ISSN 2347 - 3983
Volume 8. No. 9, September 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter14892020.pdf
https://doi.org/10.30534/ijeter/2020/14892020

Integrated Electronic Voting System Prototype for the election of projects of municipalities in Lima

Max Antony Acosta-Espinoza[1], Alexi Delgado[2]
[1]Systems Engineering Program, Universidad de Ciencias y Humanidades, Lima-Peru, maxacostae@uch.pe
[2]Mining Engineering Section, Pontificia Universidad Católica del Perú, Lima-Peru, kdelgadov@pucp.edu.pe

ABSTRACT

In Peru the electoral process as well as the approval of national projects are affected by the delay of the process since these decisions are usually carried out in the traditional way, that is to say, through paper and pencil voting; besides that it includes administrative expenses and efforts that could be replaced by a better option. For this reason, a new integral system of electronic voting is intended to be developed, based on the Scrum methodology. With this objective, the panoramic data of the country is evaluated to verify the viability of the project; therefore, the present study is decided to concentrate in the area of metropolitan Lima and its municipalities to be able to reach a platform that allows the fast and easy election or approval of national subjects in an anonymous way, like the traditional, and secure. The results of this study will serve as a basis for local and national authorities to consider the implementation of the platform as well as benefit the scientific community by addressing e-voting in detail.

Key words: Blockchain Encryption, Electronic Voting,Mockups, Scrum Methodology.

1. INTRODUCTION

Currently the elections in Peru are done manually using a pen and paper to mark the election of each individual preference[1], this generates a massive process generating a delay, operational burden, in addition to major expenses to pay to personnel, etc. Hence an electronic voting must be considered for its implementation to improve this situation taking as an example of implementations of electronic voting that began in Europe in the early 1990s in the countries of Holland and Sweden and then continued with France and Belgium among others in 1991-1992, of which Belgium is one of the veteran countries with respect to electronic voting, which was provided from previous decades until today [2]. They were carried out at the beginning as a pilot, however the result was encouraging as most of the participants of the test exercised the task of selecting their own option trough the electronic voting in an optimal manner [3]. For this reason, in the present study an interface to solve these problems is sought trough an Integral System of Electronic Voting that will allow us to be agile to make decisions of what is proposed in the system.

The agile scrum methodology is used for the development of the project in question, this methodology will help to be able to be improved as we go along [4], since if an error is found it is solved and the change proceeds. There are also other methodologies with which this project can be developed, such as rational-rose software, in which UML diagrams are made identifying actors and stakeholders to carry out the development of the prototype[5].

The prototype that will be applied in this work remains as an implementation proposal [6] for the municipalities of Metropolitan Lima. Although a great diversity of descriptions have been suggested for electronic voting[7]–[10], in this article it will be handled as the systematization of the beginning to the result of the interval of emission and data processing of the vote.

The objective of the current research study is to provide an integral electronic voting system for the approval or election of projects of the municipalities that is currently being carried out by the municipal managers through the implementation of a software prototype of an electronic voting application with security barriers in order to make the process as safe as possible.

The current research work is organized as follows. Section 2 will explain the methodology applied to this project in detail for the design of the system. Following, section 3 will show the case study. Then section 4 will display the corresponding results and discussions. Finally in section 5 the conclusions will be detailed.

2. METHODOLOGY

The present methodology to be used and explained is Scrum, which was established in the late 1990 [11].This election has been made considering that the method will facilitate the creation of the prototype itself since it allows to update and improve the software in full development, meaning that Scrum allows to make the corresponding modifications unlike a conventional methodology[12]. The phases of such methodology are represented in Figure 1.

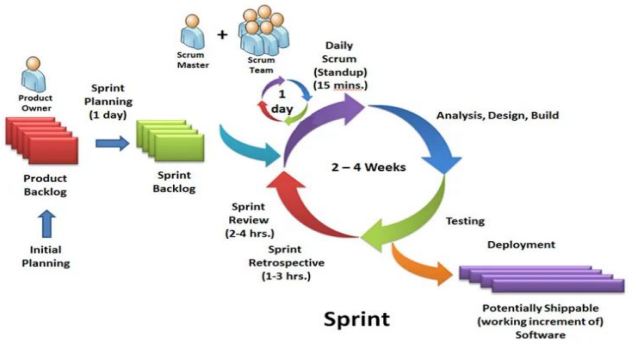

Figure 1: Scrum Stages Representation [13]

2.1. Phase I - Using Scrum

The phases of Scrum methodology are explained as follows:

A. Product Backlog

It serves as the sole basis of requirements for any changes that may be made to the product[10] .For this reason, it might not be 100% finished as improvements can be made constantly; therefore it is a competitive, dynamic and useful act to perform [14]. A representation of the activity may be seen in Figure 2.

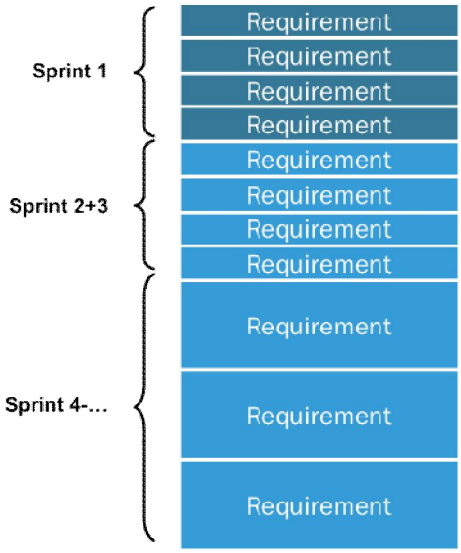

Figure 2: Schematic of the Product Backlog[14]

B. Sprint Planning

It is the activity in which each sprint is planned in order to achieve the general objective [12]. Sprint preparation tends to have a maximum time of 8 hours for a Sprint that is developed during a month in order to ensure its viability and functionality for the main purpose[15].

C. Sprint Backlog

In this stage the development group and the user forecast which function will be in the next increment and what the work will be to return that functionality in a "Ready" increment[16], a visual representation of this is shown in Figure 3.

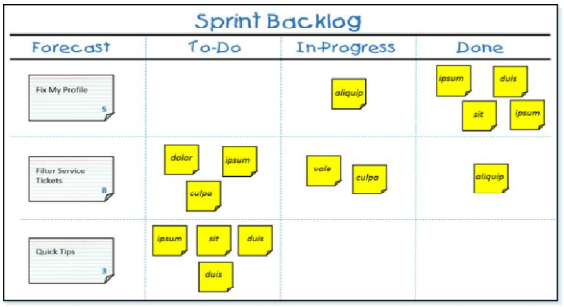

Figure 3: Schematic of the Product Backlog[16]

D. Sprint Review

According to the Agile Methodologies Scrum Guide[12], a Sprint Review is performed at the completion of each Sprint to examine the Increment and accommodate the Backlog Product if needed [17]. This is a maximum of a four-hour meeting for a month's worth of Sprints.

2.2. Phase II - Architecture

The architecture of this system counts with the interaction of the user or visitor that will handle the Electronic Voting system, in it an encrypted voting of the visitor from end to end will be found, which will allow to provide the security of his vote[18].Such programming is based on another research on the implementation of the system to be developed, therefore, within this article the process of the architecture that we will use for the prototype is shown, this clarification is applied to the current phase that is explained as well as for phase III and phase IV.

Therefore, the user's vote will be directed to one of the election nodes which will allow to validate the vote, to add to blockchain and then propagate it to the block candle as seen in Figure 4.

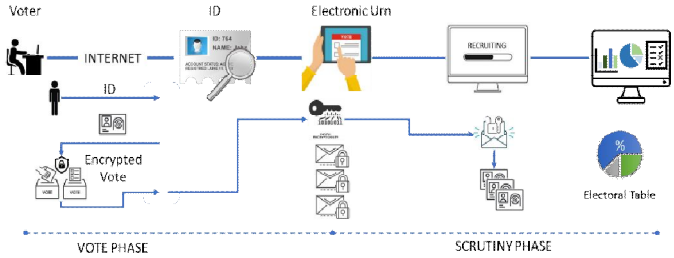

Figure 4: Stages of e-voting and development –blockchain rules in electronic voting methods

This whole process provides greater security from the origin to the destination of the vote made by the user or citizen, generating the viability of the method used for the protection of data sent through this internal system.

2.3. Phase III - Encrypted Voting

The new cryptographic cipher will be the basis for the current study, it is based precisely on the presence of only two keys, which are public and private [19], [20]. Nevertheless, it is worth to mention that regarding this encryption method is also used in order to decrypt information, meaning that one requires the other, i.e. if a message that has been encrypted from a private key is sent, that key is only known to the voter

[16], as it can only be decrypted with the public key. Frequently, those individuals who use this system announce and place their public key at their disposal so that anyone who wants to and is interested can send them information encrypted with total security that only they can decipher [14], making the electronic vote personal as the traditional one. A graphic representation of this process can be seen in Figure 5.

Figure 5: Voting process handling of blockchain protocols[18]

It is advantageous that the system has the encryption of the votes, because this ensures that the selection of the voter is correct and we can avoid any kind of fraud, as shown in Figure 6.

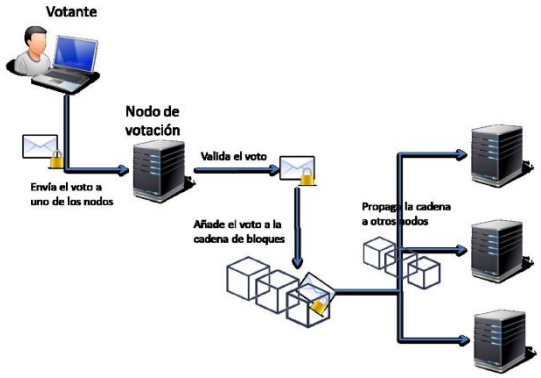

Figure 6: Electronic voting system architecture using blockchain protocol encryption for electronic voting[18]

2.4. Phase IV: Security Weakness Analysis

The layers that the system will have for the security of the servers, will be 3, of which the first layer of the web server will have the function of showing the design, the presentation and the access to web; then, the second layer of applications will contain the operations of encryption for the votes by user; and in the third layer of database will be integrated the key of the decryption and will contain all the data of the users of the system that interact with the system[18], [21], as seen in Figure 7.Then, the election system is a multi-layer architecture using a block chain, called the Bulletin Board, which is cryptographically based on the Bitcoin block chain.

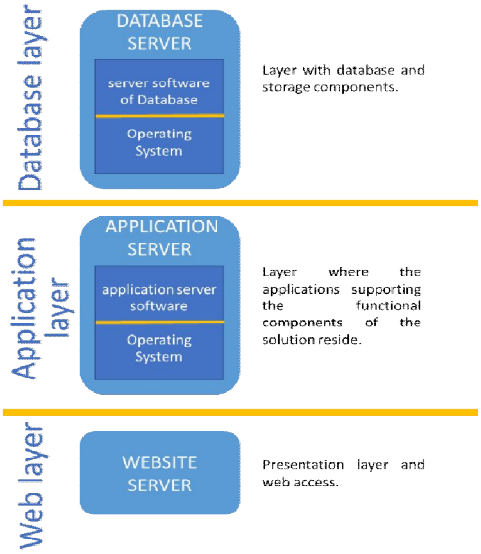

Figure 7: 3-layer web assistance architecture of blockchain rules in electronic voting methods[18]

3. CASE STUDY

From the beginning of this section until the end, the use of the scrum methodology is carried out.The detailed investigation of the figures is shown below, stating what information was found that contributes the technique used to provide the demonstration to the problem being traced. This is revealed in the following.

In the statistical table of Figure 8 the exact number of people able to vote in Peru is shown, being exactly 24'799,384, which represents 70.27% of the entire Peruvian population at the end of the fourth quarter of 2019 including voters who are both in the national territory and abroad. From that, we can also appreciate that only the capital, Lima has a population able to vote of more than 8 million being the 33.06% of the total population [22], [23].

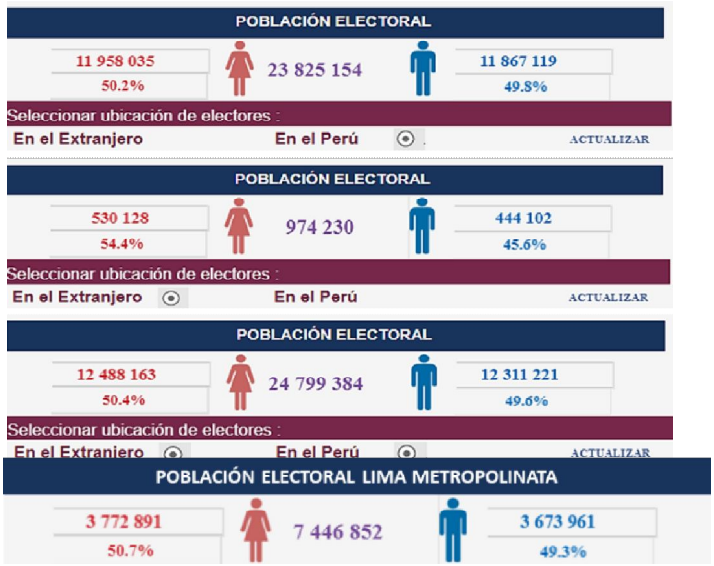

Figure 8: Population able to vote until 2020 according to Extraordinary Congress Elections 2020 [22], [23]

In Figure 9 the population that accesses the Internet until the last national census in 2018 is shown, being the 80.39% of the total population. Those statistics increased by 14.30% in 2017 and then by 10.09% until 2018, compared to the previous year. The statistical results were used for a projection analysis to find out approximately how many Peruvians will be able to access the Internet, which is assumed to reach over 90% by the current year 2020[24].

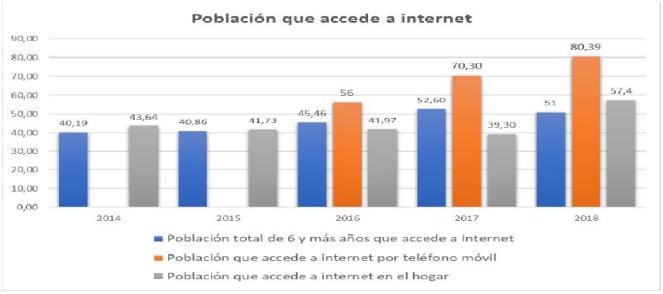

Figure 9: Current population accessing the Internet until 2018[25]

Figure 10 shows that the population according to the INEI detailed by age demonstrating that adults are also accessing the Internet for both distracting and informational activities. Nevertheless, young people have a higher use of the internet with 81.60% at a national level as shown in Figure 10.

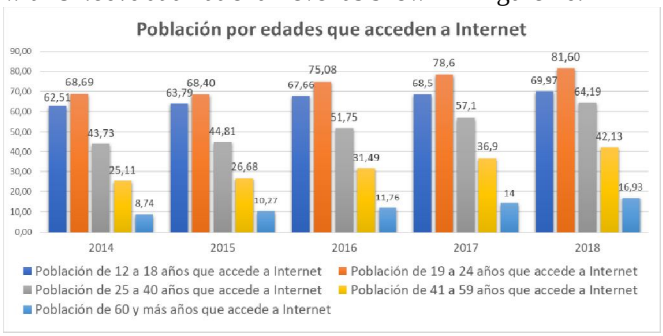

Figure 10: Population from 12 to over 60 years old accessing the Internet[26]

Moreover, an statistical graphic in Figure11enables us to see the percentage of households in Lima that have access to the Internet as well as those that have technological devices such as cell phones or computers, so that they can connect to the Internet, being able to vote without any problem if needed. This is represented in order to measure the feasibility of the project to be carried out.

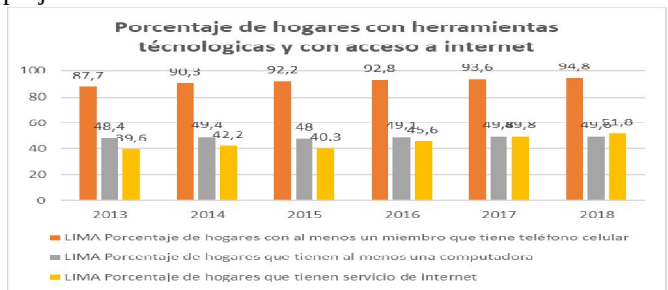

Figure 11: Population that possess technological devices to access to the internet[26]

In Figure 12, we can appreciate that almost 100% of the people in Metropolitan Lima have mobile service, which supports the fact that the application will be used by the majority of citizens, which represents 95.08% nowadays.

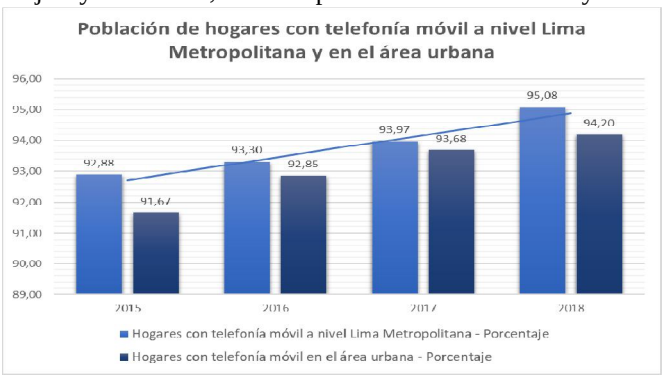

Figure 12: Population of households with a mobile phone at the level of Metropolitan Lima in the urban area [26]

Once the data is collected and the feasibility of the project is demonstrated, the prototype of the Integral System of Electronic Voting application will be elaborated by means of the use of phases II, III and phase IV with the tool called Balsamiq Mockups, as its advantages on the creating mockups process has been evidenced as it helps in such process through an interactive interface user friendly and free of charge[27]–[30].

As shown in Figure 13 the user who has entered to the application will be asked to enter his ID number (the verification digit that is located in the upper right side of the front of the document), the date of issue (which is located in the middle right side of the front), the date of birth, and finally enter the name of his father and mother in order to ensure the security of each individual and to avoid duplications of votes or mishandling of the platform, since validations will be made with the data gathered by Reniec (a Peruvian Institute of National Identification and Civil Status Registry). All this data will be necessary to enter the integral system of electronic voting, this avoids the impersonation of the voter[31]and then leading to the next screen.

Likewise, in the screen shown in Figure 13, the security and integrity of the data of the electronic voting process is a system that must be transparent and reliable, as well as safeguard the identity of the voters [9].The challenge at this step is the need to achieve the anonymity of the citizens, in other words, to eliminate the identity of the voter [19]. As a basic function of this solution, Blockchain technology has been identified as sufficiently addressing all these challenges[34].

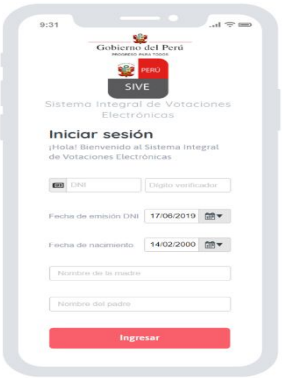

Figure 13: Log in Screen

In the voting section, shown in Figure 14, the user will have the option of selecting the project he is interested in and vote for the municipality he belongs to. In this view, a list of projects is shown, where the citizen will obtain relevant information about the chosen project, which is about the option voteand will direct him to the proposal section.

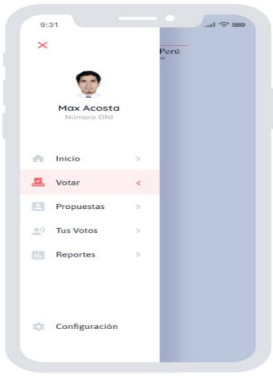

Figure 14: Main Menu

Following, the proposals of the municipalities that are state workers will be made known. Figure 15 shows a list of proposals that will be published periodically for the knowledge and awareness of the citizens. When publishing a project, it allows only nodes with valid identification to join the network, thus preventing unknown and malicious devices from entering the network [2]. This would produce an alteration such as changing information in the proposals that will be shown to the voting users.

In this screen, the candidate will be able to include general information about the project such as the amount of investment, its duration, which companies will be hired for it and a general summary of what the project is about, among other.

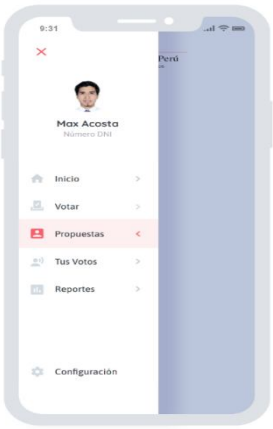

Figure 15: Proposals Menu

The screen in Figure 16, on the other hand, will show a list of all the votes made by the user up to the date in which he consults, so a record of what he did previously can be provided with that information without the need to request it from the municipality to which he belongs and generate an operational delay. This also corroborates that it is the same voter who requested it. That is why it will be useful to make your elections available to the citizen who uses them.

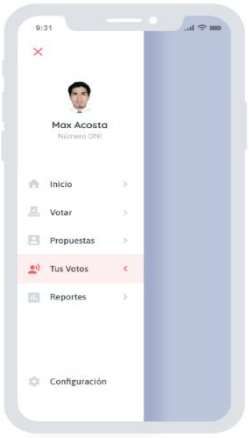

Figure 16: Votes Relation History

In the last screen of Report of Results, shown in Figure 17, the report of the final votes will be shown at the end of the voting process, this will help them to see the result online and have access to see the status of the other projects that are in the process of voting, which will be shown in different graphs so that it is understandable by the citizens that may not have experience in interpreting statistical graphs.

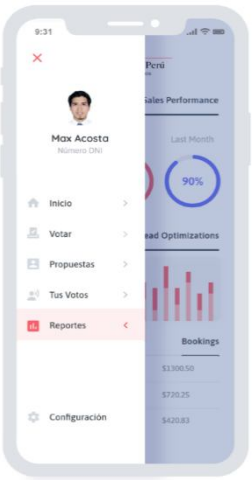

Figure 17: Reports Menu

4. RESULTS AND DISCUSSION

4.1 About the Case Study

The design of the application was carried out fulfilling the security measures for the login as well as for the use of it; the sketch that was made, is understandable and friendly for the user thanks to the use of the Balsamiq Mockups tool, which allowed us to create the application as desired using the process of phases towards its correct conformation. Likewise, this tool election is highlighted as it was intuitive and provided various functions with respect to others in the market. Between Figures 13-16, the screens showed the data that the application requested, in which entering its data will be validated and at the same time it will be registered with the

purpose of providing the citizens that belong to the corresponding municipality where it will be used, concluding in Figure 17 where the user was be able to see the result of his votes.

Regarding to a previous study called Blockchain-Based Electronic Voting System for Elections in Turkey [36], it has been observed that in its system all the voting information is kept in the highest level blocking chain, so that the voting information of the whole country can be instantly accessible at any time after it is synchronized. Thus, it will not be a problem to explain the election results, and it will save a lot of time that is being spent to count the votes. This was used to change the old inefficient system and will bring a modern and efficient system to Turkey, and will also lead to saving a lot of energy and money across the nation [36]. Although the work done in the mentioned study had a positive result, the present one is considered more accurate in comparison since relevant data have been taken into consideration such as the viability of the project in urbanized areas, making it more realistic since it must be taken into account that not all the population can access the Internet, and therefore the proposed tool.

On the other hand, with respect to another research work on the topic called Towards a Voting System that Preserves Privacy through Blocking Chain Technologies [22], we observe good practice on the use of blocking, which provided greater security over the process from the time the user interacts with the system, to when he or she votes and the operation of the validations made are processed to verify and avoid duplicate votes or errors in the process [22]. In comparison with this work, this practice is the one that will be carried out in the current project of this study; therefore the differences are found in the context given.

4.2 About the Methodology

The methodology used, Scrum, was effective and efficient as itenabled to carry out the prototype of the mentioned project helping to improve the project while it was progressing. Likewise, the encryption will be used by applying the SHA-256 algorithm [23]. Therefore, the architecture should be used to reduce the risk of possible attacks[39]. And finally, the Model View Controller (MVC) will be used for the creation of the application, which allows a correct and orderly programming. This ensures that the proposed project will be stable for its development and application in the context proposed.

5. CONCLUSIONS

Regarding the case study and considering the data obtained from the context in Metropolitan Lima, the objective of developing an application that allows citizens to vote electronically in a safe and efficient way in their respective municipalities has been optimally achieved.

Likewise, the methodology applied proved to be useful for the case study since the application of the Scrum method allowed an agile interaction open to change for constant improvements of the development during the time of elaboration of the final result of the project.

Finally, this research is open to any improvement that allows an efficient interaction of the user with the application, and can be extended to topics that cover a larger population that has technological devices, but also an Internet service, either by data or through a stable Wi-Fi network and a variety of devices to not limit its use, in which the individual is allowed to interact with the system without slowness and at the same time with the purpose of streamlining the current processes. Nevertheless, it is highly recommended to be aware of the context in which the future studies will be developed in order to measure its viability in the real life.

REFERENCES

1. C. K. Adiputra, R. Hjort, and H. Sato, **A Proposal of Blockchain-Based Electronic Voting System**,*Proc. 2nd World Conf. Smart Trends Syst. Secur. Sustain. WorldS4 2018*, pp. 185–192, 2019.
2. V. Bax, W. Francesconi, A. Delgado, **Land-use conflicts between biodiversity conservation and extractive industries in the Peruvian Andes**, Journal of Environmental Management, 232, pp. 1028-1036.
3. K. Teja, M. B. Shravani, C. Y. Simha, and M. R. Kounte, **Secured voting through Blockchain technology**, *Proc. Int. Conf. Trends Electron. Informatics, ICOEI 2019*, no. Icoei, pp. 1416–1419, 2019.
4. A. Srivastava, S. Bhardwaj, and S. Saraswat, **SCRUM model for agile methodology**, in *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2017*, 2017, vol. 2017-January, pp. 864–869.
5. J. Chen, B. Wang, D. Gu, J. Zhang, and D. Yang, **Requirements analysis of real-time systems by rational-rose UML**, *2009 2nd Int. Symp. Knowl. Acquis. Model. KAM 2009*, vol. 1, pp. 324–327, 2009.
6. C. Angsuchotmetee, P. Setthawong, and S. Udomviriyalanon, **BlockVOTE : An Architecture of a Blockchain-based Electronic Voting System**, *ICSEC 2019 - 23rd Int. Comput. Sci. Eng. Conf.*, pp. 110–116, 2019.
7. A. Rodríguez-Pérez, **Secret suffrage in remote electronic voting systems**, in *2017 4th International Conference on eDemocracy and eGovernment, ICEDEG 2017*, 2017, pp. 277–278.
8. M. R. Alam, M. Masum, M. M. Rahman, and M. A. Rahman, **Design and implementation of microprocessor based electronic voting system**, in *Proceedings of 11th International Conference on Computer and Information Technology, ICCIT 2008*, 2008, pp. 264–269.
9. S. Dey, K. Mondal, J. Nath, and A. Nath, **Advanced Steganography Algorithm Using Randomized Intermediate QR Host Embedded With Any Encrypted Secret Message: ASA_QR Algorithm**, *Int. J. Mod. Educ. Comput. Sci.*, vol. 4, no. 6, pp. 59–67, Jun. 2012.
10. R. Rezwan, H. Ahmed, M. R. N. Biplob, S. M. Shuvo, and M. A. Rahman, **Biometrically secured electronic**

voting machine, in *5th IEEE Region 10 Humanitarian Technology Conference 2017, R10-HTC 2017*, 2018, vol. 2018-January, pp. 510–512.
11. Z. Ereiz and D. Music, **Scrum Without a Scrum Master**,*2019 IEEE Int. Conf. Comput. Sci. Educ. Informatiz. CSEI 2019*, pp. 325–328, 2019.
12. A. Delgado, P. Montellanos, J. Llave, **Air quality level assessment in Lima city using the grey clustering method**, *IEEE ICA-ACCA 2018 - IEEE International Conference on Automation/23rd Congress of the Chilean Association of Automatic Control: Towards an Industry 4.0* - Proceedings, 8609699.
13. **Los 5 pasos del Scrum Master**.[Online]. Available: http://www.dimajeff.com.mx/blog/articulos/item/42-los-5-pasos-del-scrum-master. [Accessed: 18-Dec-2019].
14. Scrum.org,**What is a Product Backlog?**, 2017. [Online]. Available: https://www.scrum.org/resources/what-is-a-product-backlog. [Accessed: 08-Aug-2020].
15. Scrum.org, **What is Sprint Planning?**, *Scrum.org*, 2020. [Online]. Available: https://www.scrum.org/resources/what-is-sprint-planning.
16. Scrum.org, **What is a Sprint Backlog?**, *Scrum Org*, 2019. [Online]. Available: https://www.scrum.org/resources/what-is-a-sprint-backlog.
17. Scrum Org, **What is a Sprint Review?**,*Scrum Org*, 2019. [Online]. Available: https://www.scrum.org/resources/what-is-a-sprint-review.
18. A. Marín Bermúdez, **Estudio de la utilización de protocolos blockchain en sistemas de votación electrónica (Study of evoting System using blockchain protocol)**, 2016.
19. S. Agbesi and G. Asante, **Electronic Voting Recording System Based on Blockchain Technology**,*2019 12th C. Conf. Cybersecurity Privacy, C. 2019*, 2019.
20. K. Kost'Al, R. Bencel, M. Ries, and I. Kotuliak, **Blockchain e-voting done right: Privacy and transparency with public blockchain**,*Proc. IEEE Int. Conf. Softw. Eng. Serv. Sci. ICSESS*, vol. 2019-Octob, pp. 592–595, 2019.
21. A. Delgado, I. Romero, **Applying the Grey Systems Theory to Assess Social Impact from an Energy Project**, *Proceedings of the 2018 IEEE 25th International Conference on Electronics, Electrical Engineering and Computing*, INTERCON 2018, 8526372.
22. **JNE aprueba padrón con más de 24 millones de electores para elecciones congresales del 2020**,*TvPerú*, 16-Nov-2019.
23. **Elecciones 2020: 24 millones 799,384 peruanos votarán en enero**,*Agencia Peruana de Noticias Andina*, Lima, 16-Nov-2019.
24. F. A. Costa and I. N. de E. e I. INEI, **Estadísticas de las tecnologías de información y comunicación en los Hogares**, *Instituto Nacional de Estadística e Informática - Encuesta Nacional de Hogares.*, 2018. .
25. **Población que accede a internet en el Perú**.
26. **Acceso de los hogares a las Tecnologías de Información y Comunicación (TIC)**, Jun. 2020.
27. A. Delgado and J. Sosa, **Mobile application design of geolocation to collect solid waste: A case study in Lima, Peru**, in *Proceedings of the 2019 IEEE 26th International Conference on Electronics, Electrical Engineering and Computing, INTERCON 2019*, 2019.
28. A. Delgado and J. M. L. Amado, **The progress of the environment in Peru: Design of a computer system for bottle recycling applied in shopping centers**, *Int. J. Emerg. Trends Eng. Res.*, vol. 8, no. 6, pp. 2724–2729, 2020.
29. C. D. Mendoza-Santos and A. Delgado, **Web application design for the control process of public schools**, *Int. J. Emerg. Trends Eng. Res.*, vol. 8, no. 4, pp. 1289–1294, 2020.
30. A. Delgado, H. Chanamoth, A. Arias, and C. Carbajal, **Improving logistic management in a mass consumption distributor by web system design**, in *IEEE CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies, CHILECON 2019*, 2019.
31. V. Augoye and A. Tomlinson, **Mutual Authentication in Electronic Voting Schemes**, *2018 16th Annu. Conf. Privacy, Secur. Trust. PST 2018*, pp. 1–2, 2018.
32. M. Navarrete, R. Huancas, P. Diaz, and M. Rivadeneira, **Blockchain electronic vote system**, *IEEE Chil. Conf. Electr. Electron. Eng. Inf. Commun. Technol. CHILECON 2019*, pp. 1–7, 2019.
33. I. M. Rodiana, B. Rahardjo, and W. Aciek Ida, **Design of a Public Key Infrastructure-based Single Ballot E-Voting System**, *2018 Int. Conf. Inf. Technol. Syst. Innov. ICITSI 2018 - Proc.*, pp. 6–9, 2018.
34. B. Shahzad and J. Crowcroft, **Trustworthy Electronic Voting Using Adjusted Blockchain Technology**, *IEEE Access*, vol. 7, pp. 24477–24488, 2019.
35. Institute of Electrical and Electronics Engineers, **2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) 17th-19th October 2019, University of British Columbia, Canada**, *2019 IEEE 10th Annu. Inf. Technol. Electron. Mob. Commun. Conf.*, pp. 675–681, 2019.
36. R. Bulut, A. Kantarci, S. Keskin, and S. Bahtiyar, **Blockchain-Based Electronic Voting System for Elections in Turkey**, *UBMK 2019 - Proceedings, 4th Int. Conf. Comput. Sci. Eng.*, pp. 183–188, 2019.
37. R. Bosri, A. R. Uzzal, A. Al Omar, A. S. M. T. Hasan, and M. Z. A. Bhuiyan, **Towards a privacy-preserving voting system through blockchain technologies**, *Proc. - IEEE 17th Int. Conf. Dependable, Auton. Secur. Comput. IEEE 17th Int. Conf. Pervasive Intell. Comput. IEEE 5th Int. Conf. Cloud Big Data Comput. 4th Cyber Sci.*, pp. 602–608, 2019.
38. A. Singh and K. Chatterjee, **SecEVS : SSecure electronic voting system using blockchain technology**, *2018 Int. Conf. Comput. Power Commun. Technol. GUCON 2018*, pp. 863–867, 2019.

H. Te Wu and C. Y. Yang, **A blockchain-based network security mechanism for voting systems**, *Proc. - 2018 1st Int. Cogn. Cities Conf. IC3 2018*, pp. 227–230, 2018.