Original Research Article

Optimization of the Electoral Process with Hyperledger Fabric Blockchain: Real-Time Eligibility

Abstract

In this paper, we present an innovative model based on the Hyperledger Fabric blockchain for automating electoral eligibility checking. This model leverages Restful APIs to aggregate real-time data from selected transactional databases, integrating them directly into the blockchain. This approach enhances traditional systems and removes the need for citizens to provide documents for candidacy or census formalities during elections. As a result, this model automatically generates a reliable and legitimate list of eligible candidates and voters. The reliability, inclusiveness and legitimacy of these lists are essential to the success of any democratic electoral process. Without them, the resulting abuses can damage the peace and development of nations.

Keywords: Blockchain; Eligibility; Paperless election; Smart contract; Hyperledger fabric

1 Introduction

Holding an election entails considerable costs, not least for drawing up a permanent, computerized electoral roll, which determines who can vote. Usually, electoral authorities or election commissions carry out a population census. The data collected during this process is processed over an extended period, often with errors and omissions. These censuses are frequently marred by lost or missing data, requiring subsequent adjustments. Handling the physical documents collected, such as birth certificates, identity papers and criminal records, is complex. This information is then entered,

processed and validated in specially designed computer systems. However, shortcomings in the physical census affect the reliability of analyses and the accuracy of the data collected. These problems are particularly preoccupying in African countries, despite the efforts of leaders to establish lasting solutions accepted by all.

The creation of an inclusive electoral roll using traditional methods presents numerous challenges, such as data integrity, manipulation by interested groups, system security, protection of personal data and verifiability. The IT systems used are often based on regional databases or on a centralized database. In the first case, this raises the problem of centralizing regional data to obtain national statistics. In the second case, a centralized architecture is susceptible to distributed denial of service (DDoS) attacks. In the second case, a centralized architecture is susceptible to Distributed Denial of Service (DDoS) attacks. Trust is the essential foundation of any electoral IT system, guaranteeing its smooth operation. Faced with these challenges, and given the crucial importance of elections for the stability and development of nations, it is imperative to make reliable technological choices. These technologies must be capable of creating solutions that inspire and maintain trust at all levels.

Over the past ten years, technological advances have profoundly transformed the notion of trust, which is now firmly anchored in the digital domain [[1]]. These developments are prompting communities to embrace digital transformation to design robust, resilient and scalable solutions.

The choice of technology for an electoral system must therefore be based on its ability to meet these criteria. Recently, blockchain technology has emerged as a relevant solution to the challenges faced in many business sectors.

This article proposes a framework for automated electoral eligibility checking using blockchain. It describes blockchain in detail, gathers related researches on the application of blockchain in electoral systems, particularly for eligibility control. It also presents the proposed system, and outlines the results obtained before doing the discussions and the conclusion.

2 Related work

The report on the election of members of the 2023 National Assembly in the Republic of Benin [[2]] highlights certain ”slippages” observed during the electoral process. Among the difficulties encountered, the late submission of files created an overload of work and stress for the staff of the Autonomous National Electoral Commission (CENA). The report recommends the adoption of an electronic candidacy declaration system (e-Declaration) to modernize the process. It also highlights a lack of clarity regarding the inclusion of the death rate, applied by the Agence Nationale d’Identification des Personnes (ANIP), to determine the participation rate. The e-Declaration system is designed to receive applications without the need for further processing to obtain the list of eligible candidates.

Berbain [[3]] highlights blockchain as a key pillar of digital transformation, emphasizing its role in strengthening trust and governance within human interactions, particularly in the legal sphere.

Miah et al. [[4]] have produced a comprehensive compilation of blockchain-related trends, challenges and emerging applications, aimed at graduate students, researchers, academics, and industry professionals operating in the fields of cybersecurity, data science, and machine learning.

Benabdallah et al. [[5]] highlighted the need to rethink voting system protocols in order to meet contemporary requirements. They reviewed the most prominent blockchain-based voting systems from 2010 to 2021. They also highlighted a weakness related to the scalability of smart contracts on Ethereum. Authentication methods examined in this study include authentication via an international directory number and authentication via a scanned copy of an ID card or passport. However, it is becoming increasingly complex to design IT systems based on these scanned documents, due to the ease with which deepfakes can be created in the age of artificial intelligence.

Panja & Roy [[6]] have developed an end-to-end verifiable e-voting system, combining blockchain and a cloud server, to prevent ballot-box stuffing fraud and boost voter confidence in the vote count.

The system verifies voter eligibility, ensuring that a registered user can only vote once, with verification possible at every stage of the voting and counting process. However, as far as eligibility is concerned, the system simply checks that the user has the identity he or she claims to have, and that this identity is eligible to vote.

Reyad [[7]] presented a historical introduction to shorthand and cryptography, focusing on fundamental encryption techniques and offering definitions of related terms.

Hjálmarsson [[8]] explore the use of blockchain as a service to deploy distributed electronic voting systems, with computers installed in electoral districts. A digital wallet is assigned to each voter, enabling authentication via an identity verification API, which uses an electronic ID card and an associated PIN code, provided by the same service. The authors also propose a method of securing these wallets using the Non-Interactive Zero Knowledge Proof (NIZKP) algorithm to guarantee voter anonymity. However, this solution assumes the eligibility of voters and candidates, without addressing the issue of its verification.

Chafiq et al. [[1]] have developed a hybrid voting system combining remote and on-site voting to meet the needs of all Moroccan voters. This system is based on two layers: Distributed Permission Ledger Technology (DPLT) for verification and validation of voting data, followed by the Solana blockchain, which stores this data immutably. However, this system uses a pre-established list of candidates and voters, whose selection criteria are not specified.

Ahn [[9]] has implemented an Ethereum blockchain-based voting system to prevent electoral fraud, in response to concerns about trust and security through distributed storage. The system is based on a storage method using IPFS (InterPlanetary File System). However, their work does not address the crucial issue of the constitution of electoral lists and candidacies, which is central to guaranteeing the reliability of an election.

Ferhat & Mahamdioua [[10]] have designed a blockchain-based self-sovereign identity system that allows users to manage access and selection of their data stored on IPFS, with this data being validated by the blockchain. The system is designed for applications such as access to academic documents.

Perard [[11]] introduced low-storage (LS) nodes into blockchains, which store coded fragments to save space, promote decentralization, and facilitate scalability.

Jayakumari et al. [[12]] proposed a system to reduce authentication time, vote tampering, response times, as well as the lack of reliability, flexibility, transparency, security and financial efficiency, problems common to many e-voting systems. They have implemented a cloud-based system using a hybrid blockchain to address these challenges. However, the solution relies on already established eligibility for voters and candidates.

Faruk et al. [[13]] designed the ”Bie Vote” system, introducing a new architectural framework based on the 4+1 model. This framework includes various components, such as voter and candidate registration via facial identification and fingerprints, a ballot box connected via a RESTful API, a smart module for registration and authentication, and a central server integrated with the Hyperledger Fabric blockchain. The system focuses primarily on authenticating voters and candidates, but does not include a process to verify their eligibility prior to registration.

Park et al. [[14]] argue that blockchain voting fails to resolve many vulnerabilities in electronic voting systems and may even introduce new ones. These weaknesses are generally linked to human factors, independent of blockchain, but common to all electronic transaction systems.

Jaiswal et al. [[15]] have proposed a blockchain-based electronic voting (E-Voting) system focusing on improved privacy, transparency and verifiability. This system integrates an electoral list.

Neloy et al. [[16]] have developed a secure and transparent blockchain-based system that uses a reusable smart contract mechanism combined with artificial intelligence to authenticate the various players via facial recognition. The implementation was carried out on Ganache, a private Ethereum blockchain. The smart contract was coded in Solidity, while the AI-based facial recognition uses the Python Deepface library.

Baliga et al. [[17]] analyzed and characterized the performance of Quorum, a blockchain platform,

focusing on throughput, latency, as well as the impact of transaction parameters and smart contracts on these aspects.

Guegan [[18]] highlights both cryptography and blockchain. Cryptography ensures message security using keys and hash functions.

Li et al. [[19]] developed the "AvecVoting" system, which uses threshold encryption algorithms and a single-use ring signature. The system is based on three main entities: initiators, voters and counters, and takes place in three phases: initialization, voting and counting. After citizens have registered, the initiator is required to update the voters' list. The initiator thus acts as a manual evaluator of citizens' eligibility, with the potential power to restrict the eligibility of legitimate voters or authorize fictitious ones. This system can therefore only function effectively if the initiator is trustworthy, especially as the manual nature of the validations could slow down the system's overall performance.

Pawlak et al. [[20]] have developed an electronic voting system that integrates blockchain technology into a supervised, non-remote, online voting environment, offering complete end-to-end auditability. The architectural framework chosen for this system is ABVS (Auditable Blockchain Voting System). According to the authors, evaluations have shown that the ABVS system offers superior security and reliability to other e-voting systems. However, it is important to emphasize that this work does not deal with the prior creation of a reliable voters' list.

Rosamond [[21]] proposes an example of an encryption system called Kid Krypto, designed around disjoint cycles in a graph or network, and aimed at a very young audience. The system is designed to help teachers motivate children and awaken their interest in computing.

Amine et al. [[22]] have researched the attacks and vulnerabilities identified in hash functions and proposed solutions to address them.

Allen et al. [[23]] propose a replication model of institutional innovation, highlighting the central role of blockchain technology in transforming economic institutions. This model emphasizes the need for public policies that support blockchain adoption.

Koo et al. [[24]] explored online data authentication using the Merkle Tree. They studied solutions for improving the security and reliability of outsourced data management and proposed a new method for inserting auxiliary random sources into the integrity verification proof.

Yang et al. [[25]] have proposed a voting protocol based on a rating system, using the blockchain and publicly verifiable by any user. They combine blockchain-specific mechanisms with cryptographic tools such as ElGamal encryption, group encryption and ZKP (Zero Knowledge Proof), enabling each user to carry out the tally once the election is over, without revealing individual votes. When initialized, this protocol relies on a pre-established list of candidates and a supposedly honest registration authority for voter registration.

In the majority of these systems, the main focus is on the voting phase itself. The list of eligible voters is usually extracted from another database and used as is. Updating these databases relies on a citizen census process. However, if the eligibility data used to compile the electoral list is unreliable, the ballot box results cannot be considered legitimate.

3 Materials and Methods

3.1 Blockchain: definition, operation, features and benefits

Definition and operation

Blockchain is a distributed, unalterable ledger technology that has significantly transformed business, industry, and commerce [[26]]. It operates without the need for control by a central authority (figure 1).

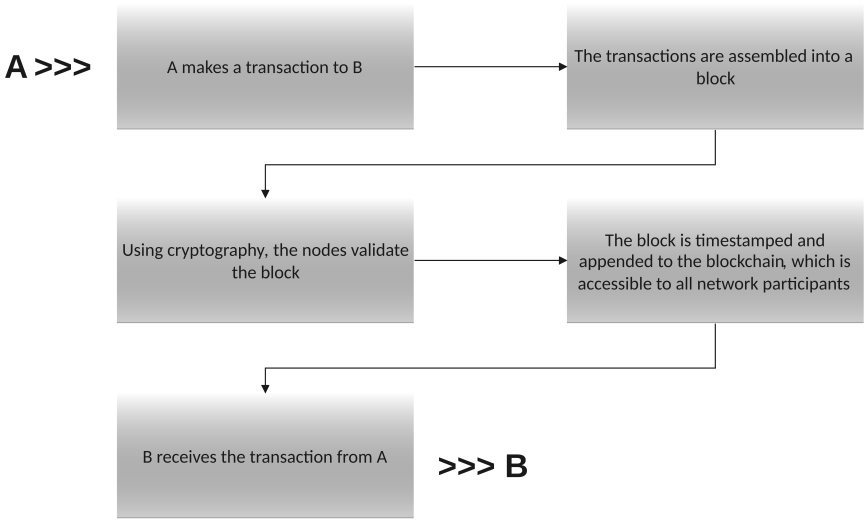

Figure 1: Blockchain operating diagram

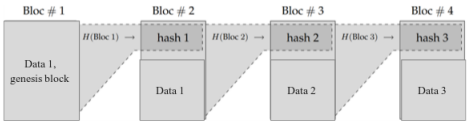

Figure 2: Block structure [[30]]

Features and benefits

Blockchain is a distributed, permanent and unalterable peer-to-peer network. It can be shared between all members of the network, making it highly accessible. Its security is enhanced by the encryption of all recorded transactions. It is based on the use of intelligent contracts and consensus algorithms, enabling autonomous decision-making. These features give it significant advantages in terms of trust, transparency, traceability and increased speed [[27]], [[28]].

As illustrated in figure 2, which describes the constitution of a block, each block $n+1$ is hashed and cryptographically linked to the preceding block n [[29]].

$$B_{n+1} = E(Tx)_{n+1} + H(B_n) + H(B_{n+1}) \tag{3.1}$$

$$H(B_{n+1}) = H(E(Tx)_{n+1} + H(B_n)) \tag{3.2}$$

(3.1) : the B_{n+1} block is made up of all E transactions Tx, the hash of the previous block and the hash of the current block $(n+1)$.

(3.2) : block $n+1$ hash $H(B_{n+1})$ is generated from the transactions contained in the current block and the hash of the previous block.

Note. The operator (+) does not indicate simple mathematical addition.

3.2 The Hyperledger Fabric blockchain

Depending on access or membership rights, there are two main types of blockchain: the public blockchain, accessible to all, and the private blockchain, owned by a restricted group of individuals. When a private blockchain is jointly managed by several organizations, it is called a consortium blockchain. Hyperledger Fabric is a modular, extensible framework designed for the creation of private or consortium blockchains. Unlike other platforms such as Ethereum, which are predominantly public and decentralized, Hyperledger Fabric has features that make it a preferred choice in areas requiring increased confidentiality, proven robustness, complex role management, and low latency [[1]] ; all essential requirements for the proposed solution. The choice of this blockchain for the implementation of the automatic eligibility control system is therefore justified, as Hyperledger Fabric offers all the necessary tools to meet the criteria of verifiability, confidentiality, resistance to attacks, etc., required by such a system. It also facilitates the declaration and management of roles for all users authorized by the system. Because of its advantages in terms of data confidentiality, advanced role management, absence of gas charges, and transaction speed, we opted for a consortium blockchain, based on the Hyperledger Fabric framework.

3.3 Proposed system

At present, verifying a candidate's eligibility requires a thorough check of various data, including identity, judicial, tax and health information. It is the candidate's responsibility to gather this data. They must go to the relevant institutions to obtain the documents needed to compile their application file. For citizens, data from census campaigns are also processed to produce the list of eligible voters, as shown in figure 3.

This procedure often entails long waiting times, expense and other inconveniences. It can also complicate the filing of candidacies, disrupt the electoral calendar or affect the voting rights of certain citizens. In addition, the documents provided by citizens can pose problems of reliability and authenticity, as they are likely to be falsified, altered, illegible or intentionally modified. Such an approach can also lead to favoritism or discrimination in the processing of candidacies, due to the prejudices of the authorities responsible for elections and eligibility checks. As a result, the current procedure lacks credibility from the point of view of candidates, and does not guarantee the confidence of all parties concerned.

Furthermore, in some elections (presidential, legislative, communal, etc.), inefficiencies are observed in the manual process, underlining the urgent need for an automatic eligibility solution. The documents required for control are issued by the public administration, which is also responsible for managing elections. It therefore seems logical that this body should use the documents issued by the same ecosystem, rather than requesting their resubmission for verification. This redundancy considerably increases processing times and introduces bias into the process.

Blockchain offers all the capabilities needed to set up an automatic eligibility checking system, relieving citizens of the numerous manual steps required to prove their eligibility. The proposed system modernizes the traditional procedure for verifying eligibility by using

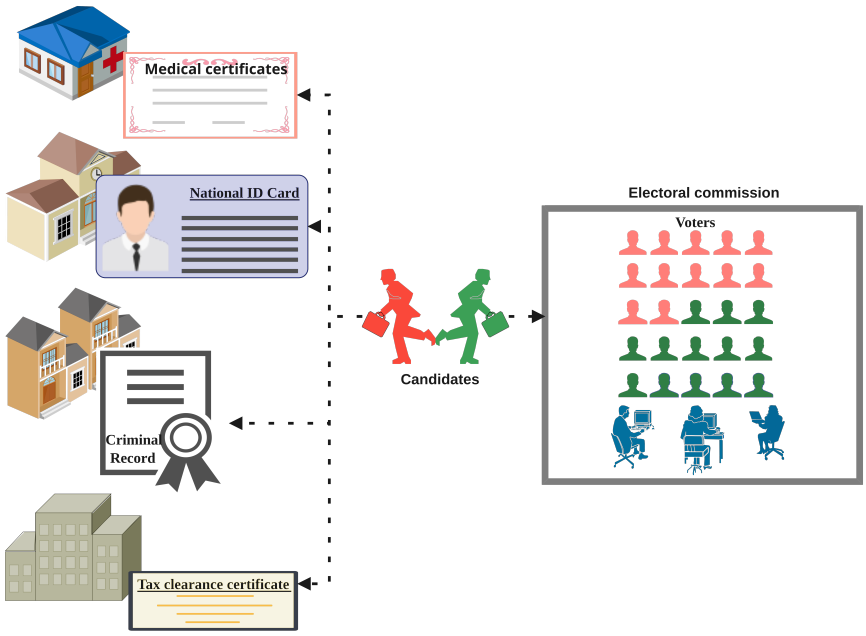

Figure 3: Traditional eligibility check procedure

intelligent contracts to validate information from the databases with which it is integrated. In this way, it enables the eligibility of each citizen for any election to be determined in real time, and provides a reliable electoral list for both voters and candidates. The system uses the databases of the judicial, tax and civil registry institutions. With such a system in place, it will be possible to organize elections based on the data of genuinely eligible candidates and voters.

The operation of the proposed system is based on three axes:

Blockchain update

Data retrieval method : RESTful API

RESTful APIs are interfaces that facilitate secure communication between two applications. REST allows great flexibility in handling various call types, response data formats, and the dynamic structure of hypermedia. Unlike other Web APIs such as RPC (Remote Procedure Call), its use does not require prior knowledge of procedure names and their parameters in a specific order.

The adoption of REST for the proposed solution offers several advantages, including decentralized management of dynamic resources, heterogeneous application ecosystems, service composition and scalability.

According to this methodology, the blockchain is updated in three stages.According to this methodology, the blockchain is updated in three stages.

Step 1: Data extraction from ecosystem databases

For each ecosystem component, a RESTful API is set up to extract the necessary data (see figure 4). This API incorporates sophisticated algorithms to ensure data integrity,

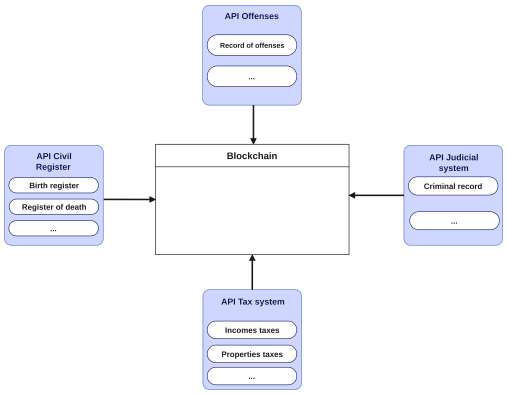

Figure 4: Retrieving data from the blockchain

```
// Fonction pour récupérer les données de MySQL
async function getMySQLData(query) {
  return new Promise((resolve, reject) => {
    const connection = mysql.createConnection(dbConfig);

    connection.connect(err => {
      if (err) reject(err);

      connection.query(query, (err, results) => {
        if (err) reject(err);

        connection.end();
        resolve(results);
      });
    });
  });
}
```

Figure 5: Portion of code from a Node.js API that retrieves data

validity and semantics. A log file is also created to track all data synchronizations between the various ecosystem components. Information such as time, date and extracted data are automatically recorded thanks to the blockchain's features, guaranteeing the reliability of the log file, which is available locally for each entity.

Step 2: Checking the data to be inserted in the distributed register

The data retrieved from each API undergoes a strict validation process before being integrated as transactions in the proposed system's blockchain. They are first formatted to ensure full compatibility with the system. A duplicate check prevents the redundant addition of data already present. When pre-existing information is updated, a consistency verification process ensures that incongruous data, such as transactions carried out by a deceased person, are not inserted.

Step 3: Inserting validated data into the blockchain

The data validated after these various checks guarantees the authenticity, reliability and consistency of the information extracted, while ensuring optimal management of resources dynamically and in real time. When a piece of information is added or updated on the blockchain, each citizen concerned receives an e-mail notification, once the consensus

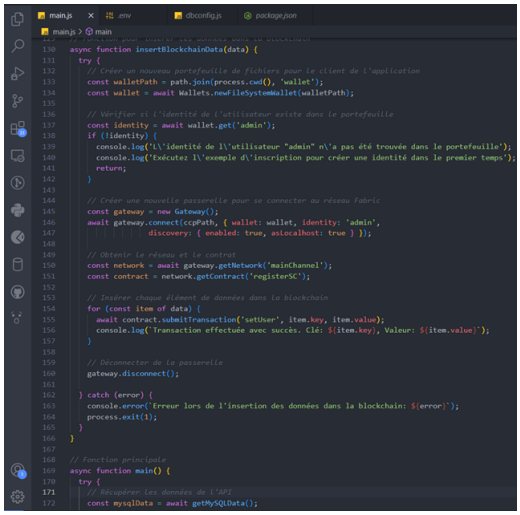

Figure 6: Portion of code for integrating verified data from an API into the blockchain

algorithm has been completed.

Transactions generated by modifications to the ecosystem's databases ensure that the proposed system remains up to date. In this way, it can access all the information needed to determine, with the help of an intelligent contract, the legal and tax status associated with each identity, and deduce the eligibility of the citizen concerned. A second intelligent contract ensures the confidentiality of the information stored, while the ZKP proof guarantees the public verifiability of the verdict without disclosing the data used to establish it.

Protecting confidentiality and anonymity

Data transmitted from the RESTful APIs to the blockchain is protected by asymmetric cryptography. Each ecosystem component uses the backend server's public key to encrypt the data before it is sent. This mechanism guarantees that the data will not be intercepted or modified during transfer to the blockchain. On arrival, the backend decrypts the data and processes it as described in the point mentioned previously.

Security of data traffic to the blockchain

With regard to anonymity and confidentiality, it is imperative that personal data be treated with the utmost confidentiality and protection, especially when transmitted over a network [[31]]. To meet this requirement widely shared by states, the proposed solution uses the capabilities of blockchain to create a system where data is fully anonymized. This system adopts a confidentiality-focused architecture using a consortium blockchain. Unlike public blockchains, which are accessible to all users, and private blockchains, which are controlled by one company, a consortium blockchain is administered by several organizations. This enables better control of exchanges and facilitates the establishment of authorizations via smart contracts. This choice guarantees the trust of stakeholders, such as the various

Table 1: Naming

Rating	Description
(d, Q)	Private and Public Key Pair (Wallet)
M	Message or data in plain text
M_e	Encrypted 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

data sources feeding the blockchain. Data entered into the blockchain can be encrypted by smart contracts, ensuring the protection of personal information. To preserve anonymity, the pseudo-code "Manyloyinceo" has been developed as a hash function. Using the hash generated by this pseudo-code, the system can associate data with an individual without disclosing his or her identity.

The institutions responsible for eligibility checks act as system actors, forming the nodes of the network. Each node has a digital wallet with a pair of cryptographic keys. Data extracted via the RESTful API is recorded on the blockchain as a transaction associated with the originating institution's wallet, guaranteeing verifiability of its authenticity. In this way, data relating to a citizen is kept within the holding institutions and is not disclosed to any other entity.

In addition, in accordance with Article 113 of the Electoral Code in the Republic of Benin, it is also necessary to enable citizens to consult their data electronically. An additional portfolio has therefore been created to serve as a single portal for all users. This portal provides access to a Decentralized Application (DApp) enabling citizens to consult information concerning them, based on their national identifier.

Some of the notations used in this document are defined in Table 1 below.

The following processes guarantee the confidentiality of the data collected:

- *Citizen registration*: Using the RESTful API, the identity system's IT agent $(Agt_{identity})$ registers citizens, their national ID (ID_u), and other information from the national identity system, then transmits them to the blockchain via the corresponding wallet $(d, Q)_{identity}$
- *Additional citizen information*: IT agents in the information systems of the police (Agt_{OFFS}), the tax assessment system (Agt_{TAX}), the judicial system (Agt_{JUST}), etc., extract additional information linked to (ID_u)s and transmit it to the blockchain via dedicated wallets. Each transaction is signed M_d using the address of the corresponding wallet, and the $H(M)$ fingerprint of this transaction is recorded in the log file.
- *First login/citizen registration* : When logging in for the first time, each user must

submit the following information: National ID, Last name, First names, Date of birth and Gender. Once this information has been provided, the system carries out the necessary checks to validate the user's registration, who can then create a Pwd_u login password.

- *Logging in and accessing the DApp*: Users who have previously defined a password can log in to the DApp by providing their identifiers (IDu and Pwdu). Once logged in, they can consult the data to which they have access. Information security is ensured on two levels: a cryptographic level and a protection level via smart contracts on the blockchain. Each connected profile receives, via a smart contract, a list of accessible information. When a citizen requests access to this information, it is encrypted $E_Q(M)$ with the wallet's public key $(d, Q)_u$ shared by all users. The smart contract ensures that only people with the corresponding (ID_u) can read the information. For public data, such as electoral lists or candidate lists, no login and password is required.

Creation of the electoral list

To create the electoral list, candidates must first pass an eligibility check via a user interface, with a minimum waiting period. After authentication, various intelligent contracts determine their eligibility and provide them with the supporting documents that led to this decision. Candidates deemed eligible can then approve their addition to the candidate list, which is recorded and made publicly accessible on the blockchain. A third smart contract is used to enumerate all remaining identities, establish their eligibility to vote, and generate the electoral list of voters, also available on the blockchain.

The overall operation of the system is illustrated in Figure 7.

4 Results and Discussion

4.1 Performance assessment

The performance of the automatic eligibility check system is evaluated using a number of criteria. These include authentication time, protection against unauthorized modification of eligibility data, as well as response time and latency.

- *Authentication time*

  The use of digital wallets for login has reduced authentication time, a key benefit of blockchain and Web3 technology. Thanks to this approach, it is no longer necessary to carry out multiple checks with external identity providers to connect a user. In general, authentication time tends to increase with the number of users registered in the blockchain network. However, experimental results, carried out with a sample of users, show that the proposed system is highly efficient in terms of authentication. Indeed, the delay observed is 1.3 ms, compared with the 2.5 ms required for similar blockchain-based e-voting systems. This improvement represents a time saving of over 50

- *Unauthorized data modification*

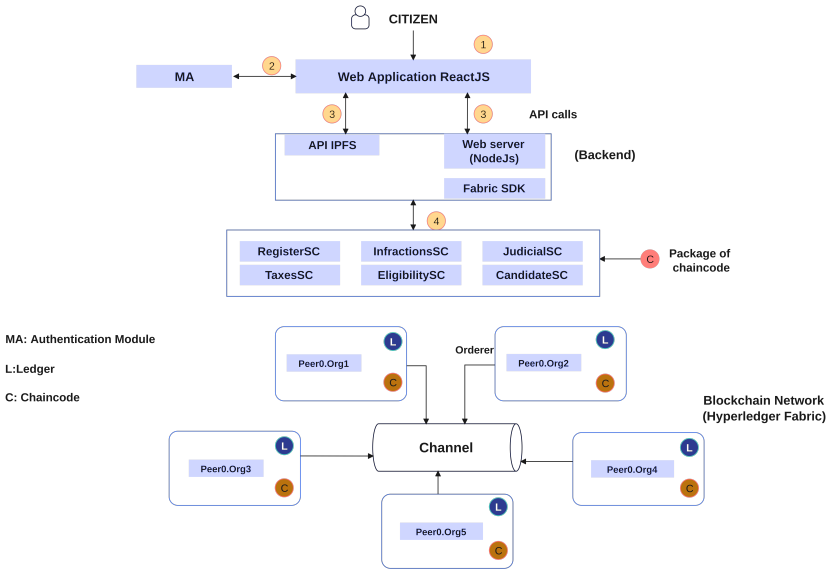

Figure 7: System operation

Data stored on a citizen cannot be modified directly via the DApp. Only modifications validated by the APIs and having passed all validation levels are accepted. Thanks to consensus algorithms, any modification coming from the source systems is notified to the citizen for approval before being recorded in the blockchain. In the event of non-validation, the data is retained with a ”contentious” indicator, and the citizen’s eligibility, if he or she is a candidate, is then compromised.

- *Response times*

  It is essential to note that the proposed system establishes a model for the submission of applications by citizens. A citizen wishing to run in an election as a candidate submits his or her application online via the DApp application. The DApp then connects to the blockchain to validate the candidate’s identity using a multi-factor authentication mechanism. Once the identity has been verified, the eligibility data becomes accessible, and the application is processed immediately. The citizen receives an acknowledgement of receipt from the system, as well as an eligibility status by e-mail. In comparison, traditional methods require the citizen to gather various documents, each with a specific processing time-for example, the time required to obtain a criminal record is a minimum of 72 hours, while a tax receipt can take a minimum of one week. With the new system, this time is reduced to around 30 seconds, thanks to smart contracts that update the citizen’s eligibility status when new data is added to the blockchain.

- *Restoring public confidence*

  When a country adopts this solution for presidential, parliamentary or local elections,

all the complex and stressful administrative procedures are eliminated. Citizens can be assured of a transparent and reliable procedure, as no central authority can arbitrarily dismiss them. The data stored on the blockchain is immutable.

4.2 Limits of the proposed system

The use of blockchain and its unique characteristics have led to the development of numerous solutions aimed at improving and securing traditional, often limited, electoral procedures. The proposed system is the first to approach the electoral process from the angle of automatic eligibility assessment. Although it offers an innovative solution for boosting citizens' confidence in the choice of legitimate candidates and voters, it also has certain limitations in its current design.

The first limitation of the system is that it does not cover the entire electoral process, from establishing eligibility to voting and counting. Indeed, although the proposed system facilitates the organization of transparent elections by establishing lists of legitimate voters and candidates, it does not in itself guarantee the reliability of voting results. It is therefore necessary to extend the solution to the voting stage, the vote count and the management of electoral disputes. As a second limitation, the choice of a consortium blockchain presents significant implementation and governance challenges. The creation and maintenance of a network of nodes distributed between the various players involved generates costs linked to the physical infrastructure.

5 CONCLUSIONS

Current methods for monitoring the eligibility of candidates for elections are often subject to various irregularities, which can lead to the intentional exclusion of certain candidates or the registration of fictitious voters. Our approach takes advantage of the specific features of blockchain to monitor the eligibility of all citizens in real time and provide an electoral roll that is both complete and unalterable. Through the use of smart contracts and ZKP proof, we ensure data confidentiality while enabling public verification of electoral rolls.

The results obtained eliminate obstacles to eligibility for all citizens, and simplify the administrative procedures involved in compiling candidacy files. This solution enhances citizens comfort and confidence, offering a guarantee to virtuous people who are able to contribute to the common good through elective positions. In addition, our research could serve as the basis for developing a reliable, fully digitalized and secure electoral process management system using blockchain. Such a system is crucial to assure voters of the integrity of electoral results, with every step being publicly verifiable while preserving the confidentiality of votes.

Disclaimer (Artificial Intelligence)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc) and text-to-image generators have been used during writing or editing of this manuscript.

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. 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 (Apr. 2023).

[3] C. Berbain, La blockchain: concept, technologies, acteurs et usages, in: Annales des Mines-réalités industrielles, no. 3, Cairn/Softwin, 2017, pp. 6–9.

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

[5] 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.

[6] 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.

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

[8] F. . Hjálmarsson, G. K. Hreiarsson, M. Hamdaqa, G. Hjálmtỳsson, Blockchain-based e-voting system, in: 2018 IEEE 11th international conference on cloud computing (CLOUD), IEEE, 2018, pp. 983–986.

[9] B. Ahn, Implementation and early adoption of an ethereum-based electronic voting system for the prevention of fraudulent voting, Sustainability 14 (5) (2022) 2917.

[10] Y. Ferhat, M. Mahamdioua, Gestion des identités numériques sur blockchain, Ph.D. thesis, Université de jijel (2022).

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

[12] 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 (1) (2024) 102–109.

[13] 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.

[14] S. Park, M. Specter, N. Narula, R. L. Rivest, Going from bad to worse: from internet voting to blockchain voting, Journal of Cybersecurity 7 (1) (2021) tyaa025.

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

[16] 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 (1) (2023) 1–17.

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

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

[19] 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.

[20] 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.

[21] F. Rosamond, Computational thinking enrichment: Public-key cryptography, Informatics in Education-An International Journal 17 (1) (2018) 93–103.

[22] A. Zellagui, N. H.-S.-A. ALI-PACHA, Sécurité des fonctions de hachage cryptographique, Communication science et technologie 17 (18) (2021) 13–21.

[23] 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.

[24] 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 (12) (2018) 2532.

[25] 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.

[26] G. Tripathi, M. A. Ahad, G. Casalino, A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges, Decision Analytics Journal (2023) 100344.

[27] O. MEKHATRIA, Conception and realization of a blockchain model for health records (2022).

[28] Y. Liu, Q. Wang, An e-voting protocol based on blockchain, Cryptology ePrint Archive (2017).

[29] S. J.-n. P. Sonon, T. Djara, A. W. BELLO, M. OUSMANE, Securing the user registration process in an ip telephony system using blockchain and kyc technologies, Journal of Scientific and Engineering Research (JSAER) 11 (1) (2024) 238–247.

[30] S. Masseport, Consensus blockchain: incitation des utilisateurs d'un réseau à la participation et à la loyauté, Ph.D. thesis, Université Montpellier (2021).

[31] 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/