Automatic check of electoral eligibility

François BEKPON[1,*,†], Tahirou DJARA[1,†], Abdou-Aziz SOBABE[1,‡] and Matine OUSMANE[1,‡]

[1]Laboratoire d'Electrotechnique de Télécommunication et d'Informatique Appliquée - LETIA, University of Abomey-Calavi, Abomey-Calavi, Benin

Abstract

The establishment of a reliable, inclusive and legitimate eligibility list is a prerequisite for the success of any democratic electoral process. Otherwise, the resulting problems jeopardize peace and development at the level of associations, organizations and nations. In this paper, we propose a blockchain-based system for automatic electoral eligibility checking without any paper usage. The system uses Restful APIs to collect real-time data from identified transactional databases and stores them in the blockchain. For any election, the system will produce the list of eligible candidates as well as the reliable and legitimate list of voters. The establishment of a reliable, inclusive and legitimate eligibility list is a prerequisite for the success of any democratic electoral process. Otherwise, the ensuing problems jeopardize peace and development at the level of associations, organizations and nations.

Keywords

Blockchain, eligibility, paperless election, smart contract

1. Introduction

Nations are investing heavily in the organization of elections, particularly in the phases of setting up a permanent, computerized electoral roll. This electoral list is used to determine the eligibility of voters. As far as candidates are concerned, the establishment of this list is becoming more rigorous and restrictive. Generally speaking, to achieve this, election management bodies organize a census of the population eligible to vote in each type of election. Depending on the means, technologies and tools used, the data collected is processed over a relatively long period of time, often containing errors and omissions. Often, census operations are marred by lost or omitted data, necessitating repetition in some places. The various documents collected (birth certificates, identity papers, etc.) are difficult to handle in their physical form. The information collected is therefore entered, analyzed and validated in computer systems designed for this purpose. However, shortcomings in the physical census process impact on the reliability of the analyses carried out and the accuracy of the data. These problems are acute in our African nations, despite the will of our leaders and their commitment to finding a lasting solution accepted by all.

Implementing an inclusive electoral roll using this traditional approach involves a number of challenges: the challenge of data integrity, the challenge of coercion by interested parties, the challenge of IT security, the challenge of data accessibility, the challenge of personal data protection, the challenge of verifiability, and so on. In most cases, the architecture of the IT systems implemented is based on regional databases or a centralized database. In the first scenario, this would pose the problem of centralizing regional data in order to produce national statistics. In the second scenario, the centralized architecture is prone to distributed denial of service (DDoS) attacks. When it comes to electoral processes, trust is the fundamental foundation on which any successful IT system should be built. Faced with these challenges, and given the importance of elections for the peace, tranquility and development of nations, it seems legitimate to opt for trustworthy technological choices. These technologies must offer the potential to build solutions that guarantee and maintain trust at all levels.

In the last ten years, characterized by rapid technological progress, the concept of trust has evolved considerably, taking deep roots in the digital domain [1]. These technological advances are gradually leading communities to embrace digital transformation for robust, resilient and scalable solutions.

Blockchain is a disruptive technology. As its understanding develops, its use cases extend beyond payment processing and money transmission, to data sharing, supply chains, power systems, healthcare systems, etc. [2].

The aim of this article is to use blockchain to set up a framework for automatically checking eligibility for an election. For the remainder of the work, in point II, related work in the field of using blockchain for electoral systems will be presented, in particular, the eligibility check phase. At point III, the proposed system will be presented in all its details. Point IV is devoted to the results obtained and discussions, and lastly, the conclusion of the article in point V.

2. Related Works

The report of the election of the members of the National Assembly of 2023 in the Republic of Benin [3] presents some ”slippages” during the elections. Difficulties arose from the late submission of files, creating a peak of work and stress for the staff of the Autonomous National Electoral Commission (CENA). The report recommended the use of an electronic declaration system (e-Declaration) for candidacies, and the modernization of the process. The report also highlighted ”the lack of precision as to whether or not the death rate applied by the Agence Nationale d'Identification des Personnes (ANIP) should be taken into account in determining the participation rate”. The e-Declaration system is designed to receive applications without going through a processing phase to obtain a list of eligible candidates.

Chafiq et al. [1] implement a hybrid voting system between remote and on-site voting to accommodate all Moroccan voters. This is a two-layer system: firstly, Distributed Permission Ledger Technology (DPLT), which verifies and validates the voting data received, and secondly the Solana blockchain, which receives the data after verification and renders it immutable. However, this system relies on a pre-

Cotonou'24: Conférence Internationale des Technologies de l'Information et de la Communication de l'ANSALB, June 27–28, 2024, Cotonou, BENIN

[*] Corresponding author.

[†] These authors contributed equally.

[‡] These authors contributed equally.

sgoother@yahoo.fr (F. BEKPON)
0009-0003-3635-9074 (F. BEKPON)

established list of candidates and voters whose criteria are unknown.

Jayakumari et al. [4] have proposed a system that reduces the authentication delay, vote tampering, response time, lack of reliability, flexibility, transparency, security and monetary efficiency that are common problems with many electronic voting systems. They are implementing a cloud-based system leveraging a hybrid blockchain to solve the issues raised.

However, the proposed solution is based on pre-established eligibility for both voters and candidates.

Panja & Roy [5] implement an end-to-end verifiable electronic voting system with blockchain and a cloud server to prevent ballot box stuffing attacks, and improve voter confidence in the vote count. This solution takes into account the verification of voter eligibility, to ensure that once registered in the system, the voter can only cast a single vote, verifiable both during the voting and the counting phases.

However, speaking of eligibility, the system merely checks that the user actually possesses the identity he or she claims to hold, and that this identity is eligible for a vote.

Yang et al. [6] propose a blockchain-based protocol for score-based voting, publicly verifiable by any user. In addition to the mechanisms inherent in blockchain technology, they combine cryptographic tools such as ElGamal encryption, group encryption and ZKP (Zero Knowledge Proof) so that each user can carry out the tally once the election has been completed, without revealing individual votes.

When initialized, this protocol is based on a pre-established list of candidates, and relies on a supposedly honest registration authority for voter registration.

Jaiswal et al. [7]propose the E-Voting system using Blockchain and taking into account confidentiality, transparency and verifiability. This voting system uses an electoral list.

Ahn [8] has implemented a voting system based on Ethereum blockchain technology for the prevention of fraudulent voting, with the aim of solving the problem of trust and security through distributed storage. The system configuration is based on an IPFS (InterPlanetary File System) storage method. However, their work does not address the issue of the constitution of electoral and candidacy lists, a central element of reliable voting.

Koo et al. [9] discuss online data authentication using the Merkle Tree. They analyze solutions for improving the security and reliability of outsourced data maintenance and present a new method for inserting auxiliary random sources into the integrity verification proof.

Pawlak et al. [10] proposed an electronic voting system integrated with blockchain technology into a supervised, non-remote Internet voting system that is end-to-end auditable. ABVS (Auditable Blockchain Voting System) was adopted as the architectural framework. Evaluation of the system has shown, according to its authors, that ABVS is more secure and reliable than any other e-voting system. It should be noted that the work was silent on the prior establishment of a reliable voters' list.

Reyad [11] provides a historical introduction to shorthand and cryptography. He focuses on basic encryption techniques and definitions of related terms.

Berbain [12] highlights blockchain as a key element of digital transformation, emphasizing its impact on trust and governance in human interactions, particularly in the legal field.

Neloy et al. [13] propose a secure and transparent system, based on the blockchain following a reusable smart contract mechanism and coupled with Artificial Intelligence for the authentication of the various actors involved thanks to facial recognition. The implementation was based on Ganache, a private Ethereum blockchain. The intelligent contract was developed using the Solidity language, while the AI-based facial recognition is based on the Deepface Python library.

Ferhat and Mahamdioua [14] propose a blockchain-based self-sovereign identity system, allowing users to control access to and selection of their blockchain-validated data stored on IPFS, for applications such as access to academic documents.

Rosamond [15] presents an example of a Kid Krypto-type encryption system, based on disjoint cycles in a graph or network and accessible to a very young audience. The system is designed to help teachers motivate and stimulate children's interest in computing.

Allen et al. [16] present a replication model of institutional innovation that highlights the crucial role of blockchain technology in transforming economic institutions. This model highlights the importance of blockchain-friendly public policies.

Li et al. [17] propose "AvecVoting" by adopting threshold encryption and single-use (circular) ring signature algorithms. This system consists of three main entities (initiators, voters and counters) and is phased in three stages: initialization, voting and counting. The system requires the intervention of the initiator after citizens have registered, before the voters' list is updated. The initiator therefore has the role of manual evaluator of citizens' eligibility, and would even be in a position to encroach on the eligibility of legitimate voters or authorize fictitious voters. Such a system is therefore only viable if it has a trustworthy initiator, not to mention the fact that the manual nature of validations can slow down the system's performance.

Mohiuddin et al. [18] provided a comprehensive compilation of emerging blockchain-related trends, issues and applications for graduate students, researchers, academics and industry practitioners working in cybersecurity, data science and machine learning.

Amine et al. [19] have surveyed known attacks and weaknesses against hash functions and propose solutions to these problems.

Park et al. [20] explained that voting via blockchain does not solve many of the vulnerabilities of electronic voting systems and could introduce new ones. These shortcomings most often refer to human factors not related to blockchain and common to all electronic transaction systems.

Baliga et al. [21] analyze and characterize the performance of quorum (one of the blockchain platforms), focusing on throughputs, latencies and the impact of transaction and smart contract parameters on the latter.

Perard [22] introduces low-storage (LS) nodes into blockchains, storing coded fragments to save space, promote decentralization and facilitate scalability.

Hjálmarsson et al. [23] evaluate the application of blockchain as a service implementing distributed electronic voting systems with computers installed in electoral districts. A wallet is associated with each voter, who will be able to authenticate himself through the system's interaction with an API from an identity verification service based on an electronic ID card and the associated PIN (provided by the same service). In addition, the authors propose an approach to secure wallets using the Non-Interactive Zero Knowledge Proof (NIZKP) algorithm to preserve voter anonymity. These voters and candidates are assumed to be eligible, so the question of establishing eligibility is not addressed in the design of this solution.

Benabdallah et al. [24] explained the need to rethink voting system protocols with the aim of meeting current expectations. They reviewed the most revealing voting systems based on blockchain technology from 2010 to 2021. They highlighted a weakness relating to the scalability of Ethereum smart contracts. The authentication methods explored in this study concern authentication with an international directory number, authentication with scanned copy of ID card or passport. However, it is becoming increasingly difficult to build IT systems based on such scanned documents due to the ease of producing deepfakes in the AI era.

Guegan [25] highlights both cryptography and blockchain. Cryptography guarantees message security through keys and hash functions.

Faruk et al. [26] implemented the ”Bie Vote” system, with a new architectural framework following the 4+1 model. The framework brings together components such as voter and candidate registration using facial identification and fingerprints, the ballot box in a RESTful API, an intelligent registration and authentication component, and a central server to be connected to the Hyperledger Fabric blockchain. The system places particular emphasis on the authentication of voters and candidates, but does not include a process for verifying their eligibility prior to enrolment.

For most of these systems, the focus is more on the voting phase itself. The eligibility list comes from another database and is used as is. These databases are updated by means of a citizen census. However, if the eligibility data used as the electoral list is unreliable, the results of the ballot box cannot be legitimate.

3. Proposed system

To check a candidate’s eligibility, current procedures require the verification of identity, legal, tax and health data. Candidates are responsible for collecting these data. Candidates must contact all the relevant institutions in order to obtain the documents they need to build up their candidacy file. On the citizens’ side, data from census campaigns are also processed to produce the list of eligible voters or electoral roll, as shown in figure 1.

This procedure often results in long waiting times, with the attendant expense and inconvenience.

This procedure can also hinder the filing of candidacies, the respect of electoral timetables and the right to vote of certain citizens. In addition, the various documents produced by citizens could pose problems of reliability and authenticity, as they could be falsified, altered, illegible or undergo any other form of intentional and deliberate modification. Such an approach could easily favor or disfavor one candidacy over another, due to the bias of the authorities in charge of elections, and especially of checking eligibility. As a result, the current procedure, from the candidates’ point of view, is not credible and does not guarantee confidence among all interested parties. Moreover, in the case of certain elections (presidential, legislative, communal, etc.), there is a kind of aberration in the manual operation which underpins the urgent need to find an automatic eligibility solution. The documents required for verification are issued by the public administration. The election management body is also a public authority and, as such, should have access to the documents issued by the same ecosystem, rather than requiring them to be resubmitted for inspection. This redundancy of control would greatly increase processing times, with all the biases that this would entail.

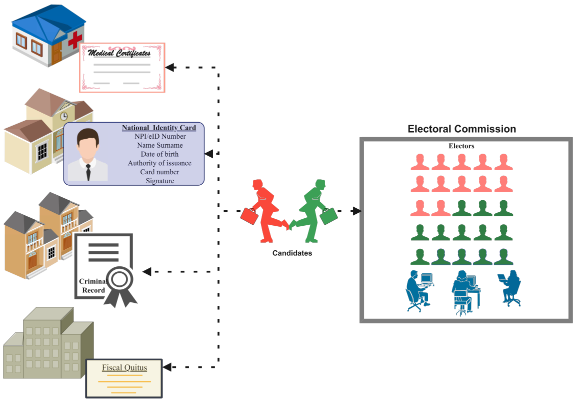

Figure 1: Traditional procedure for checking eligibility

Blockchain offers all the potential required for the deployment of an automatic eligibility checking system that will spare citizens the numerous manual steps currently required to prove their eligibility. The proposed system digitizes the traditional procedure for checking eligibility. It uses smart contracts to validate information from the databases with which it integrates in order to establish, in real time, the eligibility of each citizen for any election, and provide an electoral list that is trustworthy for both voters and candidates. These are the databases of the judiciary, tax authorities and the civil registry. With such a system, it will be possible to organize elections with the data of legitimate candidates and voters.

3.1. Updating the blockchain

Data retrieval method : RESTful API

RESTful APIs are interfaces that two applications use to communicate securely with each other. REST offers flexibility and the ability to handle different types of calls, different types of return data formats and the dynamic structure of hypermedia. Its use does not require knowledge of procedure names and their parameters in a specific order, as required by other Web APIs such as RPC (Remote Procedure Call).

The adoption of REST for the proposed solution offers advantages such as decentralized management of dynamic resources, application ecosystem heterogeneity, service composition and scalability.

Following this methodology, the blockchain is updated in three stages.

Step 1: Retrieving data from the integrated database ecosystem

For each ecosystem component, a RESTful API has been set up to extract the expected data. The various integrity, validity and semantic checks have been taken into account by complex algorithms implemented in the API construction. A log file has also been set up to track every time data is synchronized from other ecosystem components. Information such as time, date and extracted data are logged automatically due to the properties of the blockchain, ensuring the reliability of the log file available locally at the level of each entity.

Step 2: Checking the data to be integrated into the blockchain

The data extracted from each API undergoes a rigorous control process before being added as a transaction to the proposed system's blockchain. They are initially formatted for perfect compatibility with the system in place. A duplicate check avoids the repetitive addition of existing data. In the case of the evolution of previously recorded information, a consistency verification process prevents the insertion of inconsistent data, such as transactions carried out by a deceased person.

Step 3: Integrating data into the blockchain

The data retained following these various checks ensures the authenticity, reliability and consistency of the information extracted, as well as optimal management of the resources used, all dynamically and in real time. An e-mail notification is sent to each citizen concerned when any information is added to or modified in the blockchain after the consensus algorithm has been run.

Transactions issued as a result of information changes within the ecosystem's databases keep the proposed system up to date. It then has all the information it needs to establish, thanks to an intelligent contract, the legal and tax status associated with each identity, in order to deduce the eligibility of the citizen concerned. A second intelligent contract maintains the confidentiality of the information stored, while the ZKP proof enables the public verifiability of the verdict provided without revealing the information used to determine it.

3.2. Managing confidentiality and anonymity

With regard to anonymity and confidentiality, personal data must be treated confidentially and protected, particularly when processing involves data transmission over a network [27] (article 385 of the Digital Code of the Republic of Benin). As a result of this requirement common to the majority of countries, the potential of blockchain is exploited within the proposed solution to create a system with fully anonymized data. The resulting system adopts a privacy-oriented architecture based on a consortium blockchain. Unlike public and private blockchains, which are respectively open to all users or owned by a single company, a consortium blockchain is managed by several organizations. Exchanges are therefore better controlled, and it becomes easier to establish authorizations through smart contracts. The choice of this type of blockchain would reassure each stakeholder, which are the various data sources that feed the blockchain. As all data entered into the blockchain can be encrypted via smart contracts, we can guarantee the protection of personal data. As far as anonymity is concerned, the `'Manyloyinceo'` pseudo-code has been developed as a hash function. Using the hash of this pseudo-code enables the system to associate data with a person without revealing the identity of the citizen concerned..

The various institutions responsible for eligibility checks are the actors in the system in place, and thus represent the nodes of the network. These nodes each possess a digital wallet with a pair of cryptographic keys. Data extracted via the RESTful API is recorded on the blockchain as a transaction referenced to the wallet of the institution from which it originates, so that its authenticity can be verified. In this way, the data collected on any given citizen is kept within the institutions that already hold it, and is not divulged to any other.

At the same time, it is also necessary to authorize citizens to consult their data electronically, in accordance with Article 113 of the Electoral Code in the Republic of Benin. A final portfolio was created to serve as a single portal for all users. This portal gives them access to a Decentralized Application (DApp) for authentication, enabling them to consult their information on the basis of the national identifier associated with them.

Some of the ratings used in this document are described below in Table 1

The processes by which the confidentiality of the data collected is maintained are as follows:

- *Citizen registration*: Through the RESTful API, the IT agent created in the identity system ($Agt_{identity}$) registers citizens, their national ID (ID_u), as well as other information held by the national identity system, and transfers them to the blockchain through the corresponding wallet $(d, Q)_{identity}$
- *Adding additional information about the citizen*: IT agents within the information systems of the police (Agt_{OFFS}), the tax assessment system (Agt_{TAX}), the judicial system (Agt_{JUST}), etc. extract additional information associated with (ID_u)s to the blockchain via dedicated wallets. Each transaction is signed M_d thanks to the address of the corresponding wallet, and the transaction's $H(M)$ fingerprint is stored in the log file.
- *First connection/registration* : When logging in for the first time, all users must provide the following information: National ID, Last name, First names, Date of birth, Gender. Once this information has been entered, the system performs the necessary checks to authorize the user's registration. The user can then define a Pwd_u login password.
- *Logging in and accessing the DApp*: Users who have already defined a password can log in to the DApp by entering their credentials (IDu and Pwdu). They can then access all authorized data. This information is protected by two layers of security: the first is purely cryptographic, and the second is based on the blockchain's smart contract mechanisms. The smart contract associates each connected profile with a list of information that can be consulted. When the citizen makes a query concerning any of these data, the information is encrypted $E_Q(M)$ with the public key of the wallet $(d, Q)_u$ common to all users. Thanks to the smart contract in place, the logged-in user with the ID_u concerned by the information is the only one authorized to read it. To read public information such as the electoral roll or the list of candidates, login and password are not required.

3.3. Drawing up the electoral list

To draw up the electoral list, candidates are first invited to carry out an eligibility check with a minimum waiting period, via a man-machine interface. Once they have authenticated themselves, the various intelligent contracts are used to rule on the eligibility of each candidate, providing

Table 1
Naming

Rating	Description
(d, Q)	Private and Public Key Pair (Wallet)
M	Plaintext Message or Data
M_e	Ciphertext Message or Data
$\{M\}_d$	Digital signature of message M with private key d
$H(M)$	Hashing M using the hash function H
$E_Q(M)$	Encryption of M with the public key $Q[E_Q(M) = M]_e$
$D_d(M)_e$	Decryption of M with the private key $d[D_d(M_e) = M]$
ID_u	Unique user identity (NPI)
Agt_{XXX}	Digital Agent domiciled in institution XXX
Pwd_u	User login password

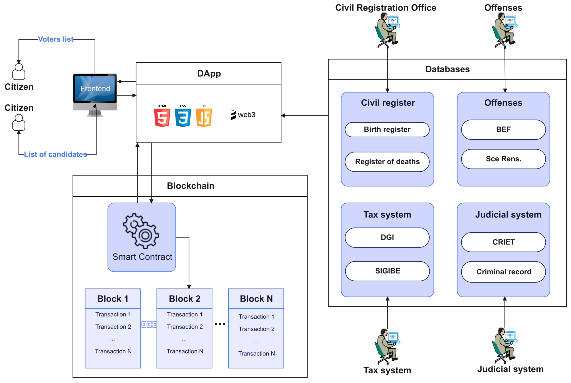

Figure 2: How the system works

them with the various documents used to reach a verdict. Eligible candidates can then authorize their addition to the list of candidates, which is saved and publicly consultable on the blockchain. A third intelligent contract is used to identify all the remaining identities in order to establish their eligibility to vote, and provide the electoral list of voters, which can also be consulted on the blockchain.

The overall operation of the system is illustrated in Figure 2.

4. Results and discussion

4.1. Performance assessment

The performance of the proposed automatic eligibility check system is evaluated according to various criteria, including authentication time, unauthorized modification of eligibility data, response time and latency.

- *Authentication time*
  Authentication time has been reduced by the use of digital wallets for login. This is one of the advantages of blockchain and Web3 technology, as it is no longer necessary to carry out a large number of checks with external identity providers in order to connect a user. As a general rule, authentication time increases as the number of users registered in the blockchain network becomes denser. Experimental results, conducted with a sample of users, attest to the authentication efficiency of the proposed system. Indeed, the delay observed is 1.3 ms, in contrast to the 2.5 ms required by similar systems (e-voting systems) based on blockchain. This significant difference represents a time saving of over 50%.
- *Unauthorized data modification*
  Modifications to data stored on a citizen are not possible through the DApp. The only modifications authorized are those coming from the APIs and having reached all the required validation levels. Due to consensus algorithms, any modification coming from the source systems is notified to the citizen for validation before being recorded in the blockchain. In the event of non-validation, the system keeps the data, but attaches a "contentious" flag to it, and the citizen's eligibility is compromised if he or she is a candidate.
- *Response times*
  It's also important to note that the proposed system will serve as a benchmark for citizen candidacy applications. Thus, a citizen wishing to participate in an election as a candidate, makes an online candidacy request on the proposed DApp application. Once the application has been submitted, the DApp connects to the blockchain to verify the citizen's identity using a multi-factor authentication mechanism. Once the verified identity is correct, the eligibility data is accessible and the request is processed instantly. The citizen receives an acknowledgement from the system, as well as the status of his or her eligibility, which is sent to him or her by e-mail. For the same service, traditional methods require the citizen to assemble various documents. It should be remembered that each of these documents has an average delivery time. For example, it takes a minimum of 72 hours for a criminal record, or a week for a tax receipt. This response time, i.e. the average delivery time, is reduced to around thirty seconds in the proposed new system, thanks to smart contracts that update the citizen's eligibility status each time new data is added to the blockchain.
- *Restoring public confidence*
  When a country adopts this solution, particularly for presidential, legislative or local elections, all the tedious and stressful administrative procedures are eliminated. Citizens have the assurance of sincerity and trust, because no central authority can arbitrarily adjust their vote. Blockchain data remains immutable.

4.2. Limits of the propose

Thanks to the use of blockchain and the intrinsic characteristics of this technology, numerous solutions have emerged in the electoral context to improve and secure traditional procedures that had many limitations. The proposed system is the first to approach the electoral process from the angle of automatic eligibility assessment. It offers a proposed solution for restoring public confidence in the choice of legitimate candidates and voters, but also presents a number of limitations in its current design.

The first limitation is that this system does not cover the entire electoral process, from establishing eligibility to voting and counting. Indeed, the proposed system contributes to the organization of a transparent election by establishing a list of legitimate voters and candidates. However, it does not in itself guarantee the reliability of voting results. The solution in place therefore needs to be extended to the voting, counting and electoral dispute management stages.

Secondly, the preference for the use of consortium blockchain raises significant challenges in terms of implementation and governance. For one thing, setting up and maintaining a network of distributed nodes between the various players involved generates costs in terms of hardware infrastructure. There is also a risk of collusion between these different players, who may collude to alter the information of a certain group of individuals.

5. Conclusion

Current methods of checking eligibility for an election remain permissive to all kinds of irregularities, creating a favorable climate for the deliberate exclusion of certain candidates, or for the registration of fictitious voters. Our work has enabled us to take advantage of blockchain's unique features to track the eligibility of all citizens in real time and provide an inclusive and incontestable electoral roll. Smart contracts and ZKP proof are used to maintain the confidentiality of the information collected, while enabling the public verifiability of the electoral list issued. The results obtained eliminate all barriers to a citizen's eligibility for any type of election. On the other hand, these results make it possible to eliminate all hassle during the administrative formalities of compiling candidacy files for any citizen who has to take part in an election. It's a solution that enhances citizen comfort and confidence, and reassures any individual with the virtue and ability to contribute to the common good of the city through elective office. Furthermore, the present work could therefore serve as a basis for the development of a trustworthy electoral process management system, digitized and secured from end to end, thanks to Blockchain. Such a system is an essential prerequisite that would enable voters to be assured of the reliability of election results, with each stage being publicly verifiable while keeping votes confidential.

References

[1] T. Chafiq, R. Azmi, O. Mohammed, Blockchain-based electronic voting systems: A case study in morocco, International Journal of Intelligent Networks 5 (2024) 38–48.

[2] L. Mosley, H. Pham, X. Guo, Y. Bansal, E. Hare, N. Antony, Towards a systematic understanding of blockchain governance in proposal voting: A dash case study, Blockchain: Research and Applications 3 (2022) 100085.

[3] L. SACCA, N. N. A. ASSOGBA, L. ADOSSOU DAVO, S. GOUNOU, F. A. ABIOLA, Élection des membres de l'Assemblée Nationale - 9e Législature, Rapport Général, CENA, 2023. URL: https://www.cena.bj/wp-content/uploads/2023/08/Election-des-membres-de-lAssemblee-nationale-9e-legislature.pdf.

[4] B. Jayakumari, S. L. Sheeba, M. Eapen, J. Anbarasi, V. Ravi, A. Suganya, M. Jawahar, E-voting system using cloud-based hybrid blockchain technology, Journal of Safety Science and Resilience 5 (2024) 102–109.

[5] S. Panja, B. Roy, A secure end-to-end verifiable e-voting system using blockchain and cloud server, Journal of Information Security and Applications 59 (2021) 102815.

[6] X. Yang, X. Yi, S. Nepal, A. Kelarev, F. Han, Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities, Future Generation Computer Systems 112 (2020) 859–874.

[7] Y. Dalvi, S. Jaiswal, P. Sharma, E-voting using blockchain, International Journal of Engineering Research & Technology (IJERT) (2021).

[8] B. Ahn, Implementation and early adoption of an ethereum-based electronic voting system for the prevention of fraudulent voting, Sustainability 14 (2022) 2917.

[9] D. Koo, Y. Shin, J. Yun, J. Hur, Improving security and reliability in merkle tree-based online data authentication with leakage resilience, Applied Sciences 8 (2018) 2532.

[10] M. Pawlak, J. Guziur, A. Poniszewska-Marańda, Voting process with blockchain technology: auditable blockchain voting system, in: Advances in Intelligent Networking and Collaborative Systems: The 10th International Conference on Intelligent Networking and Collaborative Systems (INCoS-2018), Springer, 2019, pp. 233–244.

[11] O. Reyad, Cryptography and data security: An introduction, the International Journal of Computer Science and Security (2018).

[12] C. Berbain, La blockchain: concept, technologies, acteurs et usages, in: Annales des Mines-réalités industrielles, 3, Cairn/Softwin, 2017, pp. 6–9.

[13] M. N. Neloy, M. A. Wahab, S. Wasif, A. All Noman, M. Rahaman, T. H. Pranto, A. B. Haque, R. M. Rahman, A remote and cost-optimized voting system using blockchain and smart contract, IET Blockchain 3 (2023) 1–17.

[14] Y. Ferhat, M. Mahamdioua, Gestion des identités numériques sur Blockchain, Ph.D. thesis, Université de jijel, 2022.

[15] F. Rosamond, Computational thinking enrichment: Public-key cryptography, Informatics in Education-An International Journal 17 (2018) 93–103.

[16] T. T. Allen, M. Yang, S. Huang, O. K. Hernandez, Method to allocate voting resources with unequal ballots and/or education, MethodsX 7 (2020) 100872.

[17] M. Li, X. Luo, W. Sun, J. Li, K. Xue, Avecvoting: Anonymous and verifiable e-voting with untrustworthy counters on blockchain, in: ICC 2022-IEEE International Conference on Communications, IEEE, 2022, pp. 4751–4756.

[18] M. S. U. Miah, M. Rahman, M. S. Hossain, A. Rupai, Introduction to Blockchain, 2019.

[19] A. Zellagui, N. H.-S.-A. ALI-PACHA, Sécurité des fonctions de hachage cryptographique, Communication science et technologie 17 (2021) 13–21.

[20] S. Park, M. Specter, N. Narula, R. L. Rivest, Going from bad to worse: from internet voting to blockchain voting, Journal of Cybersecurity 7 (2021) tyaa025.

[21] A. Baliga, I. Subhod, P. Kamat, S. Chatterjee, Performance evaluation of the quorum blockchain platform, arXiv preprint arXiv:1809.03421 (2018).

[22] D. Perard, Blockchain et stockage efficace, Ph.D. thesis, 2020. URL: http://www.theses.fr/2020ESAE0048, thèse de doctorat dirigée par Lacan, Jérôme Informatique et Télécommunications Toulouse, ISAE 2020.

[23] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, G. Hjálmtýsson, Blockchain-based e-voting system, in: 2018 IEEE 11th international conference on cloud

computing (CLOUD), IEEE, 2018, pp. 983–986.

[24] A. Benabdallah, A. Audras, L. Coudert, N. El Madhoun, M. Badra, Analysis of blockchain solutions for e-voting: a systematic literature review, IEEE Access 10 (2022) 70746–70759.

[25] D. Guegan, Public blockchain versus private blockhain (2017).

[26] M. J. H. Faruk, M. Islam, F. Alam, H. Shahriar, A. Rahman, Bie vote: A biometric identification enabled blockchain-based secure and transparent voting framework, in: 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA), IEEE, 2022, pp. 253–258.

[27] P. TALON, J. DJOGBENOU, A. I. ADAM SOULE, Loi N° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin, 2018. URL: https://sgg.gouv.bj/doc/loi-2017-20/.