INVESTIGACIÓN
e INNOVACIÓN
en INGENERÍAS
ISSN2344-8652

Patient identification system based on NFC and blockchain technology

Sistema de identificación de pacientes basado en tecnología NFC y Blockchain

Sebastian Ricardo Cárdenas **Fabian A. Sánchez Ruiz**

Jorge Eliecer Gómez Gómez

Universidad de Córdoba, Colombia

Abstract

Objective: To develop a system in the field of medicine that allows to identify patients by making use of security for NFC cards based on blockchain. **Methodology:** A study of the physical characteristics of NFC cards was carried out to design an external security system, supported by the decentralization of the blockchain, which allows the use of these cards in a field that handles highly sensitive information, such as medicine, in order to take advantage of the practicality of NFC technology when identifying patients in a hospital without exposing their medical history. **Results:** It was appreciated that the blockchain offers a lot of advantages in the field of security, but these advantages come with a decompensation in the times of writing new blocks and reading previous blocks. **Conclusions:** A system supported on a centralized and decentralized part provides greater security, however, a decentralized system such as the blockchain comes with a decompensation in terms of writing speed and, above all, reading speed.

Palabras clave: NFC, Blockchain, Dapps, Decentralization, HL7, FHIR, Healthcare.

Resumen

Objetivo: Desarrollar un sistema en el ámbito de la medicina que permita identificar pacientes haciendo uso de la seguridad para las tarjetas NFC basado en la blockchain. **Metodología:** Se realizó un estudio de las características físicas de las tarjetas NFC para diseñar un sistema de seguridad externo, apoyado en la descentralización de la blockchain, que permita la utilización de estas en un campo que maneje información de alta sensibilidad, como lo es la medicina, para así poder aprovechar la practicidad de la tecnología NFC al momento de identificar pacientes en un hospital de pacientes sin exponer su historial médico. **Resultados:** Se aprecio que la blockchain ofrece una gran cantidad de ventajas en el ámbito de la seguridad, pero estas ventajas vienen con una descompensación en los tiempos de escritura de nuevos bloques y la lectura de bloques anteriores. **Conclusiones:** Un sistema apoyado en una parte centralizada y descentralizada proporciona una mayor seguridad, sin embargo, un sistema descentralizado como la blockchain viene con una descompensación en cuanto a velocidad de escritura y, sobre todo, lectura.

Keywords: NFC, Blockchain, Dapps, Descentralización, HL7, FHIR, Salud.

Recibido: 07/04/2023
Aceptado: 05/06/2023
Publicado: 24/07/2023

Correspondencia de autores:
sricardocardenas26@correo.unicordoba.edu.co

Como citar (IEEE): S. Ricardo-Cárdenas., F. Sánchez-Ruiz., y J. Gómez-Gómez “Patient identification system based on NFC and blockchain technology". *Investigación e Innovación en Ingenierías,* vol. 11, n°2, 1-15, 2023. DOI: https://doi.org/10.17081/invinno.11.2.6671

Introduction

In the medical sector, data protection is essential. Hospitals handle large amounts of sensitive information belonging to their members. In addition, they must be able to access this information efficiently, without it falling into the wrong hands. The above fact is a challenge that hospitals have been facing practically since their existence, and for this, multiple methods have been developed. However, the changing nature of technology demands new ones.

In recent times, medicine and innovation have gone hand in hand thanks to the appearance of new tools. In particular, technology has been instrumental in improving accuracy in certain areas of medicine by providing help with specific tasks.

As elements to support us in this research, NFC technology is kept in mind, which will be deepened soon. The latter is included in many Smartphones which have access to and manipulation of these types of devices that contain NFC.

Knowing the main problem of patient identification and the use of NFC cards, we will talk about how to use the latter within the field of medicine, helping in the field of information assistance to the operational body of the health center where is operating at that precise moment.

The possibilities and risks of using NFC cards are purely subject to their physical construction. The classic NFC card makes use of electromagnetic bands and frequencies to communicate and send information through devices capable of reading NFC signals [1]. A simple security system might not be enough to secure the information contained within an NFC card, since NFC has no way of knowing who the information is coming to. It then becomes necessary to implement your own security solution.

For any business field, data privacy is a critical issue and plays a fundamental role for the quality and effectiveness of the services provided. This is a fact that is especially important in the medical sector. The protection and privacy of patient data is essential to ensure their security and to maintain the confidentiality of sensitive medical information. There are a number of reasons to place a high value on protecting the privacy, confidentiality and security of medical information. Some theorists describe privacy as a basic human good or right with intrinsic value [2].

When talking about data in the field of medicine, it is expected that it is easy and fast to access. A hospital must be prepared to display data on its affiliated patients at any time and moment, due to the frequency and uncertainty of visits and emergencies. Therefore, the challenge that hospitals face is to offer an optimal and efficient service when it comes to retrieving patient data, without jeopardizing the integrity of the data and the privacy of the patient. Historically, various approaches have been taken on this issue. Some of which may include cryptographic protection methods and personal electronic health record devices [2]. Throughout the investigation the possibilities of a new alternative will be explored.

On the other hand, NFC technology is not intended for communication over really close distances other than for the transmission of large amounts of data. Given that it is only designed and that it operates only by radio frequency, there is the possibility that it is always available for a reading, thus leaving all the disposition to any user to scan and obtain the information already specified in the card or device that is using the technology. that is mentioned [3].

It is frequently observed that in the vast majority of systems that make use of NFC or similar technology, they implement it in order to use it as an identifier or "key" to access different spaces, services or other systems [3] Depending on the system in which you are working, this can cause a more or less important confidentiality burden to fall on NFC cards. It is in these cases that the lack of security of conventional NFC cards becomes a problem to be solved.

For security, the integrity of the system or of the cards as such is mainly thought of, but the protection of people's private data is always ensured and expected. Something that these small NFC devices do not natively offer, since they merely offer the functionality of simple wireless communication at a short distance.

NFC cards do not natively offer any security layer by default. Due to the simple nature of the electronics inside an NFC card, this may not be possible. It is known that NFC cards have many known security flaws due to their construction and simplicity [4], so the security of these cards should not fall on the device itself, but on something external.

If a company needs a security system for a project that makes use of NFC cards, there may be multiple ways to address this problem, whether the company decides to implement its own customized version of the RFID device that fits its own system, or developing an external system that has control of the existing NFC cards in the system, etc. All of these options can add a layer of complexity to such a project and also increase development expenses.

The main challenge to be overcome is the inefficiency in the identification of patients in hospital centers in various interventions, be they emergencies, appointments, among others. Along with this main problem, lies the vulnerability of quick identification with NFC gadgets, which have security holes mentioned above; which would represent an extra problem when wanting to solve the approach mainly mentioned.

It is then proposed to explore a security system solution for NFC cards associated with a decentralized and open network, such as the Ethereum blockchain, which can be a good option due to its open-source nature, which offers a complete development environment focused on smart contracts. In addition to the above, a centralized security system is also proposed that will coexist with the decentralized system to protect confidential information that would otherwise be public on the blockchain.

This article is organized as follows: Motivations, the reasons and facts will be explored, with references to works and related research, which motivated the realization of this project; Related works, where the state of the art of medicine, NFC, Blockchain and other topics are explored; System architecture, where each section of the system that is proposed is explored part by part, etc.

Methodology

This application will consist of two parts: a centralized one, which is the standard that day-to-day applications carry and a decentralized or Dapp, where the virtues of the Blockchain environment would be taken advantage of.

The two sections of the whole application converge or are connected to a mobile application that will make connection with a database, managed by a program on the server in the form of API Rest, which follows the HL7 standards for communication and storage of clinical patient data. On the other hand, the same central (mobile) application, will be connected to the *"Web3"* [5], specifically to the Ethereum virtual machine [6], which is where the smart contracts that make the NFC identification tokens unique will inhabit.

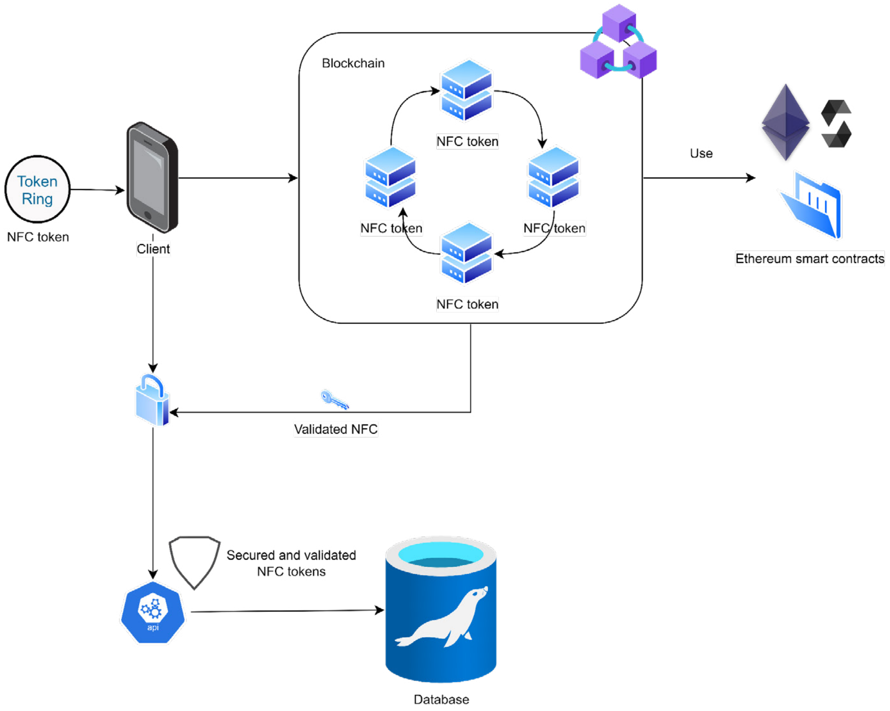
In the centralized part, there will be a server-side application developed in the JavaScript programming language, on top of the Nest.js framework [7], which was chosen for its robustness and stability. This application will follow the proposed standards for the correct communication of medical data. These data will be hosted in a relational database with MySQL engine [8].

The decentralized part will live in the Ethereum virtual machine, making use of the command interface tool such as Truffle [9], making use of Ganache, as a graphical interface, during the development of this section of the application. To designate smart contracts within this Blockchain, we have the Solidity programming language [10].

For the central application of the whole project, we used the mobile SDK designed by Google, Flutter [11], due to its virtues and facilities in the development time and the communication of the device with the NFC cards, with the Web3 and with the server application.

System architecture

Figure 1. General system architecture



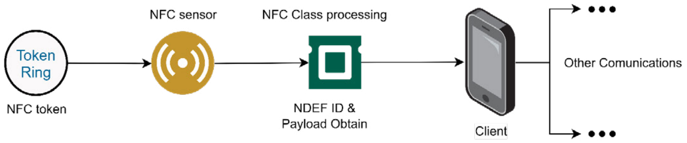
Source: Own elaboration

Client

Mobile environments, mainly those with the Android operating system, have sensor modules of all types, including NFC readers. These give rise to its use in the field of programming through the use of libraries and code fragments that promote easy use, as shown in Figure 1.

Due to this, companies or groups of developers create and contribute to the community tools that allow ease and more comfort in carrying out certain processes, such as reading and obtaining the information that it possesses through the NFC reader sensor. This tool contributed by the developer community is the Flutter SDK [11], which is the environment where the client application is built.

Figure 2. Mobile environment



Source: Own elaboration

As is evident in figure 2, it starts from the hardware, a simple close reading card, to the breakdown of the information it contains.

Once the NFC tag or gadget is brought close to the sensor, it calls the functionalities of a class in charge within the app to obtain two specific parts of the NFC format.

On the other hand, the small device that will be read, maintains a format called NDEF [4], would have a header that will contain an identifier and within the body of this, a script called "payload" [4] that would contain a written message that will be part of the verification and identification process.

Once the information that the NFC had written is decoded, it is available to the device managed mainly by the client application, in order to be used with the other modules with which the latter has a connection

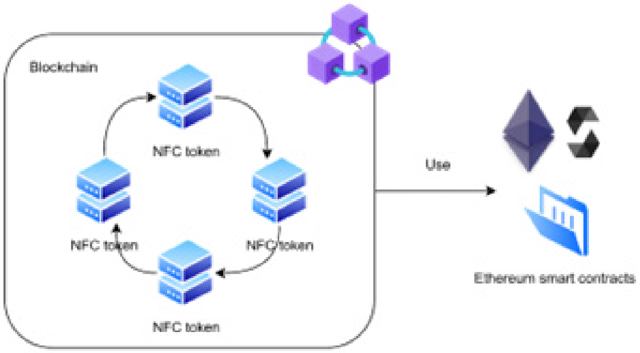
Blockchain in decentralized environments

Decentralized networks are, by definition, public. All the information stored in the blockchain can be read by anyone in the network [12]. This is no different for Ethereum, the smart contract execution platform that we will use for our identification system. It is because of the above, that it would be a bad idea to try to store sensitive patient information and medical records in a decentralized network, as well as being inefficient and extremely dangerous.

However, the public properties of these networks make them a perfect candidate for the implementation of an authentication system.

In the system that is being proposed, each authenticated client with the role of patient will be able to register and delete NFC cards, which will be the access key to their sensitive information in the centralized module. Each block on the blockchain will represent an NFC tag. Each NFC tag registered by a user as their own will be registered on the blockchain, through smart contracts, which in turn will make all other previously registered blocks aware of the new block. What has been described above can be analyzed more graphically in Figure 3.

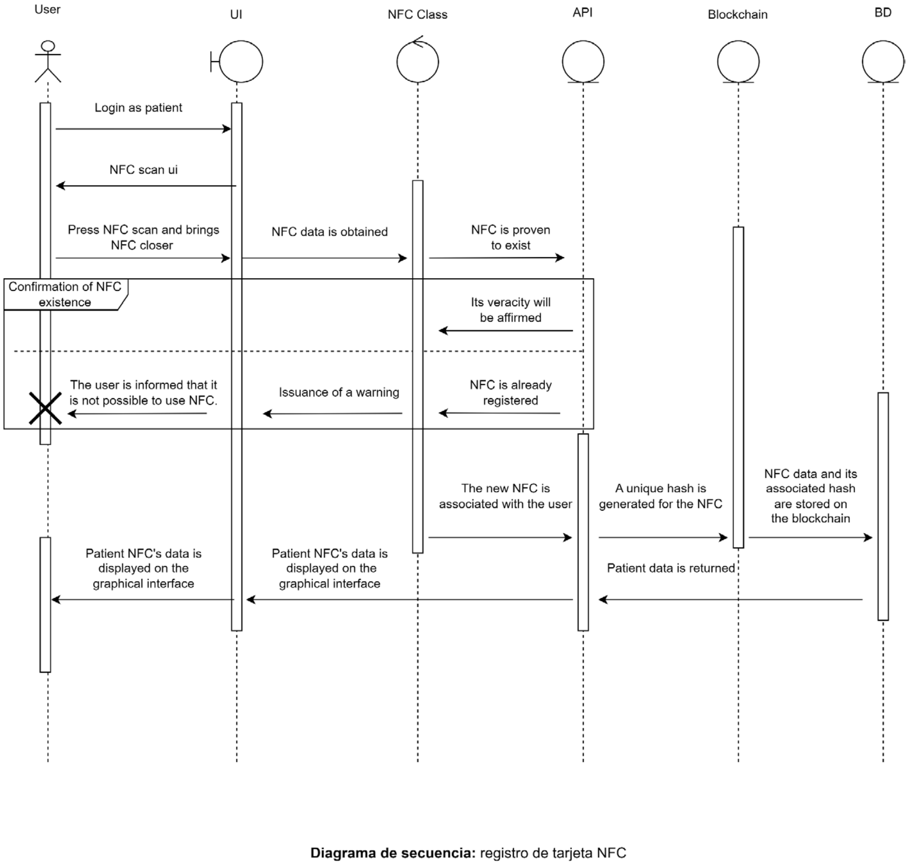
Figure 3. Decentralized environment



Source: Own elaboration

When registering a new NFC tag, the smart contract will not store any type of sensitive information that allows that block of the blockchain to be associated with the user who owns the NFC tag. On the other hand, every time a new block is created on the blockchain, it will gain a hash or unique identifier of this block on the network. This hash will be stored in the NFC payload, and as the last step of the registration flow, the NFC payload will be sent with the NFC hash and UID. Observe the data flow that occurs during the registration of an NFC in figure 4.

Figure 4. NFC card registration sequence diagram


User
UI
NFC Class
API
Blockchain
BD
Login as patient
NFC scan ui
Press NFC scan and brings NFC closer
NFC data is obtained
NFC is proven to exist
Confirmation of NFC existence
Its veracity will be affirmed
The user is informed that it is not possible to use NFC.
Issuance of a warning
NFC is already registered
The new NFC is associated with the user
A unique hash is generated for the NFC
NFC data and its associated hash are stored on the blockchain
Patient NFC's data is displayed on the graphical interface
Patient NFC's data is displayed on the graphical interface
Patient data is returned
Diagrama de secuencia: registro de tarjeta NFC

Source: Own elaboration

Centralized environment

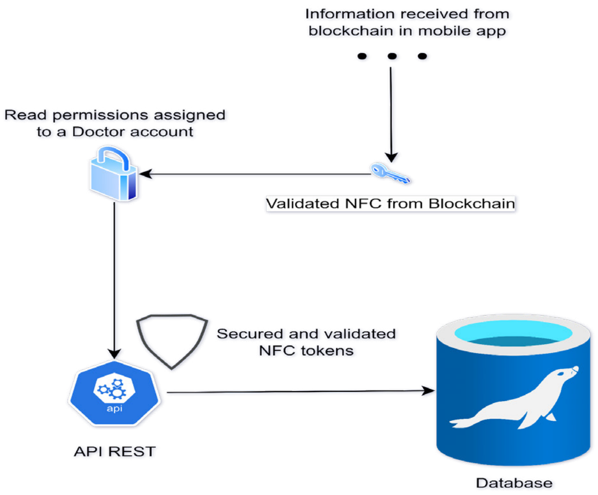
Due to the public nature of a decentralized network, the proposed security system requires a centralized storage component. This module of the system will be in charge of saving all the sensitive information of the patients and medical histories, and will be implemented in the form of a web service following the RESTful API standards [13] to be consumed by the client application of the mobile devices.

The web service will expose to the client application the endpoints needed to read, create, update and delete (CRUD) people and data related to people's medical history, as well as the special endpoints that will be used during the registration and reading of NFC cards, of which will be discussed later.

In addition to the above, the web service will have a user authentication and authorization system using the JSON Web Tokens (JWT) standard [14] to add another layer of security to the entire system. In this way, any terminal that wants to use the service must first have a valid JWT token, which is generated by means of a login endpoint, with a valid user account and password.

In addition, each of the endpoints will be protected by a role system, which depending on the type of user (ADMIN, PATIENT, DOCTOR) found in your JWT, will allow the terminal to access certain endpoints. Patients will only have access to NFC's registration endpoints and to modify their personal information. Doctors will be able to modify any patient's personal information, but they will first need to access the patient with the NFC reading endpoint. Administrators will have access to all endpoints, including user and role modification.

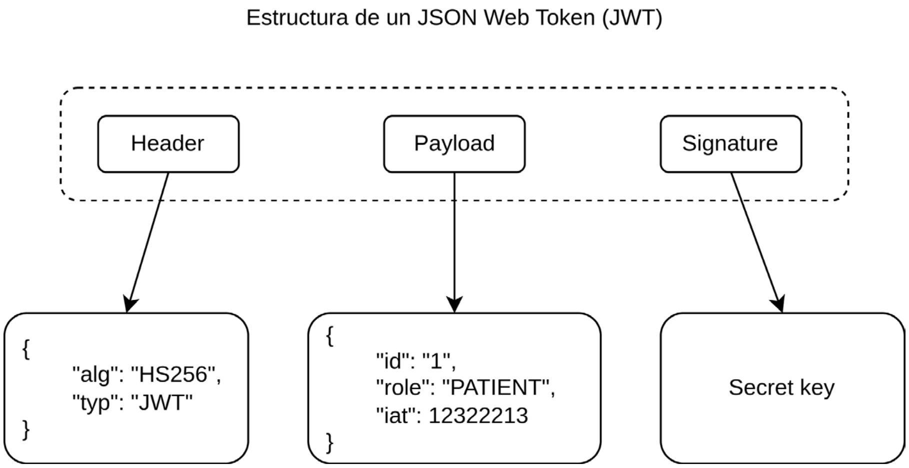
Figure 5. Centralized environment


Information received from blockchain in mobile app
Read permissions assigned to a Doctor account
Validated NFC from Blockchain
Secured and validated NFC tokens
api
API REST
Database

Source: Own elaboration

The JWT standard makes use of the HS256 [14, 15, 16, 17, 18] encryption algorithm, which occupies a secret key during the signing and signature verification process, so it will be extremely important that no one has access to this secret key and that it is generated randomly when deploying the service. In this way, if for some reason it were to leak, it would be enough to restart the service, and any previously generated token would be completely invalidated.

Figure 6. JWT signature structure

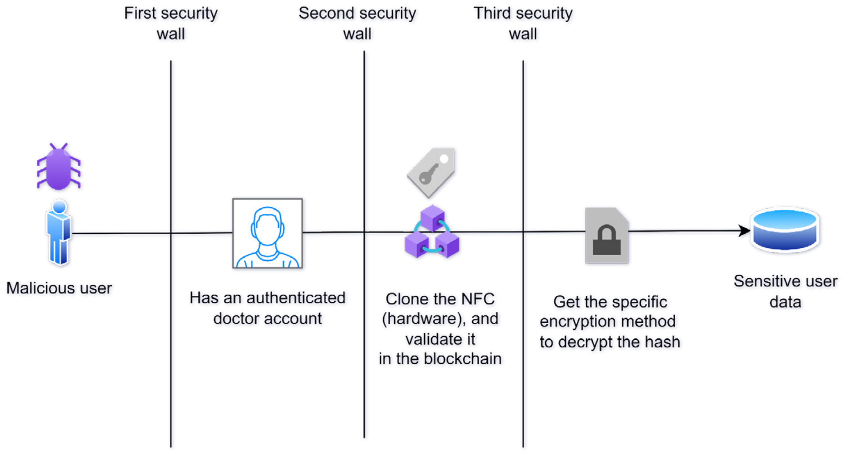


Source: Own elaboration

Figure 6 shows the standard structure of a JWT, this being a combination of three components: *Header*, which describes the structure and encryption in which the token is found; *Signature*, which is the secret key that was commented out above; and *Payload*, which contains a user's id, their role, and the token's expiration date. It should be noted that this id is not part of the user's personal information, this is a number generated by the system to identify the user in the database, but by itself it does not have any confidential value, so if any external agent were to decrypt the payload, it would not obtain relevant information that associates a person with that identifier [19, 20, 21, 22, 23].

Possible attacks

Figure 7. Security barriers


First security wall
Second security wall
Third security wall
Malicious user
Has an authenticated doctor account
Clone the NFC (hardware), and validate it in the blockchain
Get the specific encryption method to decrypt the hash
Sensitive user data

Source: Own elaboration

It is well known that no system is secure, and that most of the attacks suffered by these are due to leaked security holes or social engineering, such as the Phishing method. There are many security mechanisms that developers can use to avoid compromising data, however, no system is immune enough to social engineering.

Taking the above into account, the proposed security system consists of **3 security walls** through which a malicious entity will have to pass in order to obtain compromising data. Observe figure 9. To demonstrate the proposed security system, the following hypothetical situation is posed:

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 [24, 25].

In order for a cloned NFC card to be used in the proposed system, it is necessary that the cloning method used also clone the UID of the card, and also that the card to which the information is cloned is of the same type that it accepts. our system. Assuming the attacker's cloning method complies with the above, the attacker would have already gotten past one of System security walls.

At this point the attacker has an NFC with the exact payload and UID of a patient's NFC [26, 27], data that still does not 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 *DOCTOR*. As mentioned in the section on the centralized environment, user accounts created in the system always have the *PATIENT* role by default, so getting a *DOCTOR* account would only be possible through social engineering.

Results

Next, the results obtained by performing a series of stress tests on the blockchain will be explored, which will serve to expose the limitations of the technology and its nature of operation.

Readings on the blockchain

To perform an analysis at reading speed of the blocks contained in the blockchain, scenarios are proposed.

Knowing that the blockchain is a data structure called Linked List or Linked List [28], we will check the reading speeds within it.

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

Capturing the data within the application and tabulating the following are obtained:

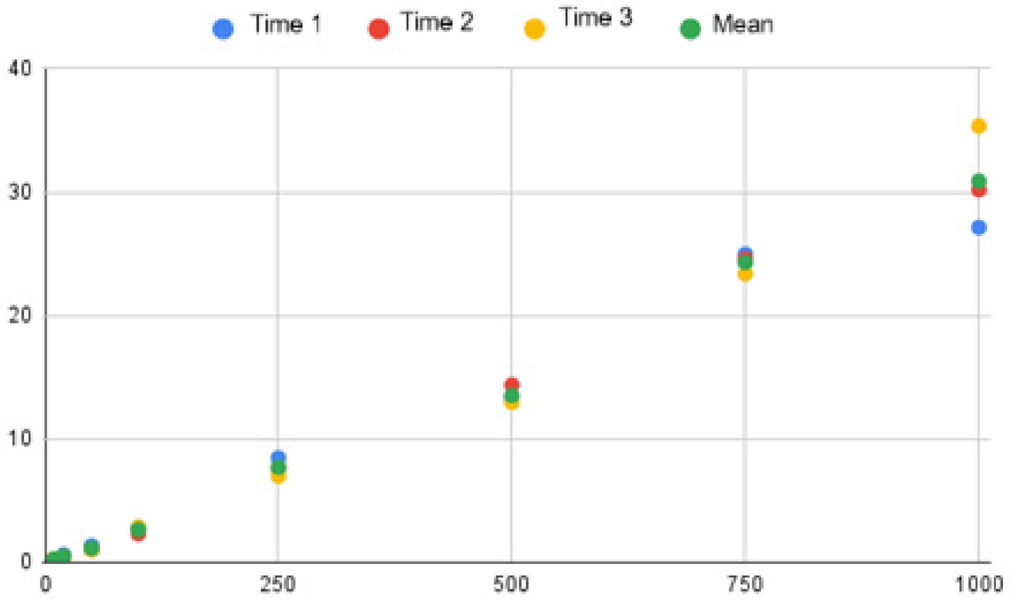
Table 1. Tabulation of reading data

Number of Blocks (Amount)	Time 1 (s)	Time 2 (s)	Time 3 (s)	Mean (s) Time
10	0,2903	0,2903	0,2868	0,29
20	0,6312	0,4731	0,4425	0,52
50	1,3605	1,0722	1,0205	1,15
100	2,799	2,3236	2,8623	2,66
250	8,4771	7,6233	7,0035	7,70
500	13,2594	14,3717	12,9688	13,53
750	24,9558	24,5813	23,3871	24,31
1000	27,1219	30,2002	35,3381	30,89

Source: Own elaboration

An analysis of three reading times was made for the same number of blocks, averaged to have a standard time. In this way, the following graph is constructed:

Figure 8. Estimated reading times



Source: Own elaboration

Starting from this scatter graph, which gives us 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.

Therefore, we proceed to calculate the mean of the amount of data and the average time:

Table 2. Arithmetic Averages

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

Source: Own elaboration

A calculation of the standard deviation is made to then calculate the correlation coefficient [28], which will indicate the relationship between the variables to demonstrate their dependence.

Table 3. Standard deviations

Formula	Outcome
$\sigma = \sqrt{\frac{\sum_{i=1}^{N}(Amount \; - \; \bar{Amount})^2}{N}}$	351,8167136
$\sigma = \sqrt{\frac{\sum_{i=1}^{N}(Time \; - \; \bar{Time})^2}{N}}$	11,03980112

Source: Own elaboration

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

Number which indicates the direction of the correlation between the variables, that is, it allows knowing how a variable behaves based on what another variable does [29].

$$S_{xy} = \frac{1}{N}\sum_{i=0}^{N} x_i y_i \; - \bar{x} \cdot \bar{y} \qquad (1)$$

Thus:

$$S_{xy} = \frac{1}{N}\sum_{i=0}^{N} Amount \cdot Time - \bar{Amount} \cdot \bar{Time} \qquad (2)$$

We obtain:

$$S_{xy} = 3874{,}498646 \qquad (3)$$

From this value the correlation coefficient is calculated.

Term that is the specific measure that quantifies the intensity of the linear relationship between two variables in a correlation analysis [29]. Where the relationship that time has with the amount of data will be observed.

It is calculated in this way:

$$r = \frac{S_{xy}}{\sigma x \cdot \sigma y} = 0.997557 \qquad (4)$$

From this result the following can be inferred:

"If the linear correlation coefficient takes values close to 1, the correlation is strong and direct, and it will be stronger the closer it is to 1" [30].

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

Having all the data, it's just a matter of finding all the unknowns in a linear equation.

$$y = mx + b \tag{5}$$

So, we need to find (a) and (b), defined like this:

$$m = \frac{r \cdot \sigma Time}{\sigma Amount} = 0.0313 \tag{6}$$

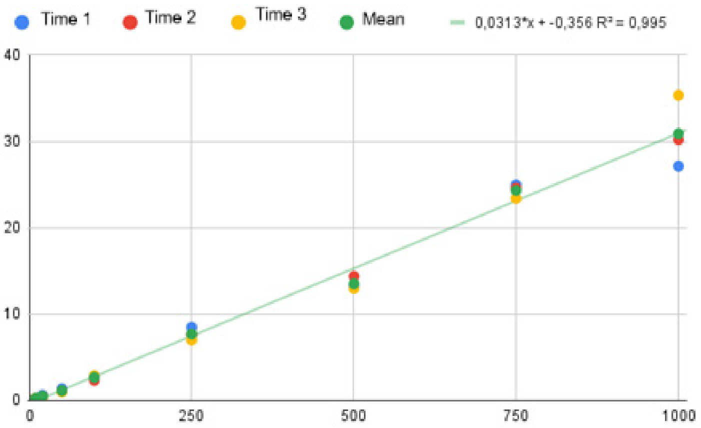
$$a = \bar{Time} - b \cdot \bar{Amount} = .0.36 \tag{7}$$

In this way:

$$y = 0{,}0313 \cdot x - 0{,}36 \tag{8}$$

When plotting together with the points obtained:

Figure 9. Estimated reading times with regression.



Source: Own elaboration

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

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 1000 data, other variables are those that participate in the result of reading time, as can be seen in figure 9.

Limitations:

1: Mandatory use of a mobile with built-in NFC technology.

2: High costs in the use of the blockchain and in production costs.

Conclusions

A security system for NFC cards based on the blockchain was developed. It has been found that one of the ways in which this can be carried out is by taking advantage of the nature of decentralized systems, in which all users have knowledge of the existence and information of other users. These types of systems are known for not having a single source of truth, instead all clients are the repository of information for the system as a whole.

In this order of ideas, the realization of a decentralized application was then considered, what is known as a Dapp (decentralized application). These types of applications can be implemented based on DLT technologies (Distributed Ledger Technologies), such as Blockchain and Ethereum, which provide developers with a way to access the creation of smart contracts through their applications. For the development of our application, we opted for the Ganache tool, which offers a whole set of tools to develop Dapps. The decentralized part was used for the security part of the NFC cards, so that each NFC card will have a unique code that represents a block of the blockchain, which makes the card identifier completely unique in the system.

It has been possible to develop a mobile application prototype which can recognize and extract useful information from NFC cards through its dedicated hardware for the control of this technology, extracting all this data in order to build a unique and non-copyable object which will be hosted along with others in a chain of objects that will build the blockchain. In turn, the mobile application communicates with a server connected to a relational database which stores all sensitive patient information. Every time a user registers a new NFC card, it mines the blockchain for a unique identifier, and then communicates with the server-side application to try to assign the new NFC card to the user. In this way, it is ensured that the NFCs are unique in the centralized system, thus protecting sensitive patient data from possible cloned NFC cards.

The combination of centralized and decentralized systems provides a high level of security in data validation. On the one hand, the validation of an authentic NFC token on the blockchain ensures the authenticity and integrity of the data, thanks to decentralization and cryptography that make counterfeiting difficult. On the other hand, validation of authorized users in the centralized data center adds an extra layer of security by using additional authentication, such as passwords or access keys, to restrict access to only authorized users. Taken together, the overlap of these systems ensures strong and robust data validation security.

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

1. E. Haselsteiner and K. Breitfuß, “Strengths and Weaknesses,” Ipn.mx. 2006. Page 2.
2. Committee on Health Research and the Privacy of Health Information: “The HIPAA Privacy Rule, Board on Health Sciences Policy, Board on Health Care Services, and Institute of Medicine, Beyond the HIPAA privacy rule: Enhancing privacy, improving health through research”. Washington, D.C., DC: National Academies Press, 2009. DOI: 10.17226/12458
3. A. Anaya-Cantellán and I. López-Martínez, “La tecnología NFC en teléfonos celulares, sus retos y aplicaciones,” Ipn.mx. 2006. DOI: 10.13053/rcs-77-1-9
4. Instituto Nacional de Tecnologías de la Comunicación, “LA TECNOLOGÍA NFC: APLICACIONES Y GESTIÓN DE SEGURIDAD,” Ufsc.br, 2013. Available: https://egov.ufsc.br/portal/sites/default/files/cdn_nfc_final.pdf.
5. M. A. Mayer and A. Leis, “Concepto y aplicaciones de la Web 3.0: una introducción para médicos,” Aten. Primaria, vol. 42, no. 5, pp. 292–296, 2010. DOI: https://doi.org/10.1016/j.aprim.2009.06.025
6. “Ethereum development documentation,” ethereum.org. Available: https://ethereum.org/en/developers/docs/.
7. “NestJS Documentation. NestJS - A progressive Node.js framework”. nestjs.com. Available: https://docs.nestjs.com/
8. “MySQL Documentation”. Mysql.com. Available: https://dev.mysql.com/doc/
9. “Truffle Documentation”. trufflesuite.com. Available: https://trufflesuite.com/docs/truffle/
10. “Solidity — solidity 0.8.20 documentation,” Soliditylang.org. Available: https://docs.soliditylang.org/en/v0.8.20/.
11. Adam. “How Flutter Works. Build Flutter”. 2018. Available: https://buildflutter.com/how-flutter
12. “What is Blockchain Technology - IBM Blockchain,” Ibm.com. Available: https://www.ibm.com/mx-es/topics/blockchain.
13. “What is REST,” REST API Tutorial, 29-May-2018. https://restfulapi.net.
14. M. B. Jones, J. Bradley, and N. Sakimura, “RFC 7519: JSON Web Token (JWT),” IETFDatatracker,19-May-2015. Available: https://datatracker.ietf.org/doc/html/rfc7519.
15. Luna, A. R. F. “Sistema para la gestión del historial clínico de los pacientes en una clínica de salud privada, usando NFC para dispositivos móviles.” INSTITUTO POLITÉCNICO NACIONAL. 2014.
16. A. S. C. Barahona, C. F. C. Ortiz, M. I. U. Fassler, G. N. S. Erazo, C. D. R. García, and D. G. B. Maggi, “Modelo de seguridad para garantizar la integridad de pagos móviles sobre near field communication (NFC) security model to guarantee the integrity of mobile payments on near field communication (NFC),” Revistaespacios.com Available: https://www.revistaespacios.com/a18v39n19/a18v39n19p16.pdf.
17. “NFC forum,” Nfc-forum.org. Available: https://nfc-forum.org. 2022. Available: https://nfc-forum.org
18. “Health Level Seven International,” Standardsportal.org. [Online]. Available: https://www.standardsportal.org/usa_en/sdo/HL7.aspx. [Accessed: 01-Oct -2022].
19. J. Martínez Garcés y J. . Barreto Fereira, “Modelo de planeación para la inversión tecnológica en centros de investigación universitarios”, *Investigación e Innovación en Ingenierías*, vol. 7, n.º 2, jul. 2019. DOI: https://doi.org/10.17081/invinno.7.2.3448
20. NFC Forum. Nfc-forum.org. “NFC Forum Specifications”. 2022. Available: https://nfc-forum.org/build/specifications

21. F. Abascal López. “Security using NFC devices,” Unican.es. 2016. Available: https://repositorio.unican.es/xmlui/bitstream/handle/10902/9200/Abascal%20Lopez%20Fidel.pdf?sequence=1.

22. PINEDO GARCÍA, I. “Protección de datos sanitarios: la historia clínica y sus accesos. Revista CESCO De Derecho De Consumo”. (8), 306–318. 2014.

23. C. D. Retamal, J. B. Roi, and J. L. M. Tapia, “La blockchain: fundamentos, aplicaciones y relación con otras tecnologías disruptivas,” Universitat Politécnica de Catalunya. 2017. Available: https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/405/DOLADER,%20BEL%20Y%20MU%C3%91OZ.pdf

24. E. A. Guzmán, “Sistema autónomo de cobro de pasajes para el transporte público con Blockchain,” Universidad Siglo 21, Argentina, 2020. Available: https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/20428/TFG%20-VINF01999%20Enrique%20Guzman%20-%20Enrique%20Guzm%c3%a1n.pdf?sequence=1&isAllowed=y

25. ISO/IEC 14443 Identification cards – Contactless integrated circuit cards – Proximity cards, 2000

26. F. PORTILLA. “Fundamentos Mensajería.” Edu.Uy. 2016. Available: https://eva.fing.edu.uy/pluginfile.php/123521/course/section/13441/Clase4-mensajeriaHL7_v1.pdf

27. J. Bullinaria. Lecture Notes for Data Structures and Algorithms. University of Birmingham. 2019. Chapter 3, page 13.

28. “Coeficiente de correlación,” Jmp.com, 22-Sep-2021. [Online]. Available: https://www.jmp.com/es_co/statistics-knowledge-portal/what-is-correlation/correlation-coefficient.html.

29. “Covarianza,” Material Didáctico - Superprof. [Online]. Available: https://www.superprof.es/apuntes/escolar/matematicas/estadistica/disbidimension/covarianza.html/

30. “Coeficiente de correlacion,” Material Didáctico - Superprof. [Online]. Available: https://www.superprof.es/apuntes/escolar/matematicas/estadistica/disbidimension/coeficiente-de-correlacion.html/.