

Blockchain-based e-voting system in a university

Adil Marouan¹, Morad Badrani¹, Nabil Kannouf², Abderrahim Zannou³, Abdelaziz Chetouani¹

¹LaMAO Laboratory, ENCG, Mohamed First University, Oujda, Morocco

²LSA Laboratory, ENSA, Abdelmalek Essaadi University, Tetouan, Morocco

³ERCI2A, FSTH, Abdelmalek Essaadi University Sciences, Tetouan, Morocco

Article Info

Article history:

Received Jan 16, 2024

Revised Feb 19, 2024

Accepted Mar 4, 2024

Keywords:

Authentication

Blockchain

Digital signature

E-voting

Security

ABSTRACT

The blockchain-based electronic voting (e-voting) system, offers universities a safe, easy-to-use platform that enhances accuracy and integrity. Despite that, it is challenging to integrate the blockchain-based e-voting system with current platforms and private data. Managing latency is another requirement during the blockchain transactions (votes/elections). In this work, we suggested a novel system that uses smart contracts on the consortium blockchain to address these constraints. The voters and electors in a university can vote and elect respecting the rules established in smart contracts. The miners validate transactions using proof of work (PoW) and proof of stake (PoS). Data integrity and voter validity are ensured via the SHA-256 hash algorithm and the ECDSA signature. The implementation results demonstrate that the suggested method works better than the state-of-the-art. exceeds the state-of-the-art in terms of gas cost and execution time.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Adil Marouan

LaMAO Laboratory, ENCG, Mohamed First University

Oujda, Morocco

Email: adil.marouan@ump.ac.ma

1. INTRODUCTION

Several globally renowned educational institutions, including the University of Edinburgh (Scotland), the University of Surrey (England), the University of Canberra (Australia), and the University of Toronto (Canada), have explored or adopted electronic voting systems for various purposes such as student government elections, faculty decisions, and academic council meetings. However, the Moroccan electoral system remains rooted in traditional methods, primarily relying on paper ballots and manual vote counting [1]. Blockchain technology [2] has drawn a lot of interest since it is a new, disruptive, and promising technology. It entails building many chains of successive transaction blocks. In this manner, every block is encrypted and impossible for anyone to decipher without agreement. Numerous advantages are provided by it, including dependability, precision, cost savings, autonomy, and redundancy. Although blockchain technology is frequently linked to e-voting because of its potential for security and transparency, not all e-voting platforms make use of it [3]. Centralized databases and encryption are essential components of many conventional electronic voting systems. Here are several instances of blockchain free electronic voting platforms: Clear Ballot, Scytl, and Smartmatic. These platforms have a number of noteworthy flaws and drawbacks, including a lack of transparency, problems with audibility and accessibility, challenges with voter identification and privacy, cost and upkeep [4].

In this study, we design and develop a unique and efficient decentralized voting system that promotes anonymity, transparency, and self-taling features. By storing all communications on the Ethereum blockchain and protecting each voter's privacy with an incredibly powerful ring signing technique, we guarantee the voting process's transparency. The most significant feature of our system is that it can continue

to self-tally results, removing the requirement for a reliable third party to do so. We also verify the efficiency of the system by looking at the amount of Ethereum gas needed for each voter. Our method is unique in two ways: first, we provide a platform that uses a public blockchain and a consortium blockchain (Ethereum) to enable remote voting for representative elections while producing results that are automatically generated to reduce the possibility of fraud or errors. This article's remaining sections are organized as follows: The proposed method is presented in section 2, the simulation results are discussed in section 3, and the final paper is concluded and future work is presented in section 4.

2. METHOD

This section outlines a novel use of blockchain technology in an e-voting system. The system is intended to function as a safe platform for voting by university staff. As indicated in the introduction, several factors, such as security, confidentiality, execution time, and gas cost, could influence this system. The main uniqueness of our system is that it takes care of all criteria.

2.1. System overview

Our project's objective is to use blockchain technology to develop an effective mechanism for evaluating problems with the e-voting system while accounting for the main flaws found in earlier research. We provide a summary of the main elements and crucial procedures in our recommended e-voting system below. Universities are groups of buildings that accommodate staff university. Furthermore, administrators can be linked with either establishments or the university itself. The institution drives innovation, upholds ethical standards, and raises awareness, all of which play a major part in the blockchain network for e-voting systems. It leads the way in research, creates safe blockchain protocols, ensures the fairness of elections, and informs interested parties about the revolutionary possibilities of blockchain technology, encouraging involvement and trust in the scholarly community.

People who identify as universality participants register on the blockchain and become voters or electors. Their participation guarantees an accountable and decentralized voting system in which each registered voter has a digital identity that can be verified. By means of blockchain technology, administrators work to mold the democratic future of their university, cultivating a climate of confidence, diversity, and responsible digital citizenship. Elections within the educational institution are revolutionized as the establishment works in tandem with academics and students to build a strong e-voting ecosystem.

The following is a procedure for introducing blockchain -based e-voting in college elections:

- Entities and functions: The system revolves around three main entities: university, establishment, and staff administrators. Each university contains multiple establishments, with each establishment comprising students, professors, and the possibility of administrators being part of either an establishment or the entire university. Specific system requirements encompass diverse vote types and essential functionalities like user authentication and vote confidentiality.
- Blockchain implementation: In this e-voting system, a consortium blockchain serves as the foundational network infrastructure. This blockchain is the key technology driving the entire e-voting system, providing transparency, security, and trust among the involved entities. Integration of blockchain ensures the realization of these critical aspects within the system. Leading blockchain platforms facilitating consortium blockchain creation encompass Hyperledger Fabric, R3 Corda, and Quorum (an Ethereum-based platform) [4], [5].

These platforms provide tailored tools for constructing and managing consortium blockchain networks. Our implementation specifically employs the Ethereum platform.

- Smart contract implementation: our developed smart contracts establish the rules for voting, encompassing identity verification [6], [7] vote recording, and result calculation. These self-executing contracts, embedded in the blockchain with predefined rules, ensure the smooth and secure execution of various aspects of the e-voting. The consortium blockchain, along with these smart contracts, is pivotal in ensuring the integrity and reliability of the e-voting system.
- User interface optimization: a user-friendly interface has been crafted for participants, including staff administrators, facilitating easy and intuitive voting. Prioritizing security and user-friendliness, this interface ensures a seamless and secure user experience. The registration process is designed to be user-friendly, collecting and verifying participant identities through a secure interface. blockchain is employed to store verified identities, ensuring data integrity and preventing unauthorized access.
- Security measures: Our system is fortified against potential threats, such as attacks and fraud, incorporating encryption mechanisms, secure authentication protocols, and regular code audits. Robust API authentication and secure communication are ensured through the use of tokens and keys between the

web interface and blockchain nodes. Digital signatures, employing Keccak-256 and ECDSA algorithms [8] authenticate transactions and data sent from the university server, ensuring sender authenticity and data integrity [9]. Consistent superior performance of the ECDSA algorithm, in terms of speed and efficiency, led to its selection over ECDSA.

- Consortium node configuration: The setup involves authorized staff administrators, actively participating in the consensus process. Nodes, representing authorized participants, include staff administrators [10]. Miners, a subset of nodes, validate transactions and create new blocks in the blockchain using either proof of work (PoW) [11] or proof of stake (PoS) [12]. In our implementation, both PoW, and PoS mechanisms are utilized.
- E-voting system deployment and integration: The blockchain-based e-voting system [13] is deployed and seamlessly integrated into the university environment, utilizing a cloud service, as illustrated in Figure 1.

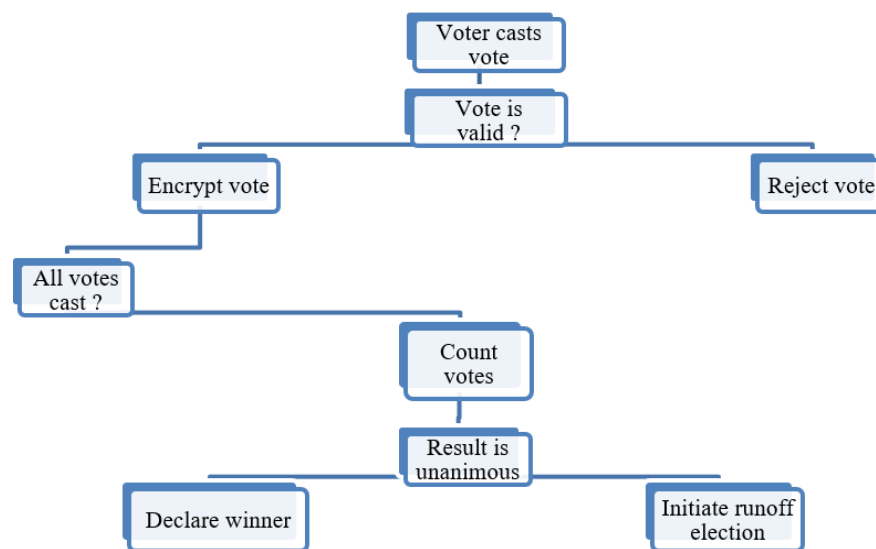


Figure 1. The flowchart that shows the crucial steps in the voting procedure

2.2. Consortium

We develop the Ethereum blockchain system for use in universities, using Consortium as our private blockchain solution in particular. Using this strategy, institutions-including different organizations like institutes, faculties, and schools-are connected. Every establishment uses the consortium platform to run its own private blockchain [14]. The choice of Consortium is motivated by its ability to provide a secure environment, crucial for restricted access. Only students affiliated with the respective institute are authorized users of the voting platform [15]. This decision ensures a clear student count, guaranteeing that only eligible individuals participate in the voting process. Consortium technology has been selected as the chosen consensus mechanism, wherein each voting process leads to an increment in the count of votes for the selected candidate. An encrypted transaction is appended to the consortium's blockchain, recording both the voter's choice and the user's identity. Despite the encryption, the data allows for the verification of whether an individual has cast their vote, and the authority for verification lies solely with the voter.

Public/private key pairs are used in a security protocol employed [16]. Every transaction is encrypted using the user's private and public keys, which are connected to the consortium blockchain's administrative node [17]. The administrator's private key and the user's public key are needed for decryption in order to be verified. The institute's management gains access to a tailored portal, simplifying data gathering and departmental results block mining on the consortium blockchain. This portal also integrates with the university's Ethereum platform.

2.3. Signature and hash

Implementing an e-voting system within a university demands meticulous attention to technical details, with the integration of a signature component being pivotal for enhancing security and authenticity [18]. A comprehensive plan for this integration involves prioritizing secure user authentication methods, including multi-factor authentication through SMS, email, or authentication apps, and verifying users before

allowing access to the e-voting system. Digital signatures play a crucial role, ensuring the integrity and authenticity of votes through unique key pairs for each user [19]. This involves a confidential private key for generating digital signatures and a publicly shared key for verification.

It is essential to ensure secure transmission, which involves encrypting all communications between the user's device and the e-voting server to prevent unauthorized access and tampering with data during transmission [20]. The consideration of secure web-based communication protocols, such as HTTPS, adds an additional layer of protection. Ensuring tamper-proof storage involves storing votes and signatures in a database or ledger, and blockchain technology presents a promising application due to its immutability and transparency. Regular auditing and monitoring of the database are essential for identifying and addressing any indications of suspicious activity.

In tandem with these measures, the implementation of an audit trail system is incorporated to log all activities within the e-voting system, providing a means to identify and investigate any anomalies or potential security breaches [21]. Moreover, the university's e-voting system employs cryptographic hash functions to bolster security and integrity [22]. This includes ensuring ballot integrity through the computation of cryptographic hashes, timestamping each vote to prevent retroactive changes, and implementing verification processes conducted by election officials. Privacy preservation is addressed by hashing ballot data in a manner that makes it computationally challenging to reverse and determine voter choices. Secure storage practices, including encryption and access control measures, are applied to voting data, ensuring protection against unauthorized access and tampering. The use of cryptographic hash functions creates a chain of custody for voting data, emphasizing established standards like SHA-256 for data security within the university's e-voting systems [23].

2.4. Consensus

Choosing the right consensus method is a critical aspect of implementing a secure and reliable electronic voting system within a university setting. Ethereum's versatile blockchain technology serves as the foundation, allowing the development of self-executing contracts (SCs) that efficiently manage the entire voting process from registration to the final vote count. The university's unique requirements dictate the selection of a suitable consensus mechanism, and options like PoW or a custom consensus mechanism are considered. Each has its advantages, with PoW being a well-established mechanism that validates transactions based on computational resources.

Voter authentication [24] is a paramount consideration to ensure the integrity of the voting process. Robust authentication methods, utilizing university-issued credentials and implementing multi-factor authentication, help secure the system against unauthorized access. Balancing transparency and privacy are achieved by leveraging techniques like zero-knowledge proofs or confidential transactions, which protect voter anonymity while recording transactions on the blockchain for transparency. The implementation of rigorous security measures, including secure handling of private keys, regular audits, and encryption of sensitive data, is crucial to guard against potential hacking and fraud.

In addition to technical considerations, the development of a user-friendly interface is paramount for a successful e-voting system. Ensuring accessibility and intuitiveness for all participants students, faculty, and administrators contributes to the overall effectiveness of the system. Designing the system for auditability allows for independent verification of election results, enhancing transparency and building trust in the voting process. The scalability of the system is also vital, especially in universities with a large number of potential voters, where the transition to Ethereum 2.0's PoS [12] mechanism may offer improved scalability and energy efficiency. Compliance with legal and regulatory requirements ensures that the e-voting system aligns with national and local laws related to elections and data privacy [25]. Thorough testing and user education further contribute to a smooth and successful deployment of the e-voting system within the university environment.

3. RESULTS AND DISCUSSION

3.1. Gas cost analysis

At an estimated gas price of 1 Gwei, the setup cost for an election administrator overseeing 83 voters is 0.0869 ether, while each voter incurs a cost of 0.124 ether. The overall expenditure, influenced by factors like contract reusability and the necessity for the voting administrator to upload time points and public key lists, appears relatively high given the current ether price.

To analyze cost fluctuations corresponding to the number of voters, ten experiments were carried out. The cost distribution, depicted in Figure 2, indicates that while the expenses associated with installing the election administrator remain constant, the costs related to downloading information and public keys

exhibit a linear increase in tandem with the total number of voters. Consequently, the overall cost incurred by the election administrator demonstrates a linear relationship with the number of voters.

For individual voters, the number of information uploads and the cost associated with ballot verification through a linkable ring signature exhibit linear connections to the total number of voters. The cost of sub-secret uploads remains constant. Overall, the cost for each entity demonstrates a nearly linear correlation with the total number of voters.

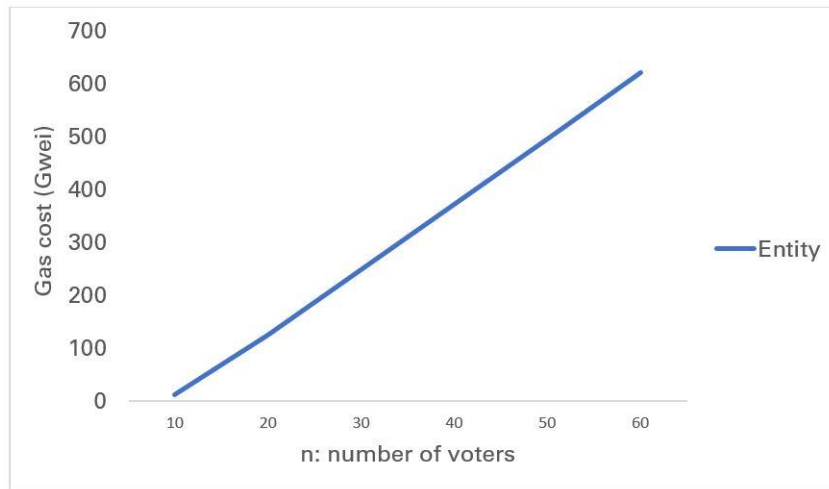


Figure 2. Gas expenses for individual entities

3.2. Time analysis

As shown in Figure 3, the time consumption can be evaluated by examining the length of time needed to finish each blockchain transaction. The system’s response time is shown in Figure 3(a), which shows a discernible increase as the number of voters and votes increases. According to its computational capability, the blockchain instructs each node to reply, in accordance with the decentralization tenet on which it was founded. Given that scalability makes up 60%, the blockchain’s size increases proportionately with the number of voters and votes cast.

Response times gradually increase as more nodes line up in the miners. Adaptive consensus techniques are used to overcome this difficulty and guarantee that the chain’s efficiency is continuously scalable. This is still the case even in the event that scalability increases by 60% and the total number of voters involved in the process increases, as Figure 3(b) illustrates.

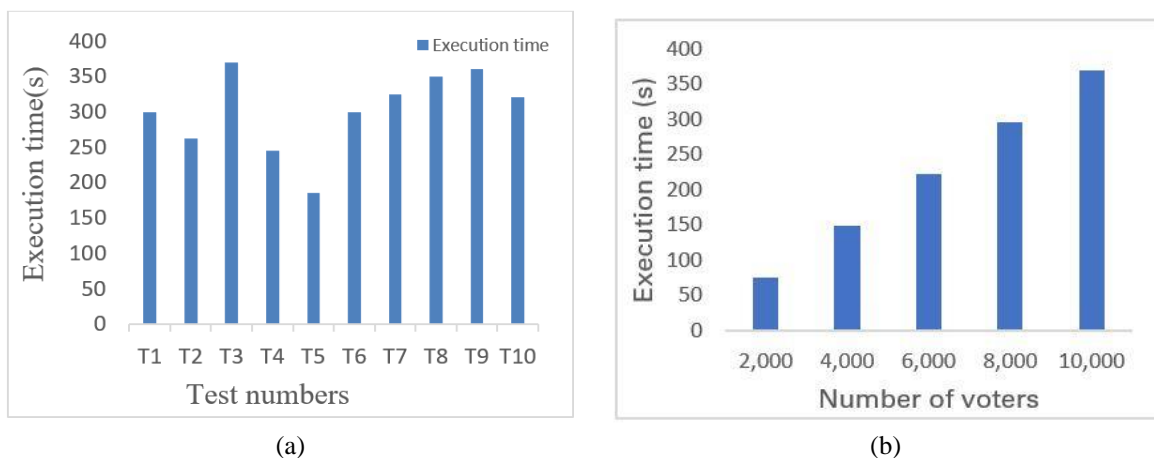


Figure 3. Execution time based on the quantity of (a) tests numbers and (b) the number of voters

3.3. Comparative analysis

A comprehensive analysis of test execution times is outlined in Table 1, providing a detailed summary for each test in both methodologies. The “Test number” column identifies individual tests, and the “Execution time” columns present the time taken in seconds for both our innovative approach involving 83 voters and the method employed by Llanos *et al.* [26]. In this study, we conduct a comparative examination of test execution times, assessing the performance of two methods: our innovative approach with 83 voters and the method by Llanos *et al.* with the same voter count. The objective is to elucidate the relationship between the number of voters and execution times, aiming to enhance efficiency and scalability. Llanos *et al.* [26] vs. our approach (83 voters): our approach showcases a significant improvement in execution time compared to Llanos *et al.* [26] in scenarios involving 83 voters. These efficiency gains suggest that our approach is more optimized and performs better in this specific voter count setting.

Table 1. Comparison between Llanos *et al.* [26] approach and our approach

Test number	Execution time	
	Llanos <i>et al.</i> [26] (83 voters)	Our approach (83 voters)
1	25	10
2	30	8.59
3	28	12.28
4	26	8.13
5	30	6.14
6	29	10
7	27	10.59
8	28	11.52
9	29	12
10	27	10.52
Average	27,9	10.077
Average/Numbers of voters	0.33	0.12

3.4. Discussion

Incorporating a blockchain-based e-voting system with existing platforms and securing private data poses significant challenges. Another issue is managing latency during blockchain transactions, particularly concerning votes or elections (scalability). Additionally, it's crucial to minimize the gas cost fee required for each transaction to enhance efficiency and overall usability.

Our analysis of the blockchain-based election system shows a rise in response time with increased voters and votes, with scalability contributing 60% to this effect. The decentralized blockchain adjusts its size as participants grow, enhancing scalability and engagement by 60%. Despite escalating response times with more nodes, adaptive consensus techniques mitigate efficiency and scalability issues. Notably, at a gas price of 1 Gwei, deployment costs for an administrator overseeing 83 voters are 0.0869 ether, while individual voters incur 0.124 ether each. However, the overall expenditure, influenced by factors like contract reusability and administrator duties, appears relatively high, correlating almost linearly with total voter count at the current ether price. As mentioned in sub-section 3.3, we obtained the time execution is fewer than Llanos *et al.* [26], due to in our case, we design a smart contract that consider the managing the voters and voters. Our system delegate certain computations and verifications to off-chain processes, which can reduce the burden on the blockchain network and decrease response time.

The e-voting system-based blockchain being autonomous pieces of code, is dependent to human error during development, potentially leading to coding flaws that consume an amou. Additionally, external factors such as software bugs or attacks could compromise the security and reliability of smart contracts. Furthermore, the complexity of SC interactions may introduce unforeseen consequences. Ensuring the integrity of e-voting systems requires thorough testing, audits, and ongoing monitoring to mitigate these risks and maintain trust in the electoral process.

To ensure the effectiveness of blockchain-based e-voting systems, it is imperative to investigate advanced methods such as parallel computing. Additionally, optimizing user experience through mobile interfaces can effectively address scalability issues, particularly during peak voting periods. Moreover, exploring legal frameworks, integrating with existing university systems. While this discussion emphasizes security and reliability, specific details on input time execution and gas cost in blockchain transactions provide a more comprehensive evaluation of the system's efficiency and cost-effectiveness.

Our study focuses on the nuances of a blockchain-based e-voting system in a university. Addressing gaps in previous research, we find that response times increase slowly with the increased number of voters participation. Cost analysis indicates challenges, emphasizing the need for optimization, based that, the future

research should prioritize advanced security, user experience, and legal frameworks for effective university e-voting systems.

4. CONCLUSION

In this study, we developed an e-voting system characterized by transparency, decentralization, and anonymity. This system simplifies the voter interaction process, reducing the reliance on participant trust. Moreover, it incurs only Ethereum gas costs per voter by providing all participants with identical information stored on the Ethereum blockchain, ensuring election transparency. The system mitigates the risk of a single point of failure by preserving the independence of each ballot during the counting process. Through a comparison of two methods based on average vote execution time, we have concluded that our method demonstrates efficient scalability with minimal influence on execution time as the number of votes grows, maintaining a low ratio of 0.06.

In addition to university elections, our system is applicable to national elections in our country, enhancing the efficiency of the electoral process. Moreover, it can be utilized in regional elections, simplifying the process of choosing city council members, mayors, or regional representatives, offering voters a convenient voting method. In future research, our focus will be on enhancing the user-friendliness and accessibility of e-voting systems for a broader demographic, including individuals with disabilities or those with limited technological literacy.





REFERENCES

- [1] T. Habibu, K. Sharif, and S. Nicholas, "Design and implementation of electronic voting system," *International Journal of Computer and Organization Trends*, vol. 7, no. 4, pp. 1–6, Aug. 2017, doi: 10.14445/22492593/ijcot-v45p301.
- [2] A. Marouan, M. Badrani, N. Kannouf, and A. Chetouani, "Empowering education: leveraging blockchain for secure credentials and lifelong learning," *Blockchain Transformations: Navigating the Decentralized Protocols Era*. Cham: Springer Nature Switzerland, 2024, pp. 1–14.
- [3] A. Marouan, M. Badrani, N. Kannouf, K. El Makkaoui, and A. Chetouani, "Elliptic curve cryptography signing algorithms behind blockchain 2.0," in *ACM International Conference Proceeding Series*, May 2023, pp. 1–6, doi: 10.1145/3607720.3607747.
- [4] M. Pawlak and A. Poniżewska-Marańda, "Implementation of auditable blockchain voting system with hyperledger fabric," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12742 LNCS, 2021, pp. 642–655.
- [5] P. Zheng, Q. Xu, Z. Zheng, Z. Zhou, Y. Yan, and H. Zhang, "Meepo: sharded consortium blockchain," in *Proceedings-International Conference on Data Engineering*, Apr. 2021, vol. 2021-April, pp. 1847–1852, doi: 10.1109/ICDE51399.2021.00165.
- [6] S. Abed, R. Jaffal, B. J. Mohd, and M. Al-Shayegi, "An analysis and evaluation of lightweight hash functions for blockchain-based IoT devices," *Cluster Computing*, vol. 24, no. 4, pp. 3065–3084, Dec. 2021, doi: 10.1007/s10586-021-03324-1.
- [7] L. Zhang, M. Peng, W. Wang, Z. Jin, Y. Su, and H. Chen, "Secure and efficient data storage and sharing scheme for blockchain-based mobile-edge computing," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 10, Oct. 2021, doi: 10.1002/ett.4315.
- [8] A. Dolmeta, M. Martina, and G. Masera, "Comparative study of keccak SHA-3 implementations," *Cryptography*, vol. 7, no. 4, p. 60, Nov. 2023, doi: 10.3390/cryptography7040060.
- [9] S. Pal, A. Dorri, and R. Jurdak, "Blockchain for IoT access control: recent trends and future research directions," *Journal of Network and Computer Applications*, vol. 203, Jul. 2022, doi: 10.1016/j.jnca.2022.103371.
- [10] Q. Aini, N. Azizah, R. Salam, N. P. L. Santoso, and S. Millah, "iLearning education based on gamification blockchain," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 26, no. 1, pp. 531–538, Apr. 2022, doi: 10.11591/ijeecs.v26.i1.pp531-538.
- [11] W. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han, and C. Su, "Blockchain-based reliable and efficient certificateless signature for IIoT devices," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 10, pp. 7059–7067, Oct. 2022, doi: 10.1109/TII.2021.3084753.
- [12] S. Fahim, S. K. Rahman, and S. Mahmood, "Blockchain: a comparative study of consensus algorithms PoW, PoS, PoA, PoV," *International Journal of Mathematical Sciences and Computing*, vol. 9, no. 3, pp. 46–57, Aug. 2023, doi: 10.5815/ijmsc.2023.03.04.
- [13] W. Gao, L. Chen, C. Rong, K. Liang, X. Zheng, and J. Yu, "Security analysis and improvement of a redactable consortium blockchain for industrial internet-of-things," *Computer Journal*, vol. 65, no. 9, pp. 2430–2438, Sep. 2022, doi: 10.1093/comjnl/bxab080.
- [14] M. P. McBee and C. Wilcox, "Blockchain technology: principles and applications in medical imaging," *Journal of Digital Imaging*, vol. 33, no. 3, pp. 726–734, Jun. 2020, doi: 10.1007/s10278-019-00310-3.
- [15] M. Bhagwat, J. C. Shah, A. Bilimoria, P. Parkar, and D. Patel, "Blockchain to improve academic governance," in *Proceedings of CONECCCT 2020-6th IEEE International Conference on Electronics, Computing and Communication Technologies*, Jul. 2020, pp. 1–5, doi: 10.1109/CONECCCT50063.2020.9198665.
- [16] N. Kannouf, M. Labbi, M. Benabdellah, and A. Azizi, "Security of information exchange between readers and tags," in *Security and Privacy in Smart Sensor Networks*, 2018, pp. 368–396.
- [17] M. Poblet, D. W. E. Allen, O. Konashevych, A. M. Lane, and C. A. D. Valdivia, "From athens to the blockchain: oracles for digital democracy," *Frontiers in Blockchain*, vol. 3, Sep. 2020, doi: 10.3389/fbloc.2020.575662.
- [18] U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for electronic voting system-review and open research challenges," *Sensors*, vol. 21, no. 17, Aug. 2021, doi: 10.3390/s21175874.
- [19] B. Fraunholz and C. Unnithan, "Does e-governance facilitate citizen empowerment in democracies? A critical discourse analysis," *International Journal of Electronic Governance*, vol. 2, no. 2–3, pp. 131–155, 2009, doi: 10.1504/IJEG.2009.029126.





- [20] S. Panja and B. Roy, "A secure end-to-end verifiable e-voting system using blockchain and cloud server," *Journal of Information Security and Applications*, vol. 59, Jun. 2021, doi: 10.1016/j.jisa.2021.102815.
- [21] A. Hambouz, Y. Shaheen, A. Manna, M. Al-Fayoumi, and S. Tedmori, "Achieving data integrity and confidentiality using image steganography and hashing techniques," in *2019 2nd International Conference on New Trends in Computing Sciences, ICTCS 2019-Proceedings*, Oct. 2019, pp. 1–6, doi: 10.1109/ICTCS.2019.8923060.
- [22] M. A. Al-Shareeda, M. A. Saare, and S. Manickam, "The blockchain internet of things: review, opportunities, challenges, and recommendations," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 31, no. 3, pp. 1673–1683, Sep. 2023, doi: 10.11591/ijeecs.v31.i3.pp1673-1683.
- [23] T. Zhou, Y. Zhu, N. Jing, T. Nan, W. Li, and B. Peng, "Reliable SoC design and implementation of SHA-3-HMAC algorithm with attack protection," in *Proceedings-2020 IEEE International Conference on Smart Cloud, SmartCloud 2020*, Nov. 2020, pp. 88–93, doi: 10.1109/SmartCloud49737.2020.00025.
- [24] M. Woda and Z. Huzaini, "A proposal to use elliptical curves to secure the block in e-voting system based on blockchain mechanism," *International Conference on Dependability and Complex Systems. Cham: Springer International Publishing*, pp. 466–476, 2021.
- [25] I. Nazeeh, T. H. Hadi, Z. Q. Mohammed, S. T. Ahmed, and Q. K. Kadhim, "Optimizing blockchain technology using a data sharing model," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 29, no. 1, pp. 431–440, Jan. 2023, doi: 10.11591/ijeecs.v29.i1.pp431-440.
- [26] J. Llanos, W. Coral, A. Alarcon, J. Cruz, and J. Ramirez, "Electronic voting system for universities in Colombia," in *ICINCO 2019-Proceedings of the 16th International Conference on Informatics in Control, Automation and Robotics*, 2019, vol. 1, pp. 325–332, doi: 10.5220/0007929103250332.

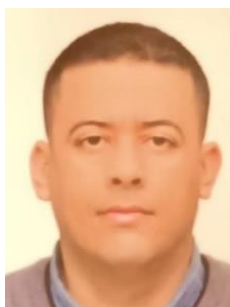
BIOGRAPHIES OF AUTHORS







Adil Marouan     is a Ph.D. student currently affiliated with the Applied Mathematics Laboratory of the Oriental (LaMAO) at ENCG Oujda. His research focus centers around Blockchain Technology for Education. Actively engaged in academic pursuits, Marouan has made significant contributions to conferences such as the 6th International Conference on Networks, Intelligent Systems, and Security (NISS23) and the 4th International Conference on Intelligent Systems and Advanced Computing Sciences (ISACS'23). Furthermore, he has authored a chapter in the book titled "Blockchain Transformations: Navigating the Era of Decentralized Protocols." These experiences have not only enhanced his perspective but also facilitated his involvement with the latest developments in his field. At Mohammed Premier University (U.M.P), Marouan's academic journey is marked by a Master's Specialization in Computer Engineering (M.2.I) from the Faculty of Sciences in Oujda (F.S.O). Prior to this, he earned a fundamental degree in Mathematical Sciences and Computer Science (S.M.I). His diverse educational background reflects his commitment to advancing his knowledge and skills in the realm of information technology and engineering. He can be contacted at email: adil.marouan@ump.ac.ma.







Morad Badrani     is a Ph.D. student in computer science at the LaMAO Laboratory, ORAS team, ENCG, Mohammed First University in Oujda, Morocco. His research focuses on the application of machine learning and deep learning algorithms to resolve some problems in the education field. With a master's degree in information engineering from Abdelmalik Essadi University in Tetouan in 2013, Badrani has a solid foundation in the field. His research interests include data science, machine learning, deep learning, and blockchain. Morad is dedicated to exploring the potential of these technologies to drive innovation and make a positive impact in the field of education. He can be contacted at email: m.badrani@ump.ac.ma.







Nabil Kannouf     is a computer science professor with a Ph.D. in Computer Sciences. He earned his master's in computer engineering in 2010 from the Faculty of Sciences, University of Mohammed Premier, Oujda, Morocco. Since 2020, he has been working as a professor of computer science at Abdelmalek Essaidi University, Morocco. Nabil has authored and published more than 10 research papers. He can be contacted at email: nabil.kannouf@gmail.com.



Abderrahim Zannou     is a professor of Computer Science at the University of Abdelmalek Essaadi University, Tetouan, Morocco. He received Ph.D. degree in computer science in Internet of Things with the LISAC Laboratory, Sidi Med Ben Abdellah University, Fez, Morocco. Dr. Abderrahim ZANNOU has published in international reputed journals and conferences. Additionally, he has played roles as a reviewer for scientific journals and has been a part of the program committee for various conferences. His research interests include internet of things, blockchain, artificial intelligence, and meta-heuristic algorithms. He can be contacted at email: a.zannou@uae.ac.ma.



Abdelaziz Chetouani     born on May 10, 1973, in Oujda, Morocco, is an accomplished academic and researcher. He earned his Bachelor's degree in Applied Mathematics from the Department of Mathematics at the Faculty of Sciences, Mohamed I University, Oujda, in 1995. Subsequently, he pursued a Master's degree in Applied Mathematics from the same institution in 1997. In 2003, he completed his Doctorate in Numerical Methods of Nonlinear Parabolic Problems with Nonlocal Boundary Conditions and Applications at the Faculty of Sciences, Mohamed I University, Oujda. Currently holding the position of Professor in the Department of CTAM at ENCGO, Mohamed I University, Oujda, since 2007, Abdelaziz Chetouani's research interests span Numerical Analysis, Artificial Intelligence, and Biomathematics. With a notable academic record, he has authored 19 papers and 2 theses. Additionally, Abdelaziz is an active member of scientific organizations, including CIMPA (2019, 2022), CIMAM (2022), and ROSA (2022). He can be contacted at email: a.chetouani@ump.ac.ma.