ISSN 1870-4069

Web Tool to Support Electronic Democracy Processes Using Blockchain

Carlos Huerta García, Axel Ernesto Moreno Cervantes,
Nidia Asunción Cortez Duarte

Instituto Politécnico Nacional,
Escuela Superior de Cómputo,
Mexico

chuertag1600@alumno.ipn.mx, axelernesto@gmail.com,
ncortezd@ipn.mx

Abstract. The traditional voting process and contemporary electronic voting systems are insufficient for meeting the needs of the users for more reliable and secure democratic processes within collective governance structures. This paper presents the development of a web tool designed to support electronic democracy processes using Blockchain. The reliability and security of the democratic processes facilitated by the tool are increased through the joint support of the electronic democracy axes, the use of a smart contract deployed on a Blockchain network, and the employment of the HTTPS protocol. Authentication, confidentiality, integrity and non-repudiation information security services are provided throughout the implementation described in this paper, while ensuring that the security provisions do not have a significant impact on the performance of the web tool. The tool was developed using SCRUM, and its quality and functionality was verified through unit, integration, stability, security, and usability testing.

Keywords: Blockchain, web application, electronic democracy, SCRUM.

1 Introduction

1.1 ICT and Blockchain

As mentioned, Information and Communication Technologies (ICT) are tools through which communication and information consultation is possible in an increasingly instantaneous and sophisticated way [1]; in this sense, the Internet has become the most promising resource for that purpose, since its appearance in the late 1970s its evolution has been manifested in Web 1.0, Web 2.0 and Web 3.0 generations. According to [2] the World Wide Web (WWW) has become the broadest medium in which users can share, read and write information through devices connected to the Internet. In [2] they point out that in Web 1.0 people connected and gathered information from the network, in Web 2.0 people connected with each other, and Web 3.0 has been treated as the

knowledge or semantic web; although [3] points out different proposals for the latter: a virtual, semantic or decentralized web. On the Web 3.0 from the proposal of a decentralized web, networks with blockchain mechanisms or Blockchain arise.

The Blockchain is a single, consensual record of transactions distributed among several nodes of a network [4, 5]. Each block is chained to the next, by means of a cryptographic mechanism. In this way, each node stores the complete chain for verification as new blocks are validated. One of the uses of this technology may be found in smart contracts. Also, [4] indicates that these are agreements in which the automatic execution of instructions written in a programming language and executed within a Blockchain network. Blockchain networks mainly consist of asymmetric cryptography techniques for the use of digital signatures to guarantee the identity of users, hash functions to ensure data integrity, as well as transaction validation mechanism called consensus algorithm [6].

The social, economic and political spheres have been transformed by the introduction of ICT throughout its generations, as they modify the ways in which individuals perceive their environment and in which they perform their daily activities, as pointed out by [1] and [2]. It is stated that the Internet has been useful to generate new ways of relating through virtual spaces, or access to online services [1]. According to [1], the political uses of technology are more recurrent, whether in the areas of public management or decision making.

Thus, the concept of electronic democracy has been established as the use of ICT in democratic political processes, linked to the area of political decision-making to realize its key functions, such as the interest articulation, decision-making processes and information exchange between actors [1]. Three axes of electronic democracy have been proposed which constitute the stages of democracy: informative, deliberative and resolutive or participatory [1, 7]. It is argued that the informative area refers to the availability of information to Internet users (as well as its dissemination) to generate knowledge through the assimilation of such information that allows political decisions to be made. As for the deliberative scope, discussions, debates, consultations, agenda proposals and online videoconferences are generated. Finally, the resolutive or participatory axis refers to the participation of citizens in public decision-making through digital means (such as Internet voting), so that their demands are considered [1, 7].

1.2 Electronic Democracy Implementations

Regarding the political sphere, nowadays several countries have opted for a democratic form of government, in which power is exercised by the people through participatory legal mechanisms for political decision making [5]. Each country has implemented different models according to its needs and circumstances. Similarly, in the economic and social sphere, democratic governance is also employed. Two principles established in Article 6 of the General Law of Cooperative Societies are democratic administration and participation in cooperative integration [8]. Article 37 mentions the requirements that a call for an ordinary or extraordinary general assembly of members must meet,

emphasizing the availability of member participation to give validity to the agreements reached.

In [5], the authors point out that the traditional voting process that currently prevails in many Latin American countries (with differences between each country) generally consists of a series of steps that conclude in the quantification of votes to make a political decision. However, they all have the same objective: to ensure a transparent, secure and reliable process.

Furthermore, it has been shown that ICTs provide alternatives to the need for safer and more reliable electoral processes, giving rise to the use of electronic voting systems [5]. Electronic voting systems can be divided in two: electronic voting: consists of voting points controlled by operators, use of electronic devices and potential use of private networks; Internet voting: consists of the ability to vote from anywhere via Internet and distributed servers. Both provide different approaches to contribute towards the electoral process, however, they present different challenges.

On several occasions, these both present the following difficulties: vote counting and scrutiny processes entail high economic costs and require significant time; electoral frauds have been alleged in the different steps of the electoral process, which causes distrust among participants; manual processes entail risks of human error; a centralized electoral process also generates a lack of trust, since anyone with access to the system could alter the results of the process; systems that make use of private networks to exchange information are vulnerable to computer attacks, risking the integrity of the data [5]. Blockchain technology has recently been employed to address information integrity vulnerabilities and data decentralization.

Table 1 compares the tool described in this paper to relevant implementations. This evaluation assesses the provision of key security services and considers the extent to which each axis of electronic democracy, as well as the decentralization in data storage.

Modelo y sistema de votación electrónica aplicando la tecnología de cadena de bloques [5] operates as an exchange of votes between citizens and candidates. In this system, votes are interpreted as transactions, with each transaction recorded in the Blockchain network.

Sistema de voto electrónico basado en blockchain [9] operates as an exchange platform between citizens and candidates. Upon registering in the system, each voter is provided with a digital wallet, through which their single vote is subsequently transferred by the system. Thereafter, voters select a single candidate from a list displayed by the system, thereby transferring their vote to the candidate's digital wallet.

Sistema Electrónico por Internet (SEI) [10] employed by the Instituto Electoral de la Ciudad de México in 2023 and 2024 for democratic processes incorporates biometrics validation, authentication, confidentiality and non-repudiation services provision. The voting process is validated through the list of voters, a double voting prevention mechanism performed twice and the use of asymmetric cryptography signature algorithms.

Table 1. Electronic democracy implementations state of the art.

Implementation	Authentication, confidentiality, integrity, and non-repudiation provision	Informative axis of electronic democracy is considered	Deliberative axis of electronic democracy is considered	Resolutive axis of electronic democracy is considered	Data storage is decentralized
[5]	Yes	No	Yes	Yes	Yes
[9]	Yes	No	Yes	Yes	Yes
[10]	No	No	Yes	Yes	No
Developed tool	Yes	Yes	Yes	Yes	Yes

1.3 Web Tool to Support Electronic Democracy Processes Using Blockchain

This article discusses the development and implementation of a web tool designed to support electronic democracy processes in its three identified axes, which are not served by any other tools jointly (i.e., assisting each axis). So that it meets the requirements for designing valid participatory processes through the proposed technology [1] the dissemination of information and awareness, the mechanisms of consultation and deliberation and those concerning the decision-making process. The tool facilitates the registration and access to information resources, the use of consultations, voting, scheduling, and interactive video streaming with chat for deliberation, as well as the display and follow-up of deliberation outcomes. In addition, a deliberation mechanism which is not usually present on current implementations in this field was developed, such as the use of interactive video streaming featuring chat-based communication.

Meanwhile, the joint support of the three axes of electronic democracy with Blockchain technology and secure communications enables to address the needs of users in the aspects of security and reliability, which are not fully satisfied and give room for the possibility of harming third parties under poor implementations in the field of collective decision-making processes, held by any institution or collective. In order to ensure that the security provisions do not have a significant impact on the performance of the web tool, this approach will be tested by measuring the performance of the web application using the quantitative research methodology.

It has been identified that any democratic regime must have the following characteristics for the process of authentic voting [11]: free, periodic, competitive, clean and decisive. To verify its compliance, the developed tool offers the following security services: confidentiality, through the encryption of the information handled; anonymity, thanks to the intrinsic features frequently present in blockchain networks such as the use of pseudonyms; integrity, achieved from the creation and validation of the blocks in the blockchain network; non-repudiation, provided by the use of private keys and the policies for their use, once the blocks in the chain are approved they become immutable and irreversible [4].

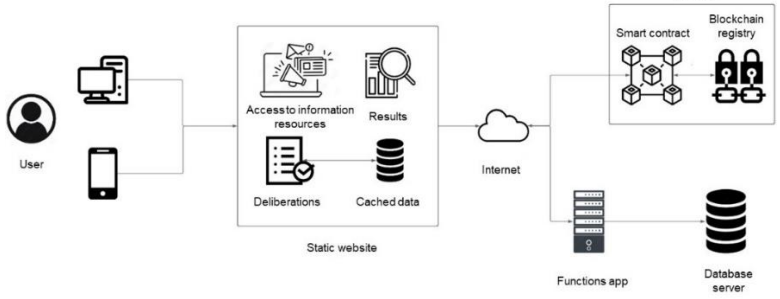

Fig. 1. Web tool architecture.

The remainder of this paper is organized as follows: Section 2 details development of the web tool. Implementation results are presented in Section 3. Conclusions and future work are discussed in Section 4.

2 Development

The web tool consists of a web application connected through the internet to the smart contract deployed on a blockchain network, to a database server for querying and storing the necessary data and to an external file server for querying the recordings of video transmissions and information resources, as shown in
Fig. **1**.

For the development of this web tool, the SCRUM methodology was chosen because of its work scheme in which work is defined, reviewed and advanced. This scheme allows to focus on the production of functional components and makes possible, by means of an incremental structure, to split the complexity of the project and to periodically satisfy determined objectives [12].

The work was organized in 7 work cycles of 3 weeks called Sprints, during which the team worked on incrementing the project. At the beginning of the development, the set of features that integrate the project were defined in 28 user stories, identifying their estimated time, priority, description and acceptance criteria. Along with the user stories, the Sprints were planned to develop the research, analysis and design, the functionality of the web tool with the database, the streaming video with chat, the methods of the smart contract, the designed user interfaces and the verified integration of components.

At the beginning of each Sprint, a planning meeting was held to define the tasks to be performed, and short meetings were held daily to synchronize activities. At the end of each Sprint, the completed work is reviewed according to the acceptance criteria for the increment and reflection is made on how to improve in the next cycle. This organization is managed through a prioritized list with all the user stories that make up the project and other similar lists with the user stories selected for each Sprint, as well as the increments produced at the end of the Sprint.

Also, within the team, roles associated with the methodology were assigned according to the experience with the methodology and the capabilities of each member. The team was composed of Carlos Huerta García, responsible for maximizing the value

of the project and managing the prioritized list of user stories; Axel Ernesto Moreno Cervantes, Nidia Asunción Cortez Duarte as facilitators of SCRUM practices and values, supporting the team to overcome any obstacles; Oliver Manuel Hernández Méndez, Rafael Hayyim Medina Sosa, Marco Antonio Ocaña Navarrete as cross-functional development team, in charge of delivering product increments at the end of each Sprint. Synthesizing the established user stories, the following actions were defined:

First, the registration process was established, where the user registers by providing his name, email and password. To gain access, users must verify their account with a one-time password that is sent to their e-mail address and reset their password through the same process. Due to the limited collection of data and the use to which it is put, it is guaranteed to satisfy the ARCO rights.

Subsequently, by accessing the tool with their email and password, a session is established which is verified at each further functionality and they have the option to create or join a collective while the collectives to which they belong or manage are displayed. To join a collective involves the use of a code displayed at the time of creation or management, while creation implies specifying the name, type and description of the collective, along with the attachment of one NEAR. Besides, when a collective is created, its administration is assigned to the user who creates it, while it is possible to assign more administrators with the email of a member of the collective who is not already an administrator.

Within the collective context, the registration of decision-making processes can be carried out, including information such as the name of the process, the expected resolution and a detailed description. Prior to initiating any deliberation, the process manager (the registrant) provides informational resources so that the collective members are fully informed before reaching a determination.

Deliberation mechanisms are a crucial part of the decision-making process. For its registration, a date is requested that meets a minimum 10-day deadline, in accordance with the General Law of Cooperative Societies. In addition, a title for the mechanism is required and, depending on the type of deliberation (whether it is a forum, voting or consultation), specific details must be provided, such as a description for the forum, the options for voting, and a set of questions and options for consultations. To participate in any mechanism, if it is the registered date participation will occur via postings, votes and video streaming. The prevention of double voting is achieved through the storage of a hash of each user who has participated. If the hash exists when the user attempts to vote for a second time, a warning is generated, indicating that the user may only cast a single vote.

Finally, at the conclusion of any deliberation, the corresponding link is entered to follow up on the resolution reached once the established date has elapsed. In the case of forums, a summary of the posts is added, thus completing the cycle of participation and follow-up on the platform.

The development of the source code was performed in a Git repository with the GitFlow framework. A team member was assigned responsible for each task and pull requests were incorporated upon completion, achieving an incremental integration of the project.

Upon tasks completion within a Sprint, a release branch was created consolidating the developed tasks with the main and development branch. In addition, Azure DevOps was implemented for continuous integration, BitBucket as a Git repository server, and Jira Software to manage issues associated with SCRUM methodology. All user stories were collected in Jira, along with the titles for each Sprint as epics and the tasks and subtasks defined related to the user stories, so that the status of each task or subtask was tracked on a Kanban board in the scope of a Sprint. At the end of each Sprint, its retrospective was posted on a Confluence page within the Jira project after analyzing the pace of work reflected in the Sprint Burndown reports generated by Jira.

Regarding the technologies employed, mongoDB was selected to store the information associated with the electronic democracy processes in a non-relational database. For the provision of the functionality, an Azure functions app with Node.js and TypeScript was determined. To consume these functionalities, a React with TypeScript static website was specified. Furthermore, the REST API approach was employed to ensure simplicity in the interactions between the functions application and the static website.

Concerning the Blockchain, it was defined to use NEAR which uses the Ed25519 signature to provide authentication, and the SHA-256 hash algorithm for integrity. It is significant to note that every communication between the various entities that comprise the web tool has been configured to be handled exclusively via the HTTPS protocol, in which the ECDHE-X25519, ECDSA-X25519, AES-256-GCM and SHA-384 algorithms usage are preferred to provide authentication, confidentiality and integrity in the exchange of information.

Two main modules were developed for the web application: a static website and a functions application. The website, built with React and managed with Yarn and Vite, integrates unit tests with Vitest. It is organized into mainly components and pages, each with an associated set of test cases for unit testing. The guidelines for design defined in Material Design 3 were followed to provide an interface that would be familiar to most users.

The implementation of features was structured around the functionalities and their associated integration test cases. For video streaming with chat, the SignalR real-time communication service was employed. In the continuous integration pipeline, it is tested, statically analyzed for code quality with SonarCloud and the site is packaged for deployment. The functions application, created with Azure Functions and Jest for testing, follows a similar process with a continuous integration pipeline of integration testing, static code quality analysis with SonarCloud and packaging. Each functionality is defined in a function triggered by HTTP requests, leveraging the elasticity of dynamic provisioning.

The smart contract is defined in a class with contract methods and function sets associated with users, collectives, decision making processes, deliberations, forums, meetings, consultations, voting and results so that the contract methods realize the functionalities of the corresponding sets. It is structured with methods for entities, managing state efficiently in associative arrays. The continuous integration pipeline used with the latter includes static analysis of code quality and contract construction, generating a compiled WebAssembly file for publication.

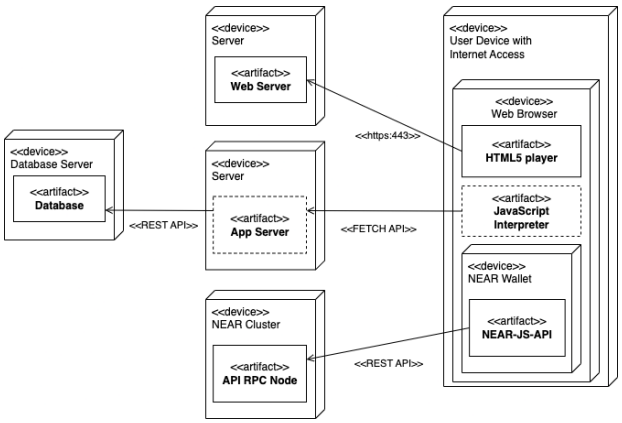

Fig. 2. Deployment Diagram.

The artifacts resulting from the integration pipelines were deployed using infrastructure as code, stored and used within the published packaging. The files that resulted from building the different projects that make up the development are unpacked and then utilized. The Azure for Students license was leveraged to deploy the dynamic website using Static Websites, configuring the redirection of paths to the input file. Also, the same license was used to deploy the functions application, configuring environment variables and resource sharing policies. In addition, an account was created on the blockchain network to deploy the smart contract, using near-cli and the compiled WebAssembly file obtained from building the source code.

Overall, each action is performed by the interaction between the static website and the user through a browser. From the website, it communicates with the functions application and the smart contract deployed on the Blockchain, so that the actions are reflected in the electronic democracy processes, displaying a feedback message of the action performed and the link to the details of the transaction recorded in the transaction browser of the blockchain network used. The distribution of each component can be illustrated as shown in the deployment diagram in Fig. 2.

3 Results

Referring to the tests performed, Table 2 shows the results obtained in the different types of tests. A total of 115 unit tests were executed with Vitest in which each branching point in the code units of the web site is tested without failures or errors in less than 27 seconds. For the acceptance tests, all the acceptance criteria established in each of the 28 user stories are met. An average response time of 43 milliseconds was recorded scaling from 20 to 100 users by increasing 5 users every minute for 20 minutes with Blazemeter, being always available. Also, using loader.io, a content display time of 1.7 seconds and an accessibility evaluation of 98/100 in PageSpeed Insights were obtained. 236 integration tests were performed with Jest in which each function

Table 2. Tests results obtained.

Tests type	Test cases	Time	Score
Unit tests	115	27 s	100
Integration tests	236	332.6 s	100
Acceptance tests	28	Not applicable	100
Performance tests	16	43 ms	Not applicable
Usability tests	8	1.7 s	98
Security tests	16	Not applicable	100

established in the web application was verified without failures or errors in less than 333 seconds. The confidentiality of information in communications between the web site, the function application and the smart contract was verified for each functional requirement through man-in-the-middle attacks using Wireshark to read network traffic and participate in the communication if possible. For all 16 functional requirements the confidentiality, integrity and authenticity of the information was rated as excellent.

As the version of the Azure functions application used at the time of tool deployment did not resolve the cold-start issue associated with serverless implementations, the performance tests revealed higher than expected average response times. However, the performance and usability tests did not reflect any significant impact on the performance of the developed tool, even with the security provisions in place.

Considering the acceptance tests results, it can be said that the three key axes of electronic democracy are fully met, contributing to the increased reliability of the democratic processes facilitated by the tool. Throughout the security tests, the provision of authentication, confidentiality and integrity services is verified. Considering the verified security services and the smart contract used in a public blockchain network for the registration of any action within a democratic process, the identified security vulnerabilities are addressed. Therefore, it can be said that the security of democratic processes carried out with the developed tool is increased. Finally, regarding the results of the unit and integration tests, it can be said that the functional application, static website and smart contract development have a remarkable quality.

4 Conclusions and Future Work

The web tool developed addresses the need to enhance the security and reliability in the decision-making processes in democratically driven collectives by utilizing a public blockchain network to record all actions within the electronic democracy processes, providing authentication, integrity and non-repudiation.

This facilitates the consultation of the actions undertaken throughout the democratic process. In addition to the use of HTTPS, the vulnerabilities present in the contemporary electronic democracy systems are mitigated. Moreover, it provides support for the three identified axes of electronic democracy. Firstly, the tool enables the provision and display of information resources in a manner that is consistent with the informative axis. Secondly, it streamlines participation through four distinct

deliberation mechanisms, namely voting, video streaming, consultations, and forums. This enables the completion of the deliberative axis and the fulfilment of the regulatory framework for cooperative societies in Mexico.

The capability to reach a resolution after collective participation and the registration of information related to the follow-up of the resolution reached fulfills the resolutive axis and concludes the electronic democracy process. The operation, stability, and usability of the tool were verified in the tests carried out.

It is proposed that a functionality be included for users to easily update their information, thereby providing flexibility and accuracy in profile management. Additionally, the implementation of an email notification system is proposed to inform collective members about new decision-making processes, information resources, updates on the status of scheduled deliberations and resolutions reached, with the aim of improving communication and participation of collective members.

In the context of the deliberation mechanisms present in the tool, it is proposed that the automatic generation of the summary of the publications in the forums be achieved with large language models based on artificial intelligence. Similarly, automatic generation of minutes in the video transmissions should be implemented using the same proposed technology. Another avenue for improvement involves the expansion of these deliberation mechanisms, with the objective of exploring and adding more tools to enrich the decision-making processes, thereby increasing the efficiency and inclusiveness of the platform.

Furthermore, the potential for decentralizing not only the validation of electronic democracy processes, but also the data associated with them, is also discussed. If a blockchain network managed by the collective is utilized, the integration of the logic of the functions application within the smart contract is contemplated. This is done to maximize decentralization, strengthen the autonomy of participants, and ensure the integrity of information in a distributed environment. Each member of the collective would possess a network node. Consequently, with the advancement of mobile computing power, it is now feasible to provide a tool to support the processes of electronic democracy that are conducted in large collectives, such as countries, with a blockchain network assisting the democratic exercise within a nation-state.

Acknowledgments. The authors would like to express their gratitude to the Instituto Politécnico Nacional (IPN) and Escuela Superior de Cómputo (ESCOM), as well as Oliver Manuel Hernández Méndez, Rafael Hayyim Medina Sosa, and Marco Antonio Ocaña Navarrete, for their invaluable contributions to the development and realization of this work.

References

1. Hernández, N.E.: El voto electrónico en la construcción de un modelo de democracia electrónica. Estudios políticos, 47, pp. 61–85 (2019) doi: 10.22201/fcpys.24484903e.2019.47.69500.

2. Nath, K., Dhar, S., Basishtha, S.: Web 1.0 to Web 3.0 - Evolution of the Web and Its Various Challenges. In: International Conference on Reliability Optimization and Information Technology (ICROIT), pp. 86-89 (2014) doi: 10.1109/ICROIT.2014.6798297.
3. Alabdulwahhab, F.A.: Web 3.0: The Decentralized Web Blockchain Networks and Protocol Innovation. In: 1st International Conference on Computer Applications & Information Security (ICCAIS), pp. 1–4 (2018) doi: 10.1109/CAIS.2018.8441990.
4. Tasende, I.: Blockchain y arbitraje: Un nuevo enfoque en la resolución de disputas. Especial énfasis en smart-contracts y criptodivisas. Revista de Derecho (Universidad Católica Dámaso A. Larrañaga), 22, pp. 138–159 (2020) doi: 10.22235/rd.vi22.2127.
5. Lucuy, G.A., Köller-Vargas, S.A., Galaburda, Y.: Modelo y sistema de votación electrónica aplicando la tecnología de cadena de bloques. Acta Nova, 9(2), pp. 236–256 (2019)
6. Olivares, J.C., Reyes-Archundia, E., Gutierrez, J.A.: Un sistema transactivo de energía ciberseguro usando cadenas de bloques de múltiples niveles. Computación y Sistemas, 27(3), pp. 851–867 (2023) doi: 10.13053/cys-27-3-4071.
7. Posada, L.J.: MIRA: Internet, participación y democracia: Las nuevas tecnologías y la reconexión con el ciudadano. Civilizar Ciencias Sociales y Humanas, 11(20), pp. 57–74 (2011) doi: 10.22518/16578953.24.
8. C.D.D.D.H.C.D. LA UNIÓN: Ley General de Sociedades Cooperativas. Diario Oficial de la Federación. Ciudad de México (2018)
9. Sánchez, S.A.: Sistema de voto electrónico basado en Blockchain. Pontificia Universidad Católica del Perú (2021)
10. Consejo General del Instituto Electoral de la Ciudad de México: Estudio de viabilidad técnica, operativa y financiera que presentan la Dirección Ejecutiva de Organización Electoral y Geoestadística y la Unidad Técnica de Servicios Informáticos para proponer el uso del Sistema Electrónico por Internet, como una modalidad adicional para recabar votos y opiniones en la Elección de Comisiones de Participación Comunitaria 2023 y en la Consulta de Presupuesto Participativo 2023 y 2024. Instituto Electoral de la Ciudad de México, Ciudad de México (2024)
11. Centro de Capacitación Judicial Electoral: Régimen democrático. Tribunal Electoral del Poder Judicial de la Federación (2010)
12. Scrum Guide: https://scrumguides.org/scrum-guide.html (2020)