# Proposal for a Model to Strengthen Trust in Data Exchange Platforms Through the use of Blockchains and National Digital Identity

Pape Mamadou Djidiack FAYE[1], Amadou Dahirou Gueye[2]

Université Alioune Diop de Bambey (Senegal)[1]
Université Amadou Makhtar Mbow(Senegal)[2]

Corresponding author: Pape Mamadou Djidiack FAYE, Email: djidiack88@gmail.com

This work presents an innovative model for enhancing trust within data sharing platforms by integrating blockchain technology and national digital identity systems. Using a consortium blockchain framework and a modular consensus model, the solution proposes a robust mechanism for validating data after it has been received through the exchange platform, thus ensuring its integrity and reliability. Detailed simulations have confirmed the effectiveness of this approach, demonstrating that exchanges of sensitive data are proactively secured. The implementation of this model promises not only to significantly increase confidence in national interoperability platforms, but also to benefit a variety of sectors, both governmental and private. By offering advanced data security and improving transaction transparency, this solution paves the way for more efficient and secure management of critical information.

**Keywords:** Blockchain, National digital identity, Data integrity, Data exchange platforms, Blockchain consortium, Modular consensus, Interoperability.

2024. In Mukesh Saraswat & Rajani Kumari (eds.), *Applied Intelligence and Computing*, 19–31. Computing & Intelligent Systems, SCRS, India. DOI: https://doi.org/10.56155/978-81-955020-9-7-3

# 1 Introduction

The Today, the profound changes brought about by digital technology are influencing economic growth. It can be said that an economy can grow in two ways: either by increasing the quantity of labor and physical capital used, or by exploiting available resources more efficiently to improve productivity. Innovation, technical progress and better training of the workforce are all ways of increasing the efficiency of available resources.

Digital technology can influence economic growth in a number of ways. It leads to increased investment in physical capital (software, servers, networks), higher productivity in the ICT sector thanks to rapid technological progress, and higher productivity in general due to the use of ICT in different branches of industry and services.

In Senegal, the SN25 strategic plan has defined a focus for a connected administration at the service of citizens and businesses. This decision is materialized by the launch of several projects, such as the implementation of a digital identity. The latter should be the common point facilitating interoperability between different services. In this same context, several digitization initiatives have been partially launched, resulting in a multiplication of platforms developed with various technologies, with no provision for interoperability. Even with the implementation of a national digital identity, there will be a problem of data exchange between the different systems already in place, using different technologies. To solve these problems of data exchange between different structures, several platforms offering a data exchange layer have been set up. These solutions offer a secure channel for institutions wishing to share data. But in these platforms, data reliability is only guaranteed at the level of the exchange channel, through the use of encryption algorithms. In fact, there is a problem with the validity of the data exchanged between the different structures. Even if the secure transit channel can guarantee the integrity of the data received by the data-consuming structure, there is a problem concerning the integrity of the data before transit through the channel. Several factors can modify the data before transit through the exchange layer, and the data-consuming structure has no means of validating the data received. It is important to ensure the reliability of data outside interoperability platforms to increase trust between third parties. This control must guarantee data sovereignty for each producing structure.

Today, the advent of modern cryptography has enabled the design and development of Distributed Ledger Technology (DLT), a digital version of registers that offers a number of guarantees previously unthinkable with paper and centralized management [1]. Blockchain is the best-known DLT technology, grouping together digital systems that record asset transactions and their details in multiple locations at once [2]. One of its key features is that it cannot be modified. In research, blockchain is used in many fields, including cryptocurrency, art and administration [3]. In Romania, the technology was deployed during the last national parliamentary elections in November this year to guarantee the integrity of the electoral process and enhance its transparency [4].

In this paper we propose a model for strengthening trust in data exchange platforms through the use of blockchains and national digital identity, taking the case of Senegal as an example.

To achieve this, the remainder of this paper will be organized as follows: Section 2 presents the state of the art in digital identity. In section 3, we'll look at some of the work related to blockchain. In section 4, we'll look at data exchange platforms and related security issues. In section 5, we will propose our solution before concluding.

# 2 State of the Art

## 2.1 Digital Identity

Often used in the plural, digital identities refer to various forms of designation, attribution and expression, involving and challenging all definitions of human identity: legal, ethical, social and technical, economic and industrial, as well as relational and psychological [5].

According to [5], as our digital environment has evolved, the question of digital identity was not initially posed in the same way. Today, this notion refers more to the problem of managing identities across major digital platforms. The management of user profiles, for example: think of the movement insisting on the need to avoid anonymity or pseudo-anonymity in order to impose a certain resemblance between classic identity and digital identity. While early studies on digital identity focused more on the polyphonic and free dimension of identity, today's debates are turning to the dilemmas of identity formatting and traceability.

According to [6] Digital identity is the set of digital traces that a person or a community leaves on the Internet. All this information, left behind during browsing, is collected by search engines such as Google, and made public. A digital identity, or IDN, can be made up of: a pseudonym, a name, images, videos, IP addresses, favorites, comments and so on. This identity on the Internet therefore has an influence on e-reputation, on how Internet users perceive a person. In short, digital identity is the image you project on the Internet, your virtual, dematerialized image.

[6] There are several types of digital identity, which correspond to different categories of information, depending on the source, content and author. This information is also sometimes circulated without the user's knowledge, and can have a harmful influence on the integrity of the corresponding person or entity.

We can easily create three distinct categories of digital identity corresponding to the origins of different sources and the information disclosed:

**Declarative Identity :** This type of digital identity corresponds to the various items of information that have been declared by the person or entity concerned, with various items of information relating to the nature of the subject, his or her civil status and other very objective elements.

**Calculated Identity :** The calculated identity is the result of the various analyses carried out on the active identity. The conclusions are used to establish a profile of the individual or of a service with which he or she is affiliated.

**Active Identity :** Active identity is determined by the user's actions on the web. For example, we can trace a user's attitudes and habits through his or her personal account. The same goes for Facebook friends. Their data will be collected in this way. By way of illustration, bank codes and passwords no longer hold any secrets for these websites. What's more, this information is a real goldmine for certain companies, who use mass data as highly instructive statistics on a commercial level.

## 2.2 Blockchains

[7] Blockchain, a distributed ledger technology, establishes a layer of trust and eliminates the need for a third party to validate transactions. Blockchain technology is an amalgam of various technologies such as distributed systems, cryptography and so on. Data and transactions stored in Blockchain blocks are protected against falsification using cryptographic hashing algorithms. Blocks are linked together with appropriate security using a hash function. This leads to a blockchain, which is a distributed ledger stored at different network nodes. Each block contains transaction details, the hash of the previous

block, the timestamp, etc., as shown in Figure 1. It is difficult for an adversary to alter the details stored at majority points. Consequently, blockchain offers better security than a centralized system [7] [8].

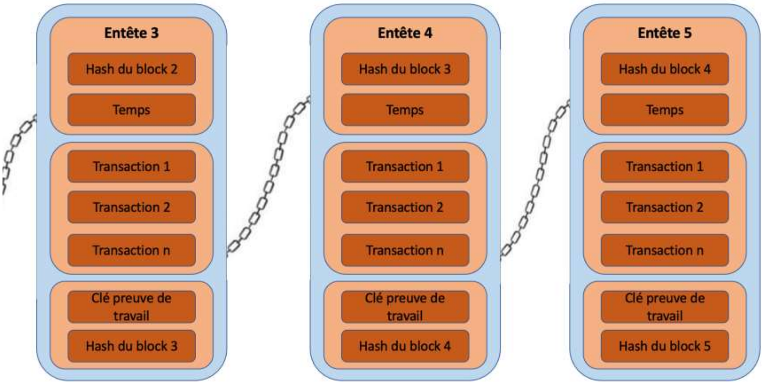


**Figure 1.** Blockchain

Data and transactions executed on the network are stored in the ledger in a decentralized way on a peer-to-peer network. Transactions are validated and verified by consensus (consensus protocols) between the nodes of the Blockchain network. Figure 2 shows the online transaction flow in a Blockchain network [7].

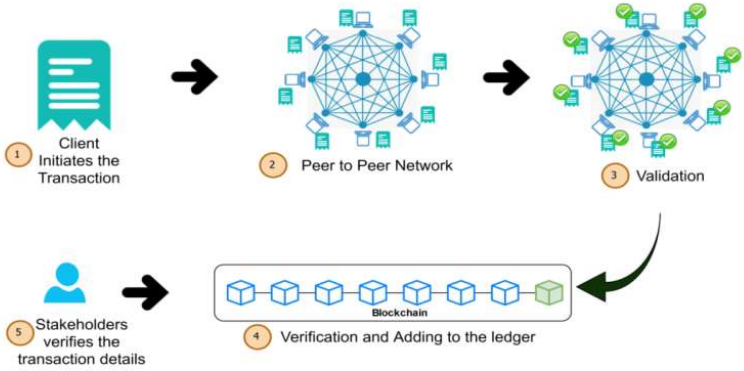

1 Client Initiates the Transaction
2 Peer to Peer Network
3 Validation
Blockchain
4 Verification and Adding to the ledger
5 Stakeholders verifies the transaction details

**Figure 2.** Online transaction flow in a Blockchain network

### Cryptographic Hash Functions

Hash functions are used to convert variable-size data into fixed-size data. In other words, whatever the length of the information you wish to convert, these functions will always produce a result of identical length. (see Figure 3)

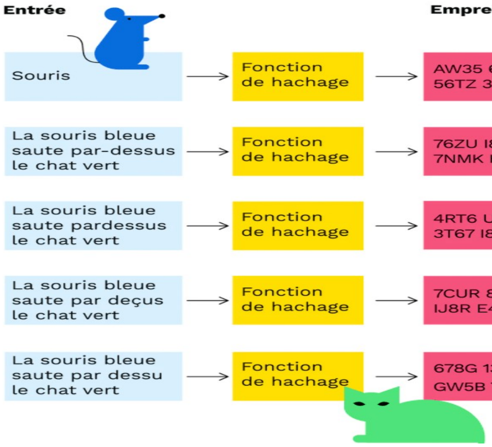

Entrée
Empreinte
Souris
Fonction de hachage
AW35 67RZ 45TZ R3ED TZ54 56TZ 34WE CB78 IO09 P9T5
La souris bleue saute par-dessus le chat vert
Fonction de hachage
76ZU I8Y3 RTH6 78D4 Z5EZ 7NMK HUU9 34TD ZX67 UI9U
La souris bleue saute pardessus le chat vert
Fonction de hachage
4RT6 U8IY 136H Z78I 0PLO 3T67 I89D 8HNB V6SE U84Z
La souris bleue saute par deçus le chat vert
Fonction de hachage
7CUR 8745 912P POJ8 CVN6 IJ8R E456 HSNB 8JJR GJE4
La souris bleue saute par dessu le chat vert
Fonction de hachage
678G 135T TZ6G OI8Z 09IR GW5B 789I SFH6 Z3FZ 67ZT

**Figure 3.** Hash functions

### Consensus Algorithms

Consensus algorithms are protocols that govern how nodes agree on a unique status (valid or invalid) for a transaction or block on a blockchain [8].

Before a transaction is validated or a block added to the blockchain, the nodes must reach a consensus regarding its validity. To do this, each of the participating nodes must choose whether to validate or invalidate the transaction. To achieve consensus, this decision must be unanimous. Consensus mechanisms also enable network nodes to be rewarded for their contribution.

There are a multitude of consensus algorithms (Proof-of-Work, Prof-of-Stake, etc.), and it's up to each blockchain to define the one it wishes to adopt. This technology is constantly being debated to determine which is the most efficient.

### Types of Blockchains

- **Public Blockchains:** Public blockchains are by definition open and accessible to all. In particular, anyone can participate in transactions (and thus hope to see them included in the blockchain subject to validity), but also collaborate in the blockchain's consensus operations that determine which block can be added to the chain and state, without the need for any particular authorization from a (possibly distributed) control authority. In particular, a public blockchain can be likened to a forgery-proof public accounting ledger. Finally, such blockchains are often permissionless: both nodes and users do not require authorization or authentication [1].
- **Private and Consortium Blockchains :** The other main type of blockchain is private blockchains, whose access and use are restricted to a certain number of players who do not necessarily trust each other completely [1]. Here, we need to distinguish between completely private blockchains, where writing rights are restricted and centralized within a single institution, and consortium blockchains, where the consensus process is controlled by a pre-selected subset of nodes and participants (whether centralized or not), who thus have a privileged role in managing the blockchain [1]. In both cases, read access to the blockchain can be fully public or restricted, either in terms of the participants who have been authorized or the number of requests made. Eventually, some systems allow access to cryptographic evidence to be restricted to only a part of the blockchain.

**The State of Blockchain Research**

A blockchain is a database distributed across several computers [1]. Its purpose is to securely document digital transactions. The technology is popular, and for good reason: it makes it impossible to manipulate data once it has been entered into a blockchain.

Businesses can therefore use blockchains to carry out transactions of all kinds securely and transparently, without the need for an intermediary or agency to certify a transaction. For this reason, it is perfectly suited to securing transaction records on production chains, carrying out financial transactions [9] or counting ballots. In addition to fintech [9], logistics and ware housing processes, more and more new fields of application are being discovered: protection of sensitive products, regulations, anti-counterfeiting, e-commerce, accounting procedures.

The authors in [10] proposed a secure data sharing solution based on blockchain technology with proxy re-encryption technology. In the solution, they used the distributed storage, decentralized management and non-forgery features of blockchain, to design a data security sharing model. This model definesaccess control strategies on the blockchain platform and uses the blockchain platform and distributed databases to store encrypted data together to prevent falsification and leakage of sensitive data.

In the field of supplychain management, several studies have been carried out to address this complexity of information visibility and traceability of physical flows in order to find practical solutions and more effective strategies for delivering services that live up to customer expectations. The authors in [11] used the power of blockchain technology to propose a solution that could produce encouraging results in terms of sustainability, trust, traceability and supplychain transparency.

In healthcare, the accuracy of a patient's medical history can be considered a matter of life and death. Confidentiality and security of healthcare data are crucial. [12] in their work have developed a secure and reliable PHR data management system using blockchain technology. This article presents a solution aimed at ensuring patient control by holding the knowledge of the encryption/decryption key that can be deduced from the previous transaction in blockchains. Hospitals have abandoned paper for record-keeping, and are using blockchain technology to store patient data, which remains confidential. The patient receives a digital identifier or digital key to access these records. In this way, the blockchain allows the patient to control who can see this data. The patient's diagnosis can also be stored so that the patient's health history can be tracked. Blockchain technology has made it possible to keep track of the serial and batch numbers of prescribed drugs [13].

Blockchain technology can be used for e-governance [3]. The key characteristics of e-governance are trust and accountability, which are very well supported by blockchain technology. Given that it is virtually impossible to falsify every piece of data or transaction recorded in the blockchain, and that transaction data is replicated by consensus between the distributed nodes of the blockchain, this technology guarantees trust between stakeholders in the digital world. This trust is further enhanced by the fact that all stakeholders have access to the same source of truth in terms of application data stored on the Blockchain network. Several countries have launched initiatives, and according to [14], the application of blockchain technology to e-governance is mainly focused on feedback systems, voting systems, vehicle certification, e-tendering platforms, port management, police complaint management, paperless government services, intellectual property rights protection and land registration.

These various authors have used the strengths of blockchain to solve problems in different fields. They use the unforgeable nature of blockchain to guarantee data integrity. So, when the challenge for governments is to promote interoperability across different domains, this strength of blockchains could be used to ensure data validation as part of a data-sharing platform. In these interoperability platforms, data sharing between government structures becomes more efficient, but data integrity is only assured in the transit channel. It would therefore be wiser for governments to have a layer enabling each structure to validate data, for greater trust between nits different structures.

### 2.3 Data Exchange Platforms

Today, to build a digital government, interoperability and data exchange are essential [15]. This is often facilitated by an interoperability and data exchange platform. Research focusing on interoperability and data exchange tends to agree that interoperability is a challenge for the public sector, that it is extremely important for the development of a successful digitized administration, and that interoperability is a socio-technical phenomenon [16] [17]. Indeed investment in government interoperability and data exchange platforms (GIDEP) is increasing. A GIDEP can be seen as the technical infrastructure and architecture that facilitates the exchange of data between organizations. Examples of such platforms include the EU's GAIA-X project and Estonia's X-Road project. These data exchange platforms have become essential components of the modern digital infrastructure, enabling secure integration and communication between different IT systems. They facilitate fast, reliable access to data between government agencies, businesses and institutions, playing a crucial role in the digitization of services worldwide [18]. They enable seamless integration of information systems, which is essential for digital service delivery, e-government, as well as supporting business processes in the private sector [19].

These platforms optimize operational processes, improve decision-making through instant access to accurate information, and reduce costs by eliminating data redundancy. The enhanced security they offer for data exchange is also a major advantage, essential in today's context of growing cyber threats [20].

Despite the advantages offered by these platforms, their use does not guarantee trust between the various third parties registered on them. Indeed, there is a problem of validity of the data exchanged between the different structures. Even if the secure transit channel can guarantee the integrity of the data received by the structure consuming the data, there is a problem concerning the integrity of the data before transit through the exchange platform. Several factors can modify the data before transit in the interoperability system, and the structure consuming the data has no means of validating the data received. In the following section, we propose a solution to reinforce trust between the various third parties.

## 3 Presentation of the Solution

In current practice, in all areas of government intervention such as taxes, social security, the Trade Register, stock exchanges, labor statistics, the workforce, pensions, national identity cards, foreign identity cards and elections, it has become apparent that the data relating to individuals is all nominative, and the organizations that manage it use identification systems that are often different, ruling out any reconciliation and resulting in a highly damaging waste of media and IT resources.

In addition, the multiplication of these managed files leads to redundancy of information, creating risks of contradictions in updating and errors during multiple entries, as well as cumbersome administrative procedures.

This organization also creates security loopholes, making it extremely difficult to verify information, and facilitating the production of false documents. For example, when submitting diplomas for competitive examinations, the organization just needs to know whether the diploma is reliable. With several interconnected systems, the structure will have access to all the data, even those it doesn't need. Another example is when applying for a position as a driver, the company only needs to know from the mining department whether the person has a driving license.

All these systems are centralized on the person's identity, after which we have other attributes that depend on the person's experience. So this attribute is filled in as the person goes through certain stages in their life. But they are filled in by different structures. For example, permits are issued by the Senegalese mining authority, health data by the health services, and diplomas by universities or training schools.... Whatever the structure responsible for production, this data is personal, and sharing it must comply with texts on the protection of personal data. But all the same, this requires the implementation of a technique that makes the data tamper-proof. All these issues are challenges that governments face in setting up a connected and secure administration, while ensuring the trust and sovereignty of data between different structures.

So, in the interests of human and economic efficiency, and to take better account of what already exists, governments have opted for solutions that automate the sharing of information between the different systems used by their organizations [18]. Despite the advantages offered by these platforms guaranteeing data security and sovereignty, there is a problem of trust between third parties, as these platforms only ensure data sharing and do not guarantee data integrity by the producing structure. To take account of this gap in the government information system, we propose a new layer enabling data to be validated by the structure consuming the data. In this new layer, we use blockchains to guarantee data integrity prior to transit through the data exchange platform.

## 3.1 The Solution Architecture

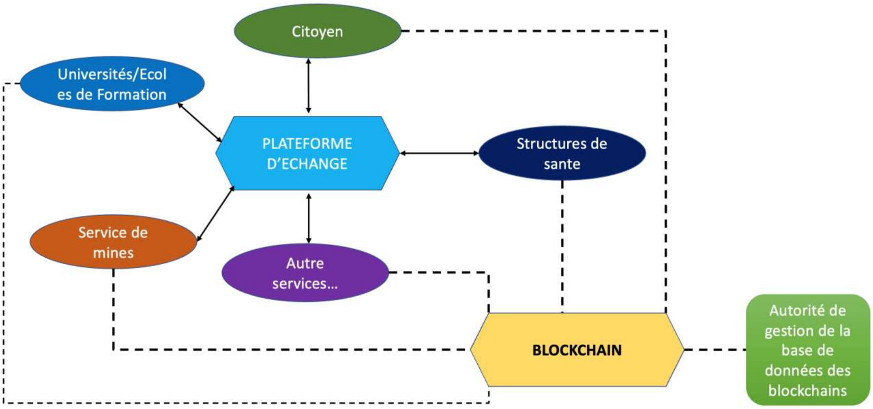


**Figure 4.** Solution architecture

In this diagram we have different components. (see Figure 4)

- **Structures:** These are the public or private structures that consume or produce data (universities, training schools, ....).
- **The Data Exchange Platform:** Which enables the exchange of data between the various structures.
- **Blockchains:** For each citizen, there is a blockchain containing the hashes of his or her various transactions.
- **Blockchain Database Management Authority:** An authority that stores all blockchains. When a new client joins the platform, this authority downloads the blockchains to keep them up to date. The client can choose to download the blockchains to the authority only when checking the validity of data received on the exchange platform. In this way, the customer

doesn't need to store blockchains all the time to save space. Each blockchain is identified in the database by the person's digital identity.

## 3.2 How the Solution Works

The proposed solution uses consortium blockchains. The modular consensus method is used.
The modular consensus model is a flexible and adaptable approach to the design of distributed systems, particularly in blockchain networks. Unlike traditional approaches, which impose a single consensus algorithm for all use cases, the modular model allows integration and choice between different consensus protocols. This gives developers and administrators the freedom to select the protocol that best suits the specific needs of their application.

This flexibility is crucial, as it enables a variety of requirements to be met, such as transaction speed, security, fault tolerance and energy consumption. For example, a private network may focus on speed and low latency, while a public network may concentrate on attack resistance and decentralization.

By enabling the integration of different consensus protocols, the modular model also makes it easier to manage the complexity of distributed systems. It supports long-term scalability by enabling adaptation to new technologies, regulatory changes and evolving security requirements.
This model fosters continuous innovation by enabling researchers and developers to propose new consensus protocols. This creates a dynamic environment where new ideas can be explored and implemented without disrupting the overall integrity and security of the distributed system.

In the proposed solution, each structure will retain responsibility for its own data. Data sharing is ensured by the exchange platform. In this way, the blockchain will enable data to be validated between different structures. In fact, when a structure makes a new transaction involving a person, the associated data is encrypted and added to the shared blockchain. The blockchain will store only the hash of the basic information, so that only the structure responsible for the data can accessit. For example, for a driver's license produced by the responsible department, a new block of the license data hash (first name, last name, number...) iscreated and stored in the blockchain. This blockchain is shared by all structures and also stored in a central database containing all blockchains. In the future, when a service such as the police would like to access the license of an ordinary person, the information is first shared via the exchange platform. Once the information has been received, the police can proceed to validate the data received by running a consistency check against the blockchain. If the hash of the information received matches that stored in the blockchain, the data received will be considered reliable.

# 4 Simulation and Results

This section presents the simulation and results illustrating a solution based on Hyper ledger Fabric for a data exchange platform. The aim is to secure and validate exchanges while guaranteeing the confidentiality of personal information. Each citizen has a dedicated blockchain channel where his or her data is stored securely in the form of hashes.

## 4.1 Technologies used

**Hyperledger Fabric:** This is an enterprise blockchain platform for creating private, permissioned blockchain networks. It uses a modular architecture that allows customization of components, such as peers and orderers, to meet the specific needs of enterprise applications. Hyperledger Fabric is used to deploy the blockchain network, where each organization (Etat Civil, Identité, Service des Mines) has its own peers. Each citizen has a dedicated channel for their data, ensuring separation and confidentiality of information.

**Docker and Docker Compose:** Docker is used to containerize the various components of the Hyperledger Fabric network (peers, orderers, CA). This simplifies the deployment and management of network nodes by isolating each component in a container. Docker is essential for deploying each peer, orderer and CA node on different containers, ensuring efficient resource management and improved network scalability.

**Hyperledger Fabric CLI:** The Hyperledger Fabric CLI (Command Line Interface) is used to interact with the blockchain network. It enables you to create and join channels, install and instantiate chaincodes, execute transactions, and view ledger status. It is used to deploy the chaincode developed in Go, to simulate the addition of data to citizen channels (registration of identity data, updates), and to verify data integrity by comparing hashes.

**Go (Programming Language for Chaincode:** This is used to develop the chaincode, also known as the smart contract, which defines the application logic on the Hyperledger Fabric blockchain. This includes defining the methods for adding, modifying and validating data stored on the blockchain.

## 4.2 The network

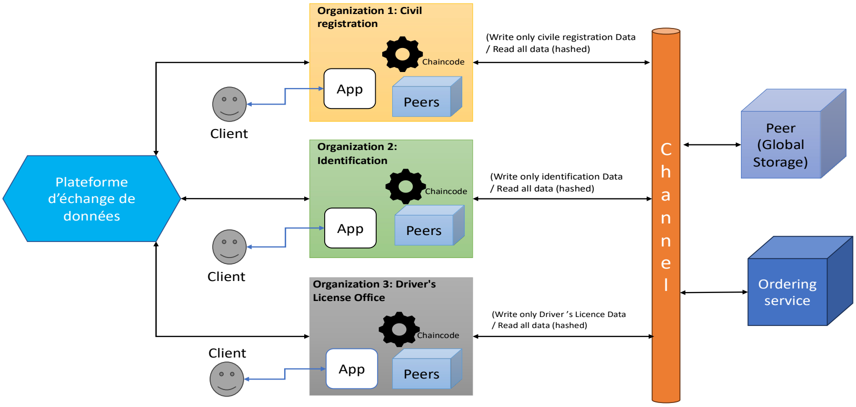

Organization 1: Civil registration
Chaincode
App
Peers
Client
(Write only civile registration Data / Read all data (hashed)
Organization 2: Identification
Chaincode
App
Peers
Client
(Write only identification Data / Read all data (hashed)
Organization 3: Driver's License Office
Chaincode
App
Peers
Client
(Write only Driver 's Licence Data / Read all data (hashed)
Plateforme d'échange de données
Channel
Peer (Global Storage)
Ordering service

**Figure 5.** Network architecture

**Participants:**
Three organizations: Civil Registration, Identity and Driver's License Office
Each organization has its own peer and can write only the data it produces.
A global storage node dedicated to storing all blockchains to enable a new organization to download all registers.

**Citizens or Client:**
Each citizen has a specific channel named after his or her NIN (National Identification Number).
Example channel name: nin100119880190.

**Stored Data**

- Hash of identity data
- Data type (identity, civil status, license, etc.)
- Record date

## 4.3 How it works

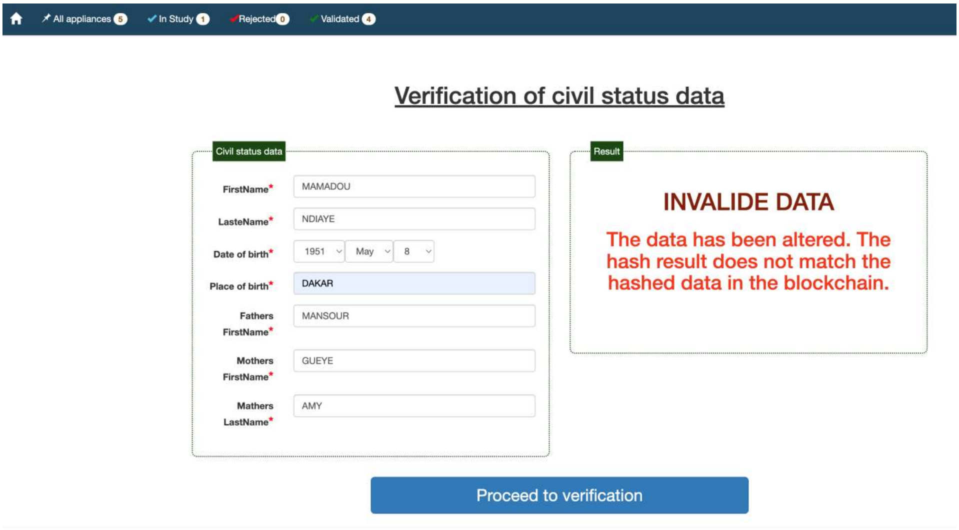
**Data Production:** Each organization produces data for a citizen, such as an identity update. It creates a transaction containing the new data hash, data type and date, and sends it to the network.
The transaction is validated by the peers and recorded on the channel corresponding to the citizen's NIN.

**Data Validation:** When a receiving structure receives data, it calculates the hash of this data and compares it with the last hash recorded on the citizen's channel for this type of data. If the hashes match, the data is validated as being unaltered since it was recorded.

**Global Storage Node:** This node collects and stores blockchains from all channels to enable new organizations to download and synchronize records.
It acts as an additional peer and maintains a complete copy of the data to facilitate the integration of new organizations.

**Results**
In order to carry out the tests, we set up a platform developed in Symfony. This platform belongs to the Identity organization. In this platform, we implemented a form to check whether an extract received by the Identity department has not been altered. We recorded the hash of a civil status certificate in the blockchain (in channel n1001198801910). We then entered data into the platform by modifying the name. As a result, the blockchain was able to detect that the data had been falsified. In a second scenario, we entered the correct data and the blockchain showed that the data was intact.

**Scenario 1:** The data has been altered. The hash result does not match the hashed data in the blockchain. (see Figure 6)



Verification of civil status data

Civil status data

FirstName* MAMADOU

LasteName* NDIAYE

Date of birth* 1951 May 8

Place of birth* DAKAR

Fathers FirstName* MANSOUR

Mothers FirstName* GUEYE

Mathers LastName* AMY

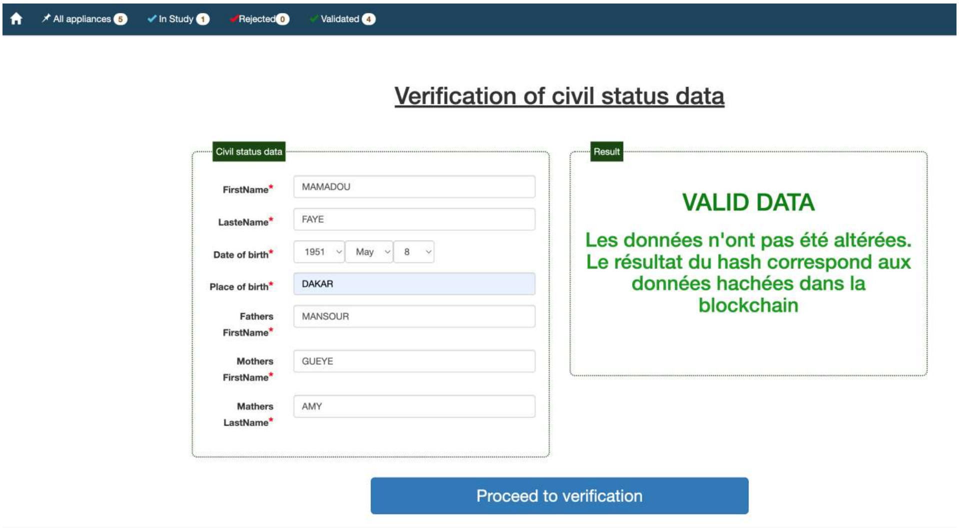
Result

INVALIDE DATA

The data has been altered. The hash result does not match the hashed data in the blockchain.

**Figure 6.** Screen shoot result of scenario 1

**Scenario 2:** The data has not been altered. The hash result corresponds to the hashed data in the blockchain (see Figure 7)



Verification of civil status data

Civil status data

FirstName*: MAMADOU

LasteName*: FAYE

Date of birth*: 1951 May 8

Place of birth*: DAKAR

Fathers FirstName*: MANSOUR

Mothers FirstName*: GUEYE

Mathers LastName*: AMY

Result

VALID DATA

Les données n'ont pas été altérées. Le résultat du hash correspond aux données hachées dans la blockchain

**Figure 7.** Screen shoot result of scenario 2

## 5 Conclusion

The interoperability of different services is a major concern for good governance today. Protecting the confidentiality of sensitive data within the administration, and ensuring the secure sharing of this information, are of paramount importance in building confidence in the interconnection of systems. Maintaining data sovereignty between the various services represents a significant potential for preserving the integrity of this ecosystem.

In this article, we have proposed a model for strengthening trust within data exchange platforms through the use of blockchains and national digital identity. Each structure retains responsibility for its own data. A secure sharing platform facilitates the exchange of information between different entities. The blockchain ensures the integrity of data exchanged between third parties outside the exchange platform, enabling any receiving structure to verify the authenticity of the data.

In our simulation, we used Hyperledger Fabric to guarantee the security, integrity and confidentiality of data exchanges between structures, by assigning each citizen a separate channel and verifying data integrity through hashes. The network ensures that each organization writes only the data for which it is responsible, while validating transactions collaboratively. This approach offers a robust and secure solution for managing personal information.

The global storage node facilitates the integration of new organizations by offering them full access to existing registers.

This system could also reinforce confidence in the electoral process by ensuring transparent and secure management of the electoral file between the various structures involved.

# References

[1] J.-G. L. P. T. A. Dumas, Les blockchains en 50 questions, Dunod, 2019.

[2] M. P. S. l. d. d. D. STOKKINK, LA TECHNOLOGIE BLOCKCHAIN Une opportunité pour l'économie sociale, 2019.

[3] F. A. M. U. Abhishek Phadke, «Applications of Blockchain in E-government,» 18 08 2022.

[4] J. M. e. R. E. Direction scientifique : Franck Macrez, «L'ÉTAT AU DÉFI DES BLOCKCHAIN,» 2021.

[5] J.-P. Fourmentraux, Identités Numériques, Expressions et Tracabilité, CNRS éditions, 2019, p. https://international.scholarvox.com/catalog/book/docid/88926331?searchterm=identite%20numerique.

[6] Semji, «Qu'est-ce que l'identité numérique ?,» [En ligne]. Available: https://semji.com/fr/guide/quest-ce-que-identite-numerique/.

[7] M. O. E. &. I. T. G. o. India, «NATIONAL STRATEGY ON BLOCKCHAIN,» INDIA, 2021.

[8] J. Maffock, «Qu'est-ce que la Blockchain□?,» Avril 2021. [En ligne]. Available: https://blockchainforafrica.com/comprendre/comprendre-la-blockchain/quest-ce-que-la-blockchain%E2%80%AF/. [Accès le 18 12 2022].

[9] H. W. W. Zhan Su, «A Financial data security sharing solution based on blockchain technology and proxy re-encryption technology,» 28 11 2020.

[10] K. O.-B. O. Agyekum, Q. Xia, E. B. Sifah, C. N. A. Cobblah, H. Xia et J. Gao, «A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain,» 2022.

[11] Y. M. A. J. A. Yassine Khaoua, «The Contribution of Blockchain Technology in the Supply Chain Management: The Shipping Industry as an Example,» 27 05 2022.

[12] T.-L. Z. e. T.-H. Chen, «A Patient-Centric Key Management Protocol for Healthcare Information System based on Blockchain,» 10 02 2021.

[13] E. F. M. Surjandy, «Essential Blockchain Technology Adoption factors in Pharmaceutical Industry,» 02 04 2020.

[14] N. M. Reema Goyal, «E-governance Through Blockchain Technology. A Review,» 09 11 2021.

[15] S. K. S.-M. V. T. M. F. Keegan McBride, "Digital Government Interoperability and Data Exchange Platforms: Insights from a Twenty Country Comparative Study," Novembre 2022.

[16] M. B. a. J. Mills, «Grounded theory : a practical guide(2 ed.),» p. 208, 2015.

[17] F. S. Commission, «API-based Financial MyData Service to be Piloted from December.,» 2021. [En ligne]. Available: https://www.fsc.go.kr/eng/pr010101/76977. [Accès le 2024].

[18] R. Saputro, I. Pappel, H. Vainsalu, S. Lips et D. Draheim, «Prerequisites for the Adoption of the X - Road Interoperability and Data Exchange Framework: A Comparative Study,» n° %12020 Seventh International Conference on eDemocracy & eGovernment (ICEDEG), 2022.

[19] P. d. l. M. CHIGUER Hicham, Livre Blanc administration digitale au Maroc, MAROC, 2023.

[20] M. Tan et Y. Li, «Design and implementation of general distributed heterogeneous data exchange system,» MAI 2011.

[21] «https://www.larousse.fr,» [En ligne]. Available: https://www.larousse.fr/dictionnaires/francais/s%C3%A9curit%C3%A9/71792. [Accès le 22 Mars 2021].

[22] Wikipédia, «https://fr.wikipedia.org,» [En ligne]. Available: https://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9. [Accès le 29 3 2021].

[23] J.-P. Fourmentraux, Identités numériques - Expressions et traçabilité, CNRS Éditions, 2015.

[24] M. P. F. K. A. Karabegovic, «Spatial data and processes integration in local governance of Bosnia and Herzegovina,» 02 07 2018.