Scientific Research Publishing

Journal of Information Security, 2023, 14, 52-75
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Towards a New Model for the Production of Civil Status Records Using Blockchain

Tankou Tsomo Maurice Eddy, Bell Bitjoka Georges, Ngohe Ekam Paul Salomon

Laboratory of Electrical Engineering Mechatronics and Signal Processing ENSPY1, University of Yaoundé 1, Yaoundé, Cameroon
Email: eddy.tankou@yahoo.fr, georges@bellbitjoka.com, pasanek@yahoo.fr

How to cite this paper: Eddy, T.T.M., Georges, B.B. and Salomon, N.E.P. (2023) Towards a New Model for the Production of Civil Status Records Using Blockchain. *Journal of Information Security*, **14**, 52-75.
https://doi.org/10.4236/jis.2023.141005

Received: September 17, 2022
Accepted: January 28, 2023
Published: January 31, 2023

Copyright © 2023 by author(s) and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/

Open Access

Abstract

The work presented in this article focuses on document forgery. Document fraud is a generic term used to designate a fraud, a falsification of a document. The said falsification can be observed in several sectors of everyday life. For a better illustration, let's consider a system for producing civil status forms. The birth certificate is generally the basis of any individual's life, and if this document is falsified, it can have repercussions at several levels, particularly in the academic field, where false diplomas, false national identity cards, false passports, false marriage certificates, etc. are obtained. It is therefore demonstrated that a secure production unit for civil status forms can be beneficial to both developed and developing countries. In addition, smart contract is proposed using a private Hyperledger fabric blockchain for validation of civil status documents, and a non-state public key management infrastructure is also proposed to authenticate the nodes that will validate the transactions. This improved blockchain solves the problem of falsification of civil status documents, as false nodes can contribute to the validation of a transaction. The contribution of such a hybrid system is of paramount importance for the identity of civil status documents on the one hand and for the identity of documents in general, and the blockchain to guarantee the distributed, unforgeable, non-repudiation, transparency and disintermediation character.

Keywords

Blockchain, Forgery, PKI, Civil Status, Documentary Identity

1. Introduction

Document fraud is a generic term used to designate the falsification of a document [1]. The said falsification of documents is a gangrene that hinders our society on a daily basis. This is the case, for example, of fraud in the civil status

system, where Cameroon Tribune published in October 2020 that the Cameroonian civil status system is gangrened. In the same newspaper, a study conducted by the General Delegation for National Security on a population of nearly 600,000 inhabitants in five regions of Cameroon showed nearly 800 cases of civil status fraud; this is largely due to the submission of false and misleading statements, which are the two main types of fraud in this area [2]. This gangrene constitutes a hindrance in achieving the Sustainable Development Goals (SDGs) defined at the United Nations General Assembly in September 2015. In the literature, the problem of document identity has been addressed especially the work of Shah, Vennis Padia, Karnika Lobo, Vivian Brian who worked on the application of blockchain to civil registration systems. In this work, the major problem that the author highlighted is the cumbersome procedures related to manual registration of births and deaths. For this purpose, he proposed a decentralized, simplified and transparent application based on ethereum blockchain technology that guarantees inalterability and provides the true origin and irrefutability of the records [3]. The work of Chin-Ling Chen *et al.* on a traceable online will system is based on blockchain and smart contract technology. In this work, the authors raise the issue of the complexity, falsification, slowness and high cost of drawing up wills; to remedy this, they propose a traceable online will system integrating a dispute arbitration strategy based on blockchain technology [4]. In the same vein, the work of Malik, Gunit Parasrampuria, Kshitij Reddy, Sai Prasanth Shah, Seema on a blockchain-based identity verification model, for the authors, the problems lie in the falsification of government documents, cumbersome, tedious tasks and long process in document verification; for this, they propose a private blockchain-based document verification model [5]. Cong Hung Tran, Dien Tam Le, Hieu Le Ngoc, Thi Xuan Dinh Ho do the same by working on the application of blockchain in the authentication of high school transcripts. The problem the authors mention is the falsification of report cards, high school certificates and university transcripts. In order to solve this problem, they propose a model for authenticating academic credentials based on Ethereum. This model is based on the Ethereum blockchain technology [6].

In this article, the problem highlighted is that of the identity of documents in general and the civil status records in particular; for this, a blockchain development platform named Hyperledger fabric version 2.0 is used coupled with the Sawthooth Framework, docker acting as a container, the Go language and NodeJS are used to create a smart contract for the management of civil status records. In addition, an enhanced public key management infrastructure per organization is integrated into a private Hyperledger fabric blockchain. This solution provides a platform to improve the availability and verify the authenticity of nodes that will validate transactions and can effectively contribute to solving document fraud in developing and developed countries. Finally, to ensure verifiable authenticity of all transactions, the problem of Byzantine generals is addressed by stipulating that all nodes must approve the transaction for it to be valid and entered into the distributed ledger.

2. Literature Review on Blockchain

2.1. History of the Blockchain

The financial crisis of October 10, 2008 caused a loss of confidence never before seen in the history of the banking sector. This crisis is the trigger for the Blockchain [7]. Satoshi Nakamoto is the pseudonym used by the group of people who developed the very first Blockchain that serves as the platform for the very first virtual currency, Bitcoin. Satoshi Nakamoto created Bitcoin as a way out of the debt-ridden banking system, which had to generate more and more growth in order to pay it back [8]. Money is based on the principle of trust, as is the case with fiduciary money (bills and coins currently in use), which uses banks as trusted intermediaries for transactions between its users. This is not the case with Bitcoin, which must operate independently of banks and in a distributed manner as far as its use is concerned. Satoshi Nakamoto is thus confronted with the search for a means of trust in a distributed environment to allow the use of this currency. In distributed computing, this problem was formalized by Leslie Lamport, Robert Shostak and Marshall Pease in 1982, who called it the "Byzantine Generals Problem". The work of Ioannis Karamitsos in proposing the blockchain according to the layered model and stating that its functioning can be summarized in five layers, namely the network layer, the transaction layer, the blockchain layer, the trust layer and the application layer [9]. Buterin, Vitalik presents the blockchain development platforms, and alludes specifically to the ethereum technology [10].

2.2. Characteristics

Blockchain is generally characterized by: disintermediation, traceability, transparency, distributed consensus, unfalsifiable, distributed structure, resilience, security and trust.

- **Désintermédiation**

Blockchain technology allows exchanges without the control of a third party. The validation and addition of a block is the result of a consensus between the user-validators.

- **Transparency**

Once a document is registered on the blockchain, it is sufficient to prove that it exists at the moment and that it has not been modified;

- **Security**

Decentralized hosting also makes blockchain a secure technology: it makes it almost impossible to delete all copies of documents, which exist on a multitude of servers around the world;

- **Autonomy**

Computing power and hosting space are provided by the network nodes, *i.e.*, the users themselves.

- **Consensus**

The term "consensus" means that all the nodes in the network must agree on an identical version of the blockchain. In other words, consensus allows the au-

thenticity of each transaction to be guaranteed from the synchronization between all the nodes of the network, thus allowing the blockchain to be updated by ensuring that each block in the chain is valid. Consensus is generally characterized by: termination, approval, validity and integrity.

2.3. Areas of Application of Blockchain

The blockchain finds its application in several areas of life including the protection of personal data where Guy Zyskind presents a decentralized system of management of personal data to ensure ownership and total control over their data. For this, they propose a protocol that allows the transformation of the blockchain into an automated access control that does not require the trust of any third party [10]. Glaser, Florian presents the fact that the blockchain being an innovative technology, it can be used in the digital sector. For this, it explores the possibilities offered by the latter in the development of digital [11]. Another application of the blockchain is its application in the field of health for the management of complaints relating to patients, for this an information system based on a blockchain is set up, this will ensure transparency, the soundness of the decentralized architecture, immutable and anonymous [12]. Mingxiao's work focuses much more on consensus algorithms which, for them, the choice of a better algorithm can significantly improve the performance of a blockchain platform, for that, he makes a review of consensus algorithms such as prof of work, prof of stake, delegation prof of stake, PBFT, RAFT, [13]. Sterne de Somboun focuses on smart contract technologies, and shows the merits of using smart contracts beyond digital money [14].

2.4. Typology of Blockchain Consensus

In the literature, there are several types of consensus; each has particular specifications.

Table 1. Prof of Work (POW) [15].

Types of consensus	Advantages	Disadvantages	
Nodes are called miners and each miner is rewarded for each block they manage to approve and confirm	Very robust; Very expensive; The whole register is objectively verifiable.	Slowness of the transaction verification system (compromising availability) Energy consuming solution, economic and ecological problem; Less developed chains are very sensitive to 51% attacks	11111A

Table 2. Prof of stake (PoS) [15].

Types of consensus	Advantages	Disadvantages
To validate a block, nodes must prove their possession of a certain amount of crypto currency, and pawn it on the network	Less energy consuming energy consumption; More ecological compared to the work proof; Strong resistance to 51% attacks	The problem of nothing in play makes PoS algorithms more complex

Table 3. Delegated Proof of Stake (DPoS) [15].

Types of consensus	Advantages	Disadvantages
Token holders can elect delegates who will validate transactions on their behalf	The speed	Reduced number of transaction validators creating a huge queue; Inefficiency of the delegate leads to poor validation.

Table 4. Proof of Authority (PoA) [15].

Types of consensus	Advantages	Disadvantages
Blocks and transactions are validated by pre-approved accounts	Energy efficiency; Extremely fast transaction.	Centralized system

Generally speaking, a blockchain transaction takes place as follows:

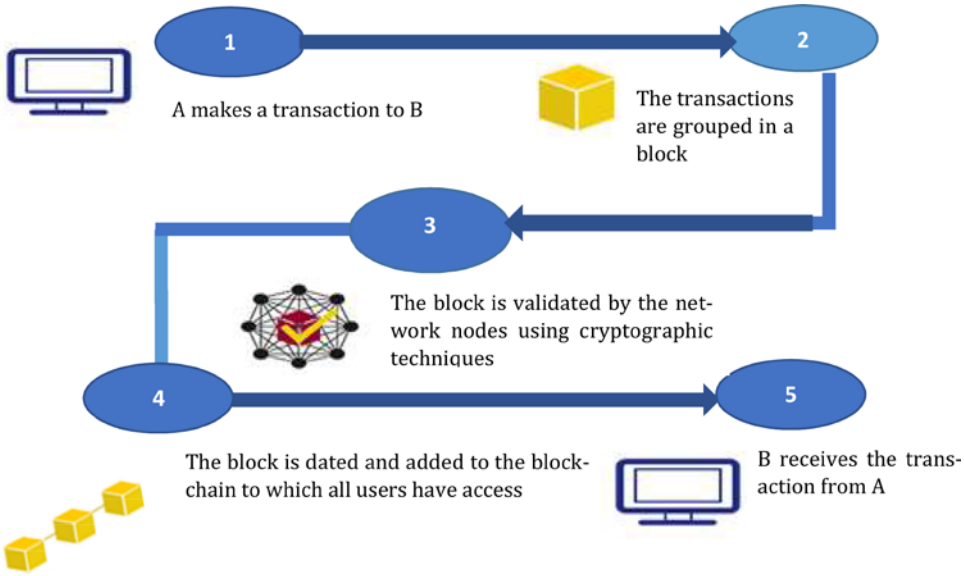

Figure 1. Transactional process in the blockchain [15].

2.5. Types of Blockchain

There are generally several types of blockchain. These different types are recorded in the table below.

Table 5. Typology of blockchain [15].

Types/characteristics Private		Public	Consortium
Consensus	Private consensus	Non-scalable network	Consensus selected
Centralization/Decentralizaon	Fully centralized	Totally decentralized	Semi-decentralized
Reading/Writing	Private reading and writing	Public reading and writing	Reserved reading and writing
Flow rate	Excellent flow	Very low flow rate	Excellent transaction throughput
Scalability	Non-scalable network	Scalable network	Non-scalable network

3. Materials and Methods

First, it is necessary to present the weaknesses and potential solutions proposed

by the distributed architecture based on the blockchain.

3.1. Weaknesses in the Birth Certificates

Table 6. Weaknesses in birth certificates.

Nature of the act	Activities	Weaknesses
Birth certificate	Declaration of birth	False declaration of birth
Birth certificate	Declaration of birth	Impossibility to verify the authenticity of the said declaration authenticity of the said declaration
	Creation of the act followed by the registration in the registers A (for the concerned civil status center), B (for the national civil status office and C (for the Justice)	Presence of the acts without stump Falsification Possibility of error that leads to the overloading of the act Possibility of creating a backdated act

3.2. Weaknesses in the Marriage Certificates

Table 7. Weaknesses in marriage records.

Nature of the act	Activities	Weaknesses
Marriage certificate	Publication of a one-month marriage band	Publication form reduced to a simple A4 format
	Establishment of the act on the day of the wedding itself	Falsification of the act Non-respect of the closures defined by the future spouse

3.3. Weaknesses in the Death Certificates

Table 8. Weaknesses in the death certificates.

Nature of the act	Activities	Weaknesses
Nature of the act	Declaration of death	reduced to an A4 form without any authenticity
	Creation of the act followed by the registration in the registers A (for the concerned civil status center), B (for the national civil status office and C (for the Justice)	Presence of the acts without stump Falsification Possibility of error that leads to the overloading of the act Possibility of creating a backdated act

3.4. Identified Problems and Blockchain Solutions

Table 9. Problems with civil status documents and solutions proposed by the blockchain approach.

Problems	Current civil status solutions	Blockchain solutions
Presentation of forgeries: False declaration of civil status records, presence of a record without a counterfoil	The declarations of act are handwritten and can be subject to several falsifications	The declaration form is identical in all the civil status centers. Once a birth has been declared, it is no longer possible to declare it in another registry office. Moreover, a unique identification number is generated for each document.

Continued

Misrepresentation: Addition or removal of parents' names; The establishment of several different birth certificates to the same citizen in different civil status centers; Birth certificates in which the place of birth is changed; Those established to a foreigner as being Cameroonian.	Addition or removal of parents' names; The establishment of several different birth certificates to the same citizen in different civil status centers; Birth certificates in which the place of birth is changed; Those established to a foreigner as being Cameroonian; The establishment of a second marriage certificate to a monogamous citizen.	Awareness of the actors involved; Regular updating of the legal framework; Formalization of civil status management procedures Civil status records established on a regular basis in the civil status registers (register A, register B, register C); Handwritten serial number with the settlement region initials of the day and year.

3.5. Methods

The methodology employed is multi-scale. First, we use the uml approach to model the interactions between entities to verify the authenticity of the authors during a transaction, we use a public key management infrastructure with high availability of root certification authorities; this is integrated into a private blockchain development platform (Hyperledger fabric) to verify the authenticity of transactions. An Ubuntu distribution is used for deployments of the solution.

In addition, a public key management infrastructure per organization and non-state character is deployed as follows to guarantee the identity of nodes during a transaction. This public key management infrastructure relies primarily on asymmetric encryption and digital signature. As for encryption, it is the transformation of a clear message M using a key to obtain an output cipher text. The diagram below illustrates the concept better.

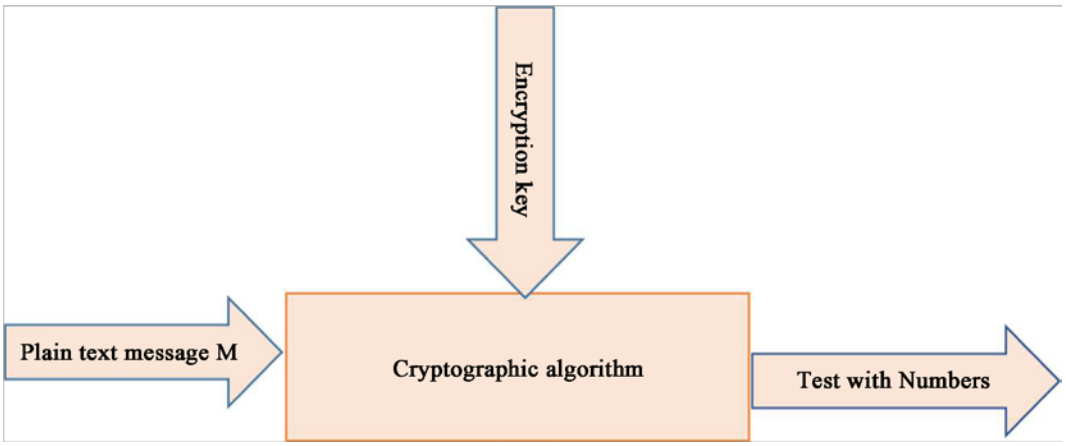

Figure 2. Principle of encryption.

There are several types of encryption namely symmetric encryption in which the encryption key Ke is identic to the decryption key Kd, and asymmetric systems in which the encryption key Ke ≠ Kd. In a public key management infrastructure, the encryption system used is the asymmetric system, especially the case of RSA. The principle of asymmetric encryption is essentially based on the factorization of very large prime numbers. In the RSA systems, an individual X

wishes to send a message to an individual Y. For that, the individual X emits a request for communication to his interlocutor Y. The individual Y sends his public key to X who in turn uses it to encrypt his message, once the encrypted message arrived to the individual Y, he uses his secret key to decrypt the content of the message. In this type of system, individuals X and Y each have a key pair, one public and the other private.

The encryption deployed in the key management infrastructure is based on the principle of:

3.5.1. Step 1: Key Generation

1) Choose two distinct very large prime numbers p and q;

2) Compute their product n called the modulus of encryption;

$$n = p \times q \tag{1}$$

3) Compute $\varphi(n) = (p-1)(q-1)$ which is the Euler indicator value;

$$\varphi(n) = (p-1)(q-1) \tag{2}$$

4) Choose an encryption exponent e such that the

$$pgcd(e, \varphi(n)) = 1 \tag{3}$$

that is prime between them.

Compute the inverse d of e modulo $\varphi(n)$ by the extended Euclid algorithm

$$d \times e \equiv 1(modulo\ \varphi(n)) \tag{4}$$

this calculation is done using the extended Euclid algorithm.

The public key is formed by the couple (n, e) and the private key is d kept confidential.

The modulo function is used to determine the remainder of the Euclidean division of two distinct prime numbers chosen when preparing the keys.

3.5.2. Step 2: Encryption

The sender transforms his message into an integer m and encrypts it using the recipient's public key (n, e), calculates the input message using the fast exponentiation algorithm and then transmits this message to the recipient.

$$X \equiv m^e \ (mod\ n) \tag{5}$$

3.5.3. Step 3: Decryption

The recipient in turn receives the message X encrypted by the sender, decrypts it using his private key

$$m \equiv X^d \ (mod\ n) \tag{6}$$

This decryption principle is essentially based on Ferma's little theorem improve that: let d be the inverse of e modulo $\varphi(n)$, *with* $n = p \times q\ (p \neq q)$

$$\text{If } X \equiv m^e \ (mod\ n) \text{ then } m \equiv X^d \ (mod\ n) \tag{7}$$

Encryption thus allows in pki to guarantee that a message can only be decrypted by the holder of the private key.

Speaking of the signature, it allows to verify that the message comes from the holder of the private key, this allows to guarantee, the authenticity of the sender and the confidentiality.

The general principle of the signature is based on the following diagram:

3.5.4. Digital Signature

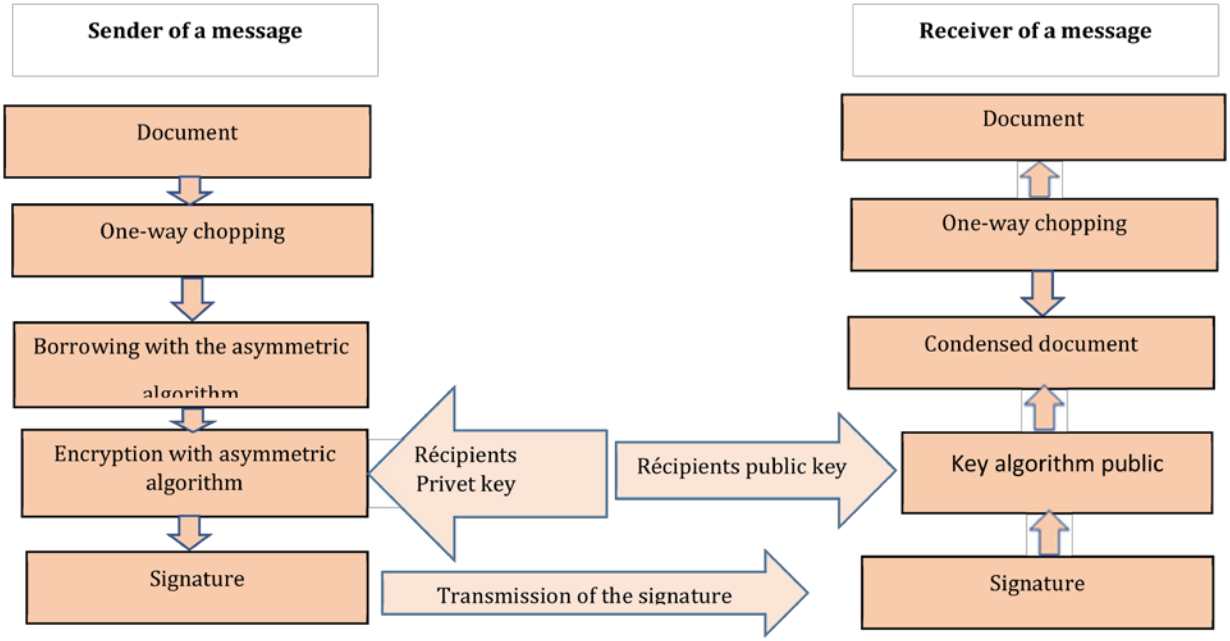

Figure 3. Schematic diagram of the signature.

3.6. System Modeling

On the other hand, in view of the increasing complexity of information systems, UML is the best approach for modeling. For a good understanding, this modeling must be accompanied by a presentation of the actors. To guarantee the authenticity of the authors' public keys, a public key management infrastructure by organization with high availability of the root authority is proposed for integration in a private blockchain.

3.6.1. Identification of the Actors of the System

As actors, we have the data entry agent of the commune, the control agent of the commune, the administrator of the commune (representative of the commune), the national office of civil status (BUNEC), the general delegation for national security (DGSN).

3.6.2. Representation of the Diagrams

The figures below illustrate the diagrams resulting from the analysis and the uml modeling.

1) Global use case diagram

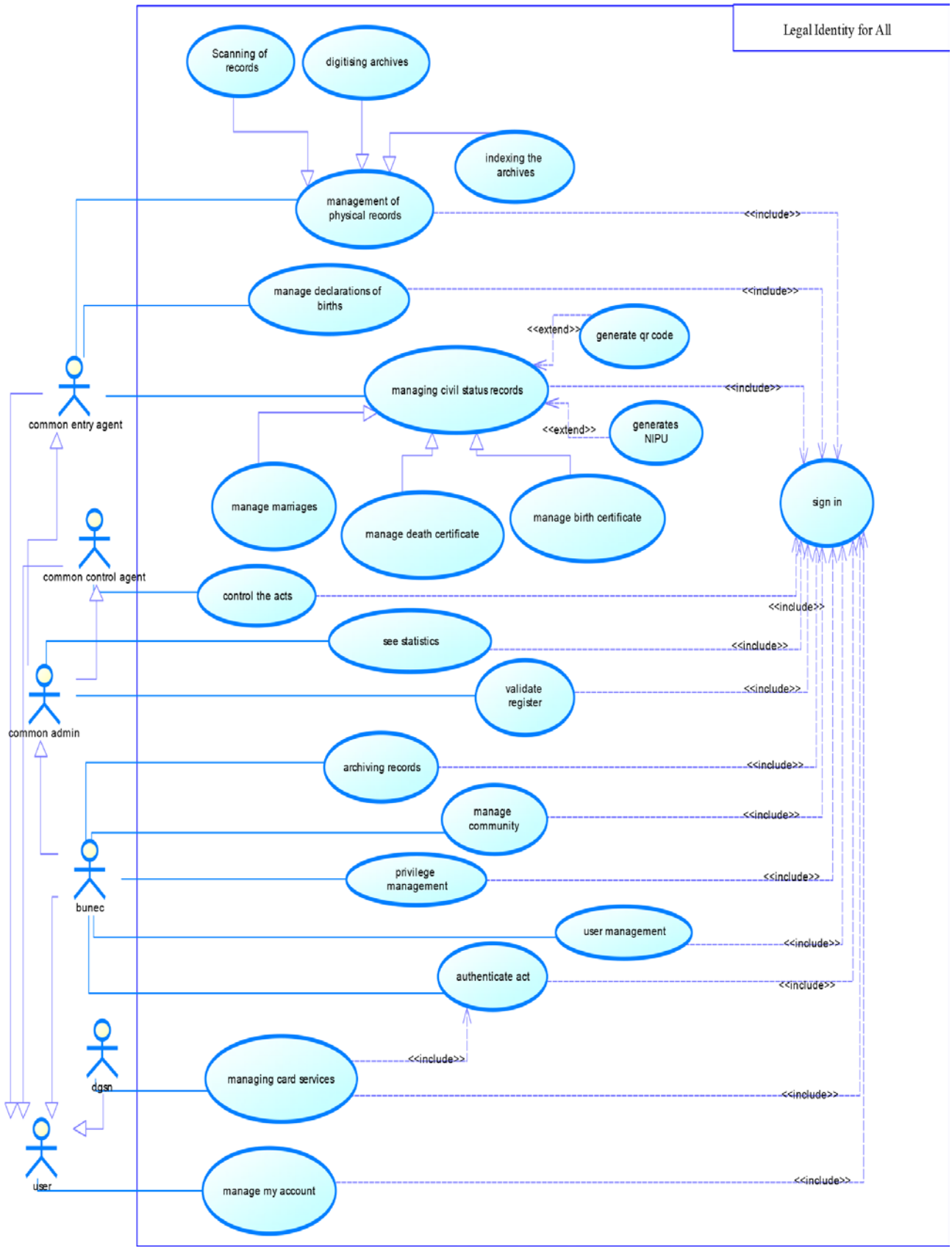

Figure 4. System use case diagram.

2) Authentication sequence diagram

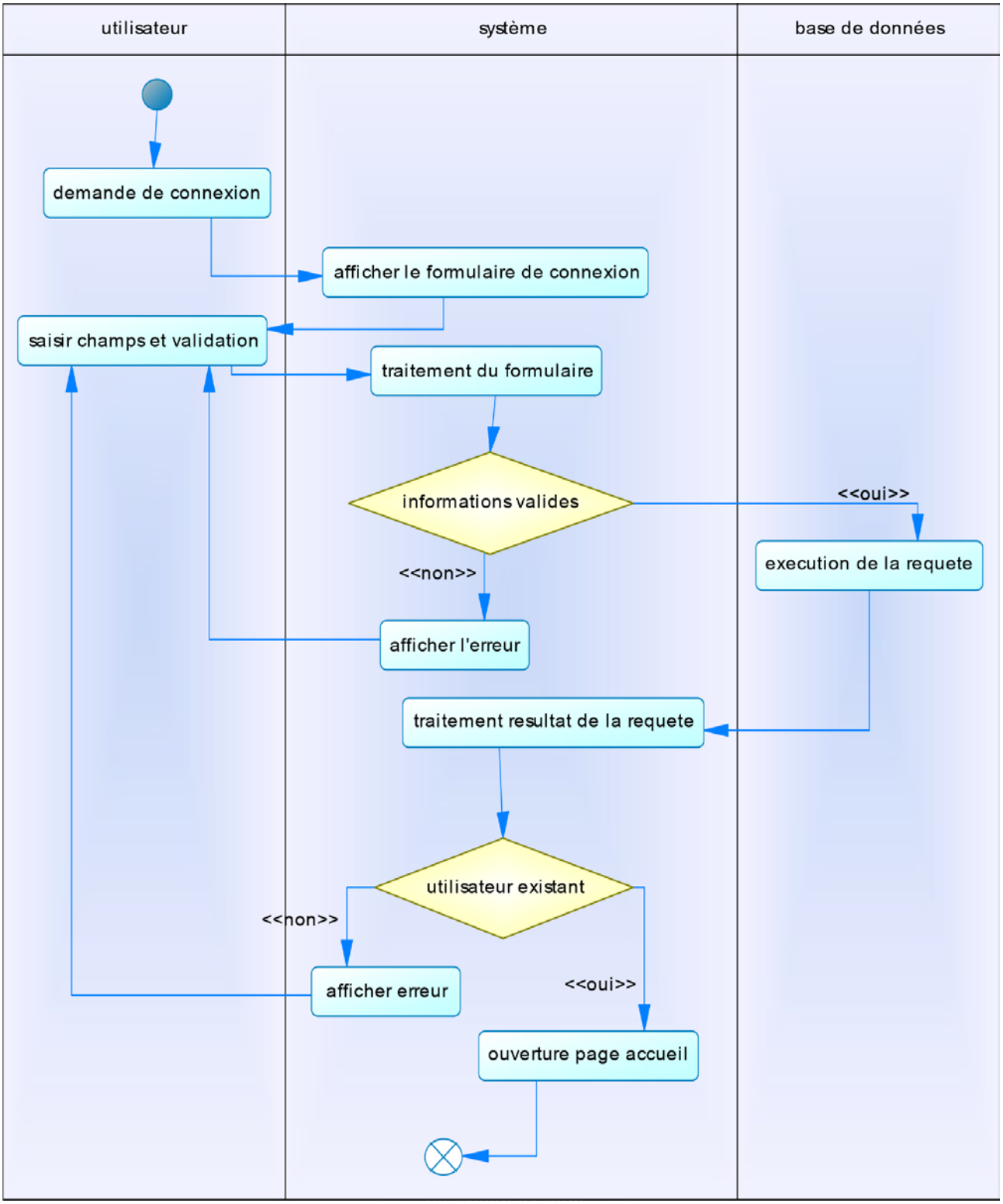

Figure 5. Authentication sequence diagram.

3) Activity diagram: case of the creation of an act

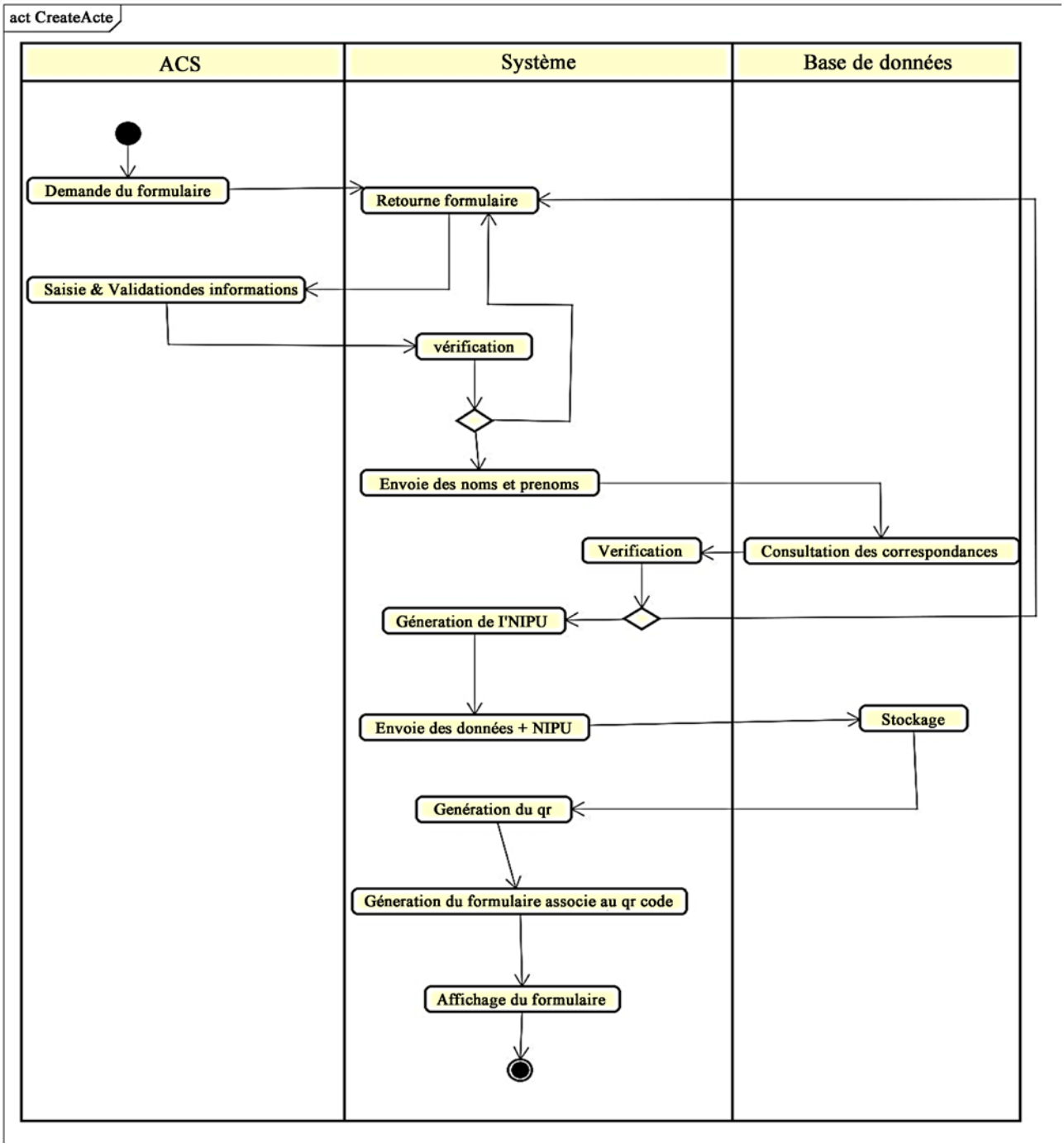

Figure 6. Activity diagram: case of the creation of an act.

4) Component diagram

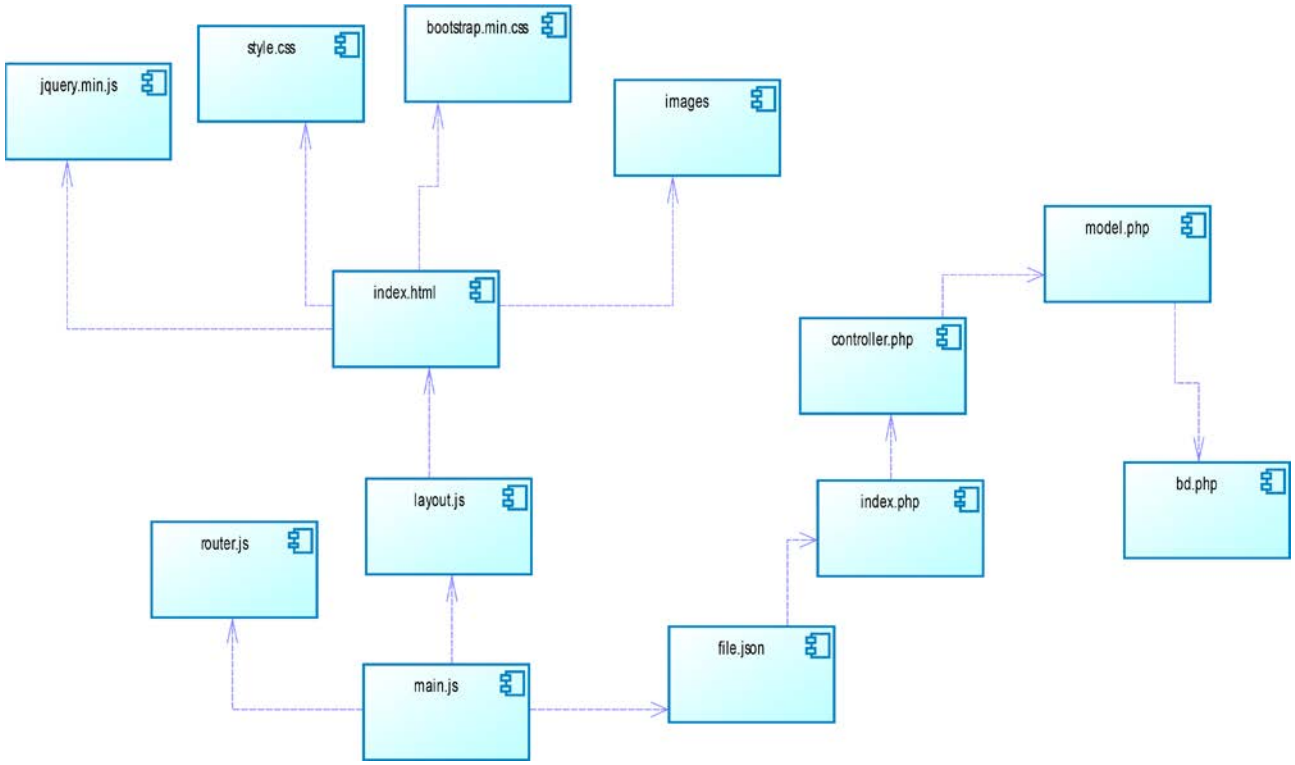

Figure 7. Component diagram.

5) Deployment diagram

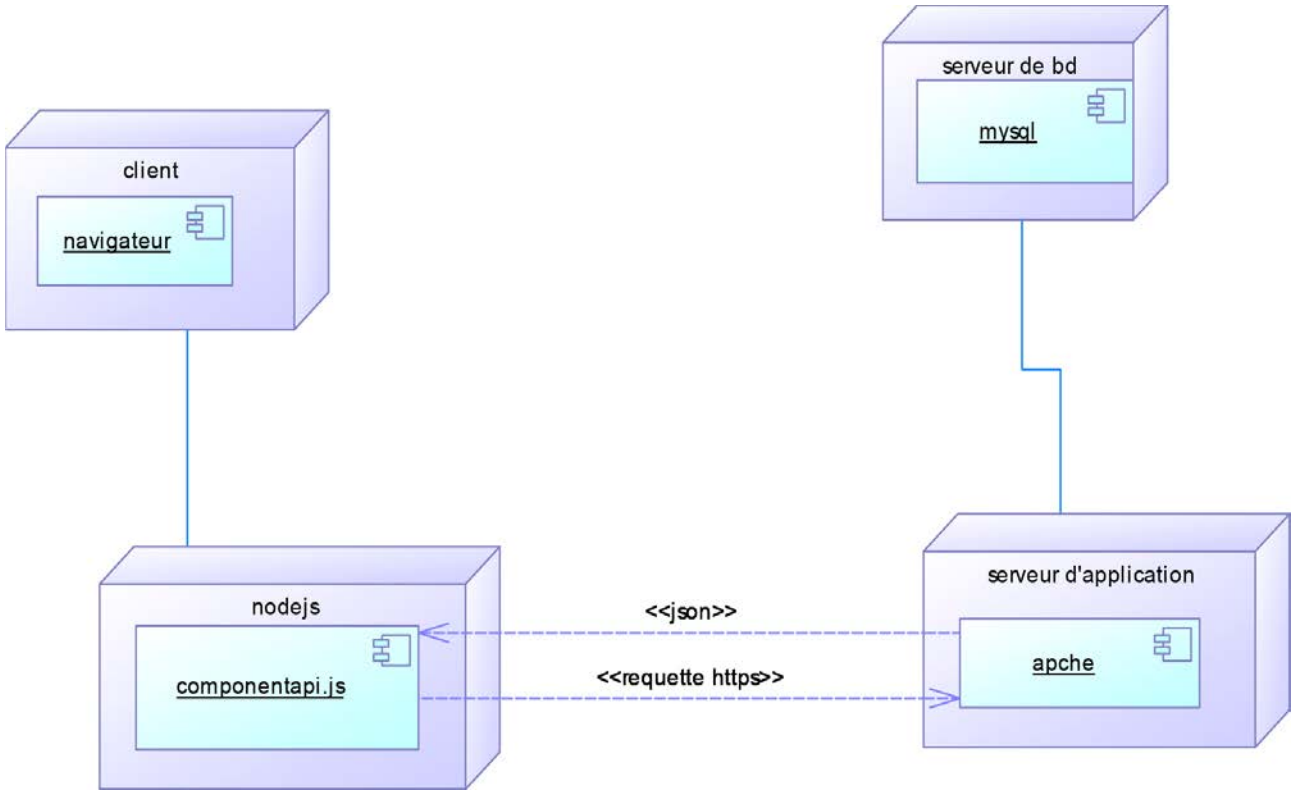

Figure 8. Deployment diagram.

6) Processing a transaction through the private

In this section, we present the results of a transactional procedure using a private blockchain Hyperledger fabric. To do so, we start by presenting the roles played by the actors of the system. Table 10 shows all the actors as nodes in the system and their roles.

Table 10. System actors in the transaction.

Actors	Descriptions	Functions
MINSANTE	Ministry of Public Health intervenes in the process through the hospitals	Declare births and deaths by a doctor
MINAT	The Ministry of Territorial Ad-ministration intervenes through the civil status centers, sub-prefectures and prefectures	Establish the publication of banns, birth, marriage and death certificates, authenti-cate and certify documents
BUNEC	National Registry Office	Archiving of the type B register

3.7. Results and Discussion

Once the actors are presented, we discuss in the results the process of processing a transaction by the private blockchain, the case of the declaration of birth or death until its insertion in the distributed register.

As indicated previously in Figure 1, the client initiates the transaction. It is the sending workstation, *i.e.* the client's workstation, which in our case is the doctor's workstation who notes the birth or the death.

In the diagram in Figure 9, we present the steps for processing a transaction (birth or death declaration) until it is inserted into the distributed registry.

1) The client application, which is that of the physician of an accredited hospital, proposes the transaction. This transaction can be a declaration of birth or death. This is done by filling in a birth or death declaration form.

2) The minsanté and minat, which are our peer approvers, simulate this transaction using the smart contract specified by the client and send back their results with their signatures. Since a single node cannot modify the network registry by itself, it must ask all other nodes to approve the validation of the registry.

3) The client, which is the physician's application, retrieves all these responses, verifies their consistency, and adds each approval's signature to the transaction.

4) It then submits the transaction to the scheduler network. It is in this part that the transaction is actually performed. It is in the scheduler network that we have a use of the consensus established between the organizations participating in the transaction, and validation of the transaction. The role of the scheduler network is to participate in the application of the consensus. In our case, the BUNEC, the MINSANTE and the MINATD have their servers playing the role of controller node. They are the ones who will participate in the application of the consensus and the verification of the intelligent contract. In our case, the infrastructure of public key management by organization is deployed, with high

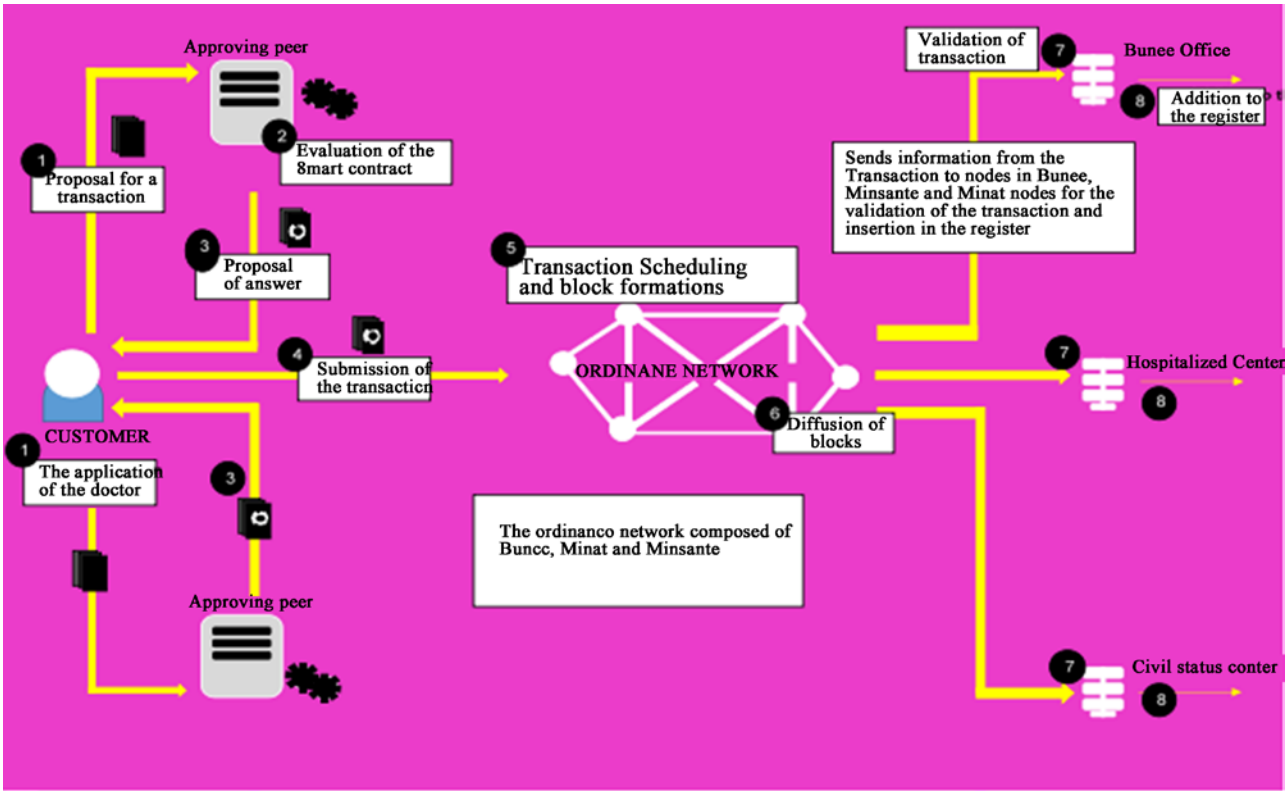

Figure 9. Processing a transaction: case of a birth or death declaration.

availability for the authenticity of the authors' public keys. For a better resolution of the Byzantine general's problem, our smart contract stipulates that all scheduler nodes must approve the transaction for it to be true, which guarantees the authenticity of the transaction's contrary to the 51% law which stipulates that if the 51% of nodes validate a transaction it is authentic. We thus demonstrate that in the 51% law, a false (illegal) node can contribute to the validation of trans-actions and ultimately distort the results of the transaction, as shown in Table 2, the Prof of stake consensus is used after a comparative study of the consensus in Tables 1-4.

The nodes of the network are MINAT, BUNEC and MINAT respectively as shown in Figure 10.

1) In this architecture, the organizations each have nodes (B1, B2, ... Bn; M1, M2, ... Mn; H1, H2 ... Hn) which allow to authenticate the transaction authors and guarantee that the transaction really comes from legitimate nodes.

2) For each member organization of our private blockchain (MINATD, MINSANTE and BUNEC), a scheduler extracts and distributes new blocks of transactions to all the peers, *i.e.* to all the nodes in its organization. Table 9 illustrates the actors mentioned.

3) Upon receipt of a block, each peer verifies that each transaction has been approved by the expected set of approbators and checks for conflicts between transactions.

4) Verification of the validity of the declaration by the peers of each organization

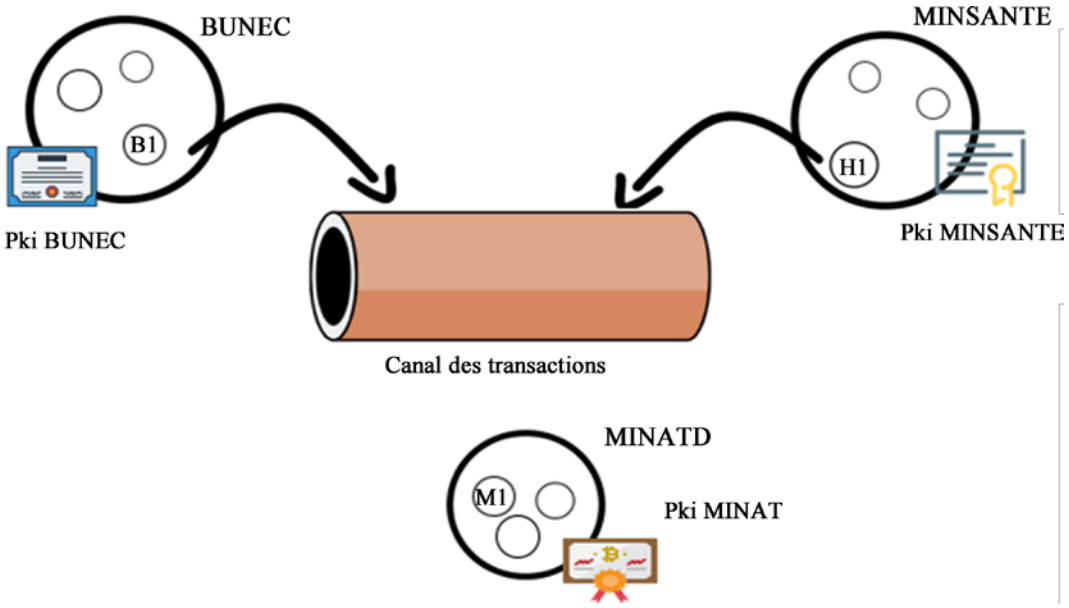

Figure 10. General architecture of the public key management infrastructure per organization.

participating in the transaction.

5) The peers add the birth, death or other declarations to their records.

3.8. Smartcontract Specifications

The specifics of our smart contract are summarized in the flowcharts in the figures below.

The digital forms are designed via the design site, produced at the production sites; once the digital production is completed, the birth and death declaration forms are sent to the hospitals and the marriage band publication forms, the birth, marriage and death certificate establishment forms are sent to the civil

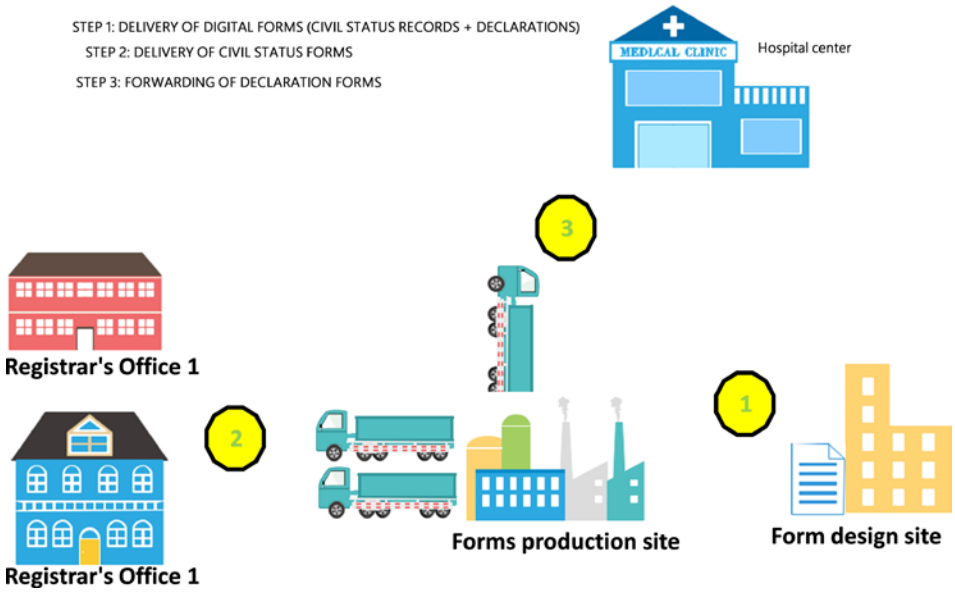

Figure 11. Proposed system functional architecture.

status centers for processing. The rules of operation of the smart contract are based on several criteria.

As far as birth and death declarations are concerned, only the doctor establishes the birth and once the birth is established, the parents of the infant have a period of 0 to 90 days to declare the birth. In this case, our smart contract must verify that the date of birth entered on the form is within the range of 0 to 90 days. On the other hand, the intelligent contract takes into account that if a declaration is not made within this interval, if the date of the declaration is included in the interval of 90 days to 6 months, it is imperative to send a request to the public prosecutor for authorization; and for a declaration made after 6 months, the treatment is submitted to the president of the competent court for a supplementary judgment All this information is valid for a legitimate child. For an unrecognized child, the digital declaration must be accompanied by the digital national identity card of the mother of the infant at the civil status center. In addition, the smartcontract verifies the documents associated with the different declaration forms for an authentic and complete record.

Given a distributed architecture based on the blockchain, all nodes in the network will receive the proposed declaration of birth or death, a high-availability key management infrastructure allows to authenticate the authors who propose the transaction if these nodes are legitimate nodes the transaction is ready to enter the consensus process. This consensus specifies that all nodes in the network (Ministry of Health, Ministry of Justice, Ministry of Territorial Administration, and National Registry) must approve the transaction for it to be validated.

Once the declaration is validated and entered in the distributed registry, a unique identification number (NIU) is issued to the parents of the infant. The parents in turn go to the local registry office and the registrar uses this number to post the record form. Once the act is established, it is submitted to the network for validation. At this level, since the pki had already authenticated the nodes, the consensus must directly come into play; its principle is based on a prior validation of all the pairs of the network. After validation, the transaction is registered in the distributed register, which can be consulted by the competent bodies.

This process is identical to the establishment of a death certificate, with the only difference that a death certificate issued by the hospital of the place of occurrence, the identity card of the deceased and two legitimate children with their card are added to the death declaration.

The above flowcharts illustrate the specifications of smart contracts for the declaration of birth, death, publication of marriage banns as well as birth, marriage and death certificates.

As indicated in Tables 6-8, the flowcharts of the smart contracts are presented taking into account the limits summarized in Table 9.

In Figures 4-8 are indicated the modeling processes with the different diagrams, using the actors presented in Table 9. Figures 12-14 represent flowcharts specifying the operating rules of the smart contract.

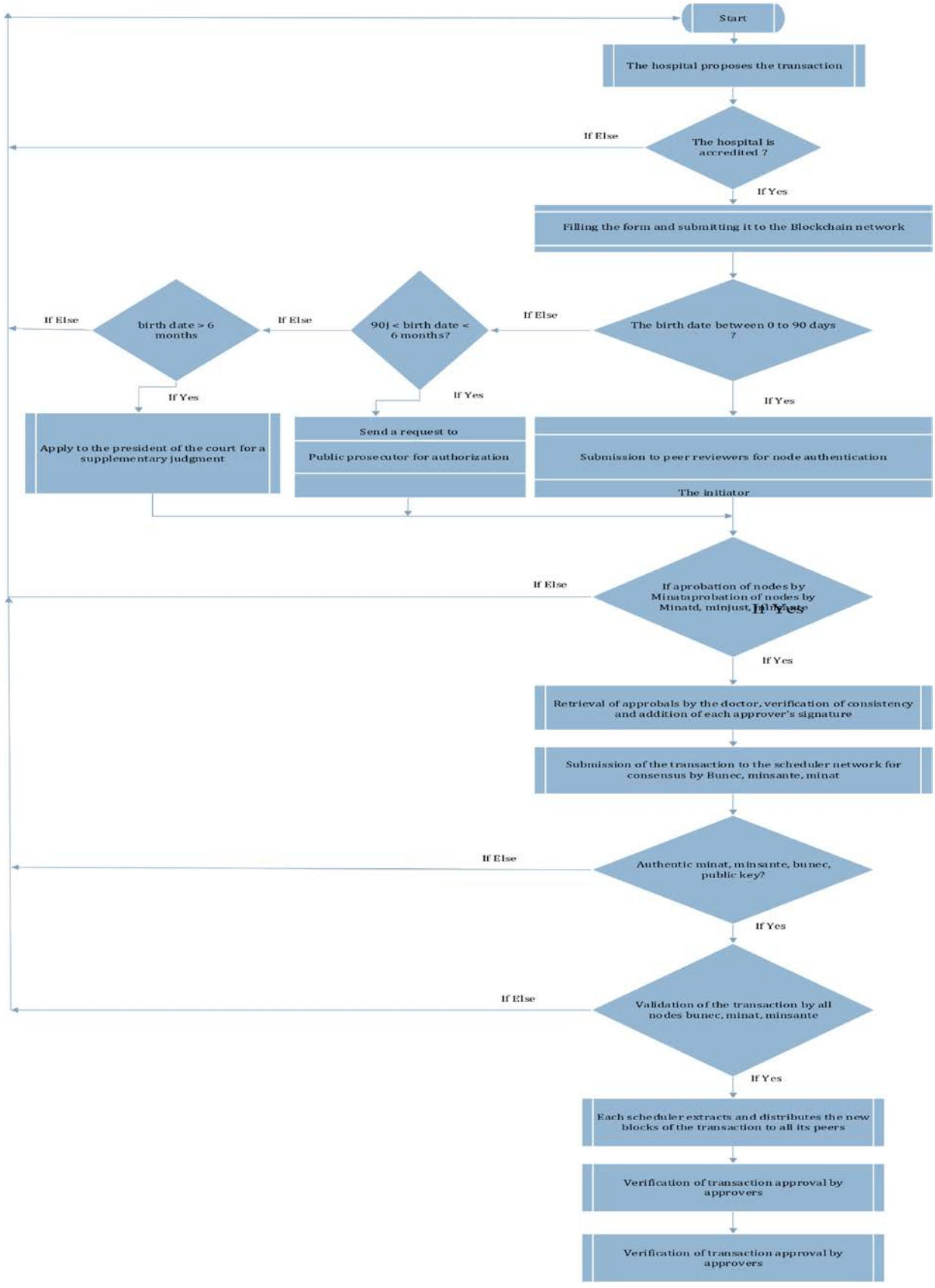

Figure 12. Specifications of the smart contract for birth.

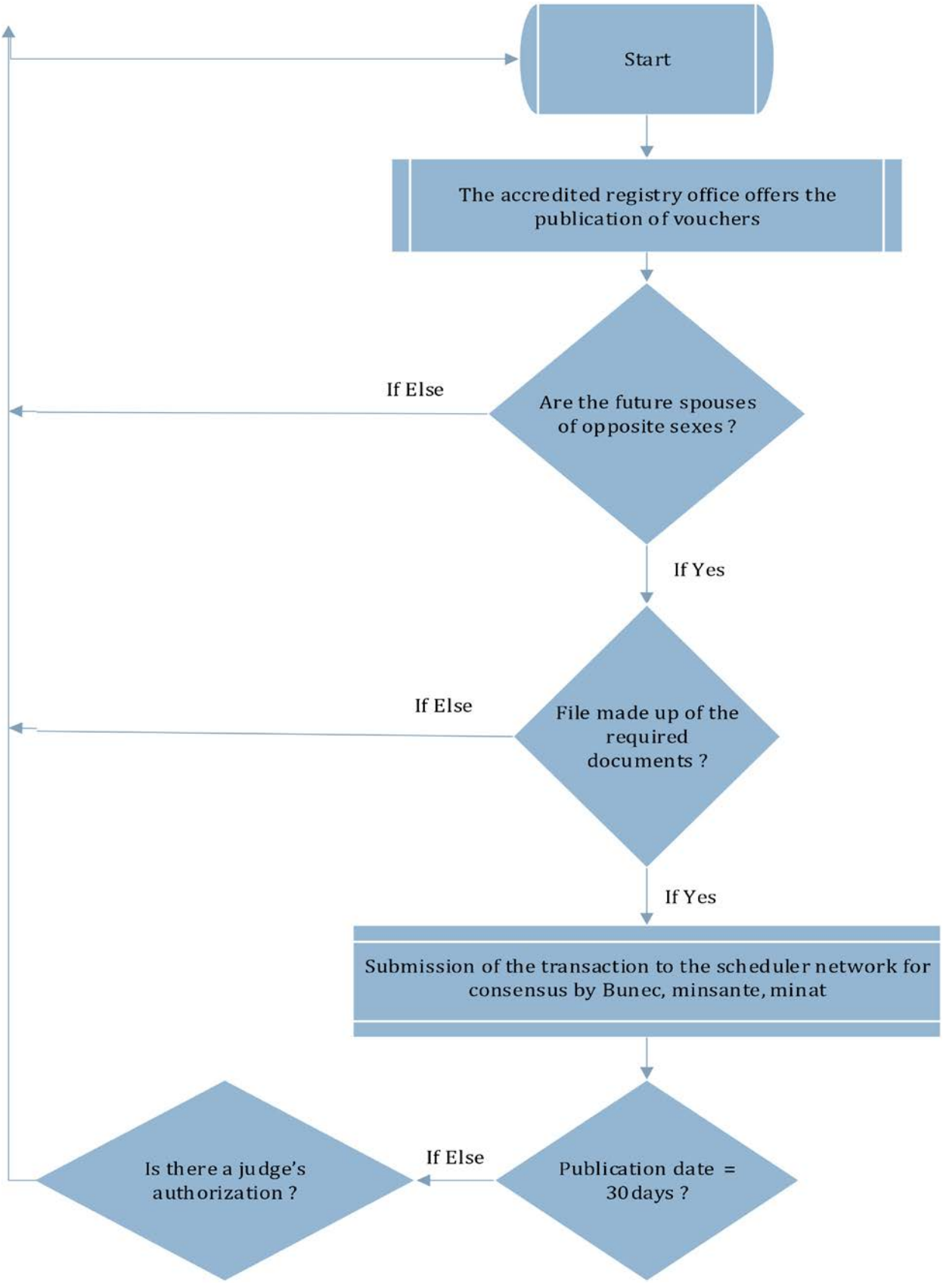

Figure 13. Specifications of the smartcontract for the wedding.

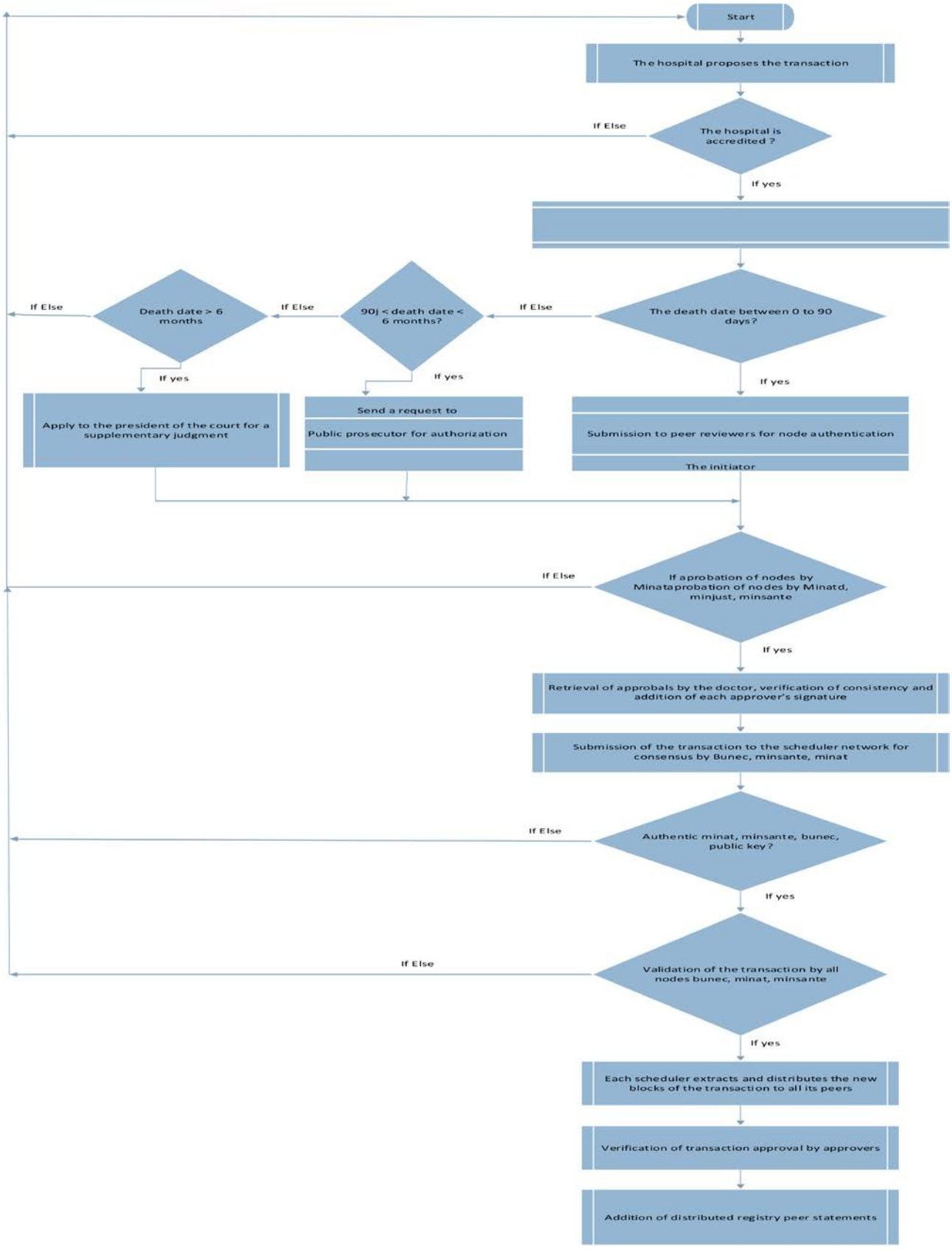

Figure 14. Specifications of the smartcontract for the death.

```
/etc/hyperledger/fabric/scripts#. /valider_chaincode.sh Validation of
the chaincode by biyemassi ...
2022-09-09 16 :56 :34.342 UTC 0001 INFO [chaincodecmd] clientwait
→txid[2730a58b5e565e5ec0620d3d17b468364f66d0078047470ff53e
0e961899fe75] committed with stat us (VALID) at peer0.Biye-
mAssi.com:7051
---------- Chaincode birth validated by BiyeMassi ----------
Validation of the chaincode by Awae ...
2022-09-09 16 :56 :39.471 UTC 0001 INFO [chaincodecmd] clientwait
→txid[02732243fe49dd2ce1e7d7b68edd23acad78ca3ef510b61e68efa
ccab07e0945] committed with stat us (VALID) at peer0.Awae.com:9051
---------- Chaincode birth validated by Awae ----------
Final agreement status of the organizations:
{
        'approvals ': {
              'AwaeMSP': true,
              'BiyemAssiMSP': true,
          }
}
```

Figure 15. Transaction identifier.

In the paragraph below is an example of a smartcontract script concerning marriage

```
/details of a marriage acttype Marriage struct {
   nom_pre string `json: "Names and surnames of the deceased"`
   date_dec string `json: "Date of death"`
   lieu_deces string `json: "Place of death"`
   date_naiss string `json: "Date of birth"`
   place_naiss string `json: "Place of birth"`
   age string `json: "Age of"`
   natio string `json: "Nationality"`
   pro string `json: "Profession"`
   situation string `json: "Marital status"`
   Father_name string `json: "Father's name"`
   Reside string `json: "Residence"`
   Mother_name string `json: "Mother's name"`
   Reside_mere string `json: "Reside"`
   decla string `json: "Declarant"`
   N_P_tem1 string `json: "Name and surname witness 1"`
   num_CNI_temoin1 string `json: "Numero CNI"`
   prof_tem1 string `json: "Nationality"`
   resi1 string `json: "Residence"`
   N_P_tem2 string `json: "Name and surname witness 2"`
   num_CNI_temoin2 string `json: "Numero CNI"`
   prof_tem2 string `json: "Nationality"`
   resi2 string `json: "Residence"`
```

Tables 6-8 present respectively the weaknesses that have been observed in the identity of civil status documents; this makes it possible to summarise the problems encountered and the solutions proposed by the blockchain as presented in

Table 9.

When a transaction is submitted to the network, it goes through an approval of all nodes. As Tables 1-4 show the types of consensus, we have proposed that for a better consensus and to solve the problem of Byzantine generals all nodes must approve the transactions to be valid. Using the private blockchain Hyperledger fabric in its version 2.0 as illustrated in Table 5. Figure 15 provides a better illustration of the identifier of a validated birth declaration transaction.

4. Evaluation des Performances du root_CA

The SCP protocol via SSH (Secure Copy Protocol) allowed us to develop a bash script that will run intermittently to ensure high availability of data in case of failure of the main root_CA of each organization). This SCP protocol allows the copying of information from a root_CA1 to a root_CA2 every 3 seconds (3s) through a bash script. This is done by authenticating with a password at the root_CA2 level. The time evaluated in this table is the authentication time at the second root_CA2 level.

This solution guarantees high availability at the level of the root certification authority. As illustrated in Figure 2 and Figure 3, a certification authority will authenticate the public keys of transaction authors. In Figure 16 below, a scrip batch is illustrated which allows the password to be copied from root certification authority 1 to root certification authority 2, thus ensuring the high availability of root certification authorities.

```
while :
do
 scp -r /home/jordan/BUNEC/ juns@192.168.5.139:"/home/juns/BUNEC/"
sleep 3
done
```

Figure 16. Bash script for copying passwords from root_ca1 to root_ca2.

Table 11. Performance evaluation of root_ca in cluster.

Time (second)	Observation
3600 s	The field for entering the root_ca2 password appears after 3600s
3 s	The password field of root_ca2 ap-pears after 3s
None	The field for entering the root_ca2 password appears 1/10 of a second

To guarantee permanent high availability, you would simply have to remove the sleep command.

5. Conclusion

The identity of documents is an issue of concern for both developed and developing countries. In this article, we have presented the problem of the falsification of documents in general and the case of civil status documents in particular.

The principle of the Byzantine generals has been studied. From this study, it appears that in a civil status transaction a false node can contribute to the validation of a transaction and distort the results of the transaction. To remedy this, we propose that all nodes (minat, minsanté, minjustice) validate the transaction to make it authentic. For this, a public key management infrastructure per organization with high availability of root_ca has been developed for integration into a private blockchain Hyperledger fabric as indicated in Table 5 regarding typology, the private blockchain Hyperledger fabric is used. In addition, a QR code is generated on the civil status forms to ensure the double authenticity of the documents handled. The said solution is all the more important in several areas to guarantee a reliable documentary identity, the authenticity of the acts, the non-repudiation of the actors. In the days to come, the implementation of the data from the civil registry will allow the General Delegation for National Security to use it for the establishment of national identity cards and the implementation of a man-machine interface in the prefectures, sub-prefectures and communes to attest the authenticity of the documents before any prior certification.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Anti-Fraude, C.E. (2022) CTMS Expert Anti-Fraude.

[2] Bounoung, Y. (2020) Fraude à l'état civil: La cote d'alerte. Cameroun Tribune.

[3] Shah, V., Padia, K. and Lobo, V.B. (2020) Application of Blockchain Technology in Civil Registration Systems. In: *IC-BCT* 2019, Springer, Berlin, 191-204. https://doi.org/10.1007/978-981-15-4542-9_16

[4] Chen, C.-L., Lin, C.-Y., Chiang, M.-L., *et al.* (2021) A Traceable Online Will System Based on Blockchain and Smart Contract Technology. *Symmetry*, **13**, 466. https://doi.org/10.3390/sym13030466

[5] Malik, G., Parasrampuria, K., Reddy, S.P. and Shah, S. (2019) Blockchain Based Identity Verification Model. 2019 *IEEE International Conference on Vision towards Emerging Trends in Communication and Networking* (*ViTECoN*), Vellore, 30-31 March 2019, 1-6. https://doi.org/10.1109/ViTECoN.2019.8899569

[6] Tran, H.C. (2020) Blockchain Application in Authenticating High-School Students' Transcript. *Journal of Science and Technology on Information and Communications*, **1**, 85-94.

[7] Motto, M.D. (2009) La fiscalité du commerce électronique.

[8] Swan, M. (2015) Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc., Sebastopol.

[9] Karamitsos, I., Papadaki, M., *et al.* (2018) Design of the Blockchain Smart Contract: A Use Case for Real Estate. *Journal of Information Security*, **9**, 177-190. https://doi.org/10.4236/jis.2018.93013

[10] Zyskind, G. and Nathan, O. (2015) Decentralizing Privacy: Using Blockchain to Protect Personal Data. 2015 *IEEE Security and Privacy Workshops*, San Jose, 21-22

May 2015, 180-184. https://doi.org/10.1109/SPW.2015.27

[11] Glaser, F. (2017) Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain Enabled System and Use Case Analysis. *Proceedings of the* 50*th Hawaii International Conference on System Sciences* (*HICSS*-50), Waikoloa Village, 4-7 January 2017, 1543-1552. https://doi.org/10.24251/HICSS.2017.186

[12] Alkhateeb, S., *et al.* (2021) Blockchain Implications in the Management of Patient Complaints in Healthcare. *Journal of Information Security*, **12**, 212-223. https://doi.org/10.4236/jis.2021.123011

[13] Du, M.X., *et al.* (2017) A Review on Consensus Algorithm of Blockchain. 2017 *IEEE International Conference on Systems*, *Man*, *and Cybernetics* (*SMC*), Banff, 5-8 October 2017, 2567-2572. https://doi.org/10.1109/SMC.2017.8123011

[14] Tern, S., *et al.* (2021) Survey of Smart Contract Technology and Application Based on Blockchain. *Open Journal of Applied Sciences*, **11**, 1135-1148. https://doi.org/10.4236/ojapps.2021.1110085

[15] Buffet, C., *et al.* (2016) Comprendre la Blockchain.