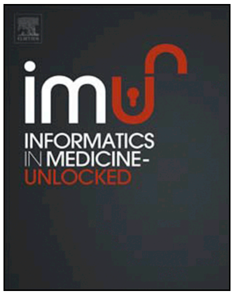


Design and implementation of a New Blockchain-based digital health passport: A Moroccan case study

Sara Ait Bennacer, Abdessadek Aaroud, Khadija Sabiri, Mohamed Amine Rguibi, Bouchaib Cherradi

PII: S2352-9148(22)00262-3

DOI: https://doi.org/10.1016/j.imu.2022.101125

Reference: IMU 101125

To appear in: *Informatics in Medicine Unlocked*

Received Date: 28 August 2022

Revised Date: 31 October 2022

Accepted Date: 1 November 2022

Design and Implementation of a New Blockchain-based Digital Health Passport: A Moroccan case study

Sara AIT BENNACER[1, *], Abdessadek AAROUD[1], Khadija SABIRI [2], Mohamed Amine RGUIBI[1], Bouchaib CHERRADI[1,3]

[1]LaROSERI Laboratory, Faculty of Sciences, Chouaib Doukkali University, El Jadida 24000, Morocco
[2]Fraunhofer Portugal AICOS, Rua Alfredo Allen, 455/461, 4200-135 Porto, Portugal
[3]STIE Team, CRMEF Casablanca-Settat, Provincial Section of El Jadida, El Jadida 24000, Morocco
* Corresponding author's Email: aitbennacer.sara@gmail.com

Abstract:

In the context of COVID-19 pandemic, the Moroccan Interior and Health Ministries have proposed to use the health pass with a QR code to identify vaccinated people. Additionally, the government suggested a mobile application to control the health passport authenticity. However, the key problem is the possibility of anyone scanning the QR code and figuring out citizens' private information, causing severe issues about individual privacy. In this work, the main contribution is integrating a private Blockchain-based digital health passport to ensure high protection of sensitive information, security and privacy among all the actors (Government, Ministry of Interior, Ministry of Health, verifiers) that comply with the CNDP (National Commission for the Control of Personal Data Protection) and the Moroccan Law 09-08. In our proposed architectural framework solution, we identify two types of actors: authorized and unauthorized, to limit and control access to the citizens' personal information. Besides, to preserve individuals' privacy, we adopt on-chain and off-chain storage (Interplanetary File Systems IPFS). In our case, smart contracts improve security and privacy in the health passport verification process. Our system implementation describes the proposed solution to grant individual privacy. To verify and validate our approach, we used Remix-IDE and Ethereum Blockchain to build smart contracts.

Keywords: Blockchain; CNDP and Law 09-08; health pass vaccination; individual privacy and security; Ethereum; smart contract.

1. Introduction

The COVID-19 pandemic [1], which paralyzed global healthcare systems via exceptional lockdowns and physical separation, has prompted the development of such digital technologies to serve a variety of healthcare needs throughout the world [2]–[4]. The set of digital technology developments has favored the coordination of large-scale operations like prediction and early diagnosis [5]–[10], population-level mass screening [11], [12], quick contact tracing [13], [14], vaccination and pharmaceutical supply chain management [15], telemedicine consultations [16], digital training [17] and e-commerce expansion [18]. Otherwise, digital technologies such as machine learning (ML) and deep learning (DL) has proved its efficiency in many computer-aided diagnosis systems for different disease [19]–[26].

Since the emergence of the coronavirus in the first months of 2020, the world has been attempting to find the best way for physicians to diagnosis the virus to prescribe the treatment [27]. In the same time, research community worked hard to find options for improving and experimenting with vaccinations to stop or restrict the rise of infection [28]. Vaccination certificates help governments and authorities to manage and formulate strategies by permitting cross-border mobility of individuals who possess this certification. A digital vaccine passport is an important solution for reopening travel in a post-COVID-19 area. In order to deploy a vaccination passport, significant issues such as security and privacy must be resolved. Civil liberties organizations and others claim that such required solutions infringe our fundamental right to anonymity and freedom and that they are a backdoor to governments giving “identification cards” to individuals [29]. This crisis has provoked public debate about data privacy. Various cities, regions, and even countries require the display of a health passport to access services. Otherwise, the use of the health pass involves privacy-related issues. Currently, the process of the health pass verification through QR code, as proposed by the Moroccan government [30], does not respect an individual’s privacy, allowing anyone to view and consult citizens’ personal information.

In the Moroccan case, the Ministry of Health and the CNDP (National Commission for the Control of Personal Data Protection)1, have signed a collaboration agreement for “DATA TIKA” program on 26th August 2021. This four-year partnership intends to support the health sector’s compliance with regard to the protection of personal medical data. The health pass as shown in Figure 3 presents two types of information 1) plain information, which is accessible to the health pass controller, contains full name, date of birth, etc., and 2) private information protected by QR code. The first type of information can be subject to abusive use, as claimed by a BBC journalist when he was controlled in a Moroccan airport on May 21th, 20222. This problem has also motivated our use of Blockchain technology. In fact, the health pass plain information could not be used by anyone even controllers without the agreement of the health pass holder. Due to its important characteristics of transparency, integrity, and resilience, Blockchain technology defines as a distributed, immutable, and tamper-proof ledger database [31], can be a potential solution to protect individual privacy.

The European Parliament established the General Data Protection Regulation (GDRP) on April 27, 2016 [32]. This regulation aims to define "rules regarding the protection of natural persons concerning the processing of personal data and rules relating to the free movement of personal data," which will come into force on May 28, 2018. In 1996, the United States Congress approved the Health Insurance Portability, and Accountability Act (HIPAA) has changed how health services, insurance, life sciences, and other organizations understand and solve health issues, security, and confidentiality [33].

The main contributions of this paper are as follows:

- Solving the health passport privacy issues in Morocco. The proposed system will keep the privacy of individuals by dividing the verifiers into two parts, the authorized and unauthorized entities, to ensure the personal information privacy displayed during the QR code scan.
- Presenting a Blockchain-based digital health passport to grant individuals data privacy in the Moroccan case.
- Data integrity: we verify the integrity of the vaccine information by comparing the hash value of the user’s data shared with that stored on the Blockchain. Our study employed an off-chain distributed file storage model based on IPFS to store encrypted personal data, such as vaccination information, for individuals. Only the hash value is saved on the Blockchain, ensuring that no personal information is revealed to others scanning the network.
- Implementing our solution by using Ethereum Blockchain and applying smart contract to ensure individual's data privacy.

The rest of this paper is organized as follows: Section 2 presents the related works according to the Blockchain technology that uses the digital health passport. Besides, Section 3 introduces the Blockchain technology background. In Section 4, we demonstrate our system model: Blockchain-based digital health passport in the Moroccan case, we define the problem of the actual scenario in the case of Morocco, we propose our system design, the architectural framework for Blockchain-

[1] https://www.cndp.ma/fr/actualite/711-programme-data-tika-signature-d-une-convention-de-partenariat-entre-la-cndp-et-le-minist%C3%A8re-de-la-justice.

[2] https://morocco.dayfr.com/local/129761.html

based digital health passport and the proposed off-chain data storage. In addition, in section 5, we explain the system implementation and in section 6, we present our results and discussion. Also, the system evaluation is presented in Section 7. Finally, we conclude this work with an outlook of our perspectives and future research directions.

2. Related Works

Authors in [34] presents a Blockchain technology deployed in supervising vaccines. The authors developed a novel intelligent system for vaccination supply chain monitoring. Furthermore, smart contracts based on Ethereum for accessing personal immunization data and vaccine activity were built to track vaccine operation information for consumers, vaccination institutions, and the government. They proved that the vaccine Blockchain technology might be applied to overcome the issue of vaccination traceability. They also created smart contracts to detect expired vaccinations, with alerts for expired vaccines delivered to regulators and organizations in the vaccine supply chain automatically.

The study [35] examines the challenges of using Blockchain in vaccine anti-counterfeiting traceability and proposes a method that combines public and private chains to combat counterfeiting. The issues of quality control and data security in vaccine anti-counterfeiting traceability have been resolved. The experiment indicates that the method outperforms previous vaccine anti-counterfeiting traceability systems in terms of anti-counterfeiting performance and extensive traceability links, as well as providing additional benefits such as privacy data protection and quality control.

In [36], the authors present NovidChain, a Blockchain-based privacy-preserving platform for granting and confirming COVID-19 test/vaccine certificates. NovidChain permits for faster verification of tamper-proof COVID-19 tests/vaccines, thus assisting in the prevention of COVID-19 disease while also safeguarding the user's right to privacy. To satisfy privacy standards such as GDPR and KYC (Know Your Customer), NovidChain depends on a set of emerging technologies such as Blockchain, uPort Self-Sovereign Identity platform, and IPFS storage.

This paper [37] adopts an architecture for a GDPR-compliant COVID vaccination passport (VacciFi). The system guarantees that vaccination data is available, traceable, and reliable. VacciFi employs permission Blockchain, permitting member authorities to operate in a more regulated environment. Since the data controller and processors can be identified, data subjects can have faith in the system. This architecture can aid to create a secure, verifiable, and trustworthy environment, which can adapt to the changing pandemic scenario and provide safe cross-border travel and business.

Table 1 summarizes the recent works and we compare them with our proposed approach:

Table 1: Summary of recent work and comparison with our approach

Ref	Problematic	Certificate type	System proposed	Blockchain platform	Model storage	Regulation compliance	Country
[34]	Vaccination traceability Security Detection expired vaccinations	Vaccine certificate	System for vaccination supply chain monitoring	Ethereum	On-chain	undefined	Australia
[35]	Vaccine anti-counterfeiting traceability Security Privacy	Vaccine certificate	Blockchain in vaccine anti-counterfeiting traceability	Ethereum	On-chain/ off-chain	undefined	China
[36]	Security Users privacy	Vaccine certificate	NovidChain	Ethereum	On-chain/ off-chain	GDPR	Tunisia

[37]	Data availability, traceability, and reliability Security Privacy	Vaccine passport	VacciFi	Consortuim Blockchain	On-chain/ off-chain	GDPR	Finland
Our proposed approach	Health passport data privacy	Health passport	Blockchain-based digital health passport	Ethereum	On-chain/ Off-chain	CNDP	Morocco

The National Commission for the Control of Personal Data Protection (CNDP) [3] was created according to Law n°09-08 on February 18, 2009, regarding the protection of individuals with respect to personal data processing. It is responsible for verifying that the processing of personal data is lawful, legal and that it does not infringe privacy and fundamental human rights. The main objective of the CNDP is to ensure that the fundamental rights and freedoms of individuals regarding the processing of personal data are guaranteed.

According to this recent work, we can address the security and privacy issues related to the digital health passport through the integration of blockchain technology.

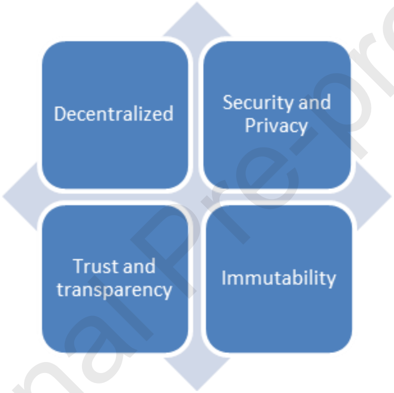


Figure 1: Blockchain key aspects

3. Blockchain technology background

Blockchain technology has attracted a large number of academics, organizations, and businesses, particularly in the usage of bitcoin, a digital currency [38]. Our proposed solution is based on the Blockchain technology using smart contract, to motivate the choice of our solution, in this section we present the main Blockchain properties and potential keys:

3.1 Decentralization

Blockchain is specified as a distributed database in which records are organized into blocks, and a hash key is used to link each block to the previous one. This technology is performed without the need for a centralized administrator or data storage management [39]. As a result, the Blockchain network is a decentralized information system that stores information about all previous transactions and runs on a predetermined protocol that specifies how transactions are performed and validated, as well as how the entire network and its members function [40].

3.2 Trust

The interactions between nodes inside the Blockchain network are what allow it to function. Instead of depending on trusted third-party organizations to conduct transactions, Blockchain network participants rely on the Blockchain network itself. The five fundamental qualities provided by existing Blockchains are immutability, non-repudiation, integrity, transparency, and equal rights [41].

[3] https://www.cndp.ma/fr/

3.3 Immutability

The key security aspect of Blockchain networks is imposed as a characteristic of immutability. The higher up the chain the block is, the more secure the data it contains is from modification [42].

3.4 Security and privacy

As transactions are uploaded to the Blockchain, the identities of the parties involved are verified, and the transactions themselves are verified by other users. Cryptography is used in the implementation of each transaction, resulting in increased security [43].

3.5 Consensus algorithms

The challenge of reaching consensus [44] in a Blockchain network is delicate and crucial, as long as all nodes in the network. The new transaction records will be added to the Blockchain, to validate the new block. It is worth noting that, after a block has been validated, it can't be changed; the Blockchains are built to function in an unsafe and risky network with malicious users. Consensus algorithms are used to design and deploy various methods.

3.6 Deployment models

The Blockchain technology had three types of deployment models, public, private and consortium:

Public Blockchain: [45] There are no restrictions on anyone joining the Blockchain network in the permission-less or public Blockchain, and they can take part in transaction validation and mining. Every peer in a public Blockchain network provides complete permission to participate in the transaction validation and block ledger maintenance processes.

Private Blockchain: Permissioned Blockchains are the opposite of public Blockchains in that they are controlled networks that need the organization's approval for each peer entering the network. Authenticated individuals govern the mining operations on permissioned Blockchains. As such, a private Blockchain employs peer-to-peer communication to alert participants of block transactions [46].

Consortium Blockchain: is defined as a hybrid form of private and public Blockchains, with the consensus processes controlled by a group of companies or participants to verify transaction validity [47].

4. System Model: Blockchain-based Digital Health Passport in the Moroccan case

4.1 Actual Moroccan system

In this section, we demonstrate the actual Moroccan scenario using the health passport and the QR code verification process.

4.1.1 Health pass scenario: Moroccan use case

The workflow describing the health pass scenario is illustrated in Figure 2:

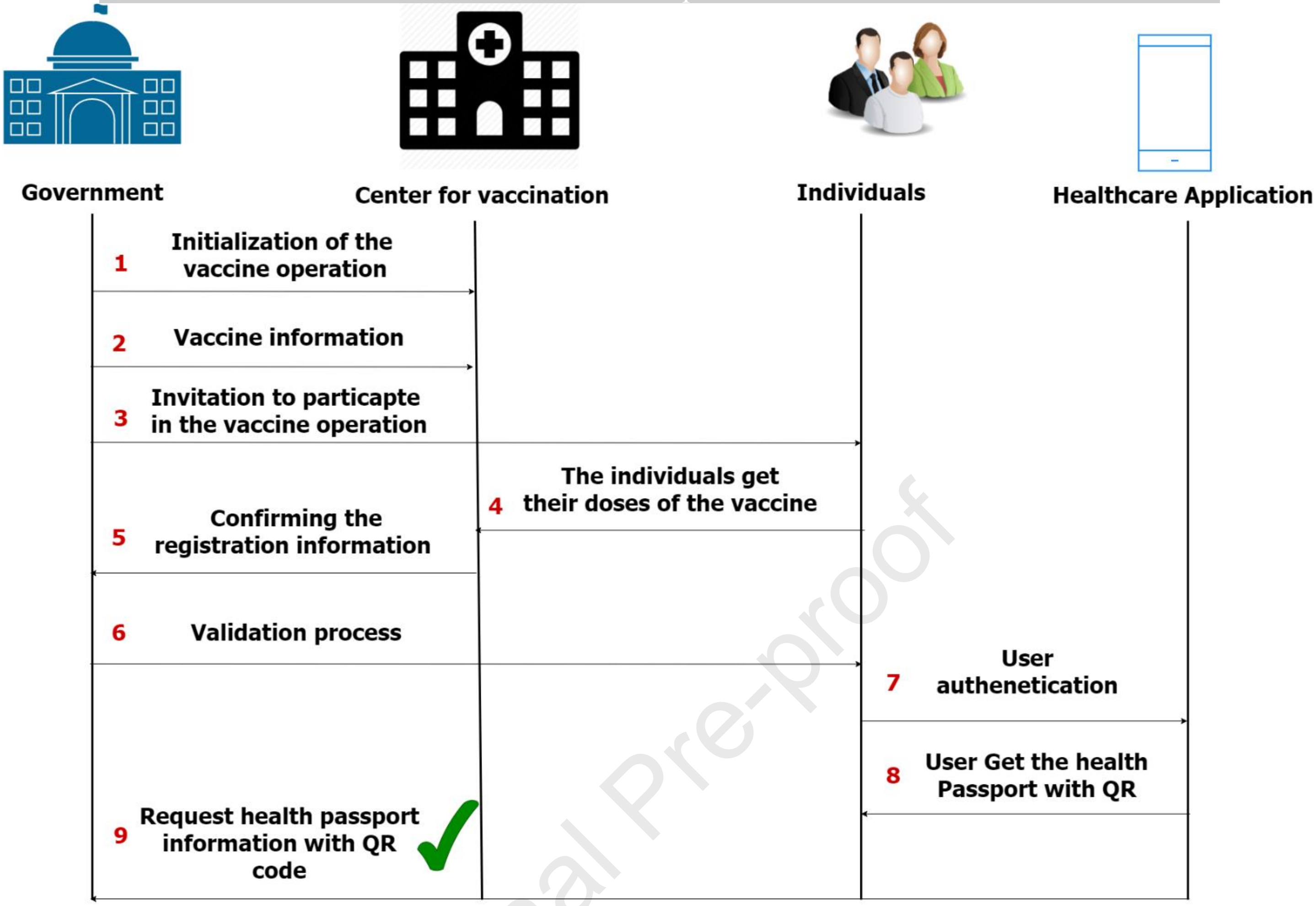

Government
Center for vaccination
Individuals
Healthcare Application
1 Initialization of the vaccine operation
2 Vaccine information
3 Invitation to particapte in the vaccine operation
4 The individuals get their doses of the vaccine
5 Confirming the registration information
6 Validation process
7 User authenetication
8 User Get the health Passport with QR
9 Request health passport information with QR code

Figure 2: Workflow for getting Moroccan health pass

The main stages of the proposed health pass design can be summarized as follow:

1- The government initiates the vaccination operation and gives authorization and agreement to the concerned institutions to vaccinate the citizens/individuals.

2- The government sends the vaccine information, such as vaccine types, doses, and a lot, to the vaccination center.

3- The government also invites individuals to participate in the vaccine operation through media, advertisements, phone messages, and awareness campaigns.

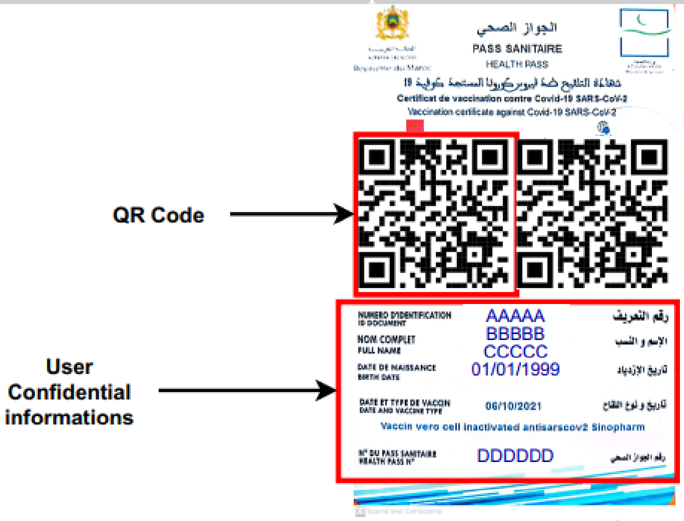
4- The individuals go to the vaccination center to get their doses of the Covid-19 vaccine.

5- After obtaining vaccination doses, the healthcare provider confirms on the platform dedicated to the vaccination registration information.

6- The government institutions send a message by phone to the individual to validate the vaccination process. This message contains the link to access the application dedicated to this fact.

7- The individual accesses the platform and authenticates using their national identity card and a two-step verification process. Furthermore, they can download it as a document or a card.

8-9 The health pass contains two QR codes: 1) the Moroccan code and the European one and 2) the individual’s confidential information that contains the national identity card number, full name, date of birth, date and vaccination type, and the health pass number as shown in Figure 3.


QR Code
User Confidential informations

الجواز الصحي
PASS SANITAIRE
HEALTH PASS

Royaume du Maroc

شهادة التلقيح ضد فيروس كورونا المستجد كوفيد 19
Certificat de vaccination contre Covid-19 SARS-CoV-2
Vaccination certificate against Covid-19 SARS-CoV-2

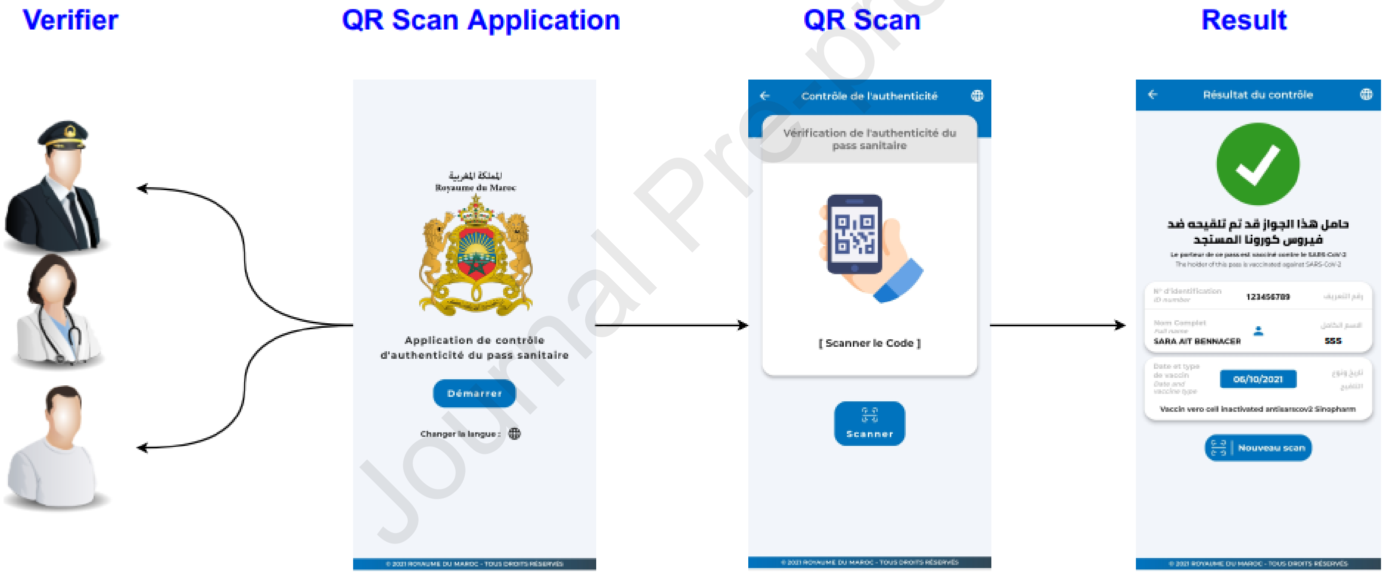
NUMERO D'IDENTIFICATION ID DOCUMENT	AAAAA	رقم التعريف
NOM COMPLET FULL NAME	BBBBB CCCCC	الإسم و النسب
DATE DE NAISSANCE BIRTH DATE	01/01/1999	تاريخ الإزدياد
DATE ET TYPE DE VACCIN DATE AND VACCINE TYPE	06/10/2021	تاريخ و نوع اللقاح
	Vaccin vero cell inactivated antisarscov2 Sinopharm	
N° DU PASS SANITAIRE HEALTH PASS N°	DDDDDD	رقم الجواز الصحي

Scanné avec CamScanner

Figure 3: Moroccan health Pass

4.1.2 *QR code verification scenario*

To verify the health pass, the government proposed an application to scan the QR code available to everyone.



المملكة المغربية
Royaume du Maroc

Application de contrôle d'authenticité du pass sanitaire

Vérification de l'authenticité du pass sanitaire

حامل هذا الجواز قد تم تلقيحه ضد فيروس كورونا المستجد
Le porteur de ce pass est vacciné contre le SARS-CoV-2
The holder of this pass is vaccinated against SARS-CoV-2

N° d'identification ID number	123456789	رقم التعريف
Nom Complet Full name SARA AIT BENNACER		الاسم الكامل SSS
Date et type de vaccin Date and vaccine type	06/10/2021	تاريخ ونوع التلقيح
	Vaccin vero cell inactivated antisarscov2 Sinopharm	

© 2021 ROYAUME DU MAROC - TOUS DROITS RÉSERVÉS

Figure 4: QR Verification

Figure 4 shows that the verifier could be a member of the Ministry of Health or the Interior, or any other individual, like a security agent, a waiter in a restaurant, a shop, or a hotel. Therefore, we observe that anyone can request to scan the QR of the health pass to see whether the person is vaccinated or not. Afterwards, the result reveals the confidential and sensitive information of the citizen, which will be available to everyone. This problem of sharing information with any entity does not respect the individual's privacy and involves a serious risk for Moroccan society.

4.2 *Design based Blockchain proposed system*

4.2.1 *Proposed approach*

This section presents a proposed approach for a Health Pass based on the Blockchain. We integrate Blockchain technology because of its potential key aspects presented in Figure 4, as trust, transparency, security, privacy, immutability and decentralized network. Our proposed system respects the Law n°09-08 in order to assuring individual data privacy.

In Section 5, we aim to improve and demonstrate our proposed solution based on the Blockchain technology and smart contract to solve the digital Health passport issues. We define the compliance of CNDP, regulations and Law 09-08 to protect Health Passport user's privacy and confidentiality. Then, we describe our system actors, and the proposed approach.

4.2.2 *Privacy regulation*

The CNDP is the Moroccan commission in charge of personal data protection. It works to ensure greater transparency in the use of personal data by public and private organizations and to guarantee a balance between respect for the individual's privacy and the need for organizations to use personal data in their activities.

4.2.3 *System actors*

Table 2 describes the actors in the system as illustrated in Figure 5:

Table 2: System actors' description

Actor	Description
Government	Interior and Health Ministries
Healthcare Provider	Health institutions or vaccination centres
Individuals	Vaccinated citizens who want to get their health pass
Verifiers	The authorized people who verify the individuals' health pass

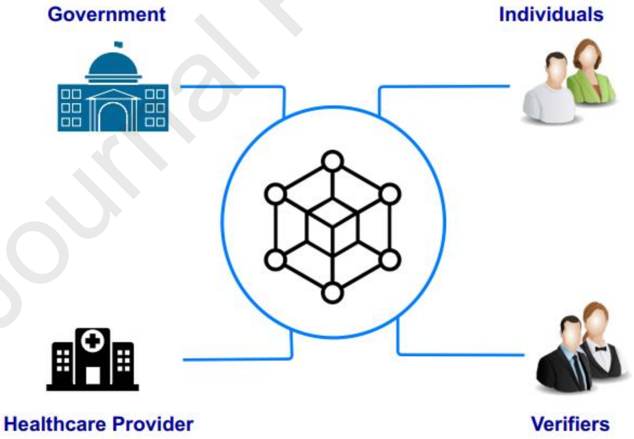


Figure 5: System actors

This section focuses on proving our proposed approach. To protect individuals' privacy and to ensure citizens' health pass sensitive and personal information confidentiality, we employ a decentralized approach by exploiting the Blockchain technology, as well as respecting the CNDP regulation to guarantee individuals data privacy with the system actors.

4.2.4 *Blockchain layer approach*

The following table explains our layer approach based on Blockchain technology as seen in Figure 6.

Table 3: Blockchain layer approach description

Layer	Description
Regulation and Privacy Law	This level concerns CNDP's compliance with Law 09-08 exploited in our study to guarantee the individual's privacy.
Security	It focuses on the security modules and algorithms applied in our system.
Blockchain	In this step, we describe the Blockchain technology components utilized in our proposal.
Storage	This layer defines our proposed system storage infrastructure.
Data	It describes the data that should be protected, that is, the personal information of individuals on the health pass.
Stakeholders	It defines the different actors of our system.

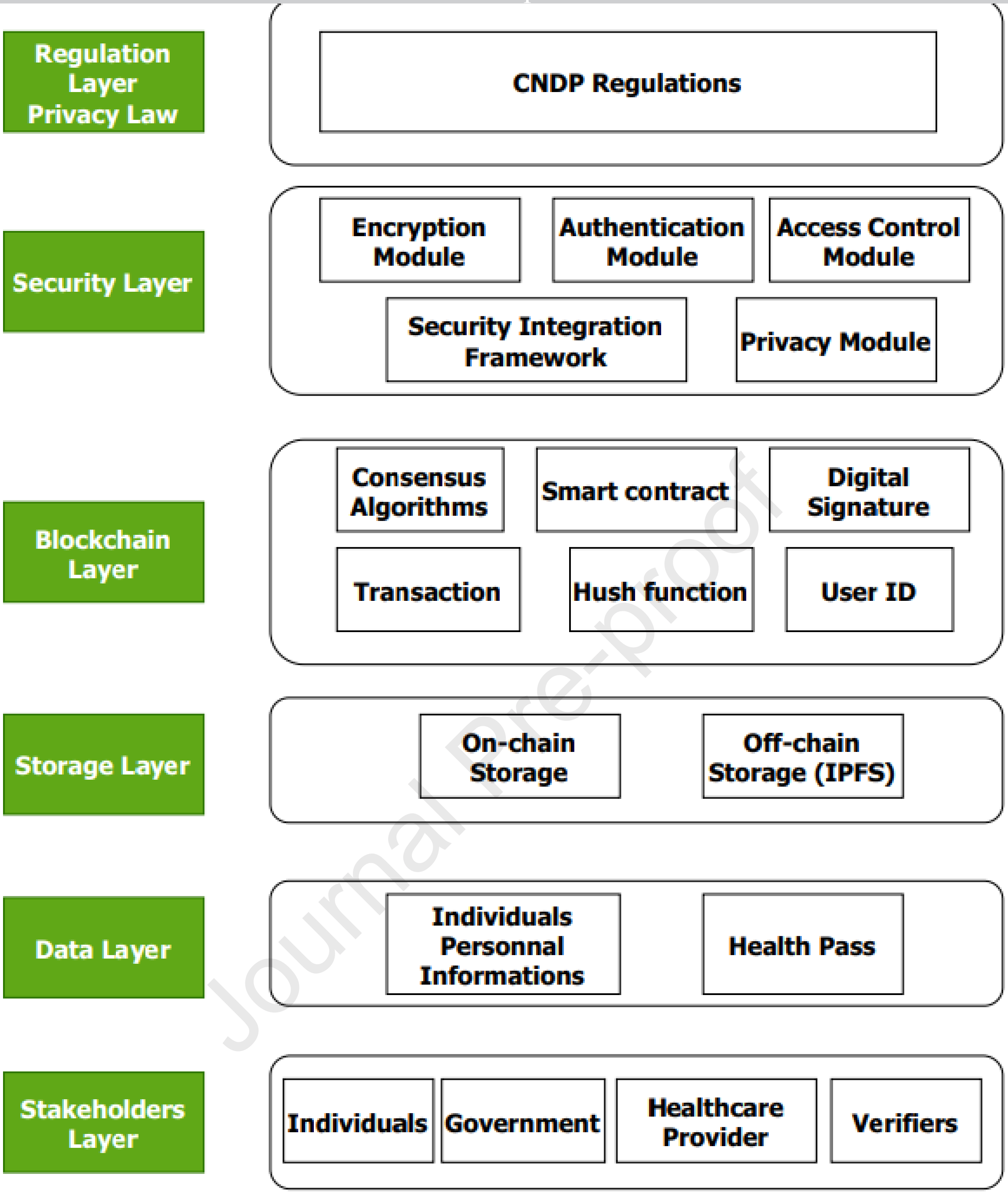


Figure 6: Blockchain Layer Approach

4.3 Architectural Framework for Blockchain-based Digital Health Passport

This section presents an architectural framework for Blockchain-based Covid-19 health pass. Our framework aims to solve the health pass problems in the Moroccan case. This framework is based on Blockchain technology, we choose the Blockchain platform Ethereum, to control and protect the health pass user's information through the network. Our proposed solution allows only authorized entities to check and verify the full individuals' confidential information. Due to its benefits, Blockchain technology grants individual information traceability, security and privacy.

QR Scan code: To protect the privacy of individuals, we propose two use cases in the QR scan code:

- The first one is dedicated to the authorized parties, who have the right to read and verify the individuals' confidential information. Therefore, the authorized parties will have a result of scanning: personal information and vaccination information.

- The second use case will be kept for unauthorized parties, whose personal information will be hashed and then it will be displayed whether the individual is vaccinated or not.

The following figure describes the proposed QR scan code use cases:

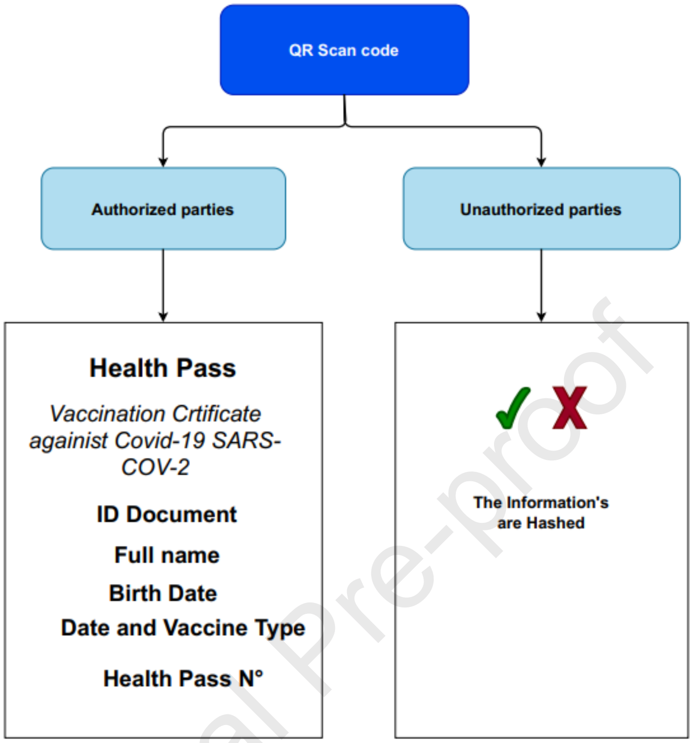


Figure 7: QR scan code use cases

4.3.1 The health pass certificate Authority issuing

Figure 8 describes how the verifier should insert the unique identification into the system and hash the digested personal information to provide to the issuing entities, in our situation, meaning the government. The issuer then obtains the data from the health pass and registers the certificate for the issuance of the Blockchain. In addition, the issuer composes and signs a transaction, including the hash values of the certificate information.

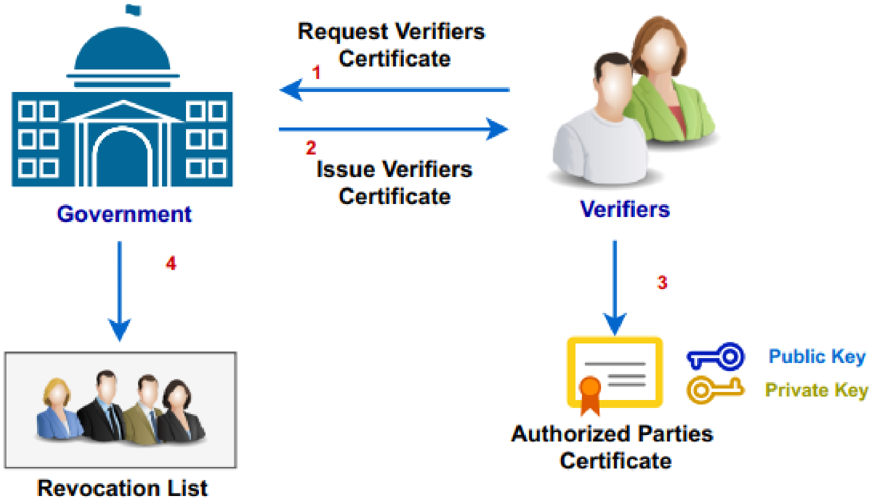

Request Verifiers Certificate
1
2
Issue Verifiers Certificate
Government
Verifiers
4
3
Revocation List
Authorized Parties Certificate
Public Key
Private Key

Figure 8: The health pass certificate issuing

When scanning the QR code on the health pass, authorized parties have a certificate of authorization to examine the individual's personal information as mentioned in Figure 9. Foreign parties who do not have the certificate will be unable to see any personal data, preserving the individual's privacy. On the other hand, a certificate revocation list is a repository for invalidating certificates. There are varieties of reasons to revoke a certificate.

A public key infrastructure (PKI) is made by the certification authorities that provide digital certificates to the participants, who need them to authenticate their identity in communication being sent from their environment. Even though a Blockchain network is much more than a communication network, it employs the PKI standard to provide secure communication amongst network users as well as to ensure that information placed on the Blockchain is properly authenticated.

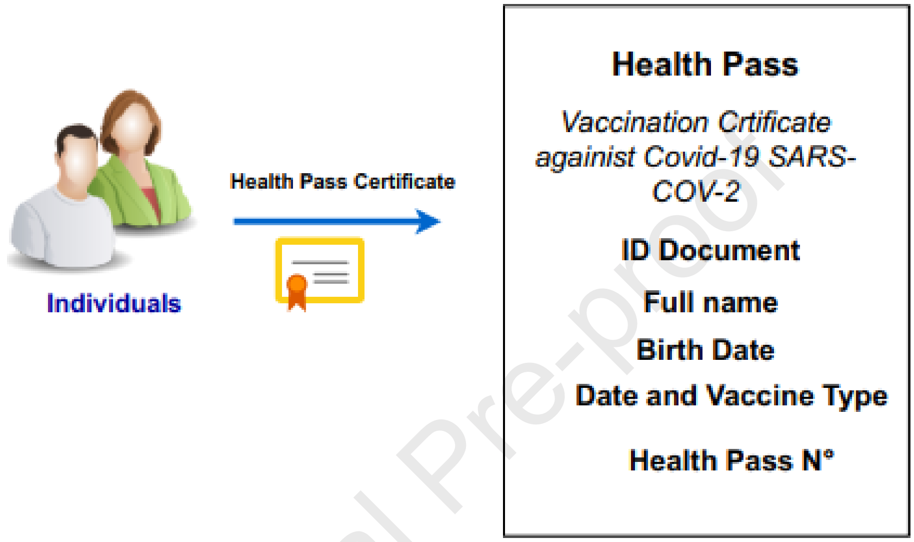


Figure 9: Individuals Health Pass Certificate

4.3.2 The health pass Verification

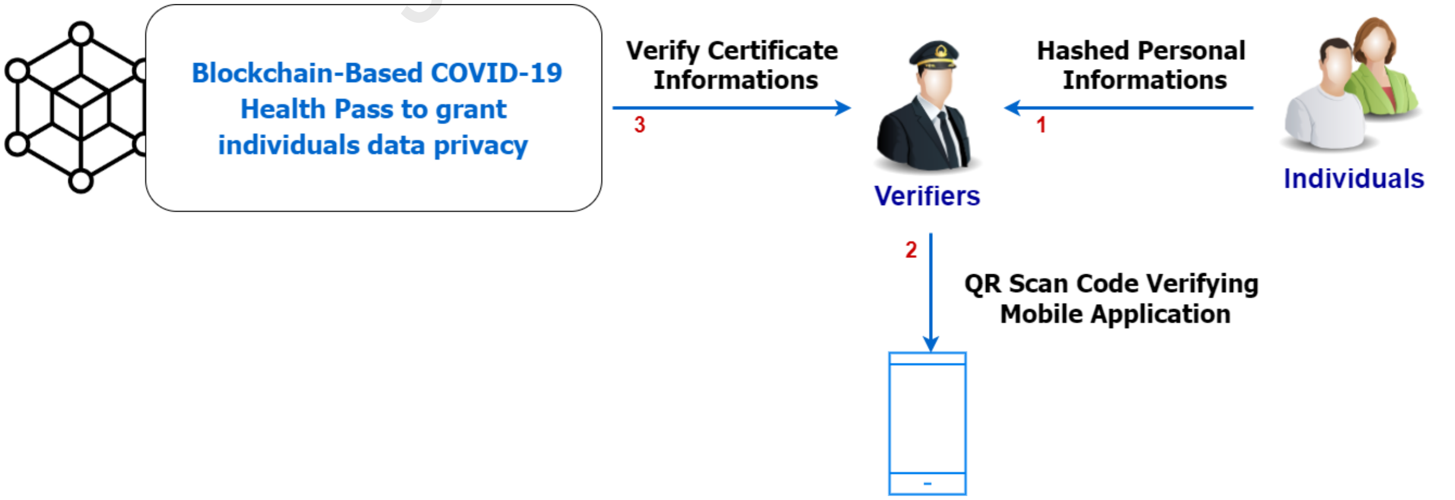

Blockchain-Based COVID-19 Health Pass to grant individuals data privacy
Verify Certificate Informations
3
Verifiers
Hashed Personal Informations
1
Individuals
2
QR Scan Code Verifying Mobile Application

Figure 10: The health pass verification process

To validate the health pass certificate, the individuals must provide the same identifier along with the transaction hash value that records the certificate issue. The verifier scans the health pass QR code via the mobile application until he examines the transaction via the Blockchain network and compares the certificate information with the hash value. Figure 10 describes this process.

4.3.3 System design overview

For the development of the proposed Blockchain platform, we consider the architecture in Figure 12. This design incorporates a vaccine permissioned Blockchain, in which the Blockchain nodes in our scenario are only allowed entities for storing vaccination information and checking the QR scan code against the individual's personal information.

To interact with the Blockchain network, the Government node can designate a Blockchain client node, which might include the ministries of the Interior and Health. This entity is also in charge of delivering vaccination information to the vaccination center or health professionals. The entity then generates vaccination certificates for those who have already been vaccinated. These certificates will identify the approved entity responsible for verifying an individual's vaccination status. The information about the vaccine's hash value is stored on the Blockchain. The registration of these companies can be done by Moroccan government authorities, which use smart contracts to present the Blockchain nodes.

In addition, the Blockchain will simply contain a hash digest of each individual's vaccination certificate, which will be created after registration and employed to facilitate the process of checking his or her vaccination status.

Individuals pass to a healthcare institution or vaccination center to get vaccinated and present their national identity card during the registration phase. The healthcare provider obtains vaccination information from the government organization and saves the individual vaccination information for this reason. After that, the government institution offered the certificate information to the individual to obtain his health pass certificate.

As shown in Figure 11, only the authorized parties have the right to check the citizen's personal information related to the CNDP and respect Law n° 09-08, in order to ensure the health pass user's privacy and protect the individual's confidential information.

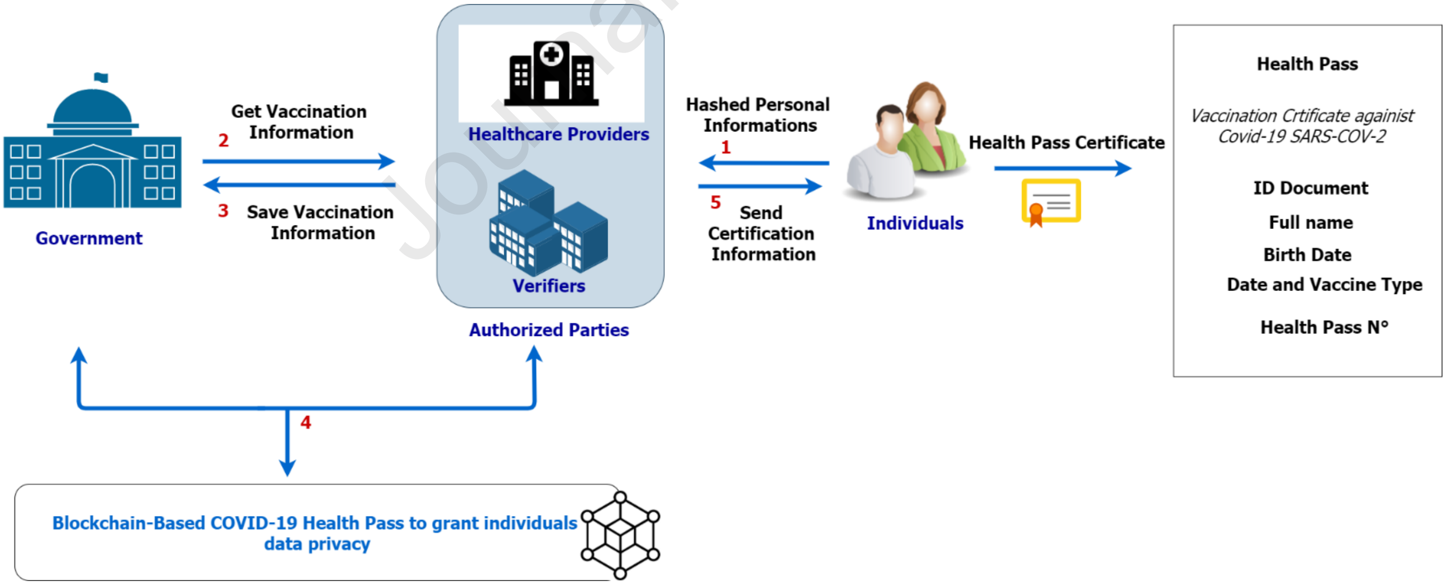

Government
2 Get Vaccination Information
3 Save Vaccination Information
Healthcare Providers
Verifiers
Authorized Parties
Hashed Personal Informations
1
5 Send Certification Information
Individuals
Health Pass Certificate
Health Pass
Vaccination Crtificate againist Covid-19 SARS-COV-2
ID Document
Full name
Birth Date
Date and Vaccine Type
Health Pass N°
4
Blockchain-Based COVID-19 Health Pass to grant individuals data privacy

Figure 11: System design

4.4 Proposed Off-Chain data storage

4.4.1 Interplanetary file system IPFS

Interplanetary file system IPFS [48] is designed to employ content-addressing for file identification in a global directory connecting all compute nodes in the network to introduce decentralization in file storage mechanisms. In peer-to-peer networks, where there is no centralized server, IPFS functions as a networking protocol for file storage, access, and distribution. IPFS is a highly secure system with exceptional performance, content addressability, block storage that is designed to help with data storage and parallel distributed user access [49]. The peer-to-peer (P2P) network used by the IPFS protocol comprises an IPFS object, a data structure that stores links and data. Data includes unstructured binary data, and the link contains an array [50]. The IPFS protocol operates as follows:

- ✓ IPFS attributes a unique cryptographic hash for each stored file.
- ✓ The duplicate files are not permitted to exist on the IPFS network
- ✓ A node on the network keeps its index and stores content.

IPFS is a peer-to-peer, open source, globally distributed file system that can be employed to store and share massive volumes of information with high throughput [51].

4.4.2 Blockchain Data structure

The proposed data structure focuses on two key components: on-chain storage and off-chain storage, both of which are discussed below:

- On-chain storage: the proposed system used the Blockchain technology to overcome the privacy challenges related to the individual vaccine’s information. The on-chain storage will include the hash address of the transaction.
- Off-chain storage: To ensure the availability of the hash in the network according to demand, the IPFS generates content-addressed hashes of the files locally by way of high-frequency requests in the system. Additionally, the IPFS provides system transparent record access, high efficiency, and secure transaction hash mapping [52]. The individual’s personal data, including vaccine and doses of information, is being stored on an off-chain (IPFS). Only the hash is stored in the Blockchain, ensuring that sensitive data is never exposed to others scanning the network. Encrypted data, for instance, can be stored off-chain from the Blockchain, with the Blockchain only storing a pointer to the encrypted data on that off-chain storage. Because hashes operate as control points to sensitive data of encrypted individuals, our method ensures that the CNDP’s confidentiality criteria are met.

The Figure 12 shows the relationship between the different parties in our proposed solution. The system actor includes government, healthcare provider, vaccination center and individuals.

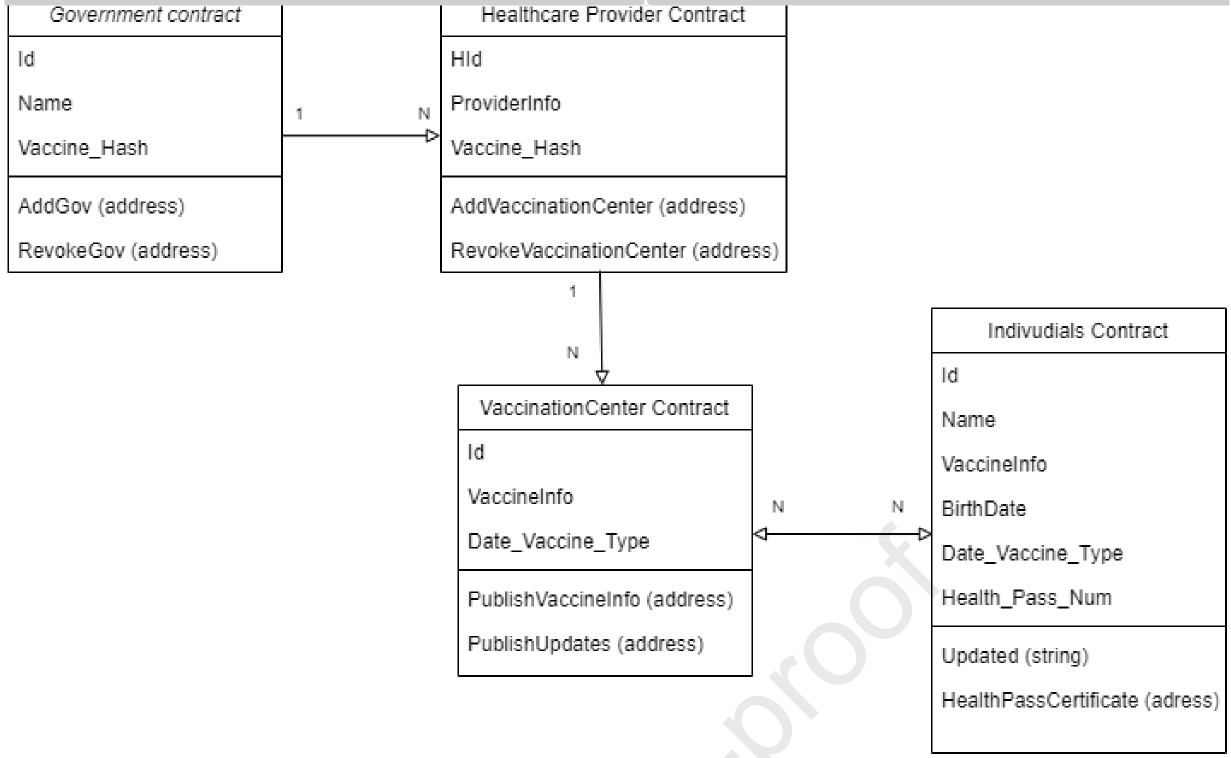


Figure 12: Relationship between parties

4.4.3 Transaction demonstration

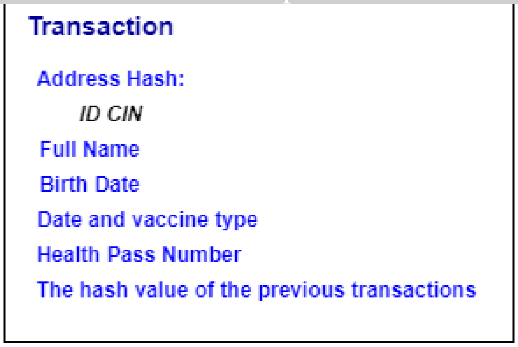
According to the literature, the following are some of the most typical sentences used to introduce data minimization: “The goal of the processing must be defined when the data is collected”. “The data should be removed when no more is necessary for the specified purpose”. “The quantity of shared data is strictly limited to the minimum needed”. “To minimize the personal information collected” [53].

Specifically, legitimate parties have access to information. For this reason, both authenticated and authorized users will be able to access shared data. Only those responsible for managing the entire content of the data should have access to it without any restrictions. In contrast, actors who just need a subset of information should have selective access to strictly required data. Minimizing data concerns the protection against excessive collection of personal information. It takes this to mean not just minimizing unjustified personal data collection, but also effectively protecting the data against illegal access or sharing, and this control should be in place throughout the system’s life cycle [54].

The advantage of exploiting data minimization in our study is that it improves information security and respects the individual’s privacy. Individual information must be valid, appropriate, and limited to what is needed with the objectives for which they are collected.

In this step, we will outline the transaction details in our case study. We define a structure, as shown in Figure 13, containing the following entries:

- ✓ Address hash that includes the necessary information: CIN identifier. Our solution aims to control access to this information to protect citizens' privacy.
- ✓ The full name and date of birth.
- ✓ Then, the date and type of vaccination.
- ✓ The number of the health pass.
- ✓ In addition, the previous transaction hash value. Each previous value refers to the number of vaccine doses taken.



Transaction

Address Hash:

ID CIN

Full Name

Birth Date

Date and vaccine type

Health Pass Number

The hash value of the previous transactions

Figure 13: Transaction illustration

We describe our On-chain and Off-chain data structure in Table 4:

Table 4: On-chain and Off-chain data

On-chain	Off-chain
• Address Hash: ✓ ID CIN	• Transaction: ✓ Address Hash ✓ Full Name ✓ Birth Date ✓ Date and vaccine type ✓ Health Pass Number ✓ The hash value of the previous transactions

The main block elements are defined as a list:

- ✓ A is a series of blocks that, like a traditional public ledger, include a complete list of transactions data.
- ✓ A hash generated on the block header using the SHA256 cryptographic hash algorithm defines each block in the Blockchain.
- ✓ A block has just one parent block unless the block header contains a previous block hash. It is interesting to note that the hashes of the block's parents would be stored on the Blockchain. A genesis block is the first block in a Blockchain that has no parent block [55].

As illustrated in Figure 15, a block includes a block header and a list of transactions. The block header, specifically, contains the following information:

- ✓ Hash value: The block cryptographic hash is generated by hashing the block header twice using the SHA256 algorithm.
- ✓ Previous hash block value: A reference to the previous block's hash on the Blockchain.
- ✓ Merkle root: A hash of the root of the Merkle tree transactions in this block.
- ✓ Timestamp: The block's estimated creation time.
- ✓ Nonce: A four-byte value that starts with 0 and rises with each hash calculation.

The block body represents a list of transactions recorded in this block. The block body defines a list of transactions recorded in this block.

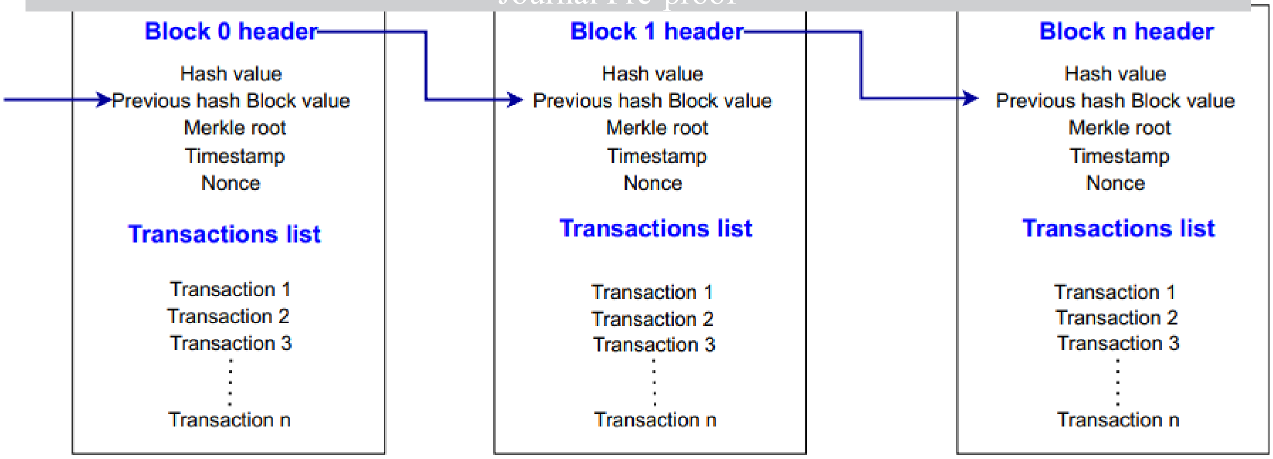


Figure 14: Blockchain structure

Figure 15 resumes our proposed Blockchain data structure as mentioned in section 5.

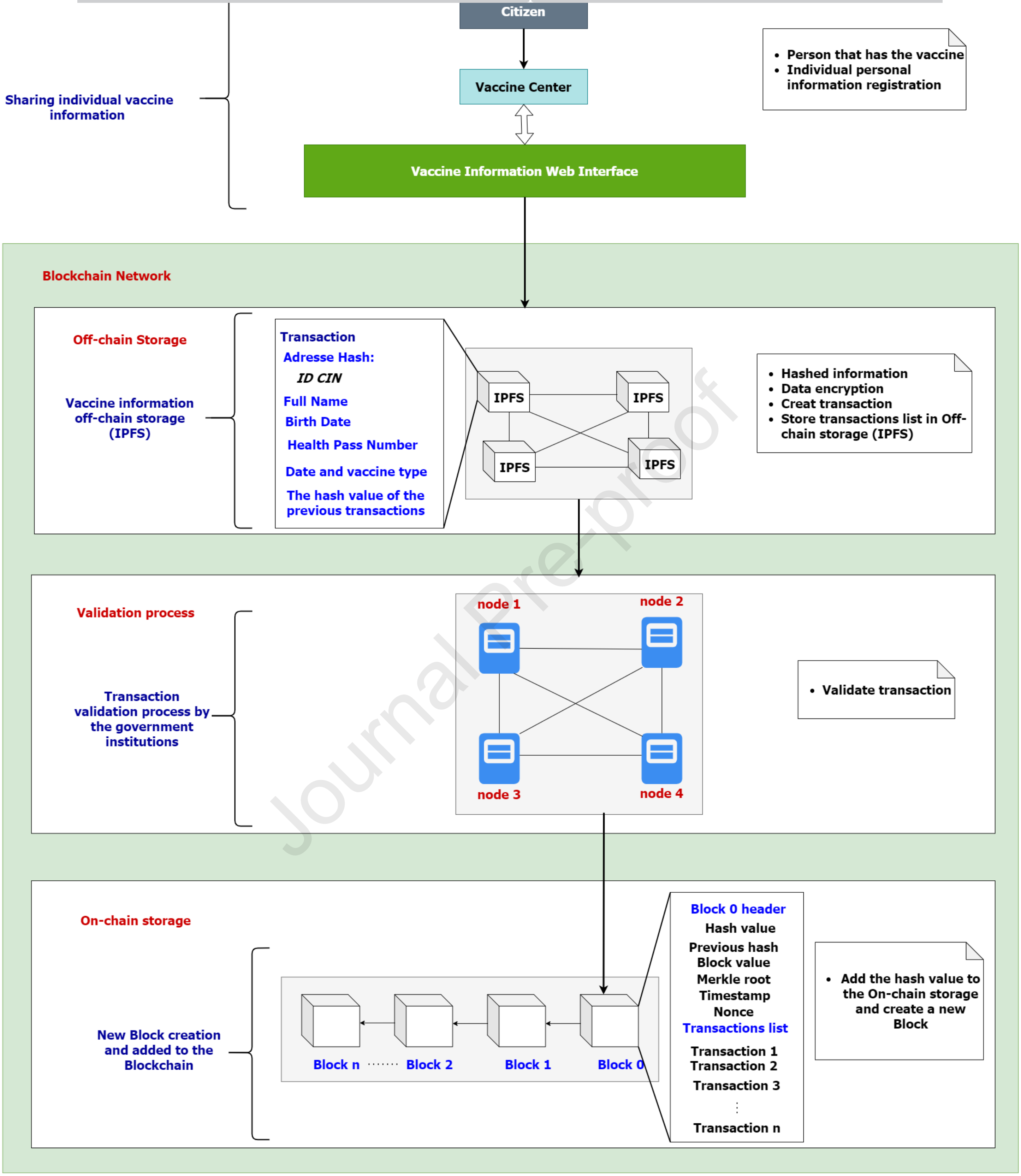


Figure 15: The proposed Blockchain data structure

5. Blockchain-based Health Passport Framework Implementation

5.1 Proposed Blockchain technology

The proposed solution is based on the Ethereum Blockchain to ensure privacy and security challenges in the

Moroccan health pass. Through this platform, we will give access to authorized parties to ensure citizens' privacy. Blockchain will provide security and data privacy as well as transparency among stakeholders.

5.2 Ethereum Blockchain

Ethereum is a peer-to-peer blockchain platform with a distributed, chronological database of transactions; it is also exchanged and maintained by nodes in the network. It owns a property of the different that allows anybody to define their characteristic, transaction protocols, and state transition algorithms. This is accomplished through the smart contract's usage, which collects cryptographic rules only performed if specific criteria are satisfied [56] [4]. Smart contracts on Ethereum are used in healthcare to generate intelligent interpretations of current medical records kept in specific network nodes. The contracts provide information on record ownership, permissions, and data integrity. Cryptographically signed instructions to manage the properties are included in the blockchain transactions in the system. The contract's state transition functions perform policies, requiring only valid transactions to change data. Any set of rules that govern a specific medical record may be implemented using such criteria, as long as they can be expressed computationally [57]. A private blockchain based on the Ethereum model has been designed to facilitate a monitoring system. In this blockchain, sensors interact with intelligent devices that use smart contracts to record events in the blockchain. The smart contracts allow for real-time healthcare management by securely sending critical notifications to patients and healthcare professionals. Patients may take ownership of their treatment while a healthcare professional is always available with real-time updates, which is vital for safe care at home [58].

5.3 System implementation

This section describes the implementation of a framework to secure and protect the individual's health pass personal information. Figure 16 describes an overview of the proposed framework based on Blockchain technology and smart contract:

[4] https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

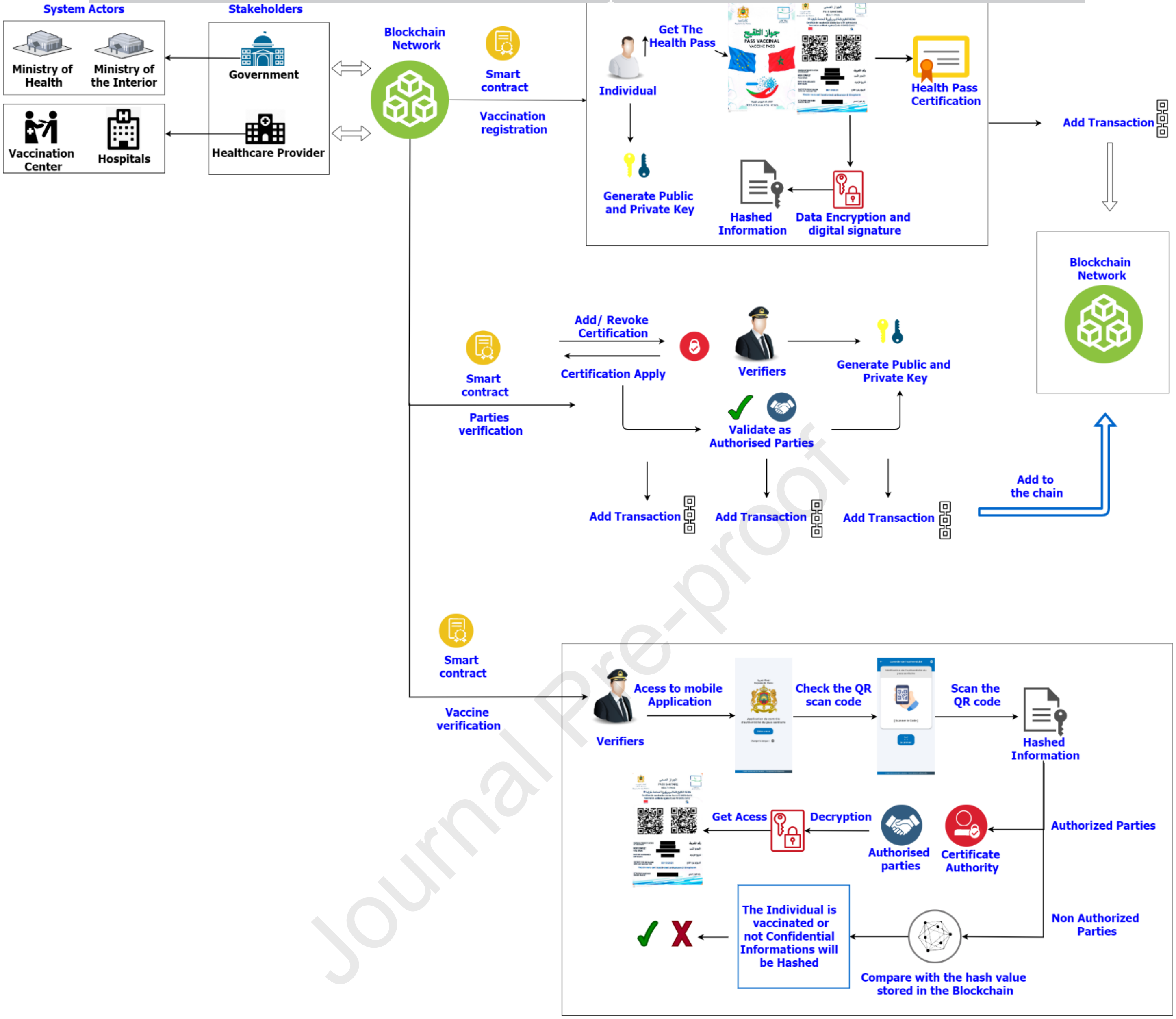


Figure 16: Overview of the proposed Blockchain-based health passport framework

To prove the following illustration, we will start with the stakeholders of our proposed system. The network of our private Blockchain includes just the authorized parties in order to ensure the traceability of communication, data security, the integrity of data, transparency among system actors, as well as privacy rights. The nodes of the Blockchain are government institutions, specifically the Ministry of the Interior and the Ministry of Health in our context of the vaccination protocol.

First, the government, which started the vaccination operation in Morocco, presents the top of our system and gives the entities, concerned the permission to vaccinate individuals. The government has two significant organizations in charge of vaccination in our country: The Ministry of the Interior and the Ministry of Health. The Ministry of the Interior holds people’s personal information and has the authority to register, write, read, and examine such information. This institution is also responsible for verifying and validating the information in order to ensure its integrity of the information. The Ministry of the Interior is responsible for sharing useful and necessary information with the Ministry of Health.

The role of the Ministry of Health is to provide the corresponding information related to the population's health status management. Here, we are interested in the participants involved in vaccination. Therefore, we mention two entities: the hospitals and the vaccination centers. These two institutions have the function of providing vaccination information: the identification card number, the full name, the date of birth, the date and the type of vaccine. The recorded information will be submitted to the Ministry of the Interior to validate it. After this phase, the Ministry of the Interior sends a message to the individual's phone containing a link to access the mobile application to download their health pass.

The goal of the vaccination process registration via our proposed system based on Blockchain technology is to protect the privacy of individuals. As shown in Figure 17, our system will generate a pair of keys for encrypting the personal information that appears on the mobile application when the verifiers check the QR code as well as the system's control and limiting access to this sensitive information. Then, our system manages the entities that are allowed to consult this information.

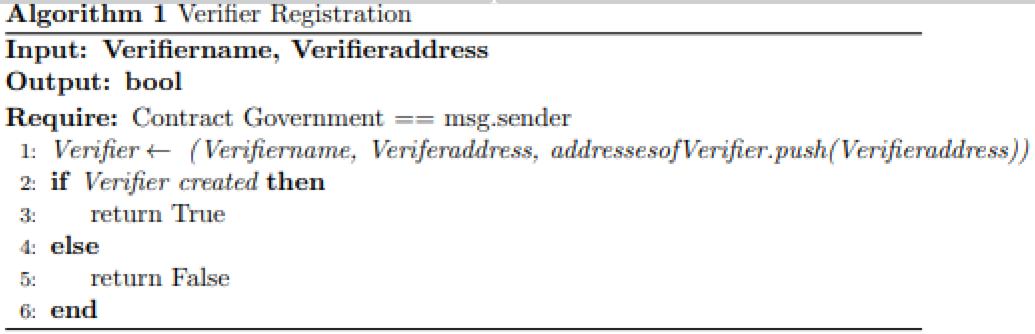
5.4 The integration of the smart contract

The smart contract [59] typically comprises a set of executive codes and conditions that a unique address may identify. Contracts are created in many programming languages, like Python or Solidity, employing particular condition instructions. After all, parties have signed the contracts, a transaction is sent to the blockchain that contains the parameters needed for the smart contract operations. The miners are then in charge of confirming and storing, the transaction in a specific block to generate a unique contract address to execute the smart contract. Then, blockchain participants can invoke the contract codes by sending a transaction to the contract, which will be confirmed by the state variable and exterior trustworthy streaming data. As a result, anytime criteria in the smart contracts are achieved, miners will execute and validate a matching response act.

Our proposed system suggests a number of smart contracts. The smart contract hierarchy includes the system actors such as government contract, healthcare provider contract, individual contract, and verifiers contract, to control and protect the user's health pass information.

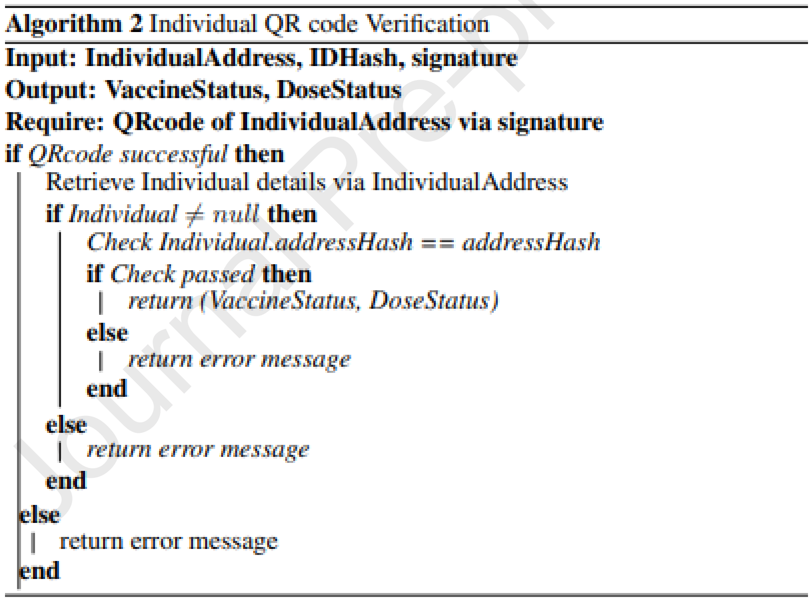
The integration of the Smart Contract for the vaccination registration process aims to provide transparency and traceability of the vaccination operation between the stakeholders of the system. In addition, the smart contract will verify the integrity of the information entered to validate the vaccinated person's health pass. Next, each transaction will be added to the Blockchain network.

A smart contract will take charge of this mission if an entity wants to verify the individual's health pass. This means that if the verifier is part of an authorized institution concerned with citizens' vaccinations, the key pairs will be generated for the decryption and access to personal information. Thus, the verifier will be validated by the government to get authorization to consult information. Then each transaction will be added to the Blockchain. Algorithm 1 describes the verifier registration process by the government to allow access to the private data:



```
Algorithm 1 Verifier Registration
Input: Verifiername, Verifieraddress
Output: bool
Require: Contract Government == msg.sender
$Verifier \leftarrow (Verifiername, Veriferaddress, addressesofVerifier.push(Verifieraddress))$
if Verifier created then
    return True
else
    return False
end
```

To verify the health pass, the verifier can access the mobile application suggested by the government to scan the QR code. To preserve individual privacy and personal information confidentiality, our system has the objective of distinguishing between authorized and unauthorized verifiers. The smart contract will search and compare the scanned hash with the one stored in the Blockchain to see if the individual is vaccinated or not. The authorized verifiers will scan the QR code and get the personal information as a result. Instead, the non-authorized verifiers will just know if the person is vaccinated or not. The information will be hashed because they do not dispose of the key pairs to decrypt the hashed information. Algorithm 2 presents the individual QR code verification scenario:



```
Algorithm 2 Individual QR code Verification
Input: IndividualAddress, IDHash, signature
Output: VaccineStatus, DoseStatus
Require: QRcode of IndividualAddress via signature
if QRcode successful then
    Retrieve Individual details via IndividualAddress
    if $Individual \neq null$ then
        Check Individual.addressHash == addressHash
        if Check passed then
            return (VaccineStatus, DoseStatus)
        else
            return error message
        end
    else
        return error message
    end
else
    return error message
end
```

According to the CNDP and relying on law 09-08, our approach will limit access to citizens' personal information without authorization by government institutions to protect the privacy of individuals.

We have implemented the smart contract related to vaccination entities in Ethereum using Solidity as the programming language. We used Remix IDE to develop and deploy smart contracts on a private Blockchain network. The smart contract code is available on GitHub[5]. Table 5 describes our system implementation characteristics:

[5] https://github.com/Sara-Bennacer/smartcontrcat_digitalHealthPass.git

Table 5: Implementation characteristics

Computer	Processor	Storage	RAM memory	Windows edition
HP computer Intel® Core (TM) i3-2370M	CPU @ 2.40GHz (2 processors)	320 Go HDD	8 Go of RAM	Windows 10

6. Results and discussion

This part focuses on testing and validating the smart contracts that define the different actors in our system. We have chosen 4 entities to test the smart contracts in our scenario: the government institute, the healthcare provider, the vaccination center and the individual.

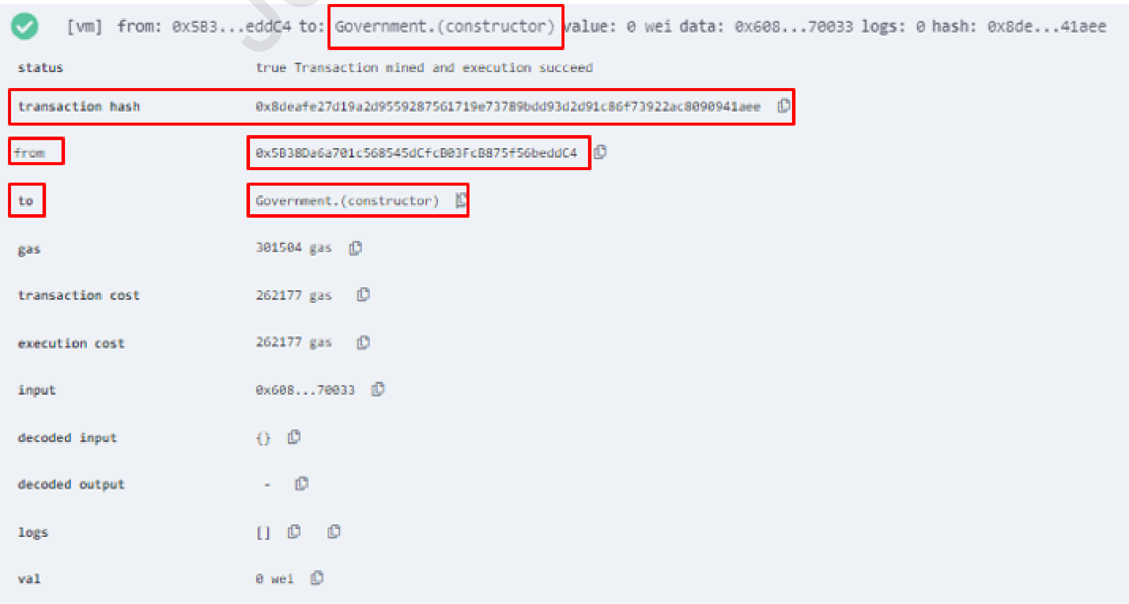
The results obtained for each on-chain operation are validated on the test network by considering the transaction hash values as illustrated in Table 6 below.

The test results take apart the transactions executed on the Blockchain, and the related Blockchain transaction receipts are provided, outlining the actor that signed the transaction, the executed call and the transaction costs in gas.

Table 6: Hash values

Entity	Hash value
Government	0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
Healthcare Provider	0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2
Vaccine Center	0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db
Individual	0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB

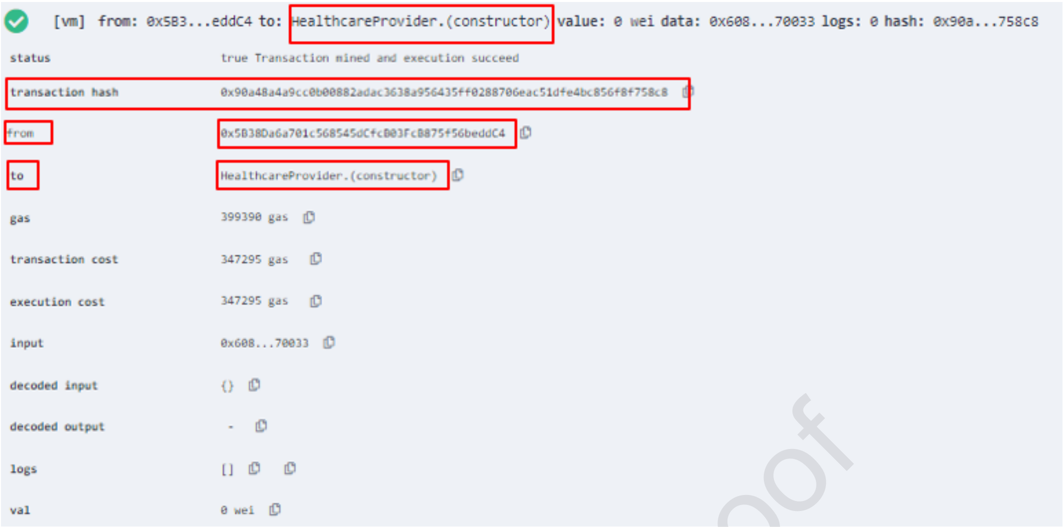
To begin, we will look at the smart contract deployment, which identifies the primary actor in our system: the government. This entity has the authority to grant or deny access to other entities, as well as to add a new vaccination center or an organization involved in this activity. The government is in charge of verifying the vaccine information and confirming the individuals' health passes, including the Ministry of Health, the smart contract is intended to manage all vaccination centers and hospitals focused with this mission.



```
[vm] from: 0x5B3...eddC4 to: Government.(constructor) value: 0 wei data: 0x608...70033 logs: 0 hash: 0x8de...41aee
status              true Transaction mined and execution succeed
transaction hash    0x8deafe27d19a2d9559287561719e73789bdd93d2d91c86f73922ac8090941aee
from                0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to                  Government.(constructor)
gas                 301504 gas
transaction cost    262177 gas
execution cost      262177 gas
input               0x608...70033
decoded input       {}
decoded output      -
logs                []
val                 0 wei
```

Figure 17: Government Smart contract test result

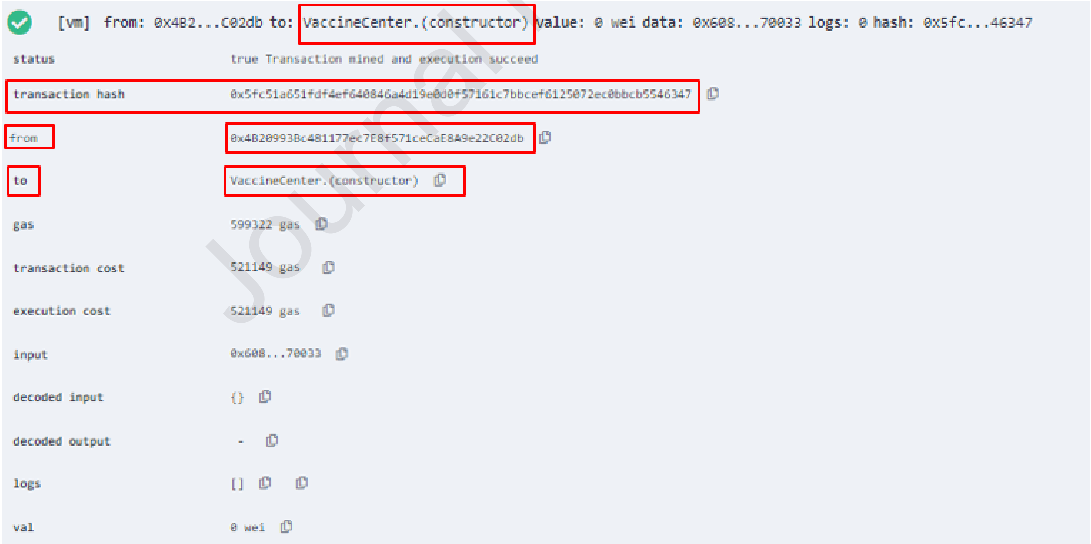
For the Healthcare provider, the smart contract controls the information concerning the citizens' vaccinations, the vaccine type, and the vaccine doses. After that, each transaction performed will be sent to the government to confirm the vaccinated person's information. Then the updates will be stored in the Blockchain.



```
[vm] from: 0x5B3...eddC4 to: HealthcareProvider.(constructor) value: 0 wei data: 0x608...70033 logs: 0 hash: 0x90a...758c8
status              true Transaction mined and execution succeed
transaction hash    0x90a48a4a9cc0b00882adac3638a956435ff0288706eac51dfe4bc856f8f758c8
from                0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to                  HealthcareProvider.(constructor)
gas                 399390 gas
transaction cost    347295 gas
execution cost      347295 gas
input               0x608...70033
decoded input       {}
decoded output      -
logs                []
val                 0 wei
```

Figure 18: Healthcare provider smart contract test result

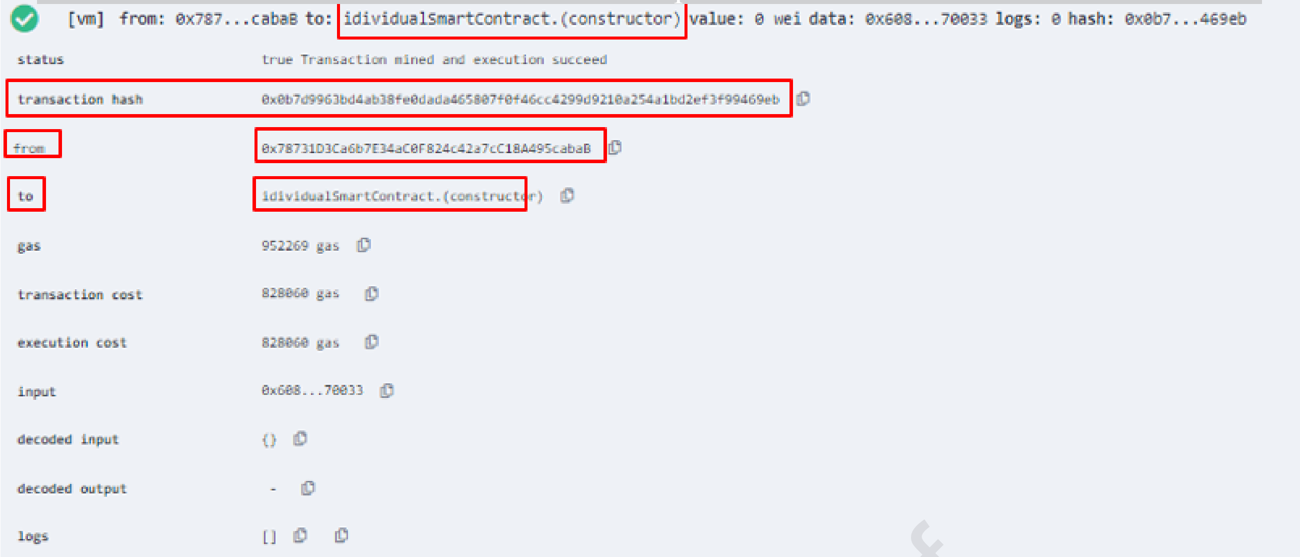
The vaccination center smart contract has the responsibility of registering the individuals' personal information related to the vaccine, health situation, and allergy history. This information will be sent to the government for validation. All transactions are encrypted to protect citizens' sensitive information. In addition, this step provides transparency and traceability between the actors of the system.



```
[vm] from: 0x4B2...C02db to: VaccineCenter.(constructor) value: 0 wei data: 0x608...70033 logs: 0 hash: 0x5fc...46347
status              true Transaction mined and execution succeed
transaction hash    0x5fc51a651fdf4ef640846a4d19e0d0f57161c7bbcef6125072ec0bbcb5546347
from                0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db
to                  VaccineCenter.(constructor)
gas                 599322 gas
transaction cost    521149 gas
execution cost      521149 gas
input               0x608...70033
decoded input       {}
decoded output      -
logs                []
val                 0 wei
```

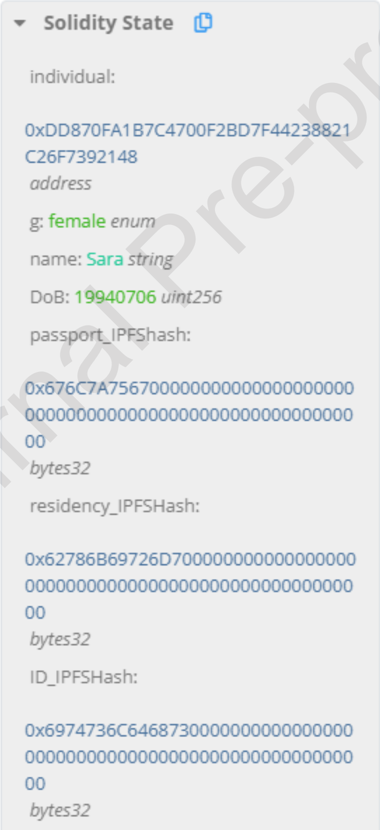
Figure 19: Vaccine center smart contract test result

An individual smart contract verifies the information and presents the individual's status and the hash address that corresponds to the personal information. Then, an individual smart contract provides the transaction information that refers to the dose number, vaccine type, and vaccination date. As shown in Figure 20, an individual smart contract that keeps personal information private. Figure 21 describes the vaccine information result of the verified individual.



```
[vm] from: 0x787...cabaB to: idividualSmartContract.(constructor) value: 0 wei data: 0x608...70033 logs: 0 hash: 0x0b7...469eb
status               true Transaction mined and execution succeed
transaction hash     0x0b7d9963bd4ab38fe0dada465807f0f46cc4299d9210a254a1bd2ef3f99469eb
from                 0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB
to                   idividualSmartContract.(constructor)
gas                  952269 gas
transaction cost     828060 gas
execution cost       828060 gas
input                0x608...70033
decoded input        {}
decoded output       -
logs                 []
```

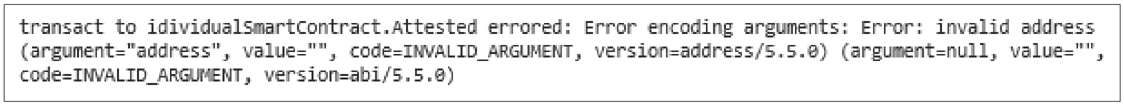
Figure 20: Individual smart contract test result



```
Solidity State
individual:
0xDD870FA1B7C4700F2BD7F44238821C26F7392148
address
g: female enum
name: Sara string
DoB: 19940706 uint256
passport_IPFShash:
0x676C7A7567000000000000000000000000000000000000000000000000000000
bytes32
residency_IPFSHash:
0x62786B69726D70000000000000000000000000000000000000000000000000000
bytes32
ID_IPFSHash:
0x6974736C646873000000000000000000000000000000000000000000000000000
bytes32
```

Figure 21: Individual verified result

For a non-vaccinated person, the result of our smart contract will indicate a transaction error; it means the individual is not yet vaccinated.



```
transact to idividualSmartContract.Attested errored: Error encoding arguments: Error: invalid address
(argument="address", value="", code=INVALID_ARGUMENT, version=address/5.5.0) (argument=null, value="",
code=INVALID_ARGUMENT, version=abi/5.5.0)
```

Figure 22: non-vaccinated individual

7. System evaluation

This section presents the costs associated with the different interactions between the proposed system's stakeholders. It is necessary to estimate the cost of deploying healthcare smart contracts while adopting medical Blockchain. The main objective is to design a system that can provide a sustainable medical health system with all of Blockchain's advantages. In the Ethereum Blockchain [60], all programmed calculations incur costs to prevent network abuse and address other computational-related challenges. Gas is the defined cost on the Ethereum Blockchain for executing all kinds of transactions, which is the price value necessary for a successful transaction or contract execution. Therefore, gas is required for all operations, computations, message calls, the creation and deployment of smart contracts, and storage.

Table 7 defines the caller name, gas used, then the transaction cost and execution cost. The transactions are executed and computed in the gas unit reported by the Remix-IDE. We provide transaction costs regarding the government, healthcare provider, vaccine center and the individual. As seen in this cost evaluation, the government and the healthcare provider contract incur costs. Besides, the health passport issuing and verification are the most frequent transaction cost of this study.

Table 7: Gas cost of Ethereum system evaluation

Actors	Gas used	Transaction cost	execution cost
Government	301504	262177	46569
HealthcareProvider	399390	347295	347295
VaccineCenter	599322	521149	23471
Individual	952269	828060	23663

8. Conclusion

This work outlines the issues related to the individual's privacy in the context of health passes. Our work explains how the adoption of the digital health passport in Morocco exposes people's privacy to fraud and infringement. In this paper, we provide the Blockchain-based digital health passport system in the case of Morocco. We designed our proposed system that respects the individual privacy Law for digital health passport. In addition, our framework comprises an innovative system of access control that respects the privacy Law 09-08. We have presented an approach based on Blockchain technology to ensure individual privacy with respect to CNDP conformity. The integration of the Blockchain aims to ensure security and privacy among the system stakeholders and thus safeguard the integrity and traceability of the vaccine information. Our system implementation is based on Ethereum Blockchain using smart contracts for testing and validation. Smart contracts application is built on the Remix-IDE. In this paper, the implementation of smart contracts enables verifiable automation; solving privacy issues and reducing information asymmetry in the health pass verification processes. The evaluation, cost, and security analysis of the proposed system highlight its feasibility in a real-world environment, addressing the challenges of privacy, and traceability securely and cost effectively. The proposed system can be adapted to address the needs of privacy, security, and traceability in other domains of activity.

References

[1] R. Ganjali *et al.*, « Clinical informatics solutions in COVID-19 pandemic: Scoping literature review », *Inform. Med. Unlocked*, vol. 30, p. 100929, 2022, doi: 10.1016/j.imu.2022.100929.

[2] J. M. Alkhalifah, W. Seddiq, B. F. Alshehri, A. H. Alhaluli, M. M. Alessa, et N. M. Alsulais, « The role of the COVID-19 pandemic in expediting digital health-care transformation: Saudi Arabia's experience », *Inform. Med. Unlocked*, vol. 33, p. 101097, 2022, doi: 10.1016/j.imu.2022.101097.

[3] S. Ilbeigipour, A. Albadvi, et E. Akhondzadeh Noughabi, « Cluster-based analysis of COVID-19 cases using self-organizing map neural network and K-means methods to improve medical decision-making », *Inform. Med. Unlocked*, vol. 32, p. 101005, 2022, doi: 10.1016/j.imu.2022.101005.

[4] H. Moujahid, B. Cherradi, M. Al-Sarem, et L. Bahatti, « Diagnosis of COVID-19 Disease Using Convolutional Neural Network Models Based Transfer Learning », in *Innovative Systems for Intelligent Health Informatics*, vol. 72, F. Saeed, F. Mohammed, et A. Al-Nahari, Éd. Cham: Springer International Publishing, 2021, p. 148-159. doi: 10.1007/978-3-030-70713-2_16.

[5] H. Moujahid *et al.*, « Combining CNN and Grad-Cam for COVID-19 Disease Prediction and Visual Explanation », *Intell. Autom. Soft Comput.*, vol. 32, nº 2, p. 723-745, 2022, doi: 10.32604/iasc.2022.022179.

[6] S. Hamida, O. El Gannour, B. Cherradi, A. Raihani, H. Moujahid, et H. Ouajji, « A Novel COVID-19 Diagnosis Support System Using the Stacking Approach and Transfer Learning Technique on Chest X-Ray Images », *J. Healthc. Eng.*, vol. 2021, p. 1-17, nov. 2021, doi: 10.1155/2021/9437538.

[7] O. E. Gannour, S. Hamida, S. Saleh, Y. Lamalem, B. Cherradi, et A. Raihani, « COVID-19 Detection on X-Ray Images using a Combining Mechanism of Pre-trained CNNs », *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, nº 6, 2022, doi: 10.14569/IJACSA.2022.0130668.

[8] O. El Gannour, B. Cherradi, S. Hamida, M. Jebbari, et A. Raihani, « Screening Medical Face Mask for Coronavirus Prevention using Deep Learning and AutoML », in *2022 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET)*, Meknes, Morocco, mars 2022, p. 1-7. doi: 10.1109/IRASET52964.2022.9737903.

[9] H. Moujahid, B. Cherradi, O. E. Gannour, L. Bahatti, O. Terrada, et S. Hamida, « Convolutional Neural Network Based Classification of Patients with Pneumonia using X-ray Lung Images », *Adv. Sci. Technol. Eng. Syst. J.*, vol. 5, nº 5, p. 167-175, 2020, doi: 10.25046/aj050522.

[10] S. Hamida, O. E. Gannour, B. Cherradi, H. Ouajji, et A. Raihani, « Optimization of Machine Learning Algorithms Hyper-Parameters for Improving the Prediction of Patients Infected with COVID-19 », in *2020 IEEE 2nd International Conference on Electronics, Control, Optimization and Computer Science (ICECOCS)*, Kenitra, Morocco, déc. 2020, p. 1-6. doi: 10.1109/ICECOCS50124.2020.9314373.

[11] B. Gavurova, V. Ivankova, M. Rigelsky, Z. Caha, et T. Mudarri, « Perception of COVID-19 Testing in the Entire Population », *Front. Public Health*, vol. 10, p. 757065, févr. 2022, doi: 10.3389/fpubh.2022.757065.

[12] C. Royo-Cebrecos *et al.*, « Mass SARS-CoV-2 serological screening, a population-based study in the Principality of Andorra », *Lancet Reg. Health - Eur.*, vol. 5, p. 100119, juin 2021, doi: 10.1016/j.lanepe.2021.100119.

[13] M. Shahroz *et al.*, « COVID-19 digital contact tracing applications and techniques: A review post initial deployments », *Transp. Eng.*, vol. 5, p. 100072, sept. 2021, doi: 10.1016/j.treng.2021.100072.

[14] F. Vogt *et al.*, « Contact tracing indicators for COVID-19: Rapid scoping review and conceptual framework », *PLOS ONE*, vol. 17, nº 2, p. e0264433, févr. 2022, doi: 10.1371/journal.pone.0264433.

[15] S. M. H. Bamakan, P. Malekinejad, M. Ziaeian, et A. Motavali, « Bullwhip effect reduction map for COVID-19 vaccine supply chain », *Sustain. Oper. Comput.*, vol. 2, p. 139-148, 2021, doi: 10.1016/j.susoc.2021.07.001.

[16] N. Alhajri *et al.*, « Physicians' Attitudes Toward Telemedicine Consultations During the COVID-19 Pandemic: Cross-sectional Study », *JMIR Med. Inform.*, vol. 9, nº 6, p. e29251, juin 2021, doi: 10.2196/29251.

[17] F.-E. Ait-Bennacer, A. Aaroud, K. Akodadi, et B. Cherradi, « Applying Deep Learning and Computer Vision Techniques for an e-Sport and Smart Coaching System Using a Multiview Dataset: Case of Shotokan Karate », *Int. J. Online Biomed. Eng. IJOE*, vol. 18, nº 12, p. 35-53, sept. 2022, doi: 10.3991/ijoe.v18i12.30893.

[18] T. Zou et A. Cheshmehzangi, « ICT Adoption and Booming E-Commerce Usage in the COVID-19 Era », *Front. Psychol.*, vol. 13, p. 916843, juin 2022, doi: 10.3389/fpsyg.2022.916843.

[19] O. Asmae, R. Abdelhadi, C. Bouchaib, S. Sara, et K. Tajeddine, « Parkinson's Disease Identification using KNN and ANN Algorithms based on Voice Disorder », in *2020 1st International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET)*, Meknes, Morocco, avr. 2020, p. 1-6. doi: 10.1109/IRASET48871.2020.9092228.

[20] B. Cherradi, O. Terrada, A. Ouhmida, S. Hamida, A. Raihani, et O. Bouattane, « Computer-Aided Diagnosis System for Early Prediction of Atherosclerosis using Machine Learning and K-fold cross-validation », in *2021 International Congress of Advanced Technology and Engineering (ICOTEN)*, Taiz, Yemen, juill. 2021, p. 1-9. doi: 10.1109/ICOTEN52080.2021.9493524.

[21] O. Daanouni, B. Cherradi, et A. Tmiri, « Predicting diabetes diseases using mixed data and supervised machine learning algorithms », in *Proceedings of the 4th International Conference on Smart City Applications*, Casablanca Morocco, oct. 2019, p. 1-6. doi: 10.1145/3368756.3369072.

[22] S. Laghmati, B. Cherradi, A. Tmiri, O. Daanouni, et S. Hamida, « Classification of Patients with Breast Cancer using Neighbourhood Component Analysis and Supervised Machine Learning Techniques », in *2020 3rd International Conference on Advanced Communication Technologies and Networking (CommNet)*, Marrakech, Morocco, sept. 2020, p. 1-6. doi: 10.1109/CommNet49926.2020.9199633.

[23] O. Terrada, B. Cherradi, A. Raihani, et O. Bouattane, « A novel medical diagnosis support system for predicting patients with atherosclerosis diseases », *Inform. Med. Unlocked*, vol. 21, p. 100483, 2020, doi: 10.1016/j.imu.2020.100483.

[24] O. Terrada, B. Cherradi, A. Raihani, et O. Bouattane, « Atherosclerosis disease prediction using Supervised Machine Learning Techniques », in *2020 1st International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET)*, Meknes, Morocco, avr. 2020, p. 1-5. doi: 10.1109/IRASET48871.2020.9092082.

[25] O. Terrada, S. Hamida, B. Cherradi, A. Raihani, et O. Bouattane, « Supervised Machine Learning Based Medical Diagnosis Support System for Prediction of Patients with Heart Disease », *Adv. Sci. Technol. Eng. Syst. J.*, vol. 5, nº 5, p. 269-277, 2020, doi: 10.25046/aj050533.

[26] O. Terrada, A. Raihani, O. Bouattane, et B. Cherradi, « Fuzzy cardiovascular diagnosis system using clinical data », in *2018 4th International Conference on Optimization and Applications (ICOA)*, Mohammedia, avr. 2018, p. 1-4. doi: 10.1109/ICOA.2018.8370549.

[27] Md. B. Hossain, S. M. H. S. Iqbal, Md. M. Islam, Md. N. Akhtar, et I. H. Sarker, « Transfer learning with fine-tuned deep CNN ResNet50 model for classifying COVID-19 from chest X-ray images », *Inform. Med. Unlocked*, vol. 30, p. 100916, 2022, doi: 10.1016/j.imu.2022.100916.

[28] Z. Alsaed *et al.*, « Role of Blockchain Technology in Combating COVID-19 Crisis », *Appl. Sci.*, vol. 11, nº 24, p. 12063, déc. 2021, doi: 10.3390/app112412063.

[29] H. Tewari, « CoviChain: A Blockchain Based COVID-19 Vaccination Passport », 2021, doi: 10.48550/ARXIV.2112.01097.

[30] M. de Vasconcelos Barros, F. Schardong, et R. Felipe Custódio, « Leveraging Self-Sovereign Identity, Blockchain, and Zero-Knowledge Proof to Build a Privacy-Preserving Vaccination Pass », *SSRN Electron. J.*, 2022, doi: 10.2139/ssrn.4036226.

[31] A. Abid, S. Cheikhrouhou, S. Kallel, et M. Jmaiel, « How blockchain helps to combat trust crisis in COVID-19 pandemic?: poster abstract », in *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, Virtual Event Japan, nov. 2020, p. 764-765. doi: 10.1145/3384419.3430605.

[32] O. Radley-Gardner, H. Beale, et R. Zimmermann, Éd., *Fundamental Texts On European Private Law*. Hart Publishing, 2016. doi: 10.5040/9781782258674.

[33] W. Moore et S. Frye, « Review of HIPAA, Part 1: History, Protected Health Information, and Privacy and Security Rules », *J. Nucl. Med. Technol.*, vol. 47, nº 4, p. 269-272, déc. 2019, doi: 10.2967/jnmt.119.227819.

[34] B. Yong, J. Shen, X. Liu, F. Li, H. Chen, et Q. Zhou, « A Blockchain based System for Safe Vaccine Supply and Supervision », *Fac. Eng. Inf. Sci. - Pap. Part B*, janv. 2020, doi: 10.1016/j.ijinfomgt.2019.10.009.

[35] Z. Qiu et Y. Zhu, « A Novel Structure of Blockchain Applied in Vaccine Quality Control: Double-Chain Structured Blockchain System for Vaccine Anticounterfeiting and Traceability », *J. Healthc. Eng.*, vol. 2021, p. e6660102, mars 2021, doi: 10.1155/2021/6660102.

[36] A. Abid, S. Cheikhrouhou, S. Kallel, et M. Jmaiel, « NovidChain: Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates », *Softw. Pract. Exp.*, vol. 52, nº 4, p. 841-867, 2022, doi: 10.1002/spe.2983.

[37] A. B. Haque, B. Naqvi, A. K. M. N. Islam, et S. Hyrynsalmi, « Towards a GDPR-Compliant Blockchain-Based COVID Vaccination Passport », *Appl. Sci.*, vol. 11, nº 13, Art. nº 13, janv. 2021, doi: 10.3390/app11136132.

[38] H. M. Hussien, S. M. Yasin, N. I. Udzir, M. I. H. Ninggal, et S. Salman, « Blockchain technology in the healthcare industry: Trends and opportunities », *J. Ind. Inf. Integr.*, vol. 22, p. 100217, juin 2021, doi: 10.1016/j.jii.2021.100217.

[39] T. McGhin, K.-K. R. Choo, C. Z. Liu, et D. He, « Blockchain in healthcare applications: Research challenges and opportunities », *J. Netw. Comput. Appl.*, vol. 135, p. 62-75, juin 2019, doi: 10.1016/j.jnca.2019.02.027.

[40] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, et J. Han, « When Intrusion Detection Meets Blockchain Technology: A Review », *IEEE Access*, vol. 6, p. 10179-10188, 2018, doi: 10.1109/ACCESS.2018.2799854.

[41] X. Xu *et al.*, « A Taxonomy of Blockchain-Based Systems for Architecture Design », in *2017 IEEE International Conference on Software Architecture (ICSA)*, avr. 2017, p. 243-252. doi: 10.1109/ICSA.2017.33.

[42] S. Saberi, M. Kouhizadeh, J. Sarkis, et L. Shen, « Blockchain technology and its relationships to sustainable supply chain management », *Int. J. Prod. Res.*, vol. 57, nº 7, p. 2117-2135, avr. 2019, doi: 10.1080/00207543.2018.1533261.

[43] S. P. Novikov, O. D. Kazakov, N. A. Kulagina, et N. Yu. Azarenko, « Blockchain and Smart Contracts in a Decentralized Health Infrastructure », in *2018 IEEE International Conference « Quality Management, Transport and Information Security, Information Technologies » (IT&QM&IS)*, St. Petersburg, sept. 2018, p. 697-703. doi: 10.1109/ITMQIS.2018.8524970.

[44] S. M. H. Bamakan, A. Motavali, et A. Babaei Bondarti, « A survey of blockchain consensus algorithms performance evaluation criteria », *Expert Syst. Appl.*, vol. 154, p. 113385, sept. 2020, doi: 10.1016/j.eswa.2020.113385.

[45] F. Tschorsch et B. Scheuermann, « Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies », *IEEE Commun. Surv. Tutor.*, vol. 18, nº 3, p. 2084-2123, 2016, doi: 10.1109/COMST.2016.2535718.

[46] A. I. Abdi, F. E. Eassa, K. Jambi, K. Almarhabi, et A. S. A.-M. AL-Ghamdi, « Blockchain Platforms and Access Control Classification for IoT Systems », *Symmetry*, vol. 12, nº 10, p. 1663, oct. 2020, doi: 10.3390/sym12101663.

[47] J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang, et Z. Wang, « Consortium Blockchain-Based Malware Detection in Mobile Devices », *IEEE Access*, vol. 6, p. 12118-12128, 2018, doi: 10.1109/ACCESS.2018.2805783.

[48] J. Jayabalan et N. Jeyanthi, « Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy », *J. Parallel Distrib. Comput.*, vol. 164, p. 152-167, juin 2022, doi: 10.1016/j.jpdc.2022.03.009.

[49] Z. Wang, X. Dong, Y. Li, L. Fang, et P. Chen, « IoT Security Model and Performance Evaluation: A Blockchain Approach », in *2018 International Conference on Network Infrastructure and Digital Content (IC-NIDC)*, Guiyang, août 2018, p. 260-264. doi: 10.1109/ICNIDC.2018.8525716.

[50] A. Shahnaz, U. Qamar, et A. Khalid, « Using Blockchain for Electronic Health Records », *IEEE Access*, vol. 7, p. 147782-147795, 2019, doi: 10.1109/ACCESS.2019.2946373.

[51] N. Nizamuddin, H. R. Hasan, et K. Salah, « IPFS-Blockchain-Based Authenticity of Online Publications », in *Blockchain – ICBC 2018*, vol. 10974, S. Chen, H. Wang, et L.-J. Zhang, Éd. Cham: Springer International Publishing, 2018, p. 199-212. doi: 10.1007/978-3-319-94478-4_14.

[52] R. Kumar et R. Tripathi, « A Secure and Distributed Framework for sharing COVID-19 patient Reports using Consortium Blockchain and IPFS », in *2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, Waknaghat, India, nov. 2020, p. 231-236. doi: 10.1109/PDGC50313.2020.9315755.

[53] Q. Ramadan, D. Strüber, M. Salnitri, J. Jürjens, V. Riediger, et S. Staab, « A semi-automated BPMN-based framework for detecting conflicts between security, data-minimization, and fairness requirements », *Softw. Syst. Model.*, vol. 19, nº 5, p. 1191-1227, sept. 2020, doi: 10.1007/s10270-020-00781-x.

[54] R. Mukta, H. Paik, Q. Lu, et S. S. Kanhere, « A survey of data minimisation techniques in blockchain-based healthcare », *Comput. Netw.*, vol. 205, p. 108766, mars 2022, doi: 10.1016/j.comnet.2022.108766.

[55] E. Balistri, F. Casellato, C. Giannelli, et C. Stefanelli, « BlockHealth: Blockchain-based secure and peer-to-peer health information sharing with data protection and right to be forgotten », *ICT Express*, vol. 7, nº 3, p. 308-315, sept. 2021, doi: 10.1016/j.icte.2021.08.006.

[56] G. A. Oliva, A. E. Hassan, et Z. M. Jiang, « An exploratory study of smart contracts in the Ethereum blockchain platform », *Empir. Softw. Eng.*, vol. 25, nº 3, p. 1864-1904, mai 2020, doi: 10.1007/s10664-019-09796-5.

[57] A. Azaria, A. Ekblaw, T. Vieira, et A. Lippman, « MedRec: Using Blockchain for Medical Data Access and Permission Management », in *2016 2nd International Conference on Open and Big Data (OBD)*, Vienna, Austria, août 2016, p. 25-30. doi: 10.1109/OBD.2016.11.

[58] H. S. Chen, J. T. Jarrell, K. A. Carpenter, D. S. Cohen, et X. Huang, « Blockchain in Healthcare: A Patient-Centered Model », *Biomed. J. Sci. Tech. Res.*, vol. 20, nº 3, p. 15017-15022, 2019.

[59] M. Sookhak, M. R. Jabbarpour, N. S. Safa, et F. R. Yu, « Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues », *J. Netw. Comput. Appl.*, vol. 178, p. 102950, mars 2021, doi: 10.1016/j.jnca.2020.102950.

[60] A. Khatoon, « A Blockchain-Based Smart Contract System for Healthcare Management », *Electronics*, vol. 9, nº 1, p. 94, janv. 2020, doi: 10.3390/electronics9010094.

Acknowledgements:

No funding to declare - None.

Highlights

Solving the Health Passport privacy issues to grant individuals data privacy from illegal actions.

Presenting a Design and Implementation of a New Blockchain-based digital health passport that respects the individual privacy Law.

The innovative access control system divides the verifiers into two parts, the authorized and unauthorized entities, to ensure the personal information privacy displayed during the QR code scan.

On-chain and off-chain storage to verify the integrity of the vaccine information.

Implementing our solution by using Ethereum Blockchain and applying smart contracts for test and validation.

Presenting a system evaluation to demonstrate the feasibility of adopting the proposed solution to address the needs of privacy, security, and traceability in other domains of activity.

Declaration of interests

☒ The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

☐ The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: