Indonesian Journal of Electrical Engineering and Computer Science
Vol. 37, No. 1, January 2025, pp. 365~379
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v37.i1.pp365-379

Blockchain and smart contracts based system for criminal record management

Manal Jlil, Kaoutar Jouti, Chakir Loqman
Laboratory of LISAC, Department of Computer Sciences, Faculty of Sciences Dhar El Mehraz (FSDM),
University of Sidi Mohamed Ben Abdellah, Fez, Morocco

Article Info

Article history:

Received May 3, 2024
Revised Sep 7, 2024
Accepted Sep 29, 2024

Keywords:

Blockchain technology
Criminal record
Data security
E-governance
Record-keeping
Smart contract

ABSTRACT

Reducing crime rate in a country is the most important concern of developing robust systems to automate the criminal record-obtaining process. Generally, the criminal record is managed manually, which makes the information collection from other criminal records very difficult. Therefore, investigations that could be carried out using criminal records to understand the purpose of crime and countering it are outdated. However, the integrity, security, and traceability of data exchange, especially for the judicial sector are the most frequent issues faced by information systems of public organizations. In this paper, we present a study of using blockchain technology and smart contracts to design a new architecture for a decentralized system to manage criminal record storage. This proposed architecture automates the process of getting a criminal record by moving past the techniques employed in developing traditional systems of data management such as centralized systems. In this study, blockchain technology is used to ensure data security, integrity, and traceability as well as ensure timely access to criminal records, and smart contracts are used to allow traceability and authenticity. This architecture will significantly reduce the impact of corruption in law enforcement by eliminating fraud cases, which will revolutionize E-governance in the Moroccan country.

Corresponding Author:

Manal Jlil
Laboratory of LISAC, Department of Computer Sciences, Faculty of Sciences
Sidi Mohamed Ben Abdellah University
30003, Fez, Morocco
Email: manal.jlil@usmba.ac.ma

1. INTRODUCTION

Governments around the world are recognizing the value of e-governance. This approach offers considerable benefits, including improved quality and availability of public services, as well as increased citizen involvement in the democratic process. Furthermore, it significantly reduces costs, increases institutional transparency, and streamlines execution time [1]. The judicial sector represents a crucial department for government organizations globally. This frequently visited department encompasses a majority of tasks related to national security.

As we work to modernize administration, our focus also includes incorporating new technologies to improve citizen's access to vital services and reduce administrative expenses. The introduction of e-government services, designed to streamline and digitize information management, is projected to signifcantly improve efficiency in this area. The information management can be defined as the process that ensures data collection, storage, and distribution within an organization, in a way to supports decision-making and business processes.

Records management and document management constitute the most important subsets in information management. Records relate to managing a company's essential information from creation through disposal. In the judicial sector, records play a crucial role in administering justice, since they support legal rights and obligations, as well as providing evidence, and contributing to accountability [2]. Notably, within legal records, court records stand out as a significant category [3]. One type of record produced by courts is the criminal record. A criminal record is a crucial legal document containing an individual's criminal history, aiding law enforcement, courts, and employers in making informed decisions [4], [5]. This judicial document has an essential impact during legal proceedings, especially during sentencing, parole, or probation hearings. So it can be considered during the judicial decision-making. To put it differently, criminal records are used to assess an individual's past interactions with criminal justice and can influence decisions related to employment, crime prediction, recidivism detection, and other aspects of life where one's background is considered. Therefore, implementing an information system to manage and store this critical document represents a challenge for the legal authorities given the sensitivity and confdentiality of information contained in a criminal record.

According to the Ministry of Justice in Morocco, over than 16,000 legal proceedings are initiated annually, for crimes committed, the majority of which include crimes carried out under the threat of using bladed weapons. This alarming figure underscores the severity of the issue, and it is imperative that concerted efforts are made to eradicate this scourge. The High Commission for Planning in Morocco released a study on crime and security in 2021, and the report includes critical information related to crime in the nation. For instance, by 2020, there will be 395,724 offenses reported to the courts, and the crime rate will be 1,086 offenses for every 100,000 citizens. In 2022, the number of reported sexual assaults exceeded 2,182 cases, indicating a 2.3 % rise over 2021 [6]. By the same year (2021), more than 1.4 million individuals were brought before various public prosecutor's offices, marking an increase of approximately 43% in the number of people brought before justice and 36% of the number of people sought and arrested, in comparison with the previous year, according to the national security services. These key figures highlight the significant impact of crime on Moroccan society, which affects the public order, quality of life, and economic development and creates fear and insecurity. In that case, it is crucial to implement preventive measures and reduce crime to maintain public order. To achieve this, Ministries of Justice or law enforcement agencies must have a good system to manage criminal records. Generally, manual methods are employed for maintaining criminal records, especially in underdeveloped countries [7], so collecting information from distinct criminal records is extremely challenging. The Moroccan Ministry of Justice also relies on traditional methods to handle the process of obtaining a criminal record, which begins with collecting data from different Moroccan courts, each maintaining a paper version of each citizen's criminal record. This dysfunctional management of electronic records leads to poor service delivery in the judiciary for citizens and organizations [8].

To fix all these issues mentioned above, the Ministry of Justice has to develop a potential information system for better criminal record management. The predominant method for implementing document management systems is the use of centralized systems that depend on centralized databases. These databases serve as the core foundation for all system operations and can be efficiently updated and utilized to support all system processes. They store all necessary information in a single central location, making it easily accessible. Additionally, the accuracy of the centralized database enables tasks like generating crime reports and conducting statistical analysis of crime data [9]. Despite advancements in centralized database systems, issues like data inconsistencies, ineffcient storage space, and insuffcient control over data management [10], [11] persist. Furthermore, centralized systems are more vulnerable to electronic attacks. Data is not stored in a highly secure environment, as well as centralized systems are always managed by humans, raising the question: can we guarantee absolute trust in a human being to monitor a system that contains critical data, such as the individual's past interactions with the criminal justice system?

The goal of this paper is to propose a new approach for a blockchain and smart contracts-based system to automate the process of criminal record acquisition. The main objective of the proposed solution is to exceed the centralized systems issues by:

i) Offering a new solution for better criminal record management by enhancing: decentralization, data security, transparency, data integrity, and trust (benefits of blockchain technology).
ii) Designing a new platform including various entities and assigning respective roles using smart contracts, to avoid unauthorized access to the system.
iii) Handling the issues of transparency and authenticity for citizens and stakeholders.
iv) Using smart contracts for managing transactions.
v) Enhancing traceability and reducing the risk of fraud.

The paper is organized as follows, section 2, provides an overview of the existing literature. Section 3 presents a detailed description of the methods to design the proposed solution. Section 4 is dedicated to the results and discussion. In this section, a detailed explanation of the tools used and the implementation of the system is presented, followed by a discussion. Then we provide a conclusion with suggestions for future works.

2. RELATED WORKS

A significant amount of research about systems for sharing data using blockchain technology has been created, some of them are mentioned in this section as well as our problem statement. Protecting personal data is the chief role of the government. This responsibility extends to local, regional, and national agencies tasked with maintaining records covering various aspects such as birth and death dates, marital status, property transfers, and criminal activity [12]. Effectively managing and using this data can be a complex task, even for well-established and advanced governmental bodies. Distinct law enforcement agencies within the government maintain individual databases, causing an impediment to the seamless flow of data between them [13]. Given the expanding volume of court's records, an effective system for record keeping and information sharing is essential in the contemporary global landscape. To uphold national security, communication among law enforcement agencies is crucial, extending across borders. The presence of accurate, time-stamped records simplifies the fulfillment of their mission [14]. Suseno *et al.* [15] affirmed that the use of computers to record and process data is considered insecure due to the vulnerability of digitally stored data manipulation and hacker attacks.

For this reason, the use of blockchain technology, smart contracts, and InterPlanetary file system (IPFS) protocol becomes evident. Blockchain technology functions as a decentralized database containing records or a public ledger that captures all transactions or digital events executed and shared among participants. Each transaction within this public ledger undergoes verification through the consensus of a majority of the system's participants [16]. Accordingly, in the study presented in [17], confirmed that blockchain technology would lead to innovation and transformation of governmental processes and the use of the blockchain technology in information sharing is more efficient. Storing information on the transactions in different nodes called a distributed ledger, reduces the dependency on a central actor and the risk of manipulation or system failure. Alghazwi *et al.* [18] proposed a blockchain technology-based infrastructure to handle genomic data. Due to its nature, genomic data poses unique challenges related to security, privacy, and responsible sharing. The emergence of blockchain infrastructure provides potential solutions to these challenges by offering secure and accountable data ownership and control. Tyagi *et al.* [19] highlighted the benefits of blockchain technology in providing transparency, immutability, and distributed storage for prisoner records. The suggested solution is built on the Hyperledger framework, and the testing results show that it is advantageous to both current and future research departments. Ahmed *et al.* [20], describes a system that uses Hyperledger blockchain and IPFS to implement a secure criminal record digitalization system. In this system, transactions are immutable and cannot be accessible to everyone, an administrator controls the system, and can generate criminal records and fugitive criminal assets, which can be updated if there are any mistakes or inaccuracies in the needed data. Makwana and Sharma [21] affirmed that the use of blockchain technology in criminal record management not only facilitates easy access to data, but also contributes to a reduction in time, cost, corruption, and paperwork. Chawhan *et al.* [22] presented a secure P2P file storage network using a distributed, decentralized blockchain for storing evidence IPFS. The system is based on Hyperledger blockchain and provides limited access to authorized staff, which ensures a record of each transaction from the moment the documentation is acquired. Fathiyana *et al.* [23] presented a blockchain-based solution to integrate a national identity system to address concerns related to data abuse and reliance on a centralized database managed by a single entity. This system enhances the use of Indonesian citizens' data by ensuring security and integrity and improving information management openness. Mullegowda *et al.* [24] confirmed that using blockchain technology and smart contracts to implement access control policies ensures that only authorized users can access the e-voting system for counting, which simplifies the authorization paradigm and enhances transparency. It is clear that the use of blockchain technology and smart contracts to develop secure platforms is the ideal solution in order to automate procedures and processes to increase the efficiency and effectiveness of public administrations.

The goal of our research is to propose a new solution for a criminal record management system that will benefit the Moroccan Ministry of Justice; this system will automate the process of storing and managing the criminal data of prisoners. The proposed system is based on Blockchain technology and smart contracts to fix all the issues mentioned above, such as centralized systems limitations, lack of data security, data integrity, and traceability without the need for a trusted third party, or a system administrator.

3. METHOD

This section provides a detailed explanation of the current system issues as well as the methods used to resolve the problem.

3.1. Problem statement

With the increasing demand for criminal records in different aspects, and in response to the efforts undertaken by the Ministry of Justice to improve the quality of services provided by this governmental organization, especially for criminal record management. The ministry has to develop a new solution for the criminal record acquisition process and provide it remotely for the benefit of citizens, whether inside or outside the country. To do so, firstly the Ministry has to automate the system of criminal record storage and update its management, to regulate aspects related to recidivism and extract analytic data. The current system is a traditional system where this critical document is managed manually, and the process is relying on "papers" exchange. An illustration of the current process management is presented in Figure 1.

As shown in Figure 1, the present system is built upon information gathered from a variety of sources, particularly the courts in the applicant's city of birth. The difficulty comes from the fact that it happens frequently for birthplaces to be different from the towns where crimes or wrongdoings have been committed, consequently, the criminal data is saved on paper cards in each court. Furthermore, public administrations and the Ministry of the Interior play a crucial role in the process. Whenever a decision with implications for an individual's liberty is made, it is imperative to communicate this decision to the Ministry of Justice for inclusion in the individual's criminal record. This requirement holds true for expulsion decisions concerning foreigners residing in the country as well.

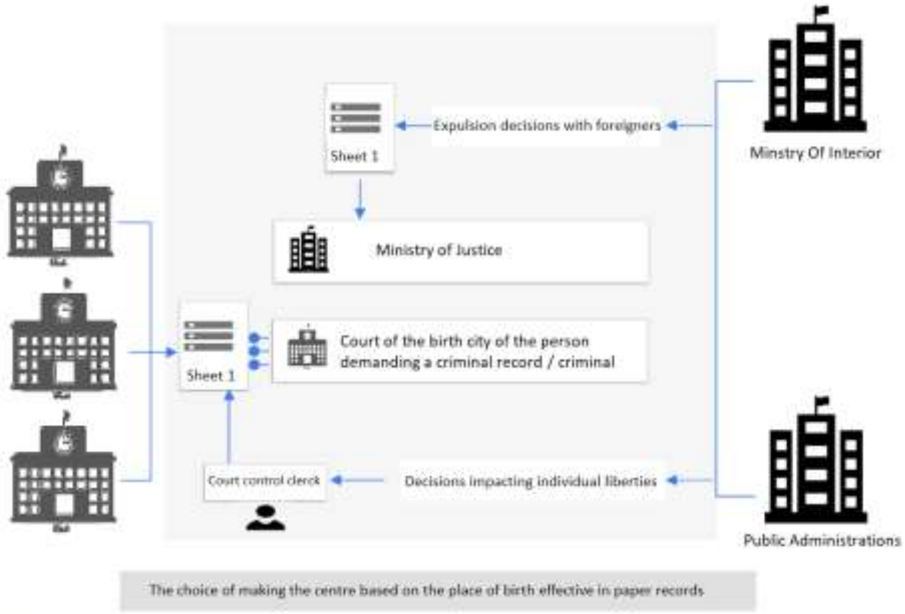

Sheet 1
Expulsion decisions with foreigners
Minstry Of Interior
Ministry of Justice
Sheet 1
Court of the birth city of the person demanding a criminal record / criminal
Court control clerck
Decisions impacting individual liberties
Public Administrations
The choice of making the centre based on the place of birth effective in paper records

Figure 1. The current process to get a criminal record

Using the current system, to get a criminal record the process is as follows: the citizen must travel to his city of birth to submit the request at the local court. Subsequently, the public prosecution, as the legal entity responsible for the criminal record system, appoints the relevant public prosecutor. The appointed prosecutor, in turn, designates the clerk responsible for gathering information about the applicant and the clerk responsible for document preparation. Once these steps are completed, the document is ready for delivery to the citizen.

To streamline the procedure, the Ministry of Justice has introduced a public platform for obtaining criminal records. This online portal eliminates the need for users to, physically, travel to their city of birth. Instead, the electronic request is submitted to the court, and the preparation process remains unchanged. Once the document is ready for delivery, it is sent to the court chosen by the applicant during the criminal record request, as well as being forwarded via email. However, this solution does not address the issue of document preparation. On the contrary, it introduces a new concern related to the security and authenticity of the document transmitted via email.

Figure 2 describes the process of getting a criminal record using the public platform developed by the Ministry. The procedure starts with the applicant submitting a request via the platform, which is then transmitted to the Ministry of Justice's server. From there, the request is forwarded to the court in the applicant's city of birth. Court clerks retrieve relevant data from various paper records and compile it into a standardized criminal record format. Once the document is prepared, the applicant receives a notification detailing the retrieval process. The applicant can then select a court for document delivery. Before the criminal record is dispatched, the prosecutor in the retrieval court signs it, to ensure its authenticity.

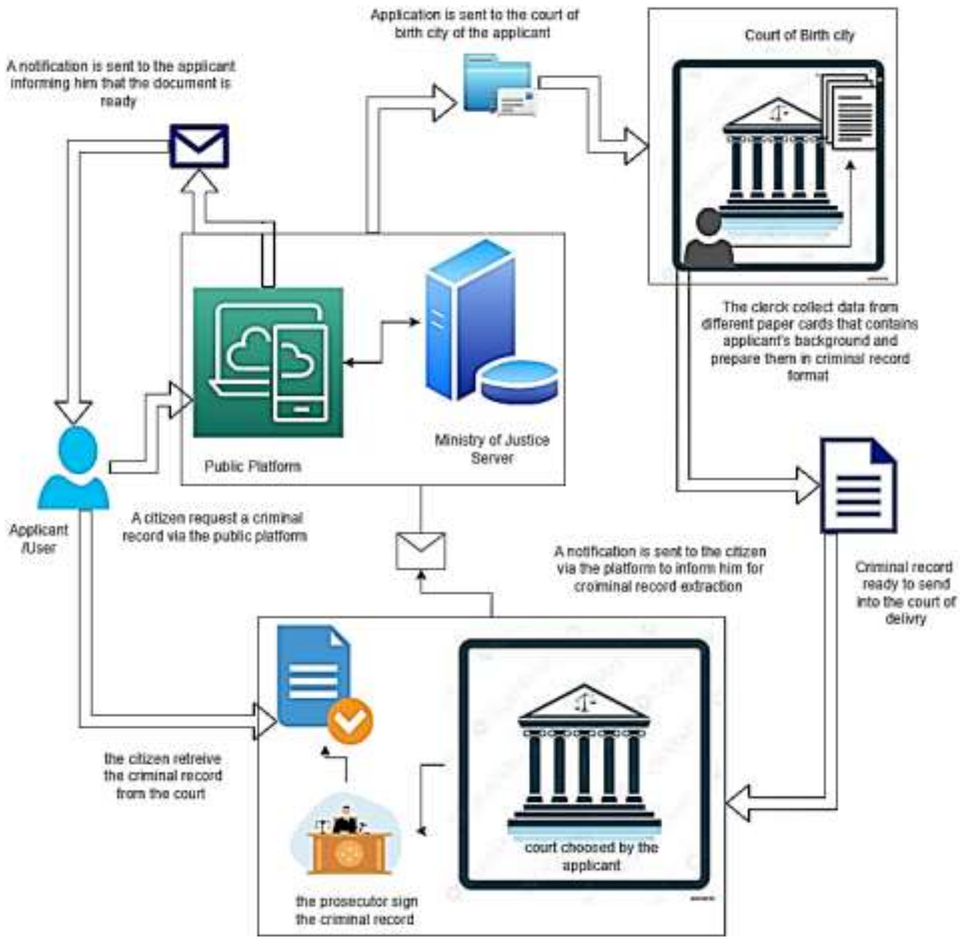

Application is sent to the court of birth city of the applicant
A notification is sent to the applicant informing him that the document is ready
Court of Birth city
The clerck collect data from different paper cards that contains applicant's background and prepare them in criminal record format
Ministry of Justice Server
Public Platform
Applicant /User
A citizen request a criminal record via the public platform
A notification is sent to the citizen via the platform to inform him for croiminal record extraction
Criminal record ready to send into the court of delivry
the citizen retreive the criminal record from the court
court choosed by the applicant
the prosecutor sign the criminal record

Figure 2. The architecture of the public platform for criminal record application developed by the Ministry of Justice in Morocco

As seen in Figure 3, the proposed approach is adopted by the ministry, to develop a centralized system for criminal record storage management, and then, to streamline the process of getting a criminal record. However, in such cases, centralized systems limitations must be considered when managing documents, especially criminal records, in fact, they contain an individual's background, which means critical data has to be secured and shared with trusted users. Another essential point to be considered is that users and entities within centralized systems depend on the central authority. Decisions made by this authority can significantly affect the entire system, potentially leading to issues of trust and control.

To summarize, the current system faces several issues, such as:

- Transferring data on paper supports from the court in which the basic rulings and decisions were issued to the birthplace court slows down the data collection process;
- This inefficiency arises due to the duplication of tasks in two different courts, leading to a lack of optimization in human resources;
- The dispersion of data across multiple courts prevents its effective use from being exploited and invested in studying the crime development and recidivism cases;
- The distance between the place of request, and the place where the criminal record data is stored slows down the process of obtaining the criminal record;
- Despite the Ministry's adoption of an electronic application to facilitate the criminal record delivery to the applicant, challenges persist in the adopted centralized solution.

In below, other aspects of centralized systems limitations are:

- Reduced resilience: centralized systems are less resilient in the face of disruptions, such as network outages or cyber-attacks. A single attack or failure can have widespread consequences.
- Security concerns: security is a significant concern in centralized systems. If the central server is breached, all data and transactions are at risk. This is particularly critical for sensitive information.
- Limited privacy: centralized systems often require users to trust a central authority with their data. This lack of privacy can be a drawback, especially in contexts where data protection is crucial.
- Higher operating costs: maintenance and operation costs for centralized systems can be higher. The need for a robust central infrastructure and continuous monitoring can result in increased expenses.

As a result, getting a criminal record is a more difficult, pricey, and lengthy process. Additionally, manual data management in a centralized location is more challenging in a world where modernizing public administrations and digitalization are required.

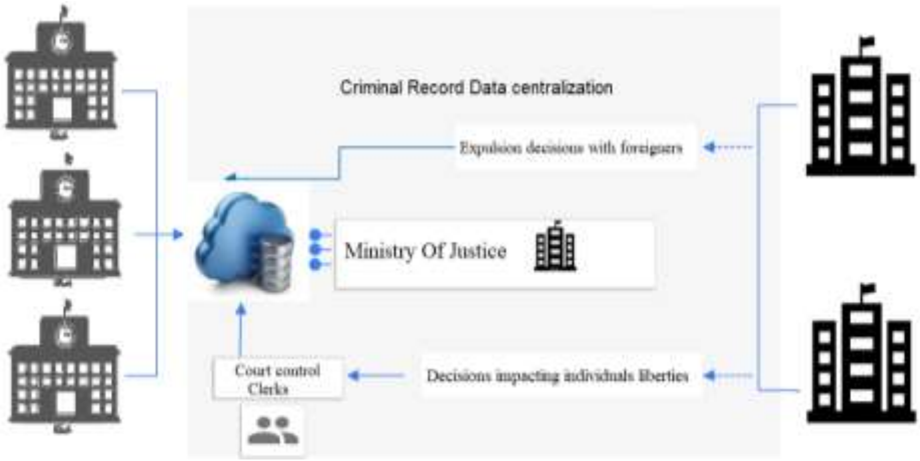

Criminal Record Data centralization
Expulsion decisions with foreigners
Ministry Of Justice
Court control Clerks
Decisions impacting individuals liberties

Figure 3. Criminal record data centralization

3.2. Proposed system

In this subsection, we present a new solution proposed for the Ministry of Justice and different entities involved in the criminal record acquisition process. The goal is to improve the criminal record management system by introducing a new architecture for criminal record storage system based on blockchain technology and smart contracts. Figure 4 illustrates the newly proposed solution for the process of a criminal record management system, starting with storage. A decentralized infrastructure to automate the process of storing a criminal record by mentioning the different parties that contribute to the inclusion of information in this critical document. The talking infrastructure is based on Ethereum blockchain and smart contracts to ensure a secured network for document exchange between the entities involved in the process, as well as traceability and authenticity of the data in criminal records.

Given the interconnection between several entities that do not belong to the same organization on one hand, and the confidentiality of the data contained on a criminal record on the other hand, our proposal involves implementing smart contracts to manage the network access control. This approach offers the advantage of regulating network access exclusively for authorized staff, and subsequently ensuring the security and confidentiality of document exchanges while maintaining traceability. Furthermore, it eliminates the need for third parties and introduces the option of appointing a network administrator (as proposed in solutions relying on Hyperledger blockchain, known for its private blockchain architecture), who may not necessarily be a trusted source. Another notable consideration when employing a blockchain-based infrastructure is the elimination of electronic signatures, as it is explicitly ensured through the use of blockchain technology, to ensure the document's confidentiality and prevent any unauthorized changes or modifications during the exchange process, the historical transactions log provides a record of all operations executed throughout the process.

Figure 5 illustrates the process of obtaining a criminal record, detailing the steps involved for both citizens and public administrations. As shown in this figure, with reference to the applicant's category, it is imperative for them to create an account within the system to initiate the document request. Based on the applicant's type (citizen or public administration); the system assigns a specific role, either "read" or "read and write”. To put it differently, when the applicant is a citizen, the system designates a “read” role, allowing them to extract data solely for the purpose of obtaining a criminal record. This restricts the citizen’s capabilities to extract information from the system without the ability to modify or add data.

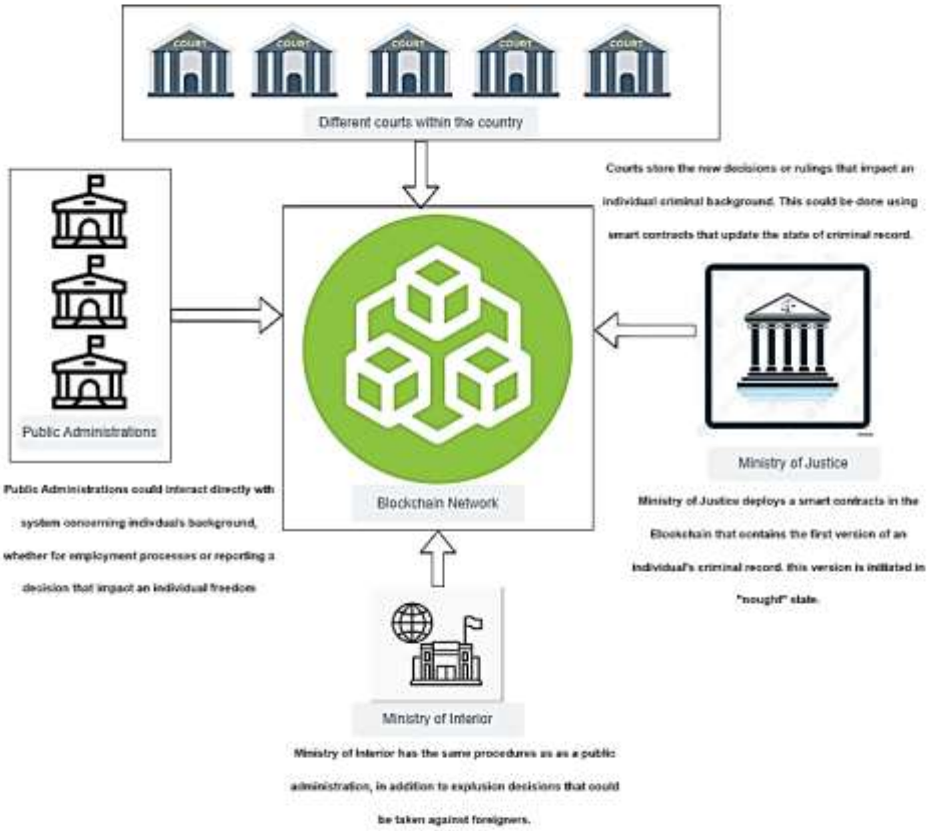

COURT
COURT
COURT
COURT
COURT
Different courts within the country
Courts store the new decisions or rulings that impact an individual criminal background. This could be done using smart contracts that update the state of criminal record.
Public Administrations
Blockchain Network
Ministry of Justice
Public Administrations could interact directly with system concerning individuals background, whether for employment processes or reporting a decision that impact an individual freedom
Ministry of Justice deploys a smart contracts in the Blockchain that contains the first version of an individual's criminal record. this version is initiated in "nought" state.
Ministry of Interior
Ministry of Interior has the same procedures as as a public administration, in addition to explusion decisions that could be taken against foreigners.

Figure 4. Blockchain-based system for criminal record management

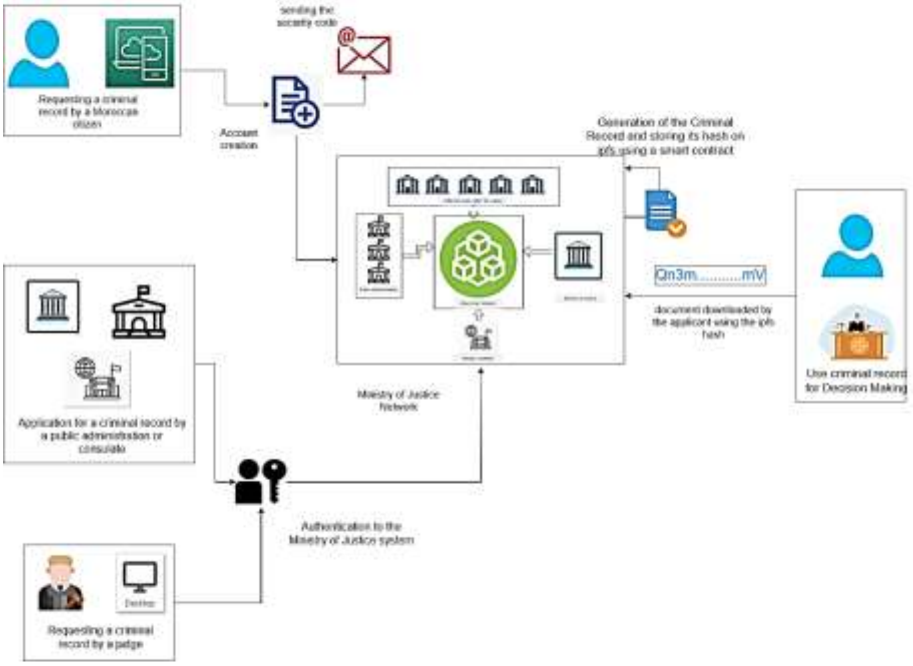

sending the security code
Requesting a criminal record by a Moroccan citizen
Account creation
Generation of the Criminal Record and storing its hash on ipfs using a smart contract
Qn3m..........mV
document downloaded by the applicant using the ipfs hash
Use criminal record for Decision Making
Ministry of Justice Network
Application for a criminal record by a public administration or consulate
Authentication to the Ministry of Justice system
Desktop
Requesting a criminal record by a judge

Figure 5. The new process of getting a criminal record

On the other hand, when the applicant is a representative of a public administration, a more extensive “read/write” role is assigned. This enables the administration user to not only retrieve necessary data for recruitment processes but also to contribute new decisions that should be taken into account for an individual’ criminal record. This functionality is especially crucial when making decisions concerning employees or foreigners, as it allows the administration user to actively engage with and update the system as needed.

3.3. System design

The following is a description of various scenarios, using sequence diagrams to detail steps for designing the new proposed system. Figure 6, presents the sequence diagram for the account creation process. As seen in the diagram the user creates an account in the blockchain network, this operation requires email verification. After the email verification, the account is created and the corresponding ID is sent to the user.

Figure 7 describes the process of applying for a criminal record. When an applicant logs into the network, the document application process is initiated. The applicant’s information is extracted from the system server, and then the document is created. Subsequently, the document is stored on the IPFS node and a hash is generated. Using the smart contract the hash of the criminal record is stored in the blockchain network and forwarded to the applicant. Through this hash, the applicant can conveniently upload the document easily from IPFS.

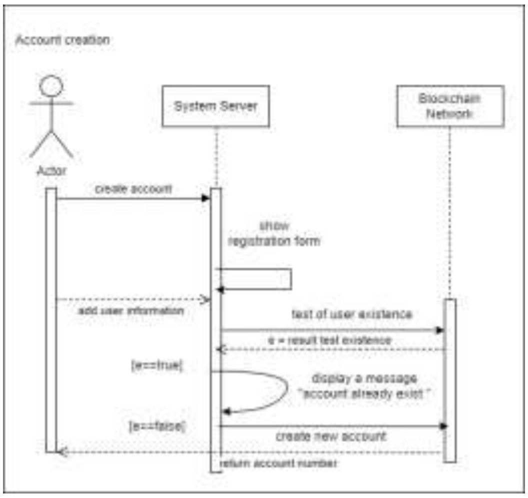


Figure 6. Diagram of sequence for the account creation process

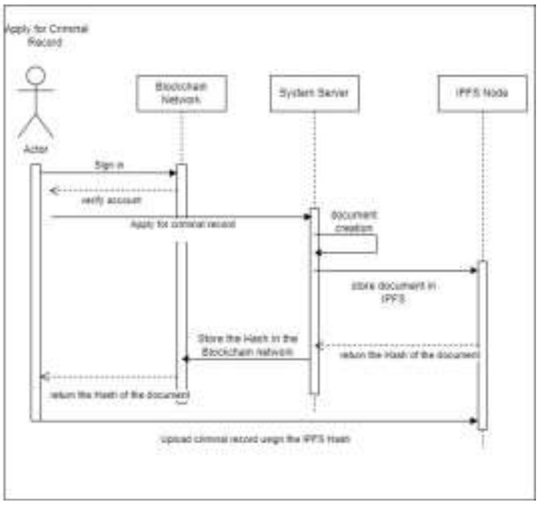

Apply for Criminal Record
Actor
Blockchain Network
System Server
IPFS Node
Sign in
verify account
Apply for criminal record
document creation
store document in IPFS
return the Hash of the document
Store the Hash in the Blockchain network
return the Hash of the document
Upload criminal record usign the IPFS Hash

Figure 7. Diagram of sequence for applying for a criminal record

The diagram in Figure 8, describes the process of adding for a criminal record. Once the user has been authenticated, they request a criminal record. At this point, a transaction is initiated, and a smart contract extracts the applicant's information from the system. When the document is ready, it is stored on IPFS. Subsequently, the Hash of the document is generated and stored on the blockchain network. The transaction ID and the hash of the document are sent to the applicant for criminal record retrieval.

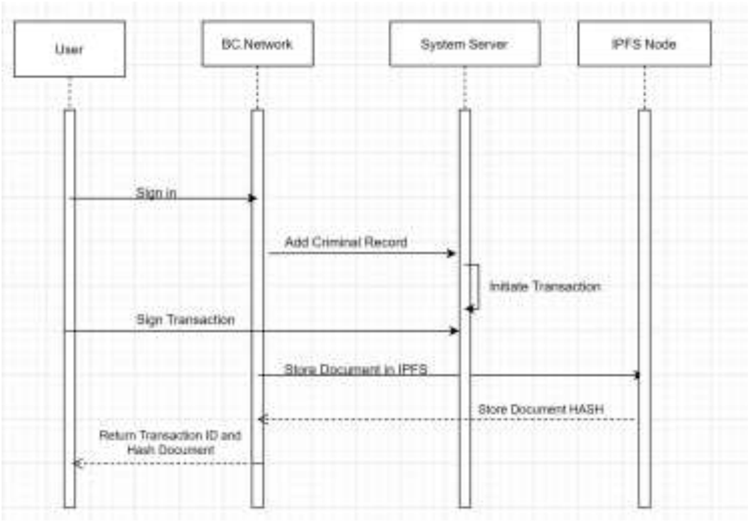


Figure 8. Diagram of sequence for adding a criminal record

4. RESULTS AND DISCUSSION

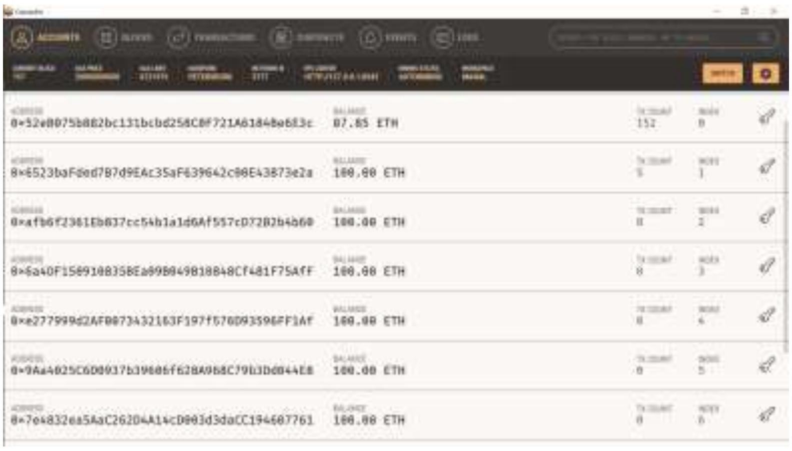
In this section, we describe the system scenarios as well as the used technologies to implement the proposed solution. Furthermore, a summary of the major findings and discussion of its performance.

4.1. Results

4.1.1. Implementation

To implement the architecture proposed, different tools have been used to design the new system. Below is a detailed description of the used tools.

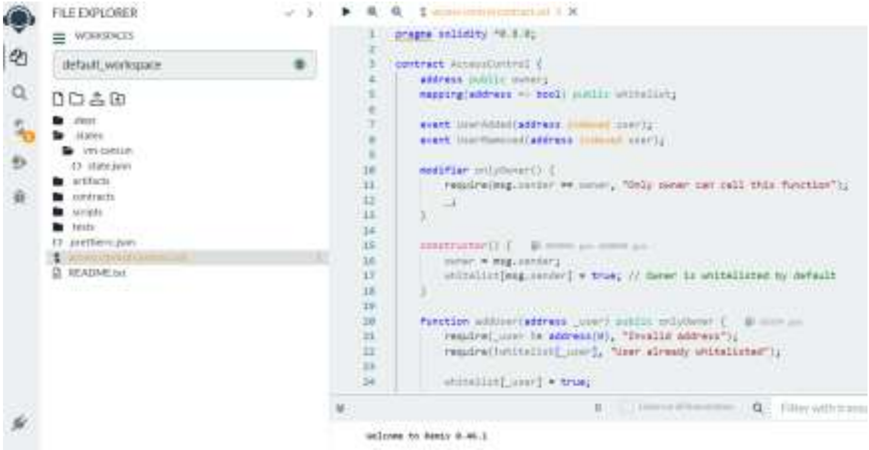
- Ganache-cli: initially, we set up ganache-cli, which serves as a Blockchain client for connecting to the network [25]. It contains a log of transactions and provides a console for inspecting and retrieving data associated with transactions, including transaction hash, timestamp, location, input data, and smart contracts. Figure 9 illustrates the interface of ganache-cli with the account addresses list provided automatically when creating a new workspace. The home interface of ganache-cli is presented in Figure 9.



ADDRESS	BALANCE	TX COUNT	INDEX
0x52e8075b882bc131bcbd258C8F721A61848e683c	87.85 ETH	152	0
0x6523baFded7B7d9EAc35aF639642c08E43873e2a	100.00 ETH	5	1
0xafb6f2361Eb837cc54b1a1d6Af557cD72B2b4b60	100.00 ETH	0	2
0x6a40F1589108358Ea09B049B18848Cf481F75AfF	100.00 ETH	0	3
0xe277999d2AF0073432163F197f576D93596FF1Af	100.00 ETH	0	4
0x9Aa4025C6D0937b39606f628A968C79b3Dd044E8	100.00 ETH	0	5
0x7e4832ea5AaC262D4A14cD003d3daCC194607761	100.00 ETH	0	6

Figure 9. Ganach-cli home interface

- Remix-IDE: in order to develop and oversee the lifecycle of smart contracts, including tasks such as compilation, testing, deployment, and updates, an integrated development environment is required. In our case study, we used Remix IDE, a web-based platform that eliminates the need for software installation. It encompasses a comprehensive set of development and deployment tools, providing an all-in-one solution for the creation and management of smart contracts [26]. Figure 10 represents the interface of smart contract coding using Remix IDE.

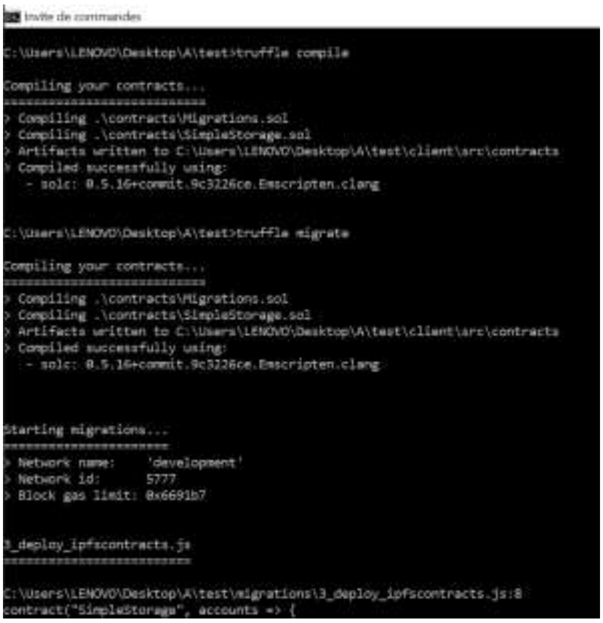


```
pragma solidity ^0.8.0;

contract AccessControl {
    address public owner;
    mapping(address => bool) public whitelist;

    event UserAdded(address indexed user);
    event UserRemoved(address indexed user);

    modifier onlyOwner() {
        require(msg.sender == owner, "Only owner can call this function");
        _;
    }

    constructor() {
        owner = msg.sender;
        whitelist[msg.sender] = true; // Owner is whitelisted by default
    }

    function addUser(address _user) public onlyOwner {
        require(_user != address(0), "Invalid address");
        require(!whitelist[_user], "User already whitelisted");

        whitelist[_user] = true;
```

```
Welcome to Remix 0.46.1
```

Figure 10. The Remix IDE platform for coding and deploying a smart contract

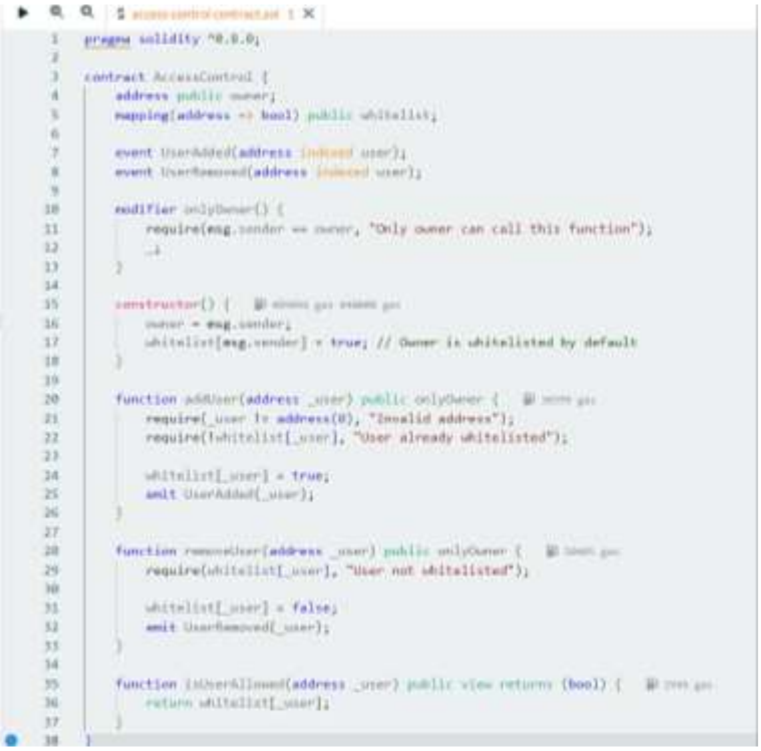
- Web3: or decentralized web, refers to a vision of the internet where data, content, and applications are decentralized and controlled by users rather than centralized authorities. It promotes P2P networks, blockchain technology, data ownership, and privacy. Interoperability and smart contracts play vital roles, aiming to create a more democratic, inclusive, and resilient internet architecture [27].
- Truffle: Truffle serves as a development environment, testing framework, and asset pipeline designed specifically for Ethereum [28]. It is a front-end tool, used to deploy and compile smart contracts and insert them into the web application. Figure 11 describes the process of deployment and migration of the smart contracts via a command prompt (CMD) line command.



```
C:\Users\LENOVO\Desktop\A\test>truffle compile

Compiling your contracts...
===========================
> Compiling .\contracts\Migrations.sol
> Compiling .\contracts\SimpleStorage.sol
> Artifacts written to C:\Users\LENOVO\Desktop\A\test\client\src\contracts
> Compiled successfully using:
   - solc: 0.5.16+commit.9c3226ce.Emscripten.clang


C:\Users\LENOVO\Desktop\A\test>truffle migrate

Compiling your contracts...
===========================
> Compiling .\contracts\Migrations.sol
> Compiling .\contracts\SimpleStorage.sol
> Artifacts written to C:\Users\LENOVO\Desktop\A\test\client\src\contracts
> Compiled successfully using:
   - solc: 0.5.16+commit.9c3226ce.Emscripten.clang



Starting migrations...
======================
> Network name:    'development'
> Network id:      5777
> Block gas limit: 0x6691b7


3_deploy_ipfscontracts.js
=========================

C:\Users\LENOVO\Desktop\A\test\migrations\3_deploy_ipfscontracts.js:8
contract("SimpleStorage", accounts => {
```

Figure 11. Example of smart contract compilation and migration using truffle

- Node JS: represents a JavaScript runtime driven by asynchronous event handling. The node is designed to create scalable network applications, especially for information systems with memberships [29].
- Smart contracts: concerning user access control, we developed a smart contract specifcally to handle this task. The code for this contract is presented in Figure 12.



```
pragma solidity ^0.8.0;

contract AccessControl {
    address public owner;
    mapping(address => bool) public whitelist;

    event UserAdded(address indexed user);
    event UserRemoved(address indexed user);

    modifier onlyOwner() {
        require(msg.sender == owner, "Only owner can call this function");
        _;
    }

    constructor() {
        owner = msg.sender;
        whitelist[msg.sender] = true; // Owner is whitelisted by default
    }

    function addUser(address _user) public onlyOwner {
        require(_user != address(0), "Invalid address");
        require(!whitelist[_user], "User already whitelisted");

        whitelist[_user] = true;
        emit UserAdded(_user);
    }

    function removeUser(address _user) public onlyOwner {
        require(whitelist[_user], "User not whitelisted");

        whitelist[_user] = false;
        emit UserRemoved(_user);
    }

    function isUserAllowed(address _user) public view returns (bool) {
        return whitelist[_user];
    }
}
```

Figure 12. The smart contract code for control the user access

4.1.2. Scenario of designed solution

The first step of the process is to log into the network as shown in Figure 13. If the user is a new applicant, an account creation is required. Consequently, the applicant needs to select his “user type” as shown in Figure 14.

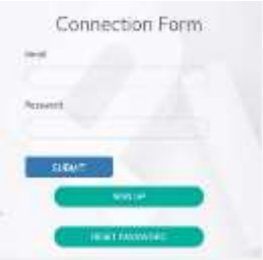


Figure 13. Connection form

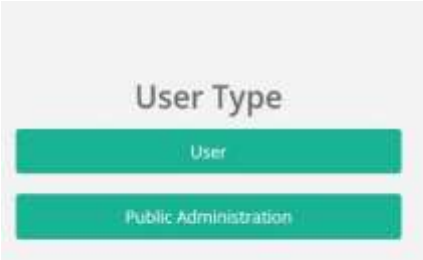


Figure 14. Selecting the user type

The next step is to fill out the forms for the account creation. When the user is a “citizen”, a card identity number or a passport ID is requested as shown in Figure 15. When the applicant is a “public administration”, an ID of the organization is requested as shown in Figure 16.

After the account is created, the user has the right to log into the network. As presented in Figures 17 and 18, and depending on the user’s role, there are two options available: for citizens, the ability to apply for a criminal record; and for public administration, the ability to apply for a criminal record and add a criminal record.

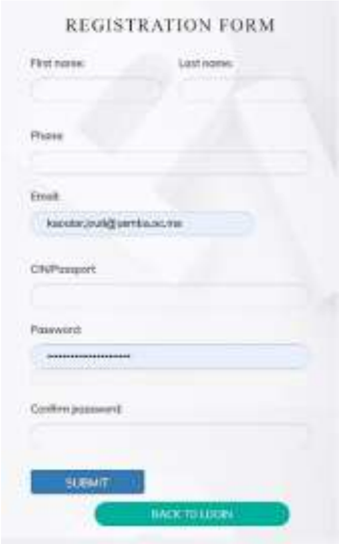


Figure 15. Registration from for the user type "citizen"

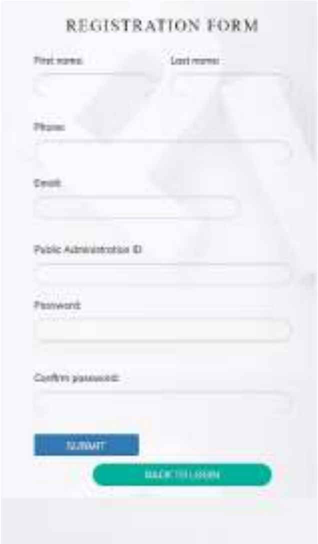


Figure 16. Registration from for the user type "public administration"

Figure 17. The options for user type "citizen"

Figure 18. options for user types "public administration"

When the user chooses to apply for a criminal record, they are automatically redirected to the existing platform. When the user chooses to add a criminal record (in the case of public administration), the interface that allows this feature is shown in Figure 19. In this step, the user is required to fll out the "contract address" of the smart contract used to store the document on the blockchain network, along with the user's private key of his blockchain account. Upon submission, the fle is uploaded to the system server, stored in IPFS, and then assigned an IPFS hash. This hash is sent to the applicant via an email, and stored in the blockchain network at the same time.

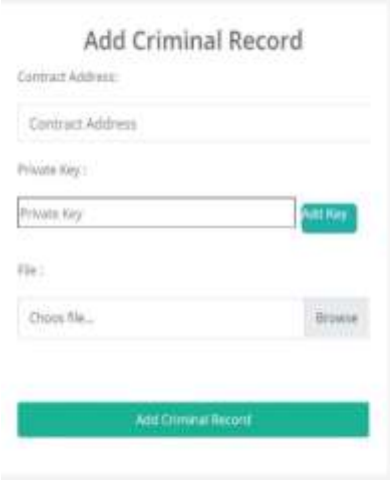


Figure 19. Interface of adding a criminal record by "public administration"

The solution proposed, focuses on the secure exchange of data between judicial authorities and stakeholders, ensuring the security and the integrity of data against any piracy or falsifcation, using smart contracts. For that reason, it is imperative to ensure that the implementation of these smart contracts is free from bugs, and vulnerabilities and fortifed against potential attacks. Additionally, preserving both: code and the information on the network is imperative, as they could be susceptible to various forms of attacks [30].

The security analysis process was performed using a tool named "SolidityScan". It's a cloud-based smart contract vulnerability scanner built to discover vulnerabilities and help publish audit reports after vulnerability mitigations. Table 1 provides an overview of the security analysis of the smart contracts "access control", which will be used to manage the users of the systems automatically. The table presents key metrics from the smart contract performance report, highlighting the overall security score, scan duration, lines of code, and issues count. The security score, rated at 73.68 out of 100, indicates an average level of security for the smart contract, suggesting that while there are some concerns, it is not critically flawed. The scan duration of 0 seconds implies that the analysis was instantaneous, likely due to the simplicity of the contract. With only 38 lines of code, the contract is relatively concise, but it contains 8 identified issues, which may require attention to enhance its security and functionality.

Table 2 provides, as well, the results for the smart contract "simple storage" which will be used to store the criminal record in the system. The security scan results indicate a high security score of 79.65 out of 100. It highlights 13 identified issues. Additionally, the scan was completed in a fraction of 0.1 seconds and analyzed 54 lines of code. Overall, these metrics provide a snapshot of the contracts's performance and areas for improvement.

Table 1. The security performance of "access control" smart contract

Metric	Value
Security score	73.68/100
Scan duration	0 s
Lines of code	38
Issue count	8

Table 2. The security performance of "simple storage" smart contract

Metric	Value
Security score	79.65/100
Scan duration	0.1 s
Lines of code	54
Issue count	13

4.2. Discussion

This study highlights the significant challenges faced by the government sector when using centralized systems, particularly concerning trust, transparency, security, and data confidentiality. Centralized systems, often governed by a single entity, can result in diminished transparency and potential power abuses. In contrast, the integration of Blockchain technology, IPFS, and smart contracts in decentralized systems presents promising solutions to these issues.

Building on previous studies, our findings indicate that adopting this architecture within the Ministry's system could profoundly transform the legal industry. Key benefits identified include enhanced transparency, improved data integrity, fortified data security, the elimination of the need for trusted third parties, and the introduction of user access control features. Looking ahead, future research could explore the scalability of these technologies in other governmental sectors and their impact on public trust. Ultimately, this study underscores the potential of decentralized systems to revolutionize legal processes, offering a more transparent and secure framework for managing criminal records.

5. CONCLUSION

In conclusion, the transition towards digital platforms offers numerous advantages, including improved efficiency, accessibility, and accuracy, especially in record retrieval. Moreover, it has the potential to streamline traditional procedures, and reduce processing time, thus enhancing public service delivery and contributing to the process of e-governance. In this paper, a blockchain and smart contract-based solution was explored, to digitize the process of obtaining a criminal record for the benefit of the Ministry of Justice in Morocco. Blockchain technology is used to ensure integrity and transparency as well as secure exchange between different independent parties, IPFS is used to ensure data security and overcome boundaries of Blockchain data storage terms and smart contracts to interact between the user interfaces and the blockchain network. The proposed solution will contribute to the development of the process of getting a criminal record in a secured platform. All users access this platform at once, each one has his own role and the document can be retrieved using its hash generated by the IPFS and stored in the Blockchain using the smart contract.

Finally, the digitization of criminal record processes holds promise for modernizing law enforcement practices and facilitating more efficient justice administration in the digital age. The perspective provides an opportunity to explore potential enhancements. The primary focus that will shape our future research direction is the use of the criminal record in predicting crime, using machine learning and deep learning techniques. The study will provide access to the proposed solution for the extraction and use of criminal records in crime prediction relying on new methodologies and analytical techniques, to address the fundamental challenges of criminal data, and to leverage big data to facilitate criminal investigations and recidivism case detection.

REFERENCES

[1] G. Ntulo and J. Otike, "E-government: its role, importance and challenges," *School of Information Sciences, Moi University*, pp. 121–154, 2018.

[2] S. Idhiarhi, "Improving record management and security of exhibits: the role of judicial administrators," 2016.

[3] A. Abioye, "Court records management and efficient administration of justice in Nigeria," *African Journal of Library Archives and Information Science*, vol. 24, no. 1, pp. 27–39, 2014.

[4] M. Denver, J. T. Pickett, and S. D. Bushway, "Criminal records and employment: a survey of experiences and attitudes in the United States," *Justice Quarterly*, vol. 35, no. 4, pp. 584–613, 2018, doi: 10.1080/07418825.2017.1340502.

[5] D. N. Lee, "The digital scarlet letter: the effect of online criminal records on crime," *SSRN Electronic Journal*, 2012, doi: 10.2139/ssrn.1939589.

[6] High Commission for Planning of Morocco, "The high commission for planing report." Morocco, 2021.

[7] S. Ali, S. A. Alvi, and A. U. Rehman, "The usual suspects: machine learning based predictive policing for criminal identification," in *2019 13th International Conference on Open Source Systems and Technologies, ICOSST 2019 - Proceedings*, 2019, pp. 54–59, doi: 10.1109/ICOSST48232.2019.9043925.

[8] D. Teffo and K. G. Chuma, "Management of electronic records to support judicial systems at Temba Magistrates' Court in the North West Province of South Africa," *Journal of the South African Society of Archivists*, vol. 56, pp. 35–54, 2023, doi: 10.4314/jsasa.v56i.3.

[9] T. Mannan, "Upgradation and maintenance of crime data management system (CDMS) and personnel information management system (PIMS)," 2020.

[10] A. Sharma and M. Shahnawaz, "Crime records management system," in *3rd International Conference on System Modeling & Advancement in Research Trends (SMART) College of Computing Sciences and Information Technology (CCSIT)*, 2014, p. 9.

[11] F. J. M. Barrow, M. J. Alam, and M. N. Mustafa, "Unique model of criminal record management system in the perspective of Somalia," *International Journal on Informatics Visualization*, vol. 3, no. 4, pp. 332–336, 2019, doi: 10.30630/joiv.3.4.255.

[12] S. Cheng *et al.*, "Using blockchain to improve data management in the public sector," *Digital McKinsey*, no. February 2017, pp. 1–10, 2017, [Online]. Available: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector%0Ahttps://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-blockchain-to-improve-data-manageme.

[13] M. A. Tasnim, A. Al Omar, M. S. Rahman, and M. Z. A. Bhuiyan, "CRAB: blockchain based criminal record management system," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11342 LNCS, pp. 294–303, 2018, doi: 10.1007/978-3-030-05345-1_25.

[14] Magar Shivani, Magar Harshad R., ambe Dipali A., Sonawane Arya S., Prof. A. B. Anap, and Mr. R. S. Kakade, "Crime Record Management System," *International Journal of Advanced Research in Science, Communication and Technology*, vol. 4, no. 1, Apr. 2024, doi: 10.48175/568.

[15] T. R. D. Suseno, I. Afrianto, and S. Atin, "Strengthening data integrity in academic document recording with blockchain and InterPlanetary file system," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 14, no. 2, pp. 1759–1769, 2024, doi: 10.11591/ijece.v14i2.pp1759-1769.

[16] M. Crosby, Nachiappan, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology - beyond bitcoin," *Berkley Engineering*, p. 35, 2016.

[17] S. Ølnes, J. Ubacht, and M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing," *Government Information Quarterly*, vol. 34, no. 3, pp. 355–364, 2017, doi: 10.1016/j.giq.2017.09.007.

[18] M. Alghazwi, F. Turkmen, J. Van Der Velde, and D. Karastoyanova, "Blockchain for genomics: a systematic literature review," *Distributed Ledger Technologies: Research and Practice*, vol. 1, no. 2, pp. 1–28, Dec. 2022, doi: 10.1145/3563044.

[19] R. Tyagi, P. Shukla, and A. Tyagi, "Implementation of blockchain on criminality record checker," *International Journal of Engineering Research and*, vol. V9, no. 04, May 2020, doi: 10.17577/IJERTV9IS040632.

[20] M. Ahmed, A. R. Pranta, M. F. A. Koly, F. Taher, and M. A. Khan, "Using IPFS and hyperledger on private blockchain to secure the criminal record system," *European Journal of Information Technologies and Computer Science*, vol. 3, no. 1, pp. 1–6, Jan. 2023, doi: 10.24018/compute.2023.3.1.81.

[21] P. Makwana and D. P. Sharma, "Criminal record keeping with blockchain," *Journal of Emerging Technologies and Innovative Research*, vol. 6, no. 4, pp. 361–365, 2019.

[22] G. Chawhan, D. Patole, Y. Borse, G. Kukreja, H. Parekh, and R. Jain, "Advantages of blockchain in digital forensic evidence management," *SSRN Electronic Journal*, 2021, doi: 10.2139/ssrn.3866889.

[23] R. Z. Fathiyana, S. N. Yutia, and D. J. Hidayat, "Prototype of integrated national identity storage security system in Indonesia using blockchain technology," *JOIV: International Journal on Informatics Visualization*, vol. 6, no. 1, p. 109, Mar. 2022, doi: 10.30630/joiv.6.1.877.

[24] R. C. Mullegowda, N. Hiremani, M. Birje, and N. K. Ramaswamy, "A novel smart contract based blockchain with sidechain for electronic voting," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 14, no. 1, pp. 617–630, Feb. 2024, doi: 10.11591/ijece.v14i1.pp617-630.

[25] P. Maya and P. A. Salam, "Implementation of a blockchain based DApp for P2P electricity trading," in *2023 5th International Conference on Energy, Power and Environment: Towards Flexible Green Energy Technologies (ICEPE)*, Jun. 2023, pp. 1–6, doi: 10.1109/ICEPE57949.2023.10201530.

[26] S. M. Jain, "Introduction to remix IDE," in *A Brief Introduction to Web3*, Berkeley, CA: Apress, 2023, pp. 89–126.

[27] M. R. Bahadure, M. R. Khasare, M. S. Mahure, M. L. Rathod, M. S. Junghare, and P. N. G. Rathi, "Thr3ebay: E-commerce Dapp using Blockchain," *International Journal for Research in Applied Science and Engineering Technology*, vol. 11, no. 5, pp. 1435–1438, May 2023, doi: 10.22214/ijraset.2023.51813.

[28] Hemani, D. Singh, and R. K. Dwivedi, "Designing blockchain based secure autonomous vehicular internet of things (IoT) architecture with efficient smart contracts," *International Journal of Information Technology (Singapore)*, Feb. 2024, doi: 10.1007/s41870-023-01712-x.

[29] J. I. Sihotang, Y. Richel, and A. F. Pakpahan, "Membership information system using node JS," *Abstract Proceedings International Scholars Conference*, vol. 7, no. 1, pp. 1729–1740, Dec. 2019, doi: 10.35974/isc.v7i1.1372.

[30] N. Nizamuddin, K. Salah, M. Ajmal Azad, J. Arshad, and M. H. Rehman, "Decentralized document version control using ethereum blockchain and IPFS," *Computers & Electrical Engineering*, vol. 76, pp. 183–197, Jun. 2019, doi: 10.1016/j.compeleceng.2019.03.014.

BIOGRAPHIES OF AUTHORS

Manal Jlil is a Ph.D. student at the LISAC Laboratory, Departement of Computer Sciences, at Faculty of Sciences, Sidi Mohamed Ben Abdellah University Fez, Morocco. In addition, she is employed in public administration. Her researches focus on new trend technologies, especially blockchain technology, including the development of new information systems for the benefit of public administration based on data exchange between different parties, with the guarantee of data confidentiality, security, and traceability. She can be contacted at email: manal.jlil@usmba.ac.ma.

Kaoutar Jouti was born in Morocco. She is a doctoral student at the Laboratory of Signals, Automation, and Cognitivism, in Doctoral Training: Information and Communication Sciences and Technologies (STIC) at Sidi Mohamed Ben Abdellah University, Fez in Morocco. Her research focuses on new blockchain technologies, including fully transparent data exchange between different parties while guaranteeing the confidentiality, integrity, security, and traceability of the data exchanged. She can be contacted at email: kaoutar.jouti@usmba.ac.ma.

Chakir Loqman is currently a professor of Computer Science with the Faculty of Sciences Dhar El Mahraz, Sidi Mohamed Ben Abdellah University, Fez, Morocco. His research interests include artificial intelligence, text mining, pattern recognition, and optimization. He can be contacted at email: loqman.chakir@usmba.ac.ma.