ISSN: 1692-7257 - Volumen 2 – Número 42 - 2023

Revista Colombiana de
Tecnologías de Avanzada

Recibido: 10 de abril de 2023
Aceptado: 15 de julio de 2023
https://doi.org/10.24054/rcta.v2i42.2670

SISTEMA DE IDENTIFICACIÓN Y CALIFICACIÓN DE ESTUDIANTES BASADOS EN TECNOLOGÍA NFC Y BLOCKCHAIN

STUDENT IDENTIFICATION AND GRADING SYSTEM BASED ON NFC AND BLOCKCHAIN BASED ON NFC AND BLOCKCHAIN TECHNOLOGY

Fabián A. Sánchez-Ruiz[*], Sebastián Ricardo-Cárdenas[*], PhD. Jorge E. Gómez-Gómez[*]

[*] **Universidad de Córdoba,** Facultad de ingeniería, Ingeniería de Sistemas y Telecomunicaciones, Semillero de investigación Pervasive Computing.
Carrera 6 No. 77- 305 Montería - Córdoba, Colombia
Tel.: 47860920, Fax + (57 604) 7860113
E-mail: {rcuetomorelo, atencioflorez61, jeliecergomez}@unicordoba.edu.co
https://orcid.org/0009-0002-0462-6935
https://orcid.org/0009-0002-8942-6405
https://orcid.org/0000-0001-8746-9386

Resumen: La problemática que se trabaja en el documento aborda la precariedad de los sistemas tradicionales de llamado a lista que tienen algunas universidades. Se investigo sobre las características de los NFC y como se pueden utilizar para un sistema de identificación de personal académico para las universidades. Se tuvo en mente utilizar la blockchain para aprovechar la naturaleza descentralizada de esa red para asegurar la confidencialidad de los usuarios del sistema de identificación. Se desarrollo una arquitectura para aplicar estas dos tecnologías en un solo sistema que aproveche lo mejor de los sistemas centralizados y las redes descentralizadas. Esto permitió desarrollar una Dapp que permite la lectura de NFC's, las cuales serán los carnets de los asistentes de la universidad, para acceder a su información, rol e identificación en la universidad.

Palabras clave: NFC, Blockchain, Dapps, Descentralización, Seguridad, Acceso.

Abstract: The problem addressed in the paper deals with the precariousness of the traditional roll-call systems that some universities have. Research was done on the characteristics of NFCs and how they can be used for an academic staff identification system for universities. It was kept in mind to use blockchain to take advantage of the decentralized nature of that network to ensure the confidentiality of the users of the identification system. An architecture was developed to apply these two technologies in a single system that leverages the best of both centralized systems and decentralized networks. This allowed the development of a Dapp that allows the reading of NFC's, which will be the ID cards of the university assistants, to access their information, role and identification in the university.

Keywords: NFC, Blockchain, Dapps, Decentralization, Security, Access.

1. INTRODUCTION

The relationship between technology and secondary education has been growing even stronger with the advancement of new technologies. In essence, technology has come to provide support for precise tasks within specific fields of middle school education. (Maguiño, G. et al, 2020)

In an environment of numerous people such as schools or universities, where access and attendance control are a primary part of attendance management, the need arises for an effective and fast method to count attendance in classrooms, libraries, computer labs and other facilities of academic interest. (A. Rodríguez. et al, 2017)

On the other hand, students possess identification elements such as ID cards or the same ID card registered in their country of origin. (S. C. Gómez, 2017) In this way, they carry an element that refers to their identification in the environment in which they live.

Part of the problem is identity theft, that in order to prove that it is the person, and when he/she was in a certain place, it is checked with his/her unique ID card.

Within this need, several alternatives arise to supply it, within which it is suggested the implementation of NFC devices within the ID cards that identify students, who will present it when entering a space that merits checking the veracity of their identity. (Quishpe, A et al, 2015)

However, in this context, we will focus on how technology can contribute to the work of educational personnel in terms of attendance and information control in various situations within a school environment, whether public or private. We will explore the various methods that educational institutions have used over time to safeguard the privacy of students and their academic information.

2. MOTIVATIONS

Traditionally, attendance control in universities is handled by means of a list of signatures that class attendees fill out one by one. Also, another common method of attendance control is that in which the professor calls out to each attendee to check their attendance. (D. Majin et al, 2020) Each of these methods accomplishes its purpose in a simple, uncomplicated manner, which is why they are widely used by default by most universities.

However, the rudimentary nature of these methods allows for large control and security gaps that jeopardize the veracity and protection of the data. In higher education institutions it is very rare for a teacher to recognize the face of each of the students in the courses he or she teaches, so it is very easy for anyone to impersonate a student who did not attend the class. This can disrupt the teacher's job of grading all students fairly and can worsen the course experience.

Another well-known system is the one in which teachers perform an activity every class (a quiz, workshop, etc.) (A. Rodríguez. et al, 2017), and by means of the delivery of the activity, attendance is taken. It is common for the teacher to ask students to write their ID on the activity to "ensure" their identity. However, this method is not secure enough to prevent a third party from infiltrating the class and impersonating a student.

Those universities that do not have a sophisticated attendance control system then tend to subject their teachers to these rudimentary attendance control systems, ruining the students' experience in their courses and leaving possible loss of attendance information.

NFC technology is one of the many possible ways to address this problem. The benefits of wireless NFC technology (based on RFID) (Haselteiner et al, 2006) greatly meet the needs of universities in terms of attendance control systems. Universities could then provide each of their assistants (teachers, students, administrators) with ID cards which will be necessary for the entrance to the institution and for the entrance to certain classrooms, depending on the role of the assistant and his/her respective schedule.

However, it is well known that NFC technology alone has large security gaps that can be easily exploited to steal information (Mulliner, 2009). Implementing an NFC identification system without an underlying system to back up the information becomes imperative if the connectivity benefits of NFC cards are to be exploited. In a decentralized environment, such as that provided by blockchain technology, it is noticeable that each participant in the network possesses access to the "information" of itself and others. This complicates the possible

actions of attackers or users with malicious intentions, who could harm the integrity of the other users and the stored data.

The use of unmediated NFC cards in systems could present security vulnerabilities (Mulliner, 2009). This is due to its conventional nature, which is defined in the ISO 14443 standard. NFC technology operates by induction in a magnetic field, where two coiled antennas are placed in their respective near fields. It operates in the 13.56 MHz frequency band, which means that it is not subject to specific restrictions and does not require a license for its use (Haselteiner et al, 2006). The lack of security protocols in the standard NFC card implementation provides the flexibility to develop a customized security system, which may or may not be necessary depending on the implications of the project.

3. RELATED RESEARCH WORKS

This section explores different studies, articles and researches that implement related technologies for similar use cases.

In (S. C. Gómez, 2017) it is proposed to combat the problem of academic fraud through the development and implementation of a new "simple and secure" attendance control system, which makes use of NFC techniques. With the implementation of compulsory attendance to classes, the institution where the research is being carried out has suffered increases in the levels of student fraud, which prompted the realization of this work. In this paper, an exhaustive analysis is made of RFID technology, the technology on which NFC is based, and also of NFC itself. The paper also makes a study of the different ID card solutions available in the market.

The objective of (A. Rodríguez. et al, 2017) is to develop a system that allows to know in real time the occupancy level of the different libraries of the Universidad Politécnica de Madrid, the site of the case study of the article. The university had been presenting obstacles derived from the impossibility of knowing exactly the current number of attendees in its libraries, due to an outdated system, which, during exam periods, caused long lines. To address the problem, CARD-CONTROL (A. Rodríguez. et al, 2017), a system that by using the university card and a FAMOCO reading device (Famoco, 2017) takes attendance and monitors the entry and exit of attendees, so as to know in real time, the number of people in the building.

(Guzman, 2020) explores the convenience of a decentralized system in the context of a public transportation ticketing system. To realize such an implementation, the paper analyzes the different alternatives of technologies to use, being Ethereum among them, the most viable, by means of smart contracts. The authentication of users is done by means of NFC cards, secured by means of the decentralized database. The architecture exposed in this degree work has been a source of great inspiration for our implementation, although they are quite different use cases.

The main objective of (Muñoz, 2019) is the use of blockchain in one of its best fields of application, such as third-party payments with a banking entity in between. The support it provides to this research lies in the use of the Ethereum machine and the Truffle suite for the creation of the app exposed in the paper.

In (Andrés, 2018) emphasis is placed on a telematic security model over NFC, which establishes several levels of protection with compatibility and integration in the development of mobile payment applications. The components that are part of this model allow controlling authentication with digital certificates, the uniqueness of transactions through tokenization and data encryption using robust algorithms, which, added to the security standards of acceptance of mobile payments, determines the effectiveness of its application to mitigate the vulnerabilities that occur in this environment.

A research article that provides relevant information is (Zheng, 2017), which mainly presents the foundations and fundamental concepts of blockchain technology, showing everything that makes up the blockchain, how it is structured both as the chain and each block that is part of it, and how it can be written and who can write within it. Trends that point to the blockchain, of which is paramount in the development of this article, the decentralization of systems.

Much of this article has been inspired by (Gomez et al., 2023; Gómez et al., 2016; Elamaran et al., 2018; Munoz-Ausecha et al., 2023; Gómez 2017; Gomez2020), an article by the same authors, which explores similar themes of centralized and decentralized systems linkage, NFC technology and blockchain, but with a focus on the field of medicine and access to medical history information. The architecture explored in (Gómez et al., 2023) has served as the basis for planting the architecture proposed in this article.

4. SYSTEM ARCHITECTURE

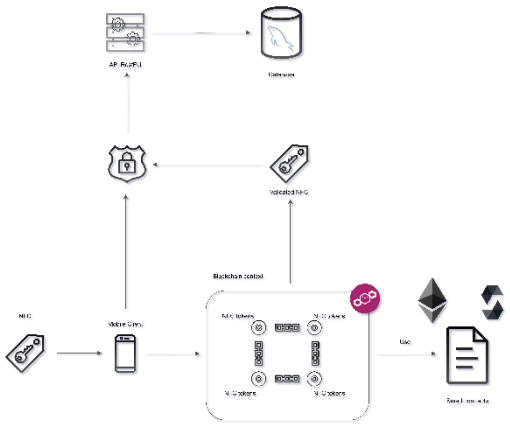

Fig. 1. General system architecture – Source: author

4.1 Client

Since the use of mobile devices became frequent, the ease of carrying many types of sensors in the pocket has increased, therefore, it is likely that the mobile device that we carry, has a device that reads cards or NFC gadgets, which is usable under specialized programming in portable devices such as phones.

Thanks to these facilities, it opens many doors to technological groups in the creation of tools that promote the programmatic use of these components of the mobile device. As it is, obtaining information stored with the help of the NFC sensor reader, such as data reading, is possible thanks to the contribution of the developer community through the use of the Flutter SDK.

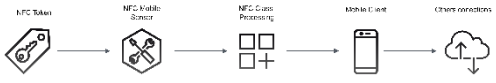

Fig. 2. Mobile client – Source: author

(Fig. 1) Above shows in a summarized and concise way how the mobile client works.

From an NFC gadget owned by the student, its authenticity is evaluated within the blockchain, Blockchain; within these there is written information which will be processed by a module dedicated to obtain the NDEF format (Haselteiner et al, 2006) of the NFC.

Once the information extracted from the NFC is obtained, it is available to the mobile application to be serialized and/or used by other services to which the application is connected.

4.2 Blockchain in descentralizad environments

Decentralized networks, by their very definition, are public in nature. In the context of blockchain, all information stored in this technology is accessible to any individual who is part of the network, as previously emphasized (IBM, 2022). This transparency feature applies equally to platforms such as Ethereum, which is selected as the main environment for the execution of smart contracts in our educational management system.

However, it is important to keep in mind that it would be unwise and potentially counterproductive to attempt to host sensitive educational information, such as academic records and student data, on a decentralized network. The need to preserve the privacy and security of these records is paramount, and while blockchain technology offers numerous advantages, it is not optimally suited to the management of sensitive educational data. Instead, alternatives should be explored that balance technological innovation with adequate protection of critical data in the secondary and university education setting.

However, the inherently public characteristics of these networks make them ideal candidates for the implementation of an advanced authentication system. The transparency and accessibility inherent in decentralized networks, such as blockchain, provide a conducive environment for ensuring the authenticity and integrity of information in an educational management system. This means that, rather than viewing these properties as limitations, we can leverage them as key advantages in the design of a robust authentication system.

In the system under development, each authenticated user with the role of "student" will have the ability to register and delete NFC cards, which will serve as access keys to their confidential information in the centralized module. Each entry on the blockchain will represent an NFC tag, and when a user registers an NFC tag as their own, this information will be recorded on the blockchain via smart contracts. This, in turn, will allow all other previously registered blockchains to be aware of the new entry. A visual representation of this process is presented in Fig. 3.

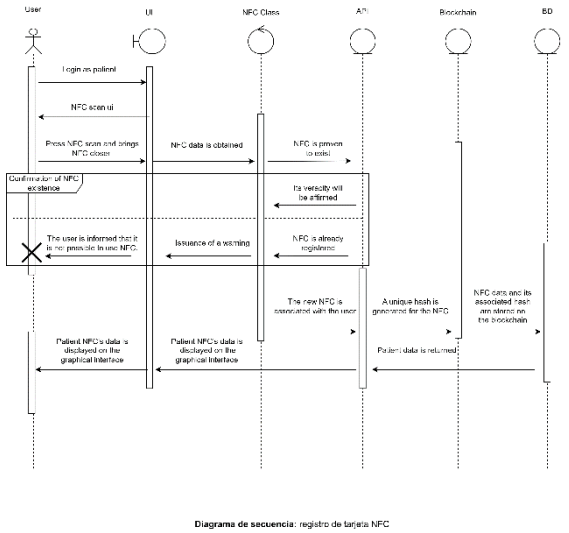

Fig. 3. Decentralized – Source: author

When carrying out the registration process for a new NFC card, it is important to note that the smart contract does not store any sensitive information that would link that block on the blockchain to the user who owns the NFC card. This ensures that students' or teachers' personal and sensitive information remains secure and confidential at all times.

Instead of storing personal data in the smart contract, each time a new block is created on the blockchain, a unique hash is generated that serves as a unique identifier for that block within the network. This hash is stored in the NFC payload, which is the information contained in the NFC card. As the last step in the registration flow, the NFC payload, along with the generated hash and the NFC UID (Unique Identifier), is sent to the system. This process ensures that the information stored in the blockchain is anonymous and that the only entity that can associate the NFC with its owner is the centralized system, which has access to the data related to the NFC's UID.

The data flow during the registration of an NFC card can be visualized in more detail in Figure 3. This design approach protects the privacy of users while enabling secure and efficient authentication in the educational context.

4.3 Centralized environment

It is known then that the decentralized network has a public character, therefore, in order to meet the standards of the proposed security approach, it is proposed to incorporate a centralized component to the architecture. This module will be responsible for storing the confidential information of each user of the public network, such as identification document, course of study, timetable, etc. To achieve the above, the module will be implemented as a web service, following the RESTful API standards (Lokesh, 2018), so that it can be efficiently consumed by any other product or service developed around the system, decoupling the service from the client.

The web service will expose the access points needed to store, read, update and delete network attendants, including all the information associated with them. In addition, it will also expose access points for reading and registering new cards, which will involve calls to the decentralized module, these are aspects that will be discussed in more detail later.

The centralized system will handle an authentication and authorization section based on the JSON Web Tokens (JWT) standard (Jones, 2015), which will strengthen the overall security of the module, protecting the access points only to those terminals that possess the secret key.

Restricting access to the module to only those terminals that possess the secret key will ensure that the decentralized module can only be accessed through the authentication section of the centralized module, which, through an access point registration and login, will yield an access token. This access token is crucial to the security of the system, as it unlocks all the access points of the centralized module to the terminals, and also provides a secure way to monitor which terminal is accessing these services.

In addition, each of the access points will be protected by a role system. Depending on the type of user (ADMIN, STUDENT, PROFESSOR) found in the JSON Web Token (JWT) provided, the terminal will be allowed access to certain buildings and/or rooms. Students will have access exclusively to access points related to NFC card registration, modification of their personal information, in addition to study buildings related to their schedules. Teachers will be able to modify any student's personal information, but must use the NFC reader access point to authenticate the student first. Administrators will have access to all access points, including those related to user and role modification. This role strategy ensures accurate and secure access control in the system, ensuring

that each user has the appropriate capability based on their role within the platform.

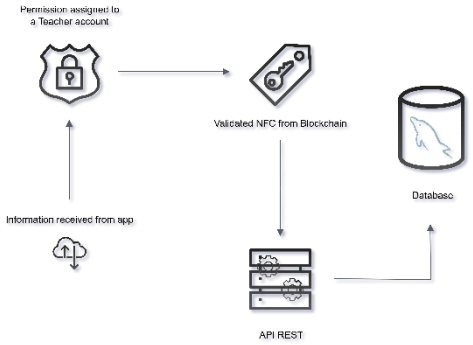

Fig. 4. Centralized environment – Source: author

The JWT (JSON Web Token) standard makes use of an HS256 encryption algorithm (Jones, 2015). This encryption algorithm is known to have a signing process in which it makes use of a secret key, which, for added security, can be randomly generated at the time of packaging the application for distribution. The use of such a secret key provides the freedom to, in the event of a leak, simply restart the application, along with a new key, and any previously generated tokens would be completely disabled.

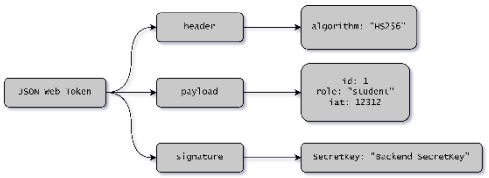

Fig.5 JWT Firm structure – Source: author

Figure 5 shows an outline of the architecture of a JWT, which is made up of: Header, which describes the structure and encryption of the token; Signature, which is the secret key mentioned above; and Payload, which contains the user's id, role and the expiration date of the token. In the proposed system, the id is not part of the user's personal information; it is a randomly generated code to identify each user in the centralized database. Because of this, this id does not have any confidential value outside the system, so if the token payload were to be exposed, it would not expose personal information.

4.4 Possible attacks

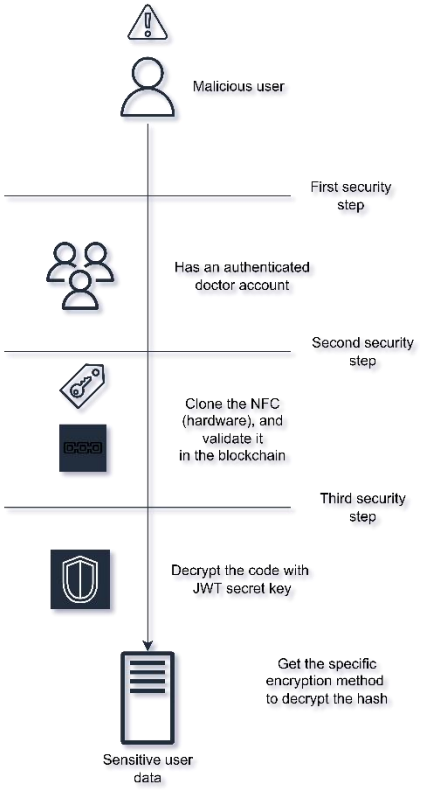

Fig.6 Security barriers – Source: author

It is well known that no system is secure, and that most attacks are due to leaked security breaches or social engineering, such as phishing. There are many security mechanisms that developers can use to avoid compromising data, however, no system is sufficiently immune to social engineering.

Considering the above, the proposed security system consists of three security walls through which a malicious entity will have to pass in order to obtain compromising data. See figure 6. To demonstrate the proposed security system, the following hypothetical situation is considered:

An attacker wants to obtain the sensitive information of a specific patient, this information is in the database. The attacker knows that the identification system works with NFC cards and discovers that these can be easily cloned, so the attacker decides to clone his victim's NFC card.

In order for a cloned NFC card to be useful in the proposed system, it is necessary that the cloning method used also clones the UID of the card, and, in addition, that the card to which the information is cloned is of the same type that our system accepts. Assuming that the attacker's cloning method

complies with the above, the attacker would have already passed one of the system's security walls, see Figure 6.

At this point the attacker has an NFC with the exact payload and UID of a patient's NFC, data that does not yet expose sensitive patient information. However, the attacker has not yet been able to pass the first security wall of the system, which requires an application user account with the role of PROFESSOR. As mentioned in the section on the centralized environment, user accounts created in the system always default to the STUDENTS role, so getting a PROFESSOR account would only be possible through social engineering.

5. SYSTEM ARCHITECTURE

5.1 Reads in the blockchain

In order to analyze the reading speed of the blocks stored in the blockchain, specific scenarios will be designed. Since the blockchain is based on a data structure known as a "Linked List"(NIST, 2023), we will evaluate the read rates within this structure.

5.2 Local Blockchain

In this section, an analysis of a blockchain with different sizes, hosted on the same machine and calling all its blocks, which will provide information on the call and presentation times, will be carried out.

Capturing the data within the application and tabulating it, the following data is obtained:

A reading analysis was performed at three different times, all with the same number of blocks, and an average was calculated to establish a standard time. With this data, the following graph was constructed:

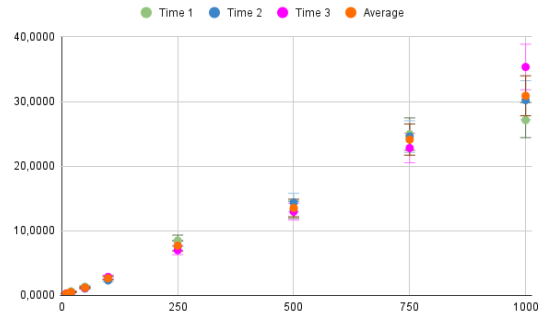

Fig.7. Estimated reading times – Source: author

Starting from this scatter plot, which gives a small summary of the times for each amount of data, it is possible to calculate the measures of central tendency and measures of dispersion.

We then proceed to calculate the mean of the number of data and the average time:

Table 1: Arithmetic averages – Source: authors

$\frac{1}{N}\sum_{i=1}^{N} Amount$	335
$\frac{1}{N}\sum_{i=1}^{N} Time$	10,13

A calculation of the standard deviation is made to then calculate the correlation coefficient (JMP, 2021) which will indicate the relationship between the variables to demonstrate their dependence.

$$\sigma = \sqrt{\frac{\sum_{i=1}^{N}(Amount-\overline{Amount})^2}{N}} = 351{,}8167136 \quad (1)$$

$$\sigma = \sqrt{\frac{\sum_{i=1}^{N}(Time-\overline{Time})^2}{N}} = 11{,}03980112 \quad (2)$$

Once we have the standard deviation and the arithmetic means, we proceed to calculate the covariance.

This is a number that shows the direction of the correlation between a pair of variables, in other words, it allows us to know how one variable behaves according to the behavior of another variable. (Marta, 2020)

In this way:

$$S_{xy} = \frac{1}{n}\sum_{i=0}^{n} x_i \cdot y_i - \overline{x}\overline{y}$$

Thus:

$$S_{xy} = \frac{1}{n}\sum_{i=0}^{n} amount \cdot time - \overline{amount} \cdot \overline{time}$$

It is obtained:

$$S_{xy} = 3874{,}498646$$

The correlation coefficient is calculated from this value.

This term is the specific measure that quantifies the strength of the linear relationship between two variables in a correlation analysis (NIST, 2023). In this context, it will be used to examine the relationship between time and quantity of data and to determine the strength and direction of this relationship. The correlation coefficient will provide information on the magnitude of the linear dependence between these two variables.

It is calculated as follows:

$$r = \frac{S_{xy}}{\sigma x \cdot \sigma y} = 0{,}9975571738$$

The following can be inferred from this result:

"Si el coeficiente de correlación lineal toma valores cercanos a 1 la correlación es fuerte y directa, y será tanto más fuerte cuanto más se aproxime a 1." (JMP, 2021) ("If the linear correlation coefficient takes values close to 1, the correlation is strong and direct, and the closer it is to 1, the stronger it is")

Knowing that you have a really strong and direct correlation, you can run a linear regression to determine or try to predict that, at a certain amount of data, how long it will take to perform.

Once you have all the data, it's just a matter of getting all the unknowns of a linear equation.

$$y = m \cdot x + b$$

Therefore, a and b, defined as follows, need to be found:

$$m = \frac{r \cdot \sigma \cdot time}{\sigma Amount} = 0{,}0313$$

$$a = \overline{Time} - b \cdot \overline{Amount} = -0{,}36$$

In this way:

$$y = 0{,}0313 \cdot x - 0{,}36$$

When plotted together with the points obtained:

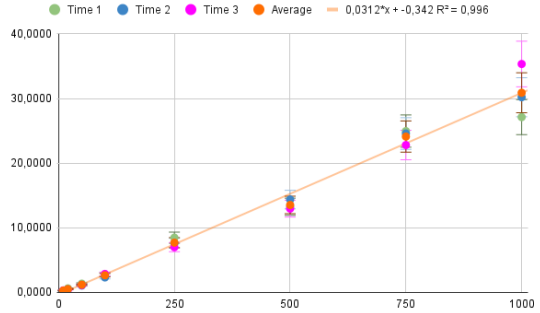

Fig.8. Estimated reading times with regression – Source: author

By concluding and analyzing all these results, several inferences were drawn.

1. A high linear relationship is shown between the number of blocks within the blockchain with the time it takes to read data from the blockchain.
2. From a high amount of data, as observed after the 1000 data, other variables are those that make participation in the result of what is the reading time

6. CONCLUSIONS

Throughout the research, literature has been reviewed in search of options for the creation of a security system for NFC cards based on the blockchain. It has been concluded that by making use of the nature of decentralized systems it is possible to take advantage of the application of this system, because all users, presented by blockchains in the blockchain, have knowledge about the existence of the other users in the network. This makes all clients the owners of the information of the entire system at any given moment, leaving aside the centralization of data as the sole source of truth.

Within this order of ideas, we propose the creation of a DAPP (decentralized application), implementing DLT technologies (Distributed Ledger Technologies), such as Blockchain and Ethereum, which expose development APIs available to developers for the creation of smart contracts that interact with their own network living in the blockchain. The Ganache development suite was selected for this purpose, which offers a whole

set of tools for the development of DAPPs. This Dapp will be responsible for the security part of the NFC inside the cards, so that each card will have a unique code that represents a block of the blockchain.

Moreover, the Dapp also makes use of the Flutter SDK to recognize and extract useful information from NFC cards through its dedicated NFC control hardware. The app will act as an NFC reader and will be used by teachers and supervisors to take roll and identify their students. This application in turn communicates with the centralized module, a server connected to a relational database which stores all the sensitive information of the system's assistants. To add a new attendee to the system, the application mines the blockchain to obtain a new unique identifier that identifies the attendee in the system, then communicates with the centralized module to try to assign the card read to the new block on the blockchain. Consequently, in order for an attendee to register in the system, the blockchain first has to admit the new user so that the NFC can be written with the information, thus preventing access to sensitive information in case of cloned NFCs.

The combination of centralized and decentralized systems is therefore possible, and provides a unique level of security that can only be achieved by combining these two systems. The veracity verification of NFCs on the blockchain ensures the authenticity of the data, thanks to decentralization. On the other hand, the centralized module acts as a storage medium for sensitive data, accessible only through the keys previously validated on the blockchain. Together, the combination of these two systems offers security and robustness in the data identification and validation system.

Acknowledgment

Thanks to the University of Córdoba for financing this research project according to the internal call with project code FI-05-19. We also thank the SOCRATES research group of the Systems Engineering and Telecommunications program for supporting the development of this project.

REFERENCES

Maguiño, G., Amaru, M., Vela, R., Lidia, S., Lozano, R., Alberto, R. Fernando, G. (2020) “Tecnología en el proceso educativo: nuevos escenarios”.

A. Rodríguez-González et al. (2017) “Uso de tarjeta universitaria y tecnología móvil para el control de acceso a instalaciones universitarias y su posterior análisis en términos de rendimiento académico y control de asistencia en clase”.

S. C. Gómez. (2017) “Control de asistencia mediante técnicas NFC”.

Quishpe A. Jorge & Villarreal, Germania & Camacho L. (2015). “NFC: La nueva tecnología para la educación universitaria”.

D. A. G. Majin and O. D. G. Tez (2020) DISEÑO Y DESARROLLO DE UNA APLICACIÓN MÓVIL EN ANDROID PARA EL CONTROL DE ASISTENCIA DE ESTUDIANTES DEL INSTITUTO TECNOLÓGICO DEL PUTUMAYO.

Haselsteiner, E., & Breitfuß, K. (2006) “Near field communication (NFC)”. pág 2.

Mulliner, C. (2009). “Vulnerability analysis and attacks on NFC-enabled mobile phones. 2009 International Conference on Availability, Reliability and Security”.

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2010). Guía sobre seguridad y privacidad de la tecnología RFID. pág 31.

Famoco (2017) “Android terminal equipment and payment solutions”.

Guzmán, E. A. (2020). “Sistema autónomo de cobro de pasajes para el transporte público con Blockchain”.

Muñoz Tapia J. (2019) “Desarrollo de una Dapp basada en Ethereum y React”.

Andrés C. Cristhian C. María U. Gonzalo S. Ciro RADICELLI. Diego B. (2018) “Modelo de seguridad para garantizar la integridad de pagos móviles sobre near field communication (NFC)”.

Zheng, Z. Xie, S. Dai, H. Chen X. Wang, H. (2017). “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends”.

J. E. Gómez Gómez, S. Ricardo Cárdenas, y F. Sánchez Ruiz, (2023) “Sistema de identificación de pacientes basado en tecnología NFC y Blockchain”, Investigación e Innovación en Ingenierías, vol. 11, n.º 2, pp. 1–15.

IBM (2022) “¿Qué es la tecnología de blockchain?”

Lokesh G. (2018) “¿What is REST? - REST API Tutorial”.

Jones, M. B., Bradley, J., & Sakimura, N. (2015). "RFC 7519: JSON Web Token (JWT). IETF Datatracker".

NIST. (2023) "Linked list".

JMP. (2021) "Coeficiente de correlación".

Marta -superprof. (2020) "Covarianza de una muestra".

Gómez, J., Oviedo, B., & Zhuma, E. (2016). Patient monitoring system based on internet of things. Procedia Computer Science, 83, 90-97.

Elamaran, V., Arunkumar, N., Babu, G. V., Balaji, V. S., Gomez, J., Figueroa, C., & Ramirez-González, G. (2018). Exploring DNS, HTTP, and ICMP response time computations on brain signal/image databases using a packet sniffer tool. IEEE Access, 6, 59672-59678.

Munoz-Ausecha, C., Gómez, J. E. G., Ruiz-Rosero, J., & Ramirez-Gonzalez, G. (2023). Asset Ownership Transfer and Inventory Using RFID UHF TAGS and Ethereum Blockchain NFTs. Electronics, 12(6), 1497.

Gómez, J. E. (2017). El internet de las cosas oportunidades y desafíos. Ingeniería E Innovación, 5(1).

Gomez, J. G. (2020). Principales desafíos y oportunidades de los sistemas de Internet de las cosas médicas-IoMT. Ingeniería e Innovación, 8(22).