executes [11]. Smart contracts aim to facilitate the execution of all types of transactions, not just financial ones.

2.3. Electronic voting

Electronic voting (e-voting) is a system that facilitates elections, records votes, and counts results using electronic means and technologies. Key criteria for an effective e-voting system include anonymity, trust, verifiability, security, transparency, and reliability, as illustrated in Fig. 2.

E-voting systems offer numerous advantages, such as faster election result processing, increased convenience for voters, fraud prevention, and more [12]. However, they also face several challenges and introduce new issues related to security, transparency, and confidentiality [12]. Given its many advantages, blockchain has the potential to address some of these issues and enable a secure, trustworthy e-voting system.

Fig. 2. E-voting criteria



2.4. The voting process in Algeria and its challenges

According to the official website of the Algerian Independent National Electoral Authority, the voting process in Algeria is preceded by voter registration, during which eligible Algerian citizens (18 or older, among other conditions) must register to participate in the election. During this step, they receive a voter card, that they must present on the day of the election [13].

After the election announcement, voting stations open nationwide to the public. Citizens are identified using their national ID card or any other official document proving their identity, after which they cast their ballot into a secure box. The vote is manually validated by their fingerprint in the presence of voting office members [14]. After polling stations close, election officials proceed to count the votes and announce the results.

Table 1 outlines the problems associated with each step of the Algerian voting process.

Table 1. Voting step and problem associated with it

The voting step	The problem
Voter registration	- The requirement for a separate voter card can be burdensome for the citizen and involves additional costs in terms of resources and paper.
Election day	- Paper ballots require Substantial resources in terms of the use of paper, transportation, secure storage and allocation of personnel.
Vote counting	- Manual counting is tedious, time-consuming and prone to human error. It also requires a significant number of personnel for the actual count and the security aspect. - The announcement of election results is often delayed.

2.5. The Algerian National Electronic Biometric Identity Card

Introduced in 2016, the Algerian national electronic biometric identity card is at the cutting edge of technology. It incorporates powerful security features that make it tamper-proof. It is equipped with two microprocessors that store the owner's personal information and support a unique National Identification Number (NIN).

It complies with current international standards, particularly regarding personal data security, as follows:

- Physical security is enhanced with a polycarbonate card body, which is protected by visual security elements and the Sealys Window anti-fraud device [15]. Polycarbonate documents are recognized for their strong security and longevity.
- Logical security is based on the Sealys ID Motion multi-

service operating system, the world's first to obtain a Common Criteria certification, including EAL7-level assurances, which represent the highest level of security assurance in the international security evaluation system [15].

- Biometrics: The Sealys BioPIN device is equipped with Match-on-Card technology for fingerprint authentication, allowing for local verification of fingerprints in high-security identification cases.

2.6. Related work

NFC, biometrics, and blockchain have been, and continue to be, used to implement more efficient electronic voting systems.

To run fair and successful elections, Prakasha et al. [16] presented a voting system that uses a two-step verification with fingerprint and iris recognition to eliminate duplicated votes. The use of such biometric technologies can increase system security, but it can also introduce limitations in terms of compatibility and hardware requirements. For instance, using the Hough transform and AlexNet CNN for iris recognition can raise accuracy issues because effectiveness may vary depending on multiple factors, including image quality. In an attempt to address the problems associated with the voting system in Iraq, Jumaa et al. introduced a blockchain-based e-voting system that incorporates face recognition and fingerprint for voters' authentication with a user-friendly mobile application for vote casting [17]. The ECC algorithm was used for vote encryption to ensure the utmost security. After a security and time-efficiency analysis, the system is believed to provide security, enhance speed, and reduce time and cost. Al-Maaitah et al. used the Hyperledger fabric platform and Raft consensus protocol to create a robust blockchain voting system to tackle some of the challenges in Jordan's voting system [18]. The proposed system achieves satisfactory performances in terms of latency, throughput, and response time after analysis, showcasing improved speed and overall efficiency. Both papers [17] and [18] presented systems that must handle a large-scale election, which means managing a high volume of transactions and a large number of voters, potentially leading to scalability and performance problems. With a focus on trust, fairness, privacy and efficiency, Golnarian et al. presented a novel decentralized remote voting system that minimizes reliance on third parties after the preparation phase. Authorities provide citizens with an identification card containing their unique private key before the elections. The authors emphasize that the system is a trustless scheme for large-scale elections that prevents coercion and provides verifiability and allows voters to cast their votes for free in a practical way [19]. The paper acknowledges the need for further research to design a reputation model for delegation servers and to develop a practical time-lock encryption scheme to improve the proposed system. Another blockchain-based e-voting system designed specifically for Turkey was proposed by Bulut et al. in [20] that uses the DPos consensus algorithm. The system architecture does not rely on a single blockchain but is structured into several levels to improve scalability, latency, and synchronization issues. The implementation of the proposed solution is required for performance and validation evaluation to support the claims of a trusted, secure, and fast voting system. Blockchain was also used by Tripathy and Das in [21] to present a novel e-voting system that addresses the voting issues in India. The promising results open the possibility of extending the work and customizing existing ATMs that are already equipped with CCTV cameras and security guards, so people can conveniently cast their votes at nearby banks, reducing government expenses. However, this may disrupt the normal functioning of ATMs, which could lead to dissatisfaction among users who need to withdraw money during the voting process. Finally, Zamir et al. developed a biometric-based Electronic Voting Machine (EVM) that uses fingerprints for voter registration [22]. This integration effectively eliminates the risks of impersonation, forgery, and tampering, thereby improving the reliability and security of the voting process. However, further research is needed to ensure the system's resilience against attacks and to preserve voters' privacy while using their biometric information. Related work discussed above is summarized in Table 2.

Table 2. Related work

Reference	Contribution	Limitations
[16]	Voting system based on Fingerprint and iris recognition	- Accuracy concerns - Hardware requirements - Database Management
[17]	Remote e-voting system based on blockchain and biometrics for voter authentication	- Scalability and performance
[18]	Blockchain-based e-voting system using Hyperledger fabric platform and RAFT consensus algorithm.	- Scalability and performance
[19]	Remote and decentralised e-voting system based on blockchain.	- In-person authentication - Scalability - Reputation Model and Time-lock Encryption
[20]	blockchain-based e-voting system that uses the DPos consensus algorithm designed specifically for Turkey	- Implementation - Lack of empirical evidence
[21]	Blockchain-based e-voting system that uses ATMs as voting stations.	- Lack of empirical evidence - Limiting ATM access
[22]	Biometric-based Electronic Voting Machine that uses fingerprints for registration.	- Security and privacy concerns.

3. Method

The proposed system introduces an innovative e-voting mechanism based on blockchain and NFC technologies, designed for efficiency and security. The system architecture, shown in Fig 3. is designed to ensure security and efficiency. It integrates multiple essential components, each with distinct functionalities to fulfil their roles and interact with the system:

3.1. Client-side

A voter-friendly interface for registration and authentication, developed as a Java desktop application, along with an intuitive and easy-to-use web page for voters to cast their votes—all accessible at the polling stations.

An admin interface that allows administrators to manage elections and candidates.

3.2. Server-side

A registration system that manages voter registration using identity cards and ensures that only eligible voters are registered.
An authentication system that ensures that only authorized voters can access the voting pages via secure NFC mechanisms.
The voting system facilitates the voting process and ensures that votes are cast securely and accurately while protecting voters' data.

3.3. Database

A secure voter database designed to safeguard sensitive voter details, ensuring their integrity and safety.

3.4. Security measures

Blockchain services are used to record votes, guaranteeing transparent and immutable elections while adding a new level of security. Blockchain guarantees that recorded votes are resistant to any alteration or modification.
NFC-based authentication ensures secure, fast voter verification using their identity cards which guarantees protected and safe authentication and reduces the risks of unauthorized access.
Advanced authentication and authorization protocols restrict system access to verified users only, reinforcing overall security.

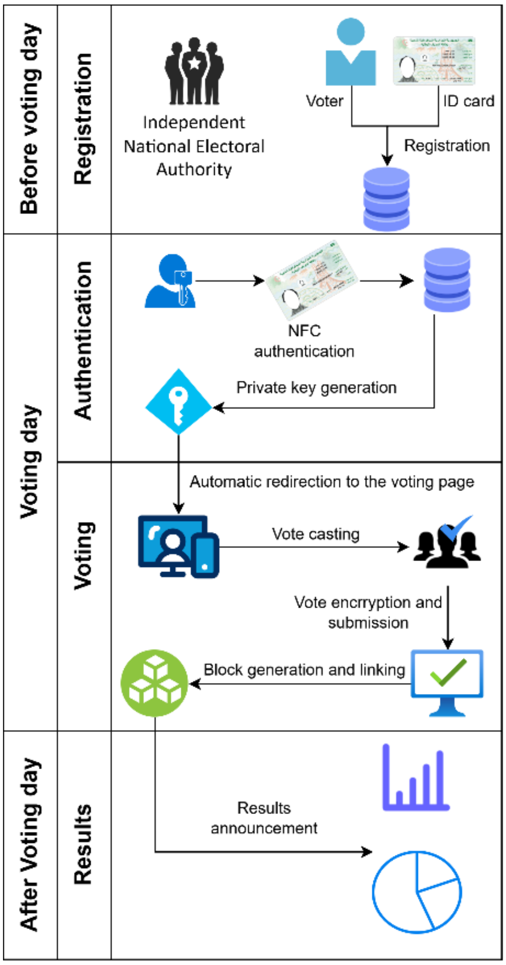


Fig. 3. System architecture

The use case diagram in Fig. 4 illustrates the interactions and functionalities of the two main actors: the voter and the administrator.

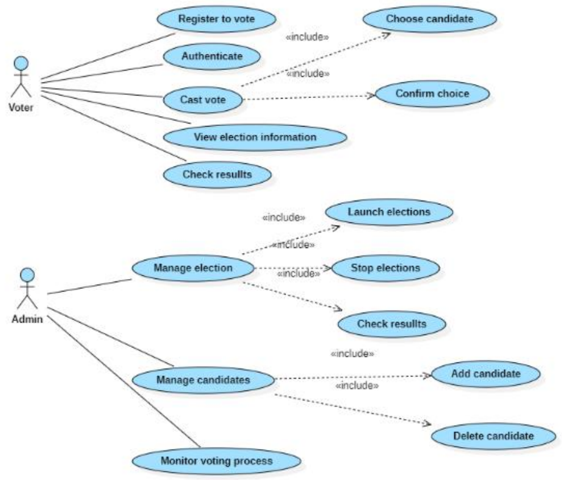


Fig. 4. Use case diagram

The class diagram shown in Fig. 5 illustrates the key components and their relationships within the proposed system, which aims to provide secure, efficient, and user-friendly voting through the integration of modern technologies.
The two main stakeholders identified in the diagram are as follows:
The Voter class represents individuals eligible to participate in the elections. The Voter class includes attributes such as a voter ID and name, as well as methods for registration, authentication, and voting.
The Admin class is responsible for managing elections within the system. It also controls functions such as starting and stopping elections, managing candidates, and overseeing the results.

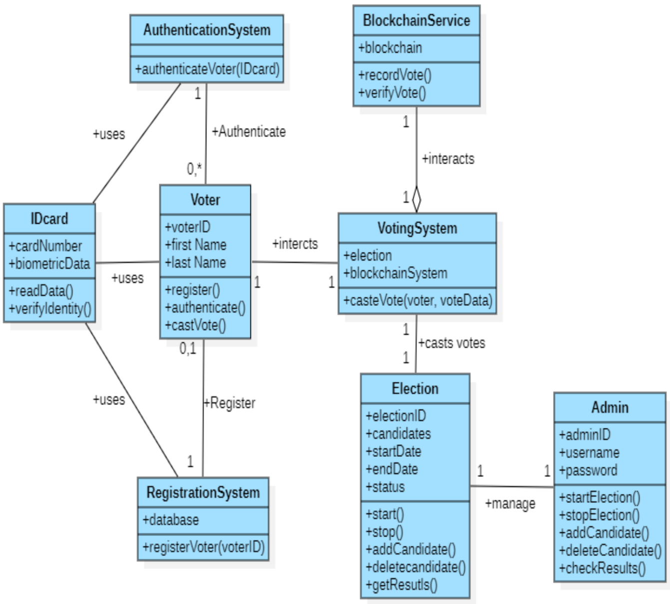


Fig. 5. Class diagram

4. Results

The system was set up and run on a Windows 10-enabled PC, equipped with an Intel(R) Core™ i5-4200M CPU @ 2.50GHz processor and 6 GB of RAM. The results show that the implemented system is secure and more efficient than the traditional Algerian voting system. It addresses the issues and challenges discussed in Section 2 and summarized in Table 1.

4.1. Registration

The registration stage of the voting process is implemented as a Java application at the polling station, as shown in Fig. 6. A staff member verifies the identity of the voter. The voter places their identity card on the NFC card reader, specifically the ACR1281U-C1 model. For additional verification, the voter must also enter their first and last names. The unique CNIBE ID number is securely retrieved, and the voter is then registered in the system's database.

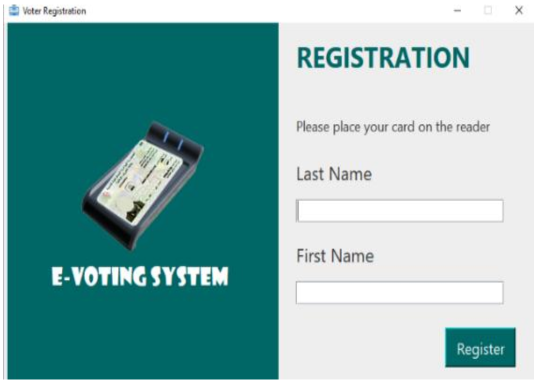


Fig. 6. Registration interface

4.2. Authentication

The authentication process is also implemented as a Java desktop application as shown in Fig. 7. In this stage, the voter places their CNIBE card on the same reader. The staff member verifies their identity and, upon successful verification of their information in the registered database, the voter is automatically redirected to the voting page.

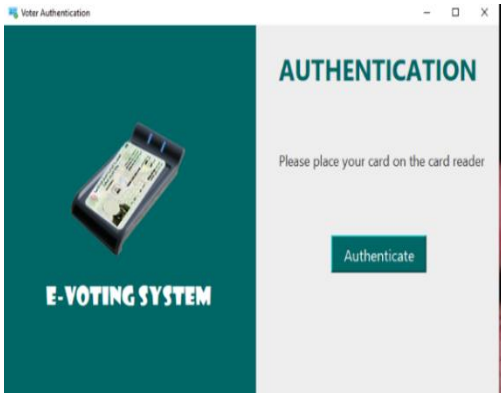


Fig. 7. Authentication interface

4.3. Voting

Once the voter is automatically redirected to the voting web page illustrated in Fig. 8, a list of candidates is presented to them. The voter makes their choice, casts their vote, and confirms it. Real-time results are displayed on the same page. The vote is transferred to the Ethereum blockchain, where it is saved as an immutable block that cannot be altered. The hash value is computed using the SHA-256 algorithm, and the mining and generation of voting blocks are carried out using a proof-of-work algorithm.

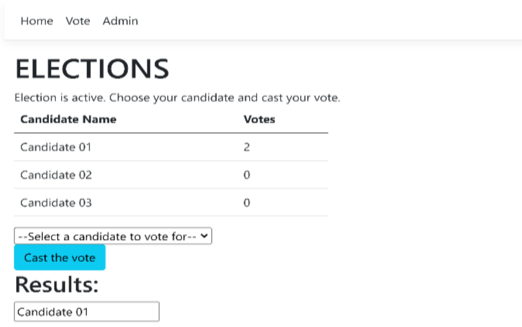


Fig. 8. Voting web page

4.4. Voting results

The voting results are calculated progressively and automatically according to Eq. 1, where xij represents the vote weight given by voter Vj to the candidate Ci, and n is the total number of voters.

$$\sum_{j=1}^{n} x_{ij} \quad (1)$$

The results are announced immediately after the polling stations close. This contrasts with the traditional method, in which votes are manually counted by a large number of staff, a process prone to human error due to its tedious and lengthy nature. The results are announced, as shown in Fig. 9.

Fig. 9. Voting results

5. Discussion

5.1. E-voting criteria analysis

The developed e-voting system addresses the e-voting criteria mentioned in Section 2. Anonymity is ensured because blockchain records votes without revealing voters' identities. Trust and transparency are established through the decentralized nature of blockchain. Security is guaranteed with the use of both technologies: blockchain protects against block tampering, and NFC ensures secure authentication. Lastly, both technologies ensure reliability, offering a robust and resilient system.

5.2. Time analysis

To compare the voting durations of a voter with and without the electronic voting system, we examined several different stages of both the traditional voting process and the e-voting process.

5.2.1. Traditional voting process

Arrival and registration: the voter arrives at the polling station and presents their card after possibly waiting in line. Officials verify their presence on the station's voters list.

Identity verification: the voter presents a piece of identification for

verification.
Distribution of ballots: the officials hand the paper ballot to the voter.
Entry into the voting booth: the voter goes to the booth to choose their candidate.
Ballot submission signature and exit: the voter signs the register to attest to their vote and leaves the station.

5.2.2. The Blockchain and NFC-based e-voting system

Arrival: the voter arrives at the polling station.
Identity verification: the voter identifies themselves by simply placing their identity card on the NFC reader.
Access to the voting interface: if access is granted, the voter is automatically referred to the voting interface.
Candidate selection: the voter makes their choice and selects their candidate.
Vote confirmation: the voter confirms their choice.
Vote recording: the vote is recorded electronically and automatically using blockchain.
Disconnection and exit: the voter disconnects and leaves the station.

5.2.3. Duration comparison

Table 3. summarizes the comparison of voting duration between the traditional voting process and the proposed system across different stages of the process.

Table 3. Voting duration comparison

Stage / System	Traditional system (estimated)	E-voting system (estimated)	Blockchain and NFC E-voting system
Arrival and registration	Few minutes	Few minutes	Few minutes
Identity verification	1-2 minutes	Instantaneous to a few minutes	Instantaneous to 1 minute
Issuance of ballot vs. access to interface	1 minute	Instantaneous to one minute	Instantaneous to 1 minute
Booth entry vs. candidate selection	3-5 minutes	2-4 minutes	2-4 minutes
Ballot submission vs. vote confirmation	1-2 minutes	1-2 minutes	1-1.5 minutes
Signature and exit vs. disconnection and exit	1 minute	A few seconds to 1 minute	Few seconds
Total	10-14 minutes	7.5-12 minutes	7.5-11 minutes

The blockchain and NFC-based e-voting system can reduce the total voting duration by 2 to 4 minutes per voter compared to the traditional method. This reduction, illustrated in Fig. 10 is due to the simplification of the overall process and the elimination of ballots and papers. It is necessary to note that voters' familiarity with the new system can affect the outcome. The more familiar voters are with it, the better the efficiency and effectiveness.

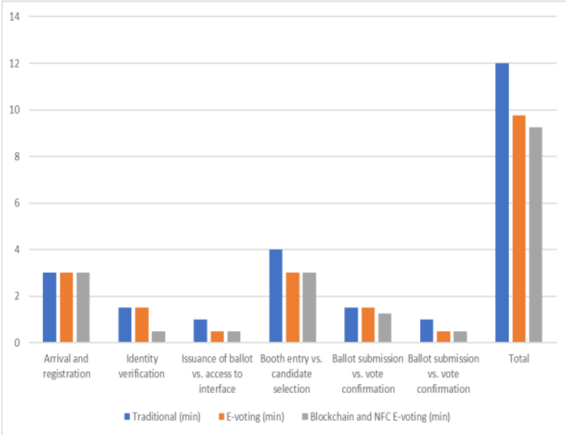


Fig. 10. Voting duration comparison

6. Conclusion and future work

Traditional voting systems that rely on a single central entity to count votes slow down the voting process and make the results less trustworthy. This resulted in the development of electronic voting systems, which aim to address these issues. Despite numerous advancements in the field, electronic voting remains relatively unexplored. Existing e-voting systems face various challenges that hinder their use. We proposed an electronic voting system based on cutting-edge technologies: blockchain and NFC. Blockchain technology is used to create a secure and dependable e-voting system. NFC adds a security layer to the authentication phase by securely delivering the voter's ID to the system and utilizing the otherwise unexploited Algerian biometric identity card. Our experimental results demonstrate significant improvements in security, efficiency, and time savings. Future work includes enhancing the registration and authentication stages by replacing in-person identity verification with biometric methods, such as face recognition or fingerprint scanning. Additionally, considering the optional ID card emulation on mobile phones can offer voters more flexibility. Furthermore, exploring scalability solutions will be crucial for accommodating large voting populations. Moving forward, these additions aim to further enhance the security, reliability, and effectiveness of the overall system. Ensuring the security of these systems within governmental and social frameworks is crucial as smart cities become more prevalent.

References

[1] V. Agate, A. De Paola, P. Ferraro, G. L. Re, and M. Morana, "SecureBallot: A secure open source e-voting system," *J. Netw. Comput. Appl.*, vol. 191, Art. no. 103165, 2021. [Online]. Available: https://doi.org/10.1016/j.jnca.2021.103165

[2] S. Al-Maaitah, M. Qatawneh, and A. Quzmar, "E-voting system based on blockchain technology: A survey," in *Proc. Int. Conf. Inf. Technol. (ICIT)*, Amman, Jordan, 2021, pp. 200–205. [Online]. Available: https://doi.org/10.1109/ICIT52682.2021.9491734

[3] H. Echchaoui, R. Roumaissa, and R. Boudour, "A proposal of blockchain and NFC-based electronic voting system," in *Adv. Comput. Tech. Renew. Energy Syst. (IC-AIRES)*, vol. 591, Lecture

Notes in Networks and Systems, M. Hatti, Ed. Cham, Switzerland: Springer, 2022, pp. 66–75. [Online]. Available: https://doi.org/10.1007/978-3-031-21216-1_7
[4] M. Pawlak, J. Guziur, and A. Poniszewska-Marańda, “Towards the blockchain technology for system voting process,” in *Cyberspace Saf. Secur. (CSS)*, Amalfi, Italy, 2018, pp. 209–223. [Online]. Available: https://doi.org/10.1007/978-3-030-01689-0_17
[5] R. Iqbal, A. Ahmad, and A. Gilani, “NFC based inventory control system for secure and efficient communication,” *Comput. Eng. Appl. J.*, vol. 3, no. 1, pp. 23–33. [Online]. Available: https://doi.org/10.18495/COMENGAPP.V3I1.50
[6] K. Ok, V. Coskun, and M. N. Aydin, “Usability of mobile voting with NFC technology,” in *Proc. IASTED Int. Conf. Softw. Eng.*, Innsbruck, Austria, 2010, pp. 16–18. [Online]. Available: https://doi.org/10.2316/P.2010.677-087
[7] D. Mahansaria and U. K. Roy, “Secure authentication for ATM transactions using NFC technology,” in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Chennai, India, 2019, pp. 1–5. [Online]. Available: https://doi.org/10.1109/CCST.2019.8888427
[8] S. S. Ahamad, “A novel NFC-based secure protocol for merchant transactions,” *IEEE Access*, vol. 10, pp. 1905–1920, 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3139065
[9] S. Nakamoto, “A peer-to-peer electronic cash system.” [Online]. Available: https://bitcoin.org/en/bitcoin-paper [Accessed: May 14, 2024]
[10] H. Echchaoui, A. Ferdenache, and R. Boudour, “Introduction to cybersecurity applications in blockchain technology,” in *Build. Cybersecur. Appl. Blockchain Smart Contracts*, E. N. Editor, D. I. Editor, and B. E. Editor, Eds. Cham, Switzerland: Springer, 2024, pp. 3–28. [Online]. Available: https://doi.org/10.1007/978-3-031-50733-5_1
[11] B. K. Mohanta, S. S. Panda, and D. Jena, “An overview of smart contract and use cases in blockchain technology,” in *Proc. 9th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Bengaluru, India, 2018, pp. 1–4. [Online]. Available: https://doi.org/10.1109/ICCCNT.2018.8494045
[12] C. Avgerou, S. Masiero, and A. Poulymenakou, “Trusting e-voting amid experiences of electoral malpractice: The case of Indian elections,” *J. Inf. Technol.*, vol. 34, no. 3, pp. 263–289, 2019. [Online]. Available: https://doi.org/10.1177/0268396218816199
[13] “كيفية التسجيل.” [Online]. Available: https://ina-elections.dz/%D9%83%D9%8A%D9%81%D9%8A%D8%A9_%D8%A7%D9%84%D8%AA%D8%B3%D8%AC%D9%8A%D9%84/ [Accessed: May 14, 2024]
[14] “كيف أنتخب.” [Online]. Available: https://ina-elections.dz/%D9%83%D9%8A%D9%81-%D8%A3%D9%86%D8%AA%D8%AE%D8%A8/ [Accessed: May 14, 2024]
[15] “La Carte Nationale d’Identité Biométrique et Electronique algérienne: lancement réussi.” [Online]. Available: https://www.thalesgroup.com/fr/europe/france/dis/gouvernement/etudes-de-cas/carte-nationale-identite-algerie [Accessed: May 14, 2024]
[16] V. R. Prakash, V. Aditya, N. Anilkumarreddy, and K. Srikanth, “Fingerprint and iris based secured voting machine using MATLAB,” in *AIP Conf. Proc.*, Tamil Nadu, India, 2022, vol. 2452, no. 1. [Online]. Available: https://doi.org/10.1063/5.0116501
[17] M. H. Jumaa and A. C. Shakir, “Iraqi e-voting system based on smart contract using private blockchain technology,” *Informatica*, vol. 46, no. 6, pp. 87–94, 2022. [Online]. Available: https://doi.org/10.31449/inf.v46i6.4241
[18] S. Al-Maaitah, A. Quzmar, and M. Qatawneh, “Blockchain-based e-voting system for election in Jordan,” *J. Theor. Appl. Inf. Technol.*, vol. 100, no. 5, 2022. [Online]. Available: https://www.jatit.org/volumes/Vol100No5/31Vol100No5.pdf [Accessed: May 14, 2024]
[19] D. Golnarian, K. Saedi, and B. Bahrak, “A decentralized and trustless e-voting system based on blockchain technology,” in *Proc. 27th Int. Comput. Conf., Comput. Soc. Iran (CSICC)*, Tehran, Iran, 2022, pp. 1–7. [Online]. Available: https://doi.org/10.1109/CSICC55295.2022.9780507
[20] R. Bulut, A. Kantarcı, S. Keskin, and Ş. Bahtiyar, “Blockchain-based electronic voting system for elections in Turkey,” in *Proc. 4th Int. Conf. Comput. Sci. Eng. (UBMK)*, Samsun, Turkey, 2019, pp. 183–188. [Online]. Available: https://doi.org/10.1109/UBMK.2019.8907102
[21] A. K. Tripathy and T. K. Das, “Advanced e-voting system using blockchain,” in *Proc. 3rd Int. Conf. Intell. Comput. Instrum. Control Technol. (ICICICT)*, Kannur, India, 2022, pp. 9–13. [Online]. Available: https://doi.org/10.1109/ICICICT54557.2022.9917830
[22] M. A. Zamir, D. A. Khan, and M. S. Umar, “Secure electronic voting machine using biometric authentication,” in *Proc. 9th Int. Conf. Comput. Sustain. Glob. Dev. (INDIACom)*, New Delhi, India, Mar. 2022. [Online]. Available: https://doi.org/10.23919/INDIACom54597.2022.9763202