RESEARCH ARTICLE OPEN ACCESS

Towards Blockchain-Based Monitoring of Legal Inquiries

Tankou Tsomo Maurice Eddy [1], Bell Bitjoka Georges [2], Ngohe Ekam Paul Salomon [3]

[1]Electrical Engineering, Mechatronics and Signal Processing Laboratory
ENSPY1, University of Yaoundé - Cameroon
[2] Electrical Engineering, Mechatronics and Signal Processing Laboratory
ENSPY1, University of Yaoundé - Cameroon
[3] Electrical Engineering, Mechatronics and Signal Processing Laboratory
ENSPY1, University of Yaoundé - Cameroon

ABSTRACT

An investigation is the search for the truth through the hearing of witnesses and the accumulation of information. In the world in general, this research process is practiced by many state organizations, notably the national gendarmerie and the general delegation for national security. These are well hierarchical organizations whose missions are to centralize and coordinate criminal data at regional and national level. However, these organizations, in their regalian missions, are confronted with numerous problems, notably the lack of information concerning an investigation procedure opened in a gendarmerie or police station at a given time throughout the Cameroonian territory, the information of the investigator, the information on the complainant, the object of the investigation, to be taken out of the state of follow-up of the said investigation, in short, the lack of traceability. In the literature, several solutions exist, in particular, solutions based on the client-server architecture and solutions based on the distributed architecture. In this case, we chose a distributed architecture based on a private Hyperledger Fabric blockchain. This solution will make it possible, with its distributed nature, to guarantee the authenticity and traceability of transactions, the originality of the authors of the transactions and non-repudiation. This solution is all the more important for both developing and developed countries. Moreover, the 51% law of the Byzantine generals is challenged, and stipulates that the validation of an investigation transaction is subject to prior approval by eleven nodes representing the ten regions on the one hand and the regulator of the national gendarmerie represented by the Ministry of Defense as the eleventh node.

Keywords: - Blockchain, legal inquiries, police, Identity

I. INTRODUCTION

An enquiry is the search for the truth by hearing witnesses and gathering information. In most countries of the world, this search process is carried out by numerous state agencies, including the judicial police, the national gendarmerie, etc. These are well-organized agencies whose mission is to centralise and coordinate criminal data. These are well hierarchical bodies whose tasks are to centralise and coordinate criminal data.

These are well hierarchical organizations whose missions are to centralise and coordinate criminal data at regional, national and global levels. However, in carrying out their tasks, they are confronted on the one hand with numerous problems due to the limitations of the existing information management systems, and on the other hand with the actual follow-up of the investigation procedures triggered by a police station or gendarmerie post, the final investigation report, information related to the investigator, status of the investigation, etc. Cameroun tribune, in one of its publications, raises the issue of the lack of availability of information necessary for magistrates in the process of solving money laundering and terrorist financing cases [1]. In the same vein, the NGO Human Right Watch reports on the unreliability of investigation reports on anti-covid funds [2]. In this article, a smart contract is developed using a private blockchain hyperledger fabric. This solution will not only notify all ten nodes of the network represented by the 10 regions of a possible open investigation, but of its status together with information related to the investigator, the complainant and the accused. This process is even more important for developed countries than for developing countries.

II. LITERATURE REVIEW

A. History of blockchain

The financial crisis of 10 October 2008 caused a loss of confidence never before seen in the history of the banking sector. This crisis is the trigger for the Blockchain [1]. 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 to pay it back [2]. Money is based on the principle of trust, as in the case of fiat money (notes and coins currently in use) which uses banks as a trusted intermediary for transactions between its users. This is not the case with Bitcoin, which must operate independently of banks and in a distributed manner with regard to its use. Satoshi Nakamoto is therefore faced with the task of finding a trusted medium in a distributed environment to enable 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".

B. Characteristics

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

- **Disintermediation**

Blockchain technology allows for exchange 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 a given moment and that it has not been modified;

- **Security:**

Decentralized hosting also makes blockchain a secure technology: it makes it virtually 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 nodes in the network must agree on an identical version of the blockchain. In other words, consensus ensures the authenticity of each transaction based on the synchronization between all nodes in 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, agreement, validity and integrity.

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

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

Table 1. Prof of Work (POW) [7]

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

Types of consensus	Advantages	Disadvantages
To validate a block, nodes must prove their possession of a certain amount of cryptocurrency, and pledge it to the network	Less energy consuming; More environmentally friendly compared to proof of work; Strong resistance to 51% attacks	The problem of nothing at stake makes PoS algorithms more complex

Table 2.Prof of stake (PoS) [7]

Types of consensus	Advantages	Disadvantages
Token holders can elect delegates who will validate transactions on their behalf	Speed	Reduced number of transaction validators creating a huge queue; Delegate inefficiency leads to poor validation.

Table 3.Delegated Proof of Stake (DPoS) [7]

Table 4.Proof of Authority (PoA) [7]

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.

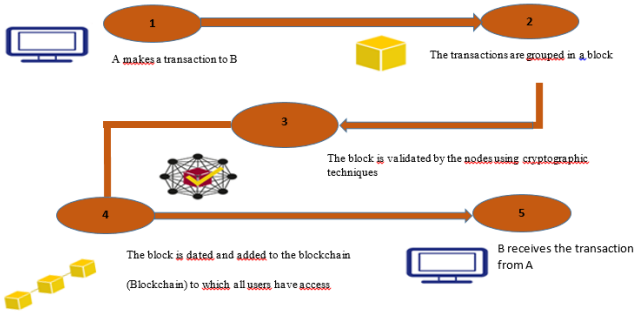

Fig. 1Transactional process in the blockchain [7]

C. Types of blockchains

In general, there are several types of blockchain, the different types are listed in the table below.

Table 5.Typology of blockchain [7]

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

D. Structure of a blockchain

Transactions are generally grouped in blocks. When they are validated, they are visible to all the holders of the register who will therefore add them to the blockchain. The structure of a blockchain is as follow.

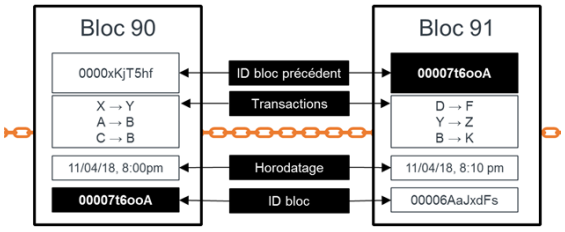

Fig. 2:Structure of a blockchain [1]

III. STATE OF THE ART ON JUDICIAL ENQUIRY

An enquiry is the research ordered by an administrative or judicial authority and intended to shed light on a fact [1]. It includes a set of activities that make it possible to determine the perpetrators of an offence, as well as the conditions in which the offence was committed. This action is generally carried out by the examining magistrate or investigator, who may in turn order all the acts he or she deems necessary in order to obtain the truth about the facts committed. It is the investigation that clearly determines whether or not the defendants are prosecuted. In order to best conduct an investigation procedure, the following steps must be observed:

a. Select the best sample(s) of individuals to be interviewed;
b. Define the type of questions that can be asked (usually open or closed questions);
c. Organize these questionnaires (form)
d. Determine the location of the survey.

E. Types of surveys

In the literature, there are several types of investigation, including:

- Flagrante delicto investigation;
- Preliminary investigation [1].

A. Flagrante delicto investigation

A flagrant offence is a crime or misdemeanor that has just occurred. On the other hand, we can consider as a flagrant offence when, in a time relatively close to the action, the alleged offender is pursued by public clamor or is found in possession of an object, or presents traces or indicators that make it possible to ascertain that the individual has participated in a criminal act or offence [1].

B. Preliminary investigation

It is a police-type investigation provided for in Article 75 and following of the Code of Criminal Procedure. The opening of a preliminary investigation can be done by:

- The judicial police officer is territorially competent;
- The public prosecutor in exceptional cases.

This type of investigation concerns offences punishable by a fine, a contravention on the one hand and on the other hand a non-flagrant offence punishable by imprisonment.

C. Current description of the follow-up to the judicial enquiry

In this section, the stage of organizing questionnaires that are recorded in a form is questioned; the form itself is a simple pre-designed word document. During an investigation, the judicial police officer conducts a progressive interrogation, the content of which is contained in a workstation. At the end of the hearing of the complainant and the accused, a report of the hearing is printed for verification by the actors and then their signatures. This approach has several limitations in terms of security, which are set out in the table below.

On the other hand, Cameroon's column in one of these editions raises the issue of judicial slowness, which is caused for the most part by a complex, tedious, traditional judicial system, etc[2].

Table 6. Weaknesses of the report form

Nature of the document	Activities	Weaknesses
Hearing form Or minutes of the hearing	Filling in the minutes during the hearing	Possibility of falsification of the said document as it is a preconceived word document, possibility of corruption of the officer (investigator), lack of traceability in the procedure, slowness

D. Literature review

In most countries around the world, the problem of the identity of judicial procedures has been the subject of several works, notably Cameroon in one of these editions, poses the problem of the lack of availability of information necessary for the magistrates in the process of solving cases of money laundering and terrorist financing[3]. In the same vein, the NGO Human Right Watch reports on the unreliability of investigation reports on anti-covid funds19[4]. The work of Md. Majharul Haque, Abu Sadat Mohammad Yasin et all follow in the same vein, this time the authors address the issue of document forgery and propose an approach to ensure authenticity, integrity, non-repudiation and availability[5]. Dodo Khan, Low Tang Jung, Manzoor Ahmed Hashmani are interested in the consensus protocols, for that it poses the problem related to the limits of consensus protocols in particular the weak flow and a strong latency, for that it proposes a consensus protocol named prof of review based on the confidence of the nodes in an organization[6]. In the same vein, the investigation into the Éseka disaster several years ago was finally curtailed. Before the verdict was given, it was difficult to have a real traceability on the status of the ongoing investigation[7].

In this article, blockchain technology is used to monitor judicial investigation procedures, thus guaranteeing the transparency and traceability of transactions, of the authors initiating investigations and of the alleged perpetrators involved; moreover, the distributed nature of the technology allows the various regions represented by nodes to be informed at a given moment of an open investigation and possibly of its progress.

III. METHODOLOGY AND RESULTS

A. Methodology

The methodology employed is multi-scale. First, we use the uml approach for modelling interactions between entities (Argo UML), to verify the authenticity of the authors of a transaction, we use a public key management infrastructure with high availability of root certification authorities; this is integrated in a private blockchain development platform (Hyperledger fabric) to verify the distributed nature of transactions. An Ubuntu 20.0.4 distribution is used for the solution deployments.

As for the public key management infrastructure, it is essentially based on asymmetric encryption and digital signature. As for encryption, it is the transformation of a clear message M with a key to obtain an output ciphertext. The diagram below illustrates the concept better.

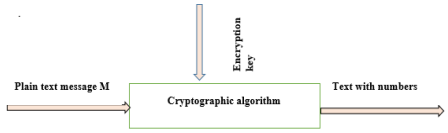

Fig. 3 Principle of encryption

There are several types of encryptions namely symmetric encryption in which the encryption key Ke is identical 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 RSA systems, an individual X wishes to send a message to an individual Y. To do this, individual X sends a communication request to his interlocutor Y. Individual Y sends his public key to X who in turn uses it to encrypt his message, once the encrypted message reaches individual Y, he uses his secret key to decrypt the contents of the message. In this type of system, individuals X and Y each have a key pair, one public and one private.

The principle of the RSA system is based on several steps, namely:

Step 1: Key generation [8]

1. Choose two distinctly large prime numbers p and q;
2. Calculate their product n=pxq called the cipher module;
3. Calculate φ(n)=(p-1) (q-1) which is the Euler indicator value;
4. Choose an encryption exponent e such that the gcd of (e, φ(n)) =1, i.e., prime between them;
5. Compute the inverse d of e modulo φ(n) by the extended Euclid algorithm $dxe \equiv 1 modulo\ \varphi(n)$
6. The public key is formed by the pair (n, e) and the private key is d kept confidential [9].

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 event series input message using the fast exponentiation algorithm $X \equiv m^e\,(mod n)$ and then transmits this message to the recipient.

Step 3 : Decryption[10]

The recipient in turn receives the message X encrypted by the sender and decrypts it using his private key d. $m \equiv X^d\,(mod n)$.

This decryption principle is essentially based on Ferma's little theorem which states that: let d be the inverse of e modulo φ(n), with n=pxq (p≠q)

If $X \equiv m^e\,(mod n)$ then $m \equiv X^d\,(mod n)$.

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

The signature verifies that the message comes from the holder of the private key, thus guaranteeing the authenticity of the sender and confidentiality.

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

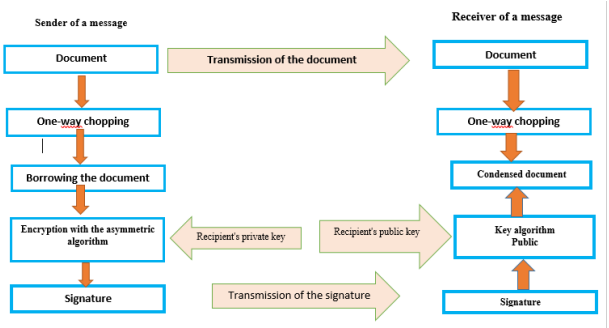

Fig. 4 Schematic diagram of the signature

B. Diagram representation

1. System use case diagram

Speaking of actors, we have mainly the interviewer, the secretary and the administrator of the platform.

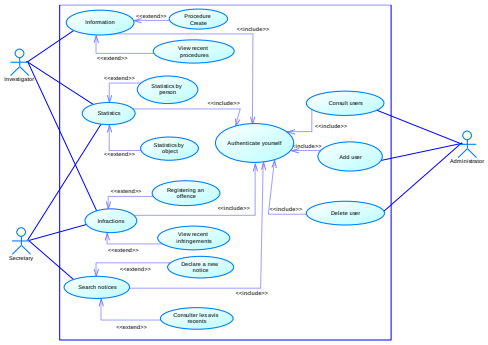

Fig. 5 System use case diagram

2. Activity diagram

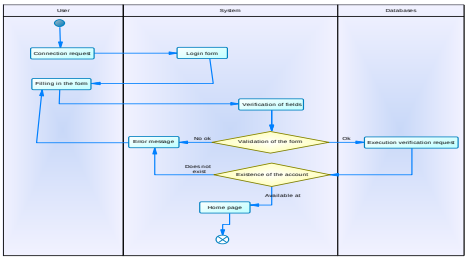

Fig. 6 Activity diagram

3. Component diagram

The figure below shows the component diagram of our system

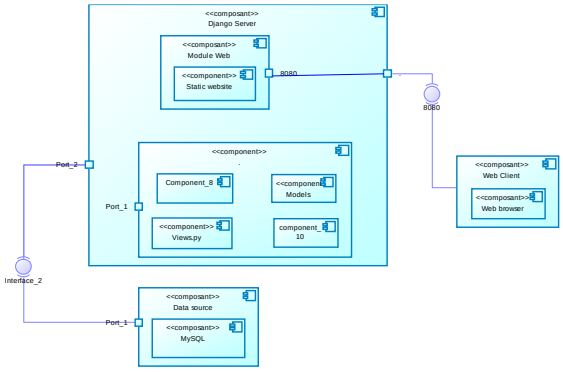

Fig. 7 Component diagram

The next step after modelling is the generation of certificates for authentication of the nodes by the transaction authors.

C. Generation of the certificate

– Step 1: Generation of certificates

After the modelling, the next step is the generation of certificates for the authentication of keys in the blockchain. For this purpose, a script has been developed for the automatic generation of certificates.

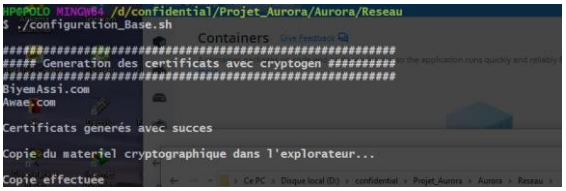

Fig. 8 Automatic generation of certificates

– Step 2: Generate the network components

Network components such as organizations, channels and the genesis block, which is the basic block of the registry, must be created for further work.

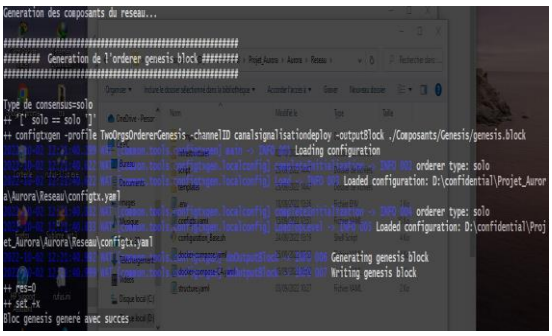

Fig. 9 Generation of network components

Fig. 10 Generation of the signaling channel transaction

Step 3: Updating the Anchor Peers

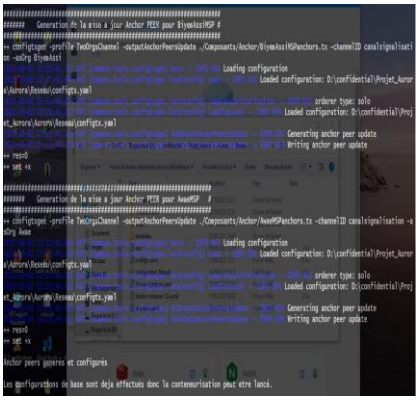

Fig. 11 Updating the Anchor Peers

Step 4: Containerization

Step 5: Creation of the channel named signaling channel

The process of creating the channel is as follows:

A node belonging to an organization or a CLI (command line interface) sends a channel creation request to the scheduler with the configuration transaction created earlier in the <<Components>>.The Scheduler will check if the initiator of the request is indeed an administrator of a channel will generate a file with the extension. Block extension. This file represents the channel creation transaction block.
The last step concerns the writing of the chaincode or smart contract named infraction and with for source code the file ContratInfraction.js

B. RESULTS

In this section, we present the home interface of our platform containing the functionalities of registration of offences, information on an individual, the wanted notice on an individual and finally statistics on current investigations.

The figure below illustrates the home interface of our investigation platform.

Fig. 12 interface of our investigation platform

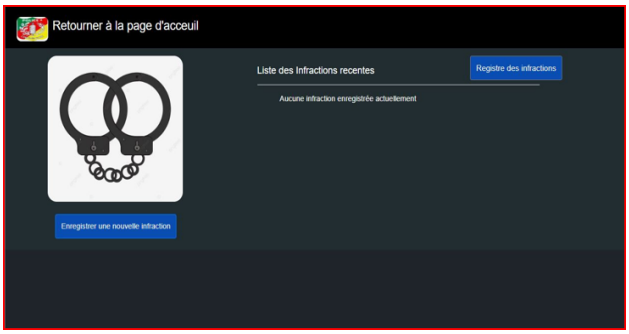

Fig. 13 register a violation

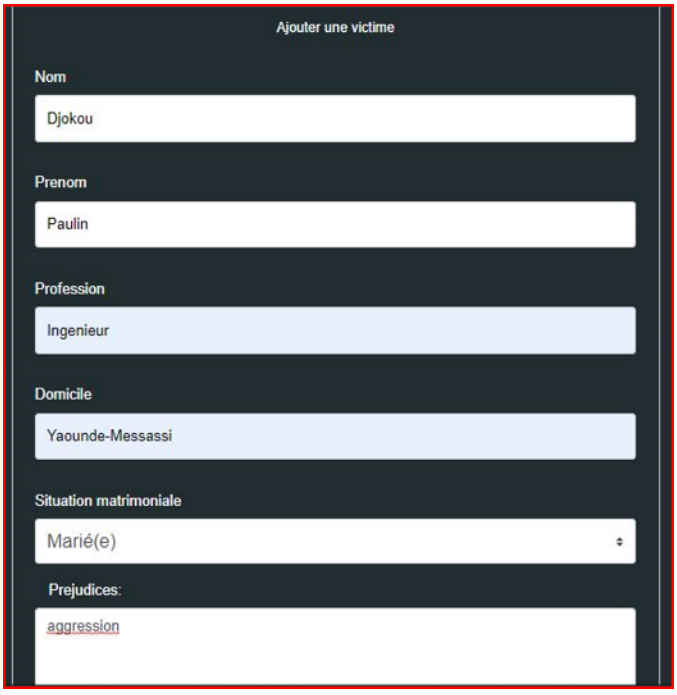

Fig. 14 Infringement form

Once the form is filled in and submitted, we can see the transaction identification in the blockchain network as shown in the figure below.

Fig. 15 transaction identification in the blockchain

Fig. 16 Statistics on search notices

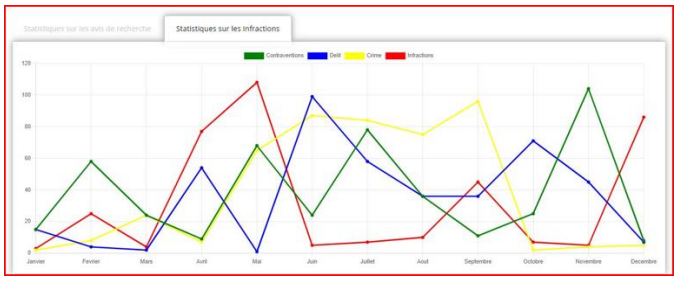

Fig. 17 Annual statistics on infringement rates

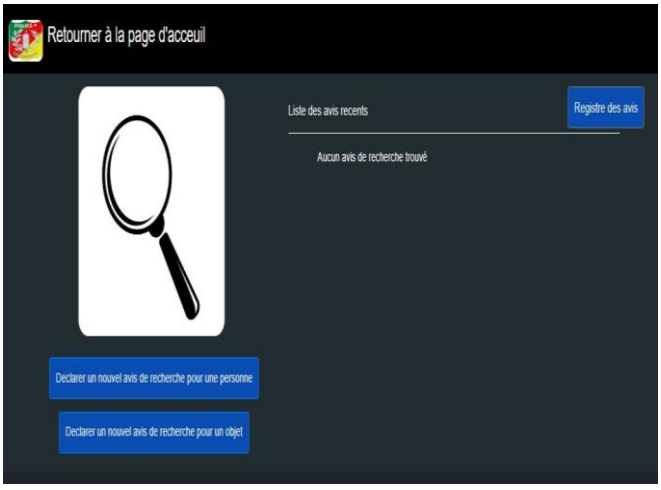

Fig. 18 Declaration of a wanted notice on an individual or an asset

Fig. 19 Form for a search notice for an object

IV. CONCLUSION

At the end of this work, the objective of which was to make a scientific contribution to the problem of monitoring judicial investigations in state structures, we first showed the approach of generating certificates for the authentication of keys by the authors of the transactions, accompanied by an uml model for the interaction between the actors of the system and finally the drafting of the smartcontract which enabled us to obtain a form for the establishment of an infraction. Moreover, it is possible from this platform to launch a search notice on an object or an individual and to have statistics on the search notices launched. This solution is all the more important for developing countries than developed countries because it ensures traceability. In the near future, we will incorporate a policy of evaluating the performance of investigators to further improve the time taken to process offences. In the near future, we will incorporate a policy of evaluating the performance of investigators in order to further improve the turnaround time of offences.

REFERENCES

[1] Ooreka, "Différents types d'enquête," 2022.
[2] E. M. SHAKUR, "Lenteur judiciaire:une croisade lancée dans les tribunaux," 2021.
[3] J. MATOCK, "Blanchiment d'argent et financement du terorisme:les poursuites judiciaire en appoint," Cameroun tribune, 2022.
[4] H. R. WATCH, "Cameroun : Assurer une enquête crédible sur la gestion des fonds de lutte contre le Covid-19," 23/04/2021.
[5] M. M. Haque et al., "An Innovative Approach of Verification Mechanism for both Electronic and Printed Documents," vol. 11, no. 8, 2020.

[6] D. Khan, L. T. Jung, M. A. J. I. J. o. A. C. S. Hashmani, and Applications, "Proof-of-Review: A Review based Consensus Protocol for Blockchain Application," vol. 12, no. 3, 2021.

[7] E. MACRON, "L'esprit d'Eséka," 02/01/2023 26 Mai 2017.

[8] B. J. C. Schneier, "A self-study course in block-cipher cryptanalysis," vol. 24, no. 1, pp. 18-33, 2000.

[9] R. L. Rivest, A. Shamir, and L. J. C. o. t. A. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," vol. 21, no. 2, pp. 120-126, 1978.

[10] M. M. Ebenezer, P. Félix, M. Yannick, S. N. P. Junior, N. N. J. I. J. o. A. C. S. Léandre, and Applications, "Contribution to the improvement of cryptographic protection methods for medical images in DICOM format through a combination of encryption method," vol. 12, no. 4, 2021.