جامعة سيدي محمد بن عبد الله بفاس
ⵜⴰⵙⴷⴰⵡⵉⵜ ⵙⵉⴷⵉ ⵎⵓⵃⵎⵎⴰⴷ ⴱⵏ ⵄⴱⴷⵍⵍⴰⵀ ⵏ ⴼⴰⵙ
UNIVERSITÉ SIDI MOHAMED BEN ABDELLAH DE FES

كلية العلوم ظهر المهراز فاس
ⵜⴰⵖⵉⵡⴰⵏⵜ ⵏ ⵜⵎⵙⵙⵓⵏⵜ ⴹⵀⴰⵕ ⵍⵎⵀⵔⴰⵣ ⴼⴰⵙ
FACULTE DES SCIENCES DHAR EL MAHRAZ FES

N° d'ordre : 89/2024

Centre des Etudes Doctorales : ***Sciences et Techniques et Sciences Médicales***

Formation Doctorale : ***STIC***

Discipline : ***Informatique***
Spécialité : ***Informatique***
Laboratoire : ***LISAC***

THÈSE DE DOCTORAT

Leveraging Sustainable Blockchain Technology for secure and efficient data sharing in E-government ecosystems

Présentée par :

Manal JLIL

Soutenue le 28/12/2024 devant le jury :

El Beqqali Omar	PES	Faculté des sciences Dhar El Mahraz, Fès	Président
En-Naimi El mokhtar	PES	FST Tanger, Université Abdelmalek Essaadi	Rapporteur& examinateur
Bennis Hamid	PES	EST de Meknès, Université Moulay Ismail	Rapporteur& examinateur
Satori Hassan	PES	Faculté des sciences Dhar El Mahraz, Fès	Rapporteur& examinateur
Amakdouf Hicham	MCH	Faculté des sciences Dhar El Mahraz, Fès	Examinateur
Haddouch Khalid	MCH	École Nationale des Sciences Appliquées, Fès	Examinateur
Loqman Chakir	PES	Faculté des sciences Dhar El Mahraz, Fès	Directeur de thèse

Année Universitaire : 2023-2024

Résumé de la thèse

L'administration publique au Maroc commence à adopter des outils informatiques qui facilitent les interactions entre les citoyens et l'administration, donnant ainsi naissance à ce que l'on appelle l'E-gouvernement.

Le but principal de cette réforme est la dématérialisation des documents et la mise en place de l'administration électronique pour améliorer la prestation des services des instituions gouvernementaux envers le citoyen en garantissant la transparence et la rapidité des services fournis. De plus le partage des données et documents représente un défi majeur dans la gestion administrative, en particulier lorsqu'il s'agit de données critiques ou personnelles qui doivent être protégées contre toutes utilisations frauduleuses ou accès non autorisé.

L'objectif de notre travail est d'étudier l'intégration de la technologie Blockchain dans les systèmes d'information des administrations publiques marocaines, étant donné le grand nombre d'avantages qu'elle offre.

En effet, grâce à ces caractéristiques uniques de décentralisation, de transparence et d'intégrité des données, la technologie Blockchain assure une transparence totale des transactions tout en maintenant la confidentialité des informations sensibles.

De plus elle permet une traçabilité parfaite des opérations, réduisant ainsi les risques de corruption et de fraude. Elle offre aussi l'utilisation des contrats intelligents ce qui permet l'automatisation de nombreuses procédures administratives, réduisant ainsi les délais et les couts. Ainsi que faciliter le partage sécurisé des données entre différentes administrations et services publiques ce qui favorise une meilleure collaboration et coordination entre les entités gouvernementales.

En résumé, l'adoption de la technologie Blockchain pour l'E-gouvernance est particulièrement bénéfique. Permettant le renforcement de la confiance des citoyens envers les services publics grâce à la transparence et l'imputabilité des actions administratives. Les processus bureaucratiques sont simplifiés, rendant les services gouvernementaux plus accessibles et rapides pour les citoyens. La gestion des identités numériques est également optimisée, offrant une protection accrue des données personnelles et facilitant l'authentification sécurisée.

Pour finir, l'intégration de la Blockchain dans l'e-gouvernance peut contribuer à moderniser les administrations et à améliorer la qualité des services offerts et à promouvoir une gestion plus efficace et transparente.

Mots clés : E-gouvernance ; Technologie Blockchain ; Contrat Intelligent; digitalisation; Partage de données; sécurité des données; Administration électronique.

UNIVERSITE SIDI MOHAMED BEN ABDELLAH DE FES
FACULTÉ DES SCIENCES ET TECHNIQUES DE FÈS

Université Sidi Mohamed Ben Abdellah

Centre des Études : Sciences et Techniques et Sciences Médicales
Formation Doctorale : Sciences et Technologies de l'Information et de Communication
Discipline : Informatique
Spécialité : Informatique
Laboratoire : Laboratoire d'Informatique, Signaux, Automatique et Cognitivisme

Thèse de doctorat

Leveraging Sustainable Blockchain Technology for secure and efficient data sharing in E-government ecosystems

---

Présentée par :

Manal JLIL

Soutenue le 28 / 12 / 2024 devant le jury composé de :

Pr. El Beqqali Omar	FSDM – Fès	Président
Pr. En-Naimi El Mokhtar	FST – Tanger	Rapporteur & Examinateur
Pr. Bennis Hamid	EST – Meknès	Rapporteur & Examinateur
Pr. Satori Hassan	FSDM – Fès	Rapporteur & Examinateur
Pr. Amakdouf Hicham	FSDM – Fès	Examinateur
Pr. Haddouch Khalid	ENSA - Fès	Examinateur
Pr. Loqman Chakir	FSDM - Fès	Directeur de thèse

Année universitaire : 2023-2024

ACKNOWLEDGMENT

Praise be to Almighty God for placing on my path, several people, whose contributions provided considerable help in the development of this doctoral thesis.

I am profoundly grateful for the enduring support of my supervisor Pr. Chakir LOQMAN whose steadfast belief in my capabilities and academic potential encouraged me to persevere even during my lowest moments. Her guidance was a beacon of light in times of doubt. Without his guidance, support, and the opportunities that he has given me, this thesis would not have been possible.

I also dedicate my gratitude to my co-authors for the scientific discussion and collaboration Kaoutar JOUTI, and Jaouad BOUMHIDI as well as for the good times and all the adventures we had during these years.

Thank you sincerely to Adil, Soufiane, and Oussama, you are my friends, brothers, and coworkers. You have been part of this journey. It would not

have been possible to finish this thesis without your dedication, attention, and emotional support, especially during the most difficult moments.

I must also express my deepest appreciation for my aunt Fatiha RGUIBI, My sister Hiba JLIL, and my Mom Latifa RGUIBI, who stepped in not only with emotional reassurance but also with critical emotional and financial support when unexpected personal challenges arose. Their unconditional love and sacrifice have been the foundation of my resilience and success.

Finally, I want to thank my family. Your love, support, encouragement, and patience have been the fuel to help me work and finish this thesis. There are no words in any language to express my love and gratitude to you.

Résumé

De nos jours, l'utilisation des nouvelles technologies est devenue incontournable en raison des avancées significatives dans le domaine de la digitalisation et des moyens de communication modernes. Par conséquent, l'adaptation des administrations publiques à ces nouvelles tendances est devenue impérative pour assurer leur efficacité et leur pertinence.

L'administration publique au Maroc commence à adopter des outils informatiques qui facilitent les interactions entre les citoyens et l'administration, donnant ainsi naissance à ce que l'on appelle l'E-gouvernement.

Le but principal de cette réforme est la dématérialisation des documents et la mise en place de l'administration électronique pour améliorer la prestation des services des institutions gouvernementaux envers le citoyen en garantissant la transparence et la rapidité des services fournis. De plus le partage des données et documents représente un défi majeur dans la gestion administrative, en particulier lorsqu'il s'agit de données critiques ou personnelles qui doivent être protégées contre toutes utilisations frauduleuses ou accès non autorisé.

L'objectif de notre travail est d'étudier l'intégration de la technologie Blockchain dans les systèmes d'information des administrations publiques marocaines, étant donné le grand nombre d'avantages qu'elle offre. En effet, grâce à ces caractéristiques uniques de décentralisation, de transparence et d'intégrité des données, la technologie Blockchain assure une transparence totale des transactions tout en maintenant la confidentialité des informations sensibles. De plus elle permet une traçabilité parfaite des opérations, réduisant ainsi les risques de corruption et de fraude. Elle offre aussi l'utilisation des contrats intelligents ce qui permet l'automatisation de nombreuses procédures administratives, réduisant ainsi les délais et les couts. Ainsi que faciliter le partage sécurisé des données entre différentes administrations et services publiques ce qui favorise une meilleure collaboration et coordination entre les entités gouvernementales.

En résumé, l'adoption de la technologie Blockchain pour l'E-gouvernance est particulièrement bénéfique. Permettant le renforcement de la confiance des citoyens envers les services publics grâce à la transparence et l'imputabilité des actions administratives. Les processus bureaucratiques sont simplifiés, rendant les services gouvernementaux plus accessibles et rapides pour les citoyens. La gestion des identités numériques est également optimisée, offrant une protection accrue des données personnelles et facilitant l'authentification sécurisée.

Pour finir, l'intégration de la Blockchain dans l'e-gouvernance peut contribuer à moderniser les administrations et à améliorer la qualité des services offerts et à promouvoir une gestion plus efficace et transparente.

Mots Clés : E-governance ; Technologie Blockchain ; Contrat Intelligent ; digitalisation ; Partage de données ; sécurité des données ; Administration électronique.

Abstract

Nowadays, the use of new technologies has become essential due to significant advances in digitalization and modern means of communication. Consequently, adapting public administrations to these new trends has become imperative to ensure their efficiency and relevance.

The public administration in Morocco is beginning to adopt IT tools that facilitate interactions between citizens and the administration, giving rise to what is called E-government.

The main goal of this reform is the digitization of documents and the establishment of electronic administration to improve the service delivery of government institutions to citizens by ensuring transparency and speed of services provided. Additionally, the sharing of data and documents represents a major challenge in administrative management, particularly when it comes to critical or personal data that must be protected against fraudulent use or unauthorized access.

The aim of our work is to study the integration of Blockchain technology into the information systems of Moroccan public administrations, given the numerous advantages it offers. Indeed, thanks to its unique characteristics of decentralization, transparency, and data integrity, Blockchain technology ensures complete transparency of transactions while maintaining the confidentiality of sensitive information.

Furthermore, this enables operations to be traced accurately, which reduces the risk of corruption and fraud. The use of smart contracts is also available, which enables the automation of many administrative tasks and reduces costs.

In addition, it enables the secure sharing of data between various administrations and public services, which encourages better collaboration and coordination between government entities.

E-governance can benefit greatly from the implementation of Blockchain technology. The transparency and accountability of administrative actions contribute to strengthening citizens' trust in public services. Government services are more accessible and faster

for citizens due to the simplification of Procedural operations.
Digital identities are managed more efficiently, providing greater protection for personal data and facilitating secure authentication. In the end, the incorporation of Blockchain in e-governance can aid in modernizing administrations, improving the quality of services provided, and promoting more efficient and transparent management.

Key Words: E-governance; Blockchain technology; smart contract; digitalization; data sharing; data security; E-government.

Abstract

Arabic abstract

CONTENTS

List Of Acronyms viii

1 Introduction **1**

1.1 Background and research motivations 2

1.2 Research Problem 3

1.3 Objectives and scope of the thesis 4

1.4 Thesis Organization 5

2 State of The Art **7**

2.1 Introduction to E-Government 8

2.1.1 Definition 8

2.1.2 Contextualizing the global digital transition 9

2.1.3 The main theories on the digitization of public administration . . . 9

2.2 Data sharing systems in E-Government 10

2.2.1 Benefits of Data sharing systems 10

2.2.2 Challenges in Implementing Data Sharing Systems 11

2.2.3 Case studies and Examples of existing data sharing systems 12

2.3 E-Government concept in the Moroccan country 12

3 Blockchain technology and E-Government 15

3.1 Introduction to Blockchain 16

3.1.1 History of Blockchain 17

3.1.2 Types of Blockchain 18

3.1.3 The Operating principle behind Blockchain technology 18

3.1.4 What constitutes a Blockchain 20

3.2 Technology choices 25

3.2.1 Blockchain Technology 25

3.2.2 Ethereum Blockchain 26

3.2.3 Hashing Algorithms 27

3.2.4 IPFS protocol 27

3.2.5 Smart Contracts 28

3.2.6 Solidity Language: 29

3.3 Software and Platforms used for deployment 30

3.4 Blockchain in E-government 33

4 Improving traceability in E-governance file-sharing systems 37

4.1 Introduction 38

4.2 State of the Art 41

4.3 Background 45

4.4 Proposed Model 48

4.5 Implementation and Challenges 50

4.5.1 System Design and Implementation 50

4.5.2 Implementation challenges 56

4.6 Evaluation and Discussion 57

4.6.1 Use case Experimentation 57

4.6.2 Security Analysis 58

4.6.3 Discussion 61

4.7 Conclusion 61

5 Blockchain and smart contracts based system for criminal record management 63

5.1 Introduction . . . 64

5.2 Literature Review . . . 67

5.3 Background . . . 69

5.3.1 Proposed System . . . 73

5.3.2 System Design . . . 77

5.3.3 Implementation . . . 79

5.3.4 Scenario of the designed solution . . . 81

5.4 Evaluation and Discussion . . . 84

5.5 Conclusion . . . 86

6 Blockchain-based System for traffic accident report's management 87

6.1 Introduction . . . 88

6.2 Literature Review . . . 89

6.3 Problem Statement . . . 90

6.4 Proposed Solution . . . 92

6.5 Evaluation and Discussion . . . 93

6.6 Conclusion . . . 97

7 Conclusion 98

7.1 Overview . . . 99

7.2 Future perspectives . . . 101

LIST OF FIGURES

2.1 E-Government Development Index Global and Regional Average Value Source: 2008-2022 Unitied Nations E-Goverment Surveys 9
2.2 Evolution of the number of complaints on the "Chikaya" portal. Source : "www.Chikaya.ma" 13

3.1 Icons of some existing altcoins 17
3.2 History of Blockchain 17
3.3 Block representation of Blockchain 19
3.4 Operating principle of Blockchain Technology source: doi: 10.13140/RG.2.2.22132.63368 20
3.5 Difference between centralized and decentralized architecture source: doi: 10.13140/RG.2.2.14730.29127 21
3.6 Different types Of Consensus Algorithms source: https://101blockchains.com/consensus-algorithms-blockchain/ 23
3.7 Home Interface of Ganache-cli 30
3.8 Screen of the Home interface of Remix IDE platform 31
3.9 Difference between web 2 and web 3 32
3.10 Representation of the Metamask Extention 32

4.1 Users and stakeholders of the judiciary system 45
4.2 Concept of old system's architecture (traditional architecture) 46
4.3 New File sharing system Architecture 48
4.4 Blockchain network (Blockchain-based architecture) 49
4.5 Sequence Diagram of the file uploading process 50
4.6 List of Accounts provided automatically in ganache environment 51
4.7 List of Recent Block Mined 51
4.8 Information about the Smart Contract executed and its related transaction 51
4.9 Writing the smart contract code using the Remix IDE 52
4.10 Compiling the Smart Contract (SC) using truffle 52
4.11 Migration of the Smart Contract 53
4.12 Connecting Metamask to the application 53
4.13 Metamask home interface 54
4.14 The User uploads the document into the Dapp 54
4.15 The hash of the document is generated 55
4.16 Document verification using the hash generated 55
4.17 Upload/download time's average using IPFS 59
4.18 Security Analysis of the first smart contract using SolidityScan 60
4.19 Security Analysis of the second smart contract using SolidityScan 60

5.1 The current process to get a criminal record 69
5.2 The architecture of the public platform for criminal record application developed by the ministry of Justice in Morocco 71
5.3 Criminal Record Data Centralization 72
5.4 Blockchain-based system for criminal record management 74
5.5 The new process of getting a criminal record 76
5.6 Diagram of sequence for the account creation process 77
5.7 Diagram of sequence for applying for a criminal record 78
5.8 Diagram of sequence for adding a criminal record 78
5.9 Transactions History 79

5.10 The smart contract code for controlling the user access into the system . . 80
5.11 Javascript code illustration of the Dapp 81
5.12 Connection Form 81
5.13 User type selection 81
5.14 Registration form when the user type is "Citizen" 82
5.15 Registration form when the user type is "Public Administration" 83
5.16 The options for user type ="citizen" 83
5.17 Options for user type ="public administration" 83
5.18 Interface of adding a criminal record by "Public Administration" 84

6.1 Example of amicable traffic accident report used in case of car crash in the Moroccan country. 91
6.2 Proposed architecture 93
6.3 The driver information form 94
6.4 Checking the vehicle type -1 95
6.5 Checking the vehicle type -2 95
6.6 Checking the accident information 96
6.7 Uploading real photos of the accident 96
6.8 Submitting the accident report 96

LIST OF TABLES

3.1 Types of Blockchain 19

4.1 Evolution of e-government indices in Morocco for the last 10 years, source: The author, based on UN reports 2012-2022 43

4.2 Number of electronic signature users 47

4.3 Upload and download time for the IPFS storage 58

5.1 The security performance of “access control” smart contract 85

5.2 The security performance of “simple storage” smart contract 85

List of Acronyms

E-govt E-government

IoT Internet Of Things

P2P Peer to peer

IPFS Interplanetary File System

SC Smart Contract

API Application Programming Interface

PoW Proof of Work

PoS Proof of Stake

BTC Bitcoin

ETH Ethereum

BCH Bitcoin Cash

DOGE Dogecoin

LTC Litecoin

XRP Ripple

DApps Decentralized Applications

IBM International Business Machines Corporation

DLT Distributed Ledger Technologies

SCJP Supreme Council of the Judicial Power

PPP Presidency of the Public Prosecution

DFS Distributed File system

ADD Agency for Digital Development

TII Telecommunication Infrastructure Index

HCI Human Capital Index

OSI Online Services Index

EGDI E-Government Development Index

DCR Digital Commitment Report

DEI Digital Developement Index

IT Information System

ITS Intelligent Transportation Systems

EVM Ethereum Virtual Machine

AI Artificial Intelligence

ICT Information and Communication Technologies

BADR Base Automaisée des Douanes en Réseau

CHAPTER

1

INTRODUCTION

1.1 Background and research motivations

Since the discovery of computing, everyday life has been simplified. Currently, individuals can easily process information using software and computer networks. Computers are replacing documents, calculators, and paper reports. Indeed, this machine aims to develop technological solutions that facilitate the day-to-day work of individuals and are applicable in different fields.

Taking the Internet as an example, this revolution, which was developed for the first time for military use, at first, it was used just for communication then it allowed information to be transmitted and received all over the world. Later, it was used for commerce, information storage, consultation, recording, and business. Thus, we are talking about a new phenomenon called: “Digitization”.

As a definition, digitization is the preservation of analog information in digital form. To put it differently, hardware media are recorded in an electronic form. This trend has had an impact on our way of living. A change has occurred thanks to the democratization of new technologies. Moreover, like every technological revolution, working methods have changed, which has led to the creation of new professions and the disappearance of others. Given the impact of these technologies on our lifestyle, we are observing a big change in our habits: digital equipment with all types of devices (computers, smartphones, tablets, etc.) has taken its place concerning physical material (papers, registers, etc.). This change has allowed us to gain in terms of productivity, through the automation of numerous tasks, as well as the capacity to process a large number of possible data. This processing is a new concept known today under the term BIG DATA, which appeared in 2012, to reflect the fact that companies are faced with increasingly considerable volumes of data to process and present significant commercial and marketing challenges. According to analyst Doug Laney [1], Big Data is defined by the three criteria:

— Volume;

— Variety (nature and level of structuring)

— Production, collection, and analysis velocity.

We can summarize that Big Data and digitization will significantly affect management, processes, acquisition, retention, and more broadly, the overall culture of companies and

organizations.

Taking the Moroccan state as an example, digital transformation emerges as a key driver of national economic growth. This profound transformation is taking place gradually in all sectors of activity, and strengthens the national digital ecosystem, for example:

- The generalization and democratization of financial services;
- Making the process of investing more easier;
- The inclusion of a large number of citizens in the formal socio-economic sphere;
- Broadening the scope of action of economic actors.

All of this necessitates the expansion of the use of new technologies, telecommunication networks, digital coverage across the national territory, and significant investments in new fundamental infrastructure.

So, the digital revolution is taking place with great strides, also giving rise to new professions and innovations in various sectors: digital administration, electronic banking, insurance, e-commerce, businesses, and start-ups. For all these sectors, digital transformation has resulted in the creation of new trends accompanied by a multitude of innovative offers: Big data, artificial intelligence, the Internet of Things, and Blockchain Technology. Indeed, digitization is on the move, pushing everything in its path.

1.2 Research Problem

Accordingly, E-governance is a broad term that defines and evaluates the impact of technologies on the operation of government administrations and the relationship between citizens and public servants. Its goals include improving service delivery facilitating the efficient management and dissemination of information to citizens and encouraging citizens to participate in public and policy decision-making.

In this way, The Moroccan government has progressed greatly in E-government services, providing online platforms for various administrative tasks. However, all of the online platforms provided rely on traditional centralized systems architecture. These systems face several issues, such as :

— Security concerns: central databases or servers are a prime target for cyberattacks.

— Single point of failure: centralized systems are not as resilient to disruptions like network outages.

— Limited privacy: users in centralized systems frequently need to trust a central authority with data, the lack of privacy can be a disadvantage, especially, in situations where data protection is vital.

— Higher operation costs: To maintain the security and integrity of a centralized system can be very expensive.

This is why the integration of Blockchain technology into the design of government information systems can offer numerous advantages and overcome the issues of centralized systems.

1.3 Objectives and scope of the thesis

This research aims to conduct an in-depth study of one of these emerging trends, namely Blockchain technology. It will explore its operating principle, as well as its different areas of application, particularly in terms of E-governance and modernization of public administrations. Furthermore, it presents new proposed architectures based on Blockchain technology to enhance the data-sharing systems for the benefit of the Moroccan government.

In e-government, stakeholders are required to share data from single or multiple departments for decision-making and service delivery. Traditional systems in the centralized environment do not guarantee secure and efficient data sharing, because unauthorized access to the database can cause data corruption. The decentralized e-government data management system is also considered inefficient, as the number of users and transactions increases. This can lead to slower processing times and higher costs, making management of large volumes of data more difficult.[2]. Blockchain prevents database managers from being corrupted as centralized systems do since it is a decentralized, immutable, and transparent ledger that is kept up to date by network miners. As an illustration, the transparency inherent to Blockchain technology guarantees that all transactions are visible and can be verified, consequently, promoting increased accountability within government organizations[3]. This transparency can significantly reduce fraud and wrongdoings, as

every transaction made on Blockchain is constantly recorded and cannot be altered.

The other major advantage of Blockchain in E-government (E-govt) is effective and safe identity management. Blockchain can provide a trustworthy for storing and verifying digital identities, simplifying processes such as voter registration, social security, and tax collection[4]. This can result in more seamless experiences between citizens and government, reducing administrative headaches while increasing service delivery and efficiency. As a result, Blockchain is the most efficient decentralized platform for secure and efficient data sharing. The Blockchain overcomes all drawbacks of the decentralized management system and centralized management system. Blockchain's decentralized nature distributes data across a network of nodes, making it more resilient to attacks[5]. This ensures that citizens' personal information is protected, bolstering trust in digital government services.

1.4 Thesis Organization

The thesis is organized into 5 chapters which are described below:

Introduction: It is a general introduction, that introduces the background and the research motivations for our work. It also presents the main objectives of the thesis.

Chapter 2: presents a description of the Concept of E-government and the data-sharing systems in E-government. Furthermore, it gives an overview of the development of the E-government concept in the Moroccan country.

Chapter 3: provides a comprehensive overview of Blockchain technology and its application in E-government. Following this, a presentation of the specific technology choices relevant to Blockchain, and used to design the new architectures proposed in this thesis. The discussion then moves to the software and platforms used for deployment.

Chapter 4 : This Chapter describes the new architecture proposed for a Blockchain-based system to improve traceability in E-governance file-sharing systems.

Chapter 5: This Chapter, presents a detailed description of a Blockchain and smart contracts-based system for criminal record management.

Chapter 6: This chapter describes a use case study of a Blockchain-based System for traffic accident report's management.

Conclusion: It is a conclusion of the thesis that highlights all important contributions of the research. It also presents an elaboration of perspectives and future directions related to the subject of this thesis.

CHAPTER

2

STATE OF THE ART

In this Chapter we introduce the context of our research, as well as the fundamental concepts related to our study.

2.1 Introduction to E-Government

2.1.1 Definition

E-government refers to a range of digital government functions, from providing online services to citizens to facilitating electronic information and service exchanges with businesses and other government entities.

According to the UN E-government survey [6], E-government, typically, can be defined as the use of Information and Communication Technologies to improve the efficiency of government departments in providing government services to citizens and businesses. Over time, the framework of E-government has expanded to encompass the use of information and communication technologies by governments, to facilitate a wide array of interactions with citizens and businesses, promote open government data, and drive innovation in governance practices.

The primary goal of e-government is to streamline government operations, improve accessibility, and make public administration more efficient and transparent [7]. By leveraging technology, e-government can transform traditional methods of governance, creating a more connected, responsive, and efficient public sector. The concept of e-government encompasses various types of digital interactions:

— G2C: government-to-citizen;

— G2B: government-to-business;

— G2G: government-to-government;

— G2E: government-to-employee.

These interactions provide different channels for communication and service delivery, aiming to reduce bureaucratic barriers, improve service quality, and enhance public trust.

Figure 2.1 illustrates the Development of the E-Government Index in the worldwide from 2008 to 2024.

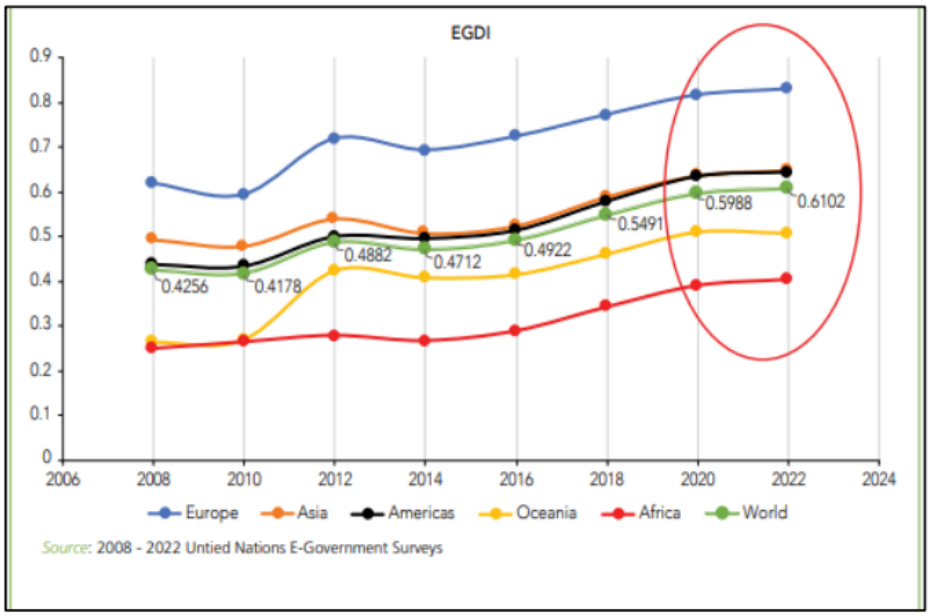

Figure 2.1 – E-Government Development Index Global and Regional Average Value
Source: 2008-2022 Unitied Nations E-Goverment Surveys

2.1.2 Contextualizing the global digital transition

Digital transformation has become imperative for governments worldwide, faced with the need to streamline operations, enhance transparency, and respond effectively to the evolving needs of society. Rapid developments in electronic communications, big data, artificial intelligence, and other technological innovations have created a landscape in which digital transformation is not only an option, but also, a strategic imperative for governments seeking to remain relevant and effective in the digital age.

Most countries have a national strategy for digital governance, as well as legislation on cybersecurity, personal data protection, national data policies, open government data, and e-participation [8].

2.1.3 The main theories on the digitization of public administration

1. Theories related to public service:

   Theories related to public service are essential for understanding state intervention and the management of essential services. They offer insights into the purpose, management, and challenges of public services, helping us better understand the

public sector's complexities and identify ways to enhance its efficiency and fairness.

2. Theories related to digitization:

   Research on public administration digitization is interdisciplinary, focusing on using Information and Communication Technologies for efficiency, transparency, and citizen engagement. Key theories include e-governance, which enhances public services and citizen participation; E-administration, which automates internal processes for efficiency; and Public Innovation Theory, which promotes innovation in public services through co-creation and experimentation with new technologies [9].

2.2 Data sharing systems in E-Government

The efficient functioning of public administrations requires the use of data-sharing systems. Government organizations are increasingly adopting data-sharing systems to improve efficiency, transparency, and collaboration.

By using these systems, government agencies can seamlessly exchange information, and improve coordination, transparency, and service delivery to citizens. Furthermore, data-sharing platforms provide public officials with a more comprehensive view of citizen's needs and offer numerous additional benefits.

2.2.1 Benefits of Data sharing systems

The use of effective data sharing in public organizations can significantly:

— Improve Service delivery: Data sharing enables multiple government departments to share and use the same information, which reduces redundancy and ensures faster and more accurate delivery of services. For example, sharing information between health and social services can result in more comprehensive care for citizens.[10];

— Enhanced Decision-Making: Public administrators have the ability to make more informed decisions by accessing shared data. Indeed, governments can improve their understanding and approach to address complex issues, such as urban planning, public health, and emergency response, more effectively by integrating data

from different sources. [11];

— Increased Transparency and Accountability: The availability of information to both government officials and the public through data-sharing systems can lead to increased transparency. This transparency encourages trust between citizens, and their governments by holding public administrations accountable for their actions and decisions. [12];

— Cost Efficiency: Data sharing reduces the need for duplicated efforts in data collection and maintenance, leading to significant cost savings. The allocation of resources can be more efficient for governments by using data from multiple departments [13].

2.2.2 Challenges in Implementing Data Sharing Systems

The implementation of efficient data-sharing systems in public administrations can be both a complex and multifaceted challenge.

Below are the main challenges detailed :

— Data Privacy and Security: Ensuring the privacy and security of sensitive information is one of the primary challenges in putting into practice data-sharing systems. It is necessary for public administrations to follow data protection regulations and prevent unauthorized access.[14];

— Interoperability issues: Sharing and integrating data seamlessly is challenging when different government departments use various systems and data formats. So, The establishment of common standards and protocols is necessary for effective data sharing. [15];

— Cultural and Organizational challenges: The implementation of data-sharing systems can face obstacles due to a lack of collaboration between departments and resistance to change. The key to overcoming these barriers is the need for strong leadership, a clear vision, and incentives for cross-department cooperation. [16];

— Technical challenges: A solid technical infrastructure and expertise are necessary for implementing data-sharing systems. For this reason, investing in modernizing their IT systems and having the necessary technical skills to manage and maintain

them is crucial for governments.[17];

— Lack of data literacy and analytical skills: Public servants may not have the necessary skills to effectively use shared data for decision-making, which requires comprehensive training.[18].

2.2.3 Case studies and Examples of existing data sharing systems

Estonia's X-Road: Estonia is a leading example of effective data sharing in public administration. The X-Road platform enables secure and efficient data exchange between various government databases and private sector entities. This system has significantly improved service delivery and citizen engagement in Estonia. [19].

United States Open Data Initiative: The U.S. government's Open Data Initiative aims to make government data more accessible and usable by the public. This initiative has led to the development of numerous applications and services that utilize government data to improve transparency and public service delivery [20].

European Union ISA Program: The ISA (Interoperability Solutions for Public Administrations) program promotes data sharing and interoperability among EU member states. By providing tools and frameworks for data exchange, the program enhances cross-border cooperation and the efficiency of public services [21].

2.3 E-Government concept in the Moroccan country

The digitization of public administration can be seen as a natural consequence of the evolving use of the Internet and social networks by the Moroccan population [22]. In Morocco's move toward advanced "regionalization", new territories have increased administrative complexity. The digitalization of public administration is crucial for enhancing governance and management in these areas. Additionally, digital platforms and social media play a vital role in mobilizing citizens and fostering political and social change [23].

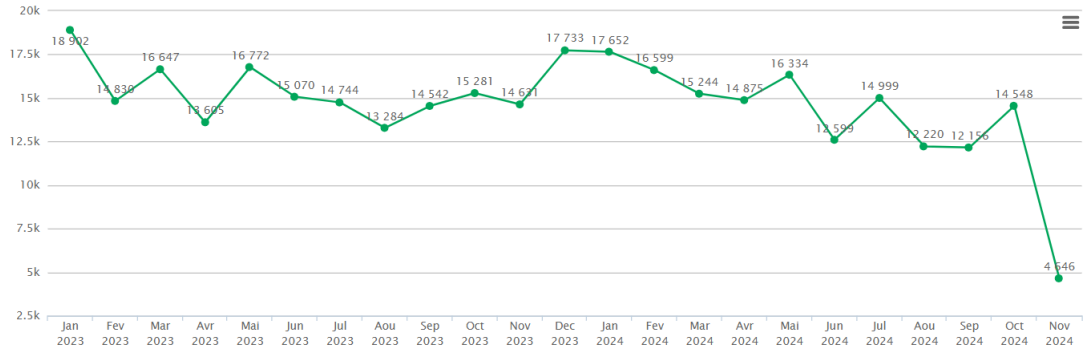

Figure 2.2 – Evolution of the number of complaints on the "Chikaya" portal.
Source : "www.Chikaya.ma"

The Moroccan government has been actively working on digitizing its public administration, with the aim of enhancing efficiency, transparency, and citizen engagement [24].

To succeed, it is crucial to develop robust and secure data-sharing systems across various government agencies as a key aspect.

Various initiatives and strategies that have been implemented over the years show the Moroccan government's commitment to digitization.

As an example: The 'Portail du Citoyen' is one of Morocco's various e-government platforms that allows citizens to access public services online, including administrative procedures and information. We also find the portal "www.chikaya.ma". This portal is a complaint system for users who encounter a problem or harm when using a public service due to illegal behavior or actions by the administration that go against the principles of justice and fairness in the country. Figure 2.2 presents a graph depicting the evolution of the number of complaints on the "www.chikaya.ma" portal for the period of: January 2023 to November 2024.

One more example is The "Maroc Numeric 2020" strategy, formerly known as "DIGITAL Morocco 2020", which was a comprehensive plan designed to encourage the use of Information and Communication Technologies (ICT) in all areas of the economy, including public administration, and promoting the national digital economy [25].

Another notable achievement is the digitization of the Moroccan Customs Administration, by the introduction of the "Base Automaisée des Douanes en Réseau (BADR)" system (in English: Automated Customs Network Database) to enable electronic declarations and payments, which has resulted in significant reductions in processing times and

enhanced transparency [26].

Although there has been a lot of progress, the implementation of data-sharing systems in Morocco is still struggling with multiple difficulties. Data privacy and security, robust infrastructure, and continuous capacity building among government staff are just some of the crucial issues [27]. Despite these challenges, ongoing efforts to address them are leading to more efficient and secure means of sharing data.

Our thesis aims to provide case studies on designing and developing innovative architectures for the benefit of Morocco's government, particularly the Ministry of Justice. The goal of these architectures is to create safe, transparent, and reliable platforms for data exchange between government agencies, stakeholders, and even the general public.

The next Chapter provides a detailed description of the Blockchain Technology and technology choices to implement the data-sharing systems proposed in this thesis.

CHAPTER

3

BLOCKCHAIN TECHNOLOGY AND E-GOVERNMENT

This chapter will provide an in-depth overview of Blockchain technology, along with the technological choices made for implementing the systems proposed in this thesis. Additionally, it will explore the relationship between Blockchain and E-government.

3.1 Introduction to Blockchain

Blockchain technology was born in 2008 with the emergence of the Bitcoin network [28], created anonymously, under the pseudonym of Satoshi Nakamoto. It has applications in many fields, such as supply chain [29], finance [30], health [31], and video games [32].

For some applications, such as the use of Blockchain within video games [33] this leads to a need to get a large number of Big data exchanges with minimal latency. These needs seem complex when integrated into a distributed architecture using Blockchain technology.

In technical terms, Blockchain is a decentralized global database that contains the history of all exchanges between its users, without intermediaries, which allows everyone to verify the chain validity [34]. What characterizes this technology is that it operates without a central control body. Each user can, at every time, using a cryptographic system, verify the validity of information and execute transactions.

Originally, this technology served as a support for the creation of the Bitcoin (BTC) cryptocurrency, it allows certifying transactions between individuals through a Peer to peer (P2P) system without the need for a third party. This means that the Blockchain system is a decentralized system that validates transactions by consensus.

This Bitcoin network has been copied and updated by many crypto enthusiasts to create several cryptocurrencies, known as altcoins, the most popular are: Bitcoin Cash (BCH), Ethereum (ETH), Dogecoin (DOGE), Litecoin (LTC), Ripple (XRP)...
After this popularization of altcoins, governments, and companies began to think about this technology more deeply, and the media beat announced that Blockchain is the real invention and not Bitcoin, which pushed companies and governments to look for other uses of the technology.
Figure 3.1, presents the different icons used to illustrate the altcoins mentioned above.



Figure 3.1 – Icons of some existing altcoins

3.1.1 History of Blockchain

The first study on cryptographically secure Blockchains was described in 1991 by Stuart Haber and W.Scott Storentta. They wanted to implement a system where the time-stamped documents could not be falsified or backdated.

In 1992, Bayer Haber and Storentta incorporated the Merkle tree concept into the system, which improved its accuracy by allowing several documents to be assembled into a single block.

The first mined block was in 2009 as the main component of digital currency BTC, developed by an unknown under the pseudonym Satoshi Nakamoto[28] (the first to apply a decentralized Blockchain), where it serves as a public registry for all network transactions. Figure 3.2 presents the history of Blockchain.

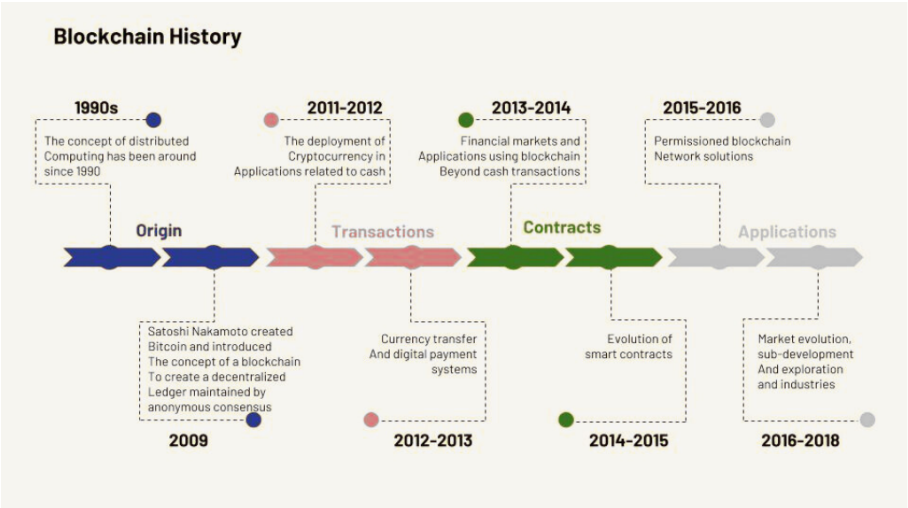

Figure 3.2 – History of Blockchain

3.1.2 Types of Blockchain

— **Public Blockchain**:

Public Blockchains are open to everyone, they can be assimilated to a public accounting ledger, without access restriction: any user can make transactions or participate in block approval at any time. There is no need for trusted third parties.

We can cite an example of this type: BTC, ETH...

The question here is since we don't need a trusted third party that is responsible for decision-making, how are those decisions made?

The answer is thanks to decentralized consensus algorithms, which we will explain later.

— **Private Blockchain:**

In contrast, a private blockchain, as its name suggests, relies on a single person who owns the Blockchain and sets its rules.

In private Blockchains, it is necessary to obtain authorization to carry out a transaction, but the reading may be public.

— **Consortium Blockchain:**

or Hybrid Blockchain combines the characteristics of public and private blockchains: the decisions are made by a limited number of nodes and the reading can be public or private. Users of this type can run a node and start mining, which can generate transactions in the string and control the string using an explorer Blockchain.

Table 3.1 summarizes the existing types of Blockchain and their use cases, as well as some examples.

3.1.3 The Operating principle behind Blockchain technology

Blockchain technology refers to a particular distributed data structure, as well as a protocol that allows the evolution of this data structure. Therefore, it ensures the transmission of information through multiple nodes of a network. Their particularity is that they do not rely on a particular control body. Notably, and unlike conventional systems, Blockchains are constructed in such a way, as to trust the nodes that run the

Table 3.1 – Types of Blockchain

Types	Designation
Public	Available to everybody to participate in the process of validation of transactions and data, it can be used when high transparency is required. Ex Bitcoin, Ethereum.
Private	Alternatively, permissioned Blockchain (not decentralized), this type is designed for the group who has the right to validate transactions it can be used when high privacy and security are required. Ex Hyperledger, Corda.
Hybrid	This type is a mixture between the public and private Blockchain, Ex Ripple network, and XRP token.
Consortium	Also known as Federated Blockchain this validates the transaction and also initiates or receives transactions. Used especially on businesses, payment processors, and banks. Ex Multichain and Tendermint.

system.

The data structure is divided into blocks, which are created at regular intervals and added to the Blockchain. A block contains headers, along with a list of transactions, which represent the atomic changes in the state of the Blockchain. Figure 3.3 describes the Block representation of the Blockchain.

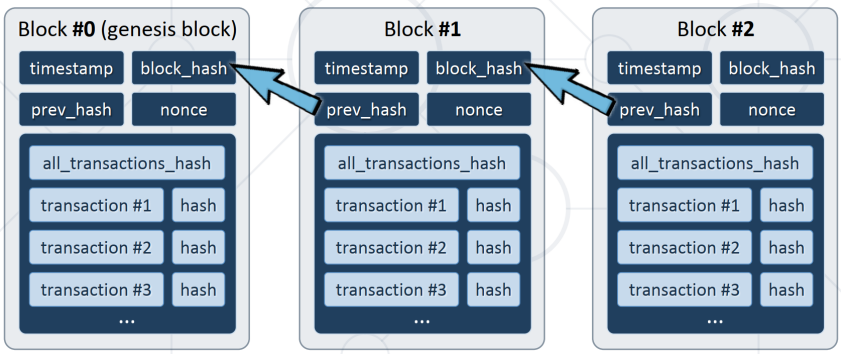

Figure 3.3 – Block representation of Blockchain

As presented in Figure 3.3, each block is cryptographically linked to the next by its hash, after validation following a consensus process. This process ensures that no information can be falsified. Indeed, if a user tries to modify a block already propagated in the network, its hash will change. As this hash value is found in all of the following blocks, the user must satisfy the rules of the consensus protocol for all these blocks, which requires significant resources.

As an example, Figure 3.4 illustrates the working principle of sending transaction from A to B, while the other nodes verify the transaction [35].

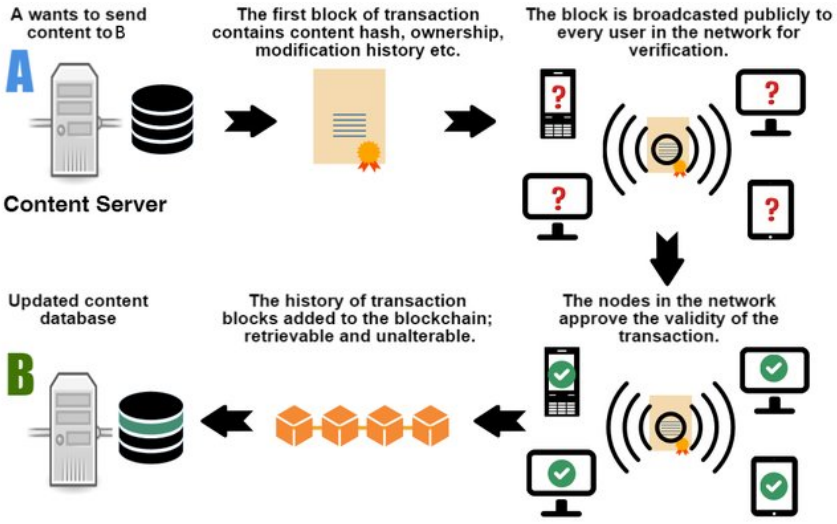

Figure 3.4 – Operating principle of Blockchain Technology
source: doi: 10.13140/RG.2.2.22132.63368

Blockchains allow a community of users to record transactions in a public registry for that community, so no transaction can be edited once published. The new blocks validated are replicated in all copies of the registry of that community, and any conflict is resolved automatically according to established rules.
Thus, this emerging technology forms a decentralized ecosystem of applications having interesting properties: transparency of transactions, auditability of applications by any user, or even resistance to censorship [36]. Decentralized applications that integrate Blockchain technology to take advantage of these properties are often referred to as Decentralized Applications Decentralized Applications (DApps) [37].

3.1.4 What constitutes a Blockchain

1. Transaction Platform:

   Transactions are validated by consensus. This is a community-denied principle for decision-making. Transactions are validated by consensus. This is a community-denied principle for decision-making. All the transactions are registered on the blockchain, so it is easy to be able to view the archives of the transactions operated on the Blockchain.

2. P2P network:

   A network where nodes can perform transactions directly between them. No intermediary intervenes in the transaction to verify and validate it [38], it is the community that takes care of it through the mining principle (which we will detail below).

3. Decentralized network:

   A blockchain is composed of all users (computers) connected to the network which stores the blockchain history on their server. They process the data by following the guidelines for the consensus protocol that is available to all members[39].

   Figure 3.5 illustrates the difference between centralized and decentralized architectures.

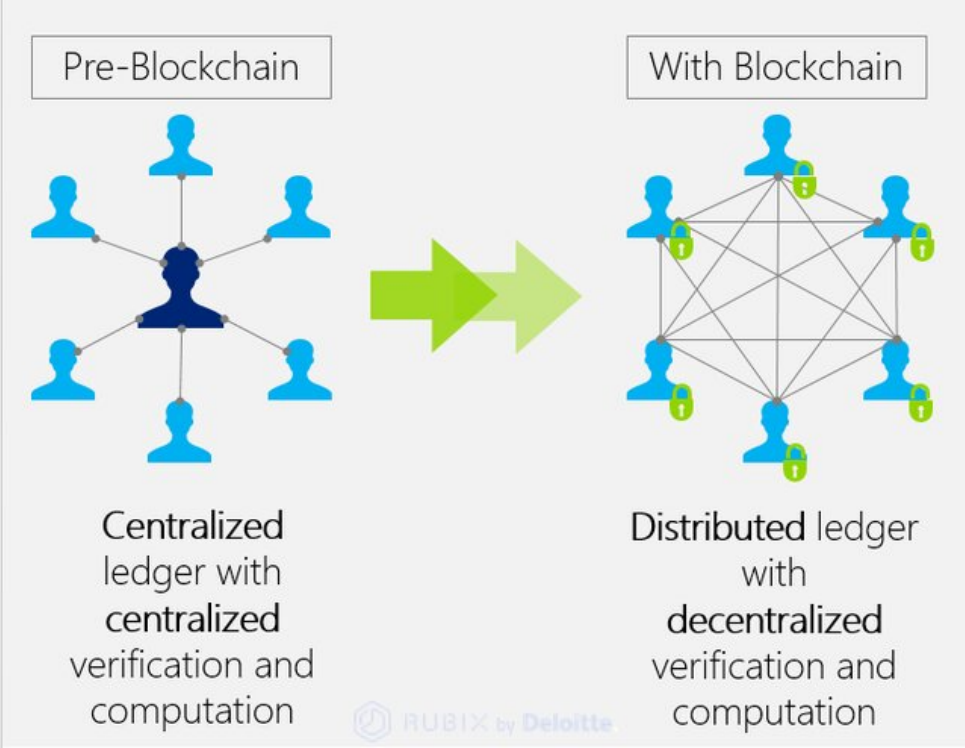

Figure 3.5 – Difference between centralized and decentralized architecture
source: doi: 10.13140/RG.2.2.14730.29127

4. Distributed ledger:

   Blockchain is a publicly distributed register where transactions are timed. Thus everyone can control transactions and avoid the problem of double spending based on the principle of Byzantine generals (explained below). It prevents you from

spending 2 times a token (that is to say spending one token that I would no longer hold)[40].

5. Consensus Algorithms:

   A consensus algorithm can be defined as the mechanism by which a network Blockchain reaches a consensus. Public Blockchains are built as distributed systems and, since they do not depend on a central authority, distributed nodes must agree on the validity of the transactions. This is where the algorithms of consensus come into play. their role is to ensure that protocol rules are respected and that all transactions politely take place so that the coin can only be spent once.

   Types Of Consensus Algorithms:

   Below is a brief description of the most popular consensus algorithms:

(a) - Proof of Work (PoW): In blockchain networks, Proof of Work is a consensus method where miners solve complex mathematical puzzles to validate transactions and create new blocks. This process demands a significant amount of computational effort, guaranteeing the security and integrity of the blockchain by making it computationally impossible for malicious actors to alter transaction history[28].

(b) - Proof of Stake (PoS): with Pos nodes are no longer selected for their computational power, but rather for their ability to offer blocks. Instead, if a user wants to be able to offer blocks to the rest of the network, they have to block a certain amount of cryptocurrency called 'token', which they can recover when they no longer want to produce blocks [41].

   Figure 3.6, outlines the different consensus algorithms that are available.

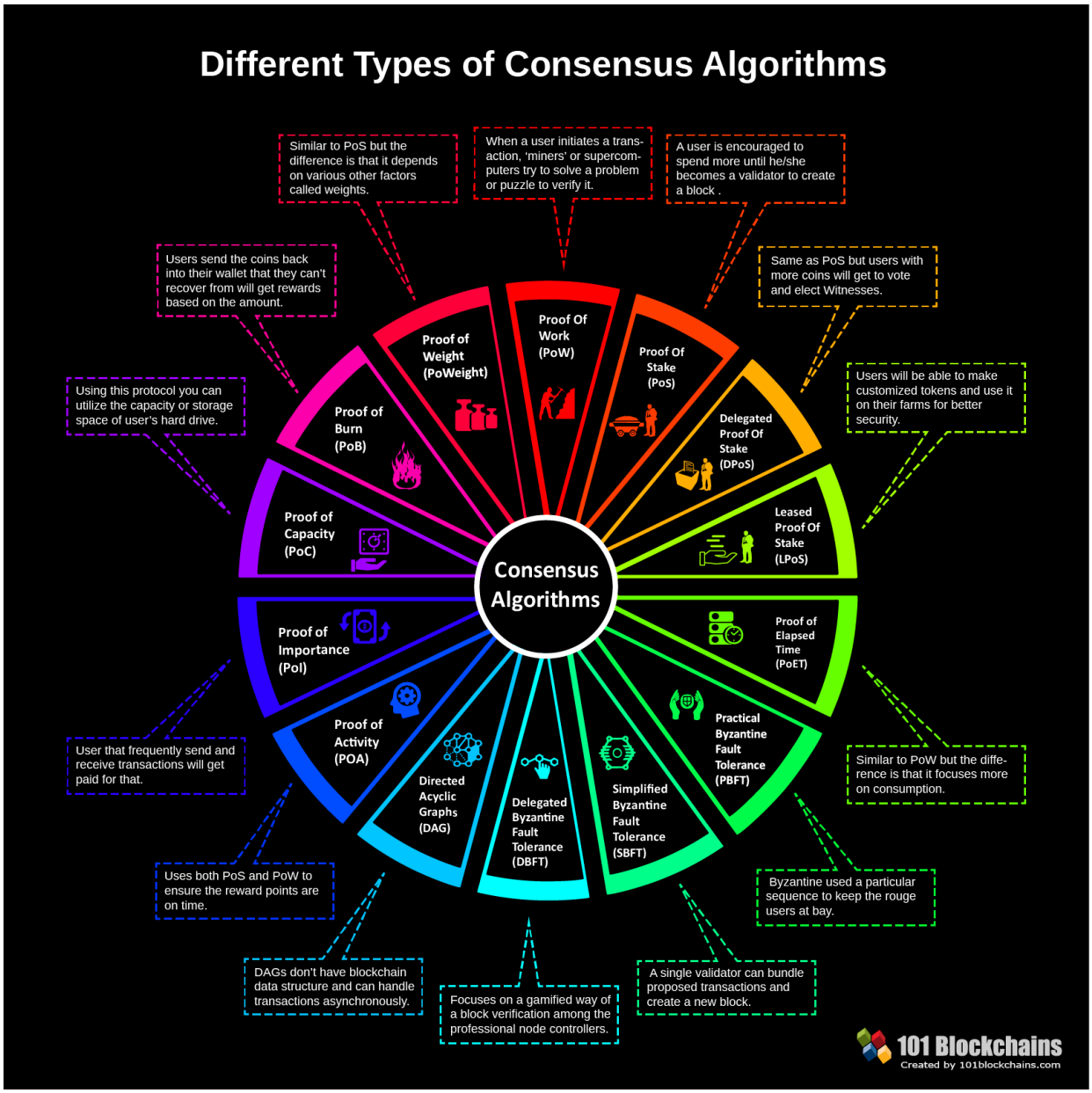

Figure 3.6 – Different types Of Consensus Algorithms
source: https://101blockchains.com/consensus-algorithms-blockchain/

6. Token:

   A cryptocurrency or token, like bitcoin or ether. It is a cryptocurrency that is used as a means of remuneration to incite minors (individuals who validate transactions by providing their computing resources) and pay the operating costs of smart contracts (autonomous contracts developed on the blockchain Ethereum that we will explain later).

7. Private / Public Key:

   Each user has a private key that allows him to access his account and a public key that is the address of his account. To receive a transaction on the blockchain, you must communicate your public key. The identity of the person appears in the form of a nickname on the network. If someone loses their private key, they can't access their account.

8. Mining:

   Blockchain technology needs servers to work. The latter are called minors. The role is to determine the information. The process of validating each transaction consists of solving an algorithmic problem associated with hash algorithms of the type: SHA-256.[42] Every miner who participates in the transaction validation by providing valid information is remunerated by cryptocurrency. It can be converted into currency such as the euro or the dollar. Those intermediaries that allow the ability of the recorded data are thus motivated by remuneration ensuring the proper functioning of the Blockchain. The mining system replaces the trust intermediary that was initially a denied institution (Bank, insurance companies, notary, etc).

9. Smart Contracts:

   In addition to the decentralized transfer of monetary value by cryptocurrencies, Blockchains can also act as information logs, which can, for example, manage a person's identity and authentications.

   Another feature of some Blockchains is the ability to run programs on the Blockchain. These programs are called "smart contracts", and their execution has the same properties as other transactions: immutability, traceability, and reliability.

   This concept was initially proposed in 1997 by Nick Szabo [43]. In 2014 Vitalik

Buterin introduced Ethereum [44], the first blockchain dedicated to smart contracts. Hyperledger Fabric[45] is another example of such Blockchains, driven by International Business Machines Corporation (IBM) and the Hyperledger consortium of the Linux Foundation.

The latter is a private Blockchain, which means that the consensus algorithm used is based on the trust that users have in the network administrators. Thus, executing a smart contract on Hyperledger Fabric is not decentralized, unlike an Ethereum smart contract. Other technologies in the category of distributed registers, or Distributed Ledger Technologies (DLT), of which Blockchains are part, can offer smart contracts. Authors in [46], present the different types of DLTthat exist today.

3.2 Technology choices

This section presents a detailed description of technologies and tools used to implement Blockchain-based data-sharing systems, proposed in the next chapters of this thesis.

3.2.1 Blockchain Technology

Recalling, Blockchain is a new technology where data is structured on a Cryptographically linked list of blocks. Those blocks contain the list of transactions. This technology is ideal for providing a ledger accessible by permission users on the network.

A hash is generated using a Cryptographic hash algorithm, identifying each block in the Blockchain. Each block possesses the hash of its parent block inside of its own header [47].

In other words, the Blockchain could be considered a ledger of transactions that combine: a P2P network, consensus protocol, hashing algorithms, and decentralized system architecture. All of these technologies are combined together to ensure a secure environment to share or store data with the guarantee of:

— Transparency: data are accessible to all participants within the Blockchain network;

— Immutability: once the data/transactions are stored on the Blockchain they cannot be altered or deleted;
— Consistency: data are visible to all future data manipulation ;
— Equal rights: due to disintermediation, every node on the network has the same rights to manipulate and access the network;
— Availability: every participant may host a full replica of the Blockchain data and the data are available as long as the least node is in the Blockchain network[48].

In traditional transfer operations, we usually spend efforts on duplicated record keeping, also a third-party institution has to ensure validations. In that case, database systems may be susceptible to fraud and cyber-attack risks. As well as the arrival of transactions that concerned Internet Of Things (IoT), the volume of these transactions has exploded. All of these business requirements may enter the Blockchain Technology. In our use case, we are using the Ethereum Blockchain which will be explained below.

3.2.2 Ethereum Blockchain

The Ethereum Blockchain was launched in 2015 by Vitalik Buterin, a former programmer of Bitcoin having decided to launch his own Blockchain. He found some applications were lacking in Bitcoin including the concept of smart contracts (which will be explained in depth afterward).

The currency used on Ethereum is Ether (ETH). At its launch in 2015, 60 million Ethers were issued and sold for Bitcoins, and 12 million were distributed to developers. The platform issues five Ehters at each mine which are paid to the miners.

Compared to Bitcoin, the mining time is much less, it is 15 seconds. Many start-ups have launched using this Blockchain as their main support. These companies were seduced by the smart contracts principle available on Ethereum. These are contracts between two individuals that operate based on an autonomous program governed according to the criteria and conditions indicated.

On Ethereum, virtual currency is used to run smart contracts. The Ethers are used to pay for the performance of contracts and to pay the miners who process the transactions. Each operation mined on Ethereum consumes what is called gas that corresponds to the

computing power required to mine the transaction. This resource converts to Ether. A medium-sized transaction costs about 21 thousand gases. The minor can choose whether or not to process a transaction based on their remuneration. A user has the right to increase his gas more to allow faster processing of his contract. However, when he no longer has gas the smart contract no longer works. The amount of gas required for a transaction depends on the computing power required for processing the operation. Conversely, the gas price is determined according to the price of Ether. These two variables therefore change according to different criteria which helps adjust the market [49].

3.2.3 Hashing Algorithms

This technology is the ledger of transactions, that uses the asymmetrical cryptography that appeared with DifeHellman in 1976, which works with a pair of keys, one public and the other private, linked together by an elliptical curve algorithm. The public key is releasable and allows receiving transactions, while the private key is kept on a secret. As long as we have the list of digital signatures when user A sends a transaction to user B, he is digitally signing a hash of the previous transaction and the public key of the next user. This system serves to verify the chain of ownership [28].

3.2.4 IPFS protocol

The interplanetary file system is a protocol designed to store and access files in a peer-to-peer decentralized and distributed file system. Basically, Interplanetary File System (IPFS) is a peer-to-peer, open source, content addressable globally that can be used for storing and sharing large volumes of files with high throughput[48]. It stores pieces of data on several nodes on the IPFS network, which can be accessed with an unchangeable address. This depends on the content to which these addresses refer, in our use case study it refers to the hash of the document.

While IPFS is a P2P distributed file system, so there is no central server. Users on this network called clients, represent the nodes of the network and need a way to be identified by the other nodes. If you just assign nodes with numbers like 1,2,3... anybody can add a node with an existing ID and claim to be that node.

To prevent that some cryptography is needed. In that case, nodes are identified like this:

— Generate a key pair (public-private);

— Hash the public key;

— The resulting hash is the node ID[50].

3.2.5 Smart Contracts

Recalling, To speed up transactions on Blockchain, a set of rules called “smart contracts”, written using a programming language called “solidity”, are stored on the Ethereum Blockchain and executed automatically. Those smart contracts can define conditions for corporate bond transfers, include terms for travel insurance to be paid and so much more, they provide the ability to execute codes that implement business logic to the Blockchain[51].

Smart contracts minimize the risk of fraud and errors, streamline procedures, and guarantee predictable and dependable contract execution by eliminating the need for middlemen. They also provide increased transparency, lower costs, and improved security.

Key Features of Smart Contracts:

— Automation:

Once deployed, Smart contracts take specified actions on their own when certain criteria are satisfied.

— Immutability:

The code of a smart contract cannot be altered after it is deployed on the blockchain, ensuring integrity and trust.

— Transparency:

The terms and execution of the contract are visible to all parties involved, enhancing transparency.

— Decentralization:

Smart contracts operate on decentralized networks, reducing reliance on central authorities.

The use of smart contracts can be applied in different industries, including different industries, including :

- Finance;
- Supply Chain management;
- Healthcare;
- Legal [52].

3.2.6 Solidity Language:

Solidity is an advanced programming language that is specifically designed for writing smart contracts on the Ethereum blockchain. It was created by Gavin Wood, Christian Reitwiessner, and other Ethereum project contributors. Solidity is a powerful language for creating sophisticated smart contracts due to its statically typed nature, inheritance, libraries, and complex user-defined types.

In other words, Solidity is :

— Statically Typed:

Ensures that types of all variables are known at compile-time, reducing runtime errors.

— Object-Oriented:

Supports concepts like inheritance and polymorphism, facilitating the development of complex contracts.

— Ethereum Virtual Machine (EVM) Compatibility:

Solidity code is compiled into bytecode that runs on the EVM, ensuring seamless deployment on the Ethereum network.

— Libraries and Inheritance:

Enables code reuse and modularity, promoting efficient contract development.

The integration of the InterPlanetary File System (IPFS), blockchain (BC), and smart contracts presents a robust framework for secure, decentralized, and efficient systems. These technologies complement each other by leveraging their unique strengths, offering a wide range of benefits across various applications. These are the main benefits of the combination of these technologies :

1. Enhanced Data Storage and Accessibility;
2. Improved Security and Integrity;
3. Smart Contract Automation and Efficiency;
4. Decentralization and Censorship Resistance;
5. Cost-Effective and Scalable Solutions.

3.3 Software and Platforms used for deployment

This section will identify the various software and tools platforms used for deploying the proposed data-sharing systems.

Ganache-Cli: This tool serves as a Blockchain client for connecting to the network [53]. 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. When creating a new workspace, this tool provides automatically a list of 10 virtual accounts for deployment and test purposes. Figure 3.7 represents the home interface of Ganache-Cli.

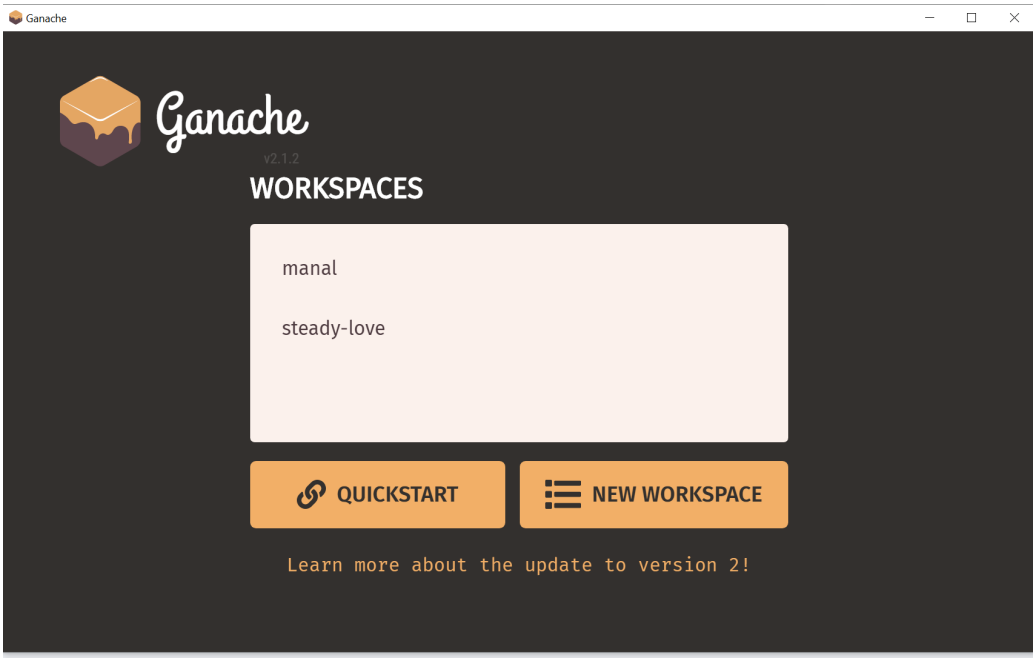

Figure 3.7 – Home Interface of Ganache-cli

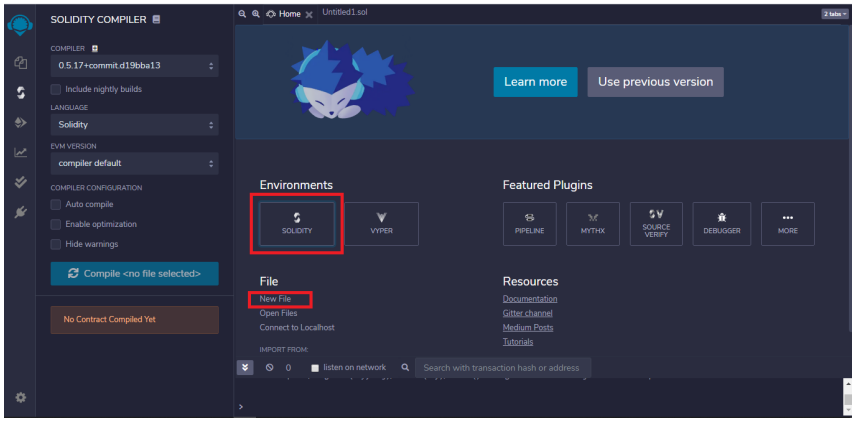

Figure 3.8 – Screen of the Home interface of Remix IDE platform

Remix IDE: 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 [54]. Figure 3.8 illustrates the home interface of Remix IDE.

Web3 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 [55]. Figure 3.9 illustrates the difference between web 3 and Web 2.

Truffle Truffle serves as a development environment, testing framework, and asset pipeline designed specifically for Ethereum[56]. It is a front-end tool, used to deploy and compile smart contracts and insert them into the web application.

Node js 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 [57].

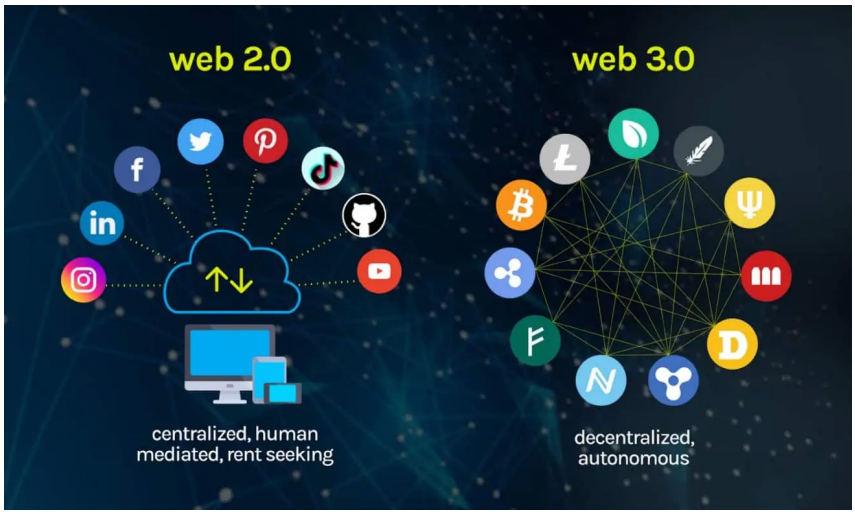

Figure 3.9 – Difference between web 2 and web 3

Meta Mask The MetaMask tool is a cryptographic portfolio and a gateway for applications based on Ethereum Blockchain, available as a web extension. Metamask allows users to manage their Ethereum accounts, store tokens, and run Decentralized Applications (Dapps) without being a real Ethereum Node (in virtual mode) [58]. In addition, it's used to generate accounts to hold Ethers that will be used for smart contracts deployment.

Figure 3.10 describes the Metamask tool extension.

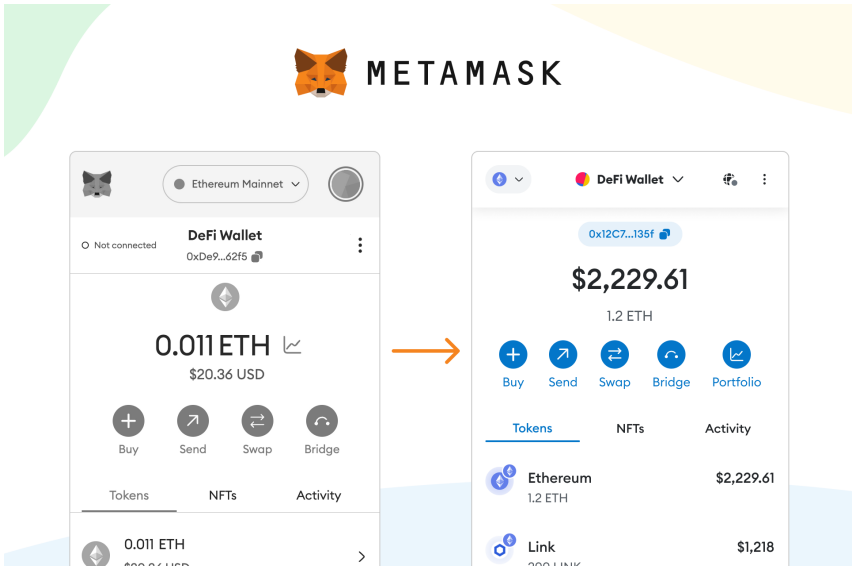

Figure 3.10 – Representation of the Metamask Extention

Concerning the Application Programming Interface (API) integration, web3.js libraries were used to ensure the interactions between smart contracts and the Blockchain network with the mobile application.

3.4 Blockchain in E-government

Governments worldwide are exploring and implementing blockchain solutions in various applications to improve public services and governance. The decentralized, immutable, and transparent qualities of Blockchain technology are revolutionizing the public sector by enhancing:

1. Transparency and Accountability such as:
   - Voting Systems:

     Secure and transparent voting systems are being created through the use of Blockchain technology. The integrity of elections is maintained by these systems by providing a tamper-proof ledger of votes that is accessible to any participant and can be audited. [59] .

     As for example the country of ESTONIA has explored Blockchain technology to secure its online voting system, which enables citizens to vote from anywhere with high levels of security;
   - Public Records Management:

     Blockchain has the potential to transform the management of public records, including land registries, birth certificates, and other important documents. Blockchain can be used to store records in a decentralized manner, which reduces the risk of fraud and ensures their immutability.

     Sweden, for instance, has implemented a Blockchain-based land registry to streamline property transactions and enhance security [60].
   - Supply Chain Transparency:

     In public procurement and the distribution of goods, governments are using Blockchain to improve transparency and traceability of supply chains. This is a way to prevent corruption and ensure that goods are sourced ethically and delivered efficiently. For instance, The United Nations World Food Program (WFP) has employed Blockchain technology to track food distribution to refugees, making sure that aid is delivered to its intended recipients [61].
2. Efficiency and Reducing Costs :
   - Identity Management:

A Blockchain-based digital identity system can make the process of identity verification more secure and efficient. These systems allow citizens to have a unified digital identity that can be used across all government services. The ID2020 initiative is an example of how blockchain can be used to provide digital identities and improve access to services for underserved populations.[62].

— Tax Collection and Compliance:

Blockchain can simplify tax collection and improve compliance by allowing financial transactions to be transparent. This has the potential to reduce tax evasion and ensure tax collection efficiency.

As a model, The Australian Taxation Office has explored the use of Blockchain to streamline tax reporting and reduce administrative burdens [63].

— Smart Contracts for Government Services:

Smart contracts, which are contracts that execute themselves and have their terms written in code, have the ability to automate a range of government processes. This is capable of reducing paperwork, speeding up transactions, and decreasing administrative costs. As proof, the Dubai Government has implemented SC to automate SCand streamline its government services as part of its Blockchain Strategy [64].

3. Security and data integrity:

— Cybersecurity:

The decentralized nature of Blockchain can enhance cybersecurity by decreasing the risk of a single point of failure. Hence, Blockchain is an effective tool for governments to secure sensitive data and protect critical infrastructure from cyberattacks [65].

— Healthcare Data Management:

Patient records can be accurately and tamper-proof thanks to Blockchain's ability to secure and manage healthcare data. This can improve patient care by providing healthcare providers with reliable access to medical records [66].

Adopting blockchain technology in public administration systems offers significant benefits, but it also faces various barriers that hinder its widespread implementation.

These barriers include:

1. Technical Challenges:
   — Integration Complexity: It can be technically challenging to integrate blockchain with legacy systems that currently exist, necessitating major adjustments to the current IT infrastructure;
   — Energy Consumption: Certain blockchain protocols, such as Proof-of-Work (PoW), have high energy consumption, which might conflict with public administration's sustainability objectives.
2. Lack of Skilled Professionals:
   Blockchain development and implementation require expertise in cryptography, distributed systems, and smart contracts. The shortage of skilled personnel in these areas slows adoption.
3. Legal and Regulatory Barriers:
   — Unclear Regulations: Many governments lack comprehensive legal frameworks for blockchain technology, creating uncertainty about its legal status and application in public administration;
   — Data Privacy Concerns: Storing sensitive personal or governmental data on a blockchain may conflict with data protection regulations like GDPR or similar laws in other regions.
4. Financial Constraints:
   — High Initial Costs: Implementing blockchain involves significant upfront investment in infrastructure, training, and development;
   — Cost of Transition: Migrating from traditional systems to blockchain-based systems is expensive and time-consuming, creating a barrier for resource-constrained administrations.
5. Interoperability and Standardization:
   — Lack of Standards: There are no universally accepted standards for blockchain, making it difficult for systems from different organizations to interoperate;
   — Fragmentation of Solutions: Different organizations may adopt incompatible blockchain platforms, creating silos instead of seamless integration.

6. Organizational Resistance:
   — Lack of Awareness: Decision-makers and public administration employees may lack understanding of blockchain technology and its benefits.
   — Cultural Resistance: Resistance to change within bureaucratic systems can slow the adoption of innovative technologies like blockchain.
   — Trust Issues: Public administrators might be hesitant to trust decentralized systems over centralized control.

In order to get past these obstacles, governments need to put a high priority on raising awareness, establishing laws that support it, funding research and development, and encouraging cooperation between the public, commercial, and academic sectors.

Chapter 4 will discuss improving traceability in E-governance systems for data sharing.

CHAPTER

4

IMPROVING TRACEABILITY IN E-GOVERNANCE FILE-SHARING SYSTEMS

In this Chapter, we present a case study that proposes a new architecture for the system used by the Moroccan Ministry of Justice, which is a file-sharing system based on Blockchain technology, IPFS, and smart contracts to manage data sharing in a decentralized, trusted, and secured environment exchange.
This system architecture's aim is to exceed the traditional centralized data-sharing platform's problems and guarantee the persistency, auditability, scalability, and traceability of data, as well as the elimination of the third party. In this way, the new architecture proposed will be an outstanding revolution for the Ministry of Justice and so on for the E-governance In Morocco.

4.1 Introduction

E-governance may be defined as the use of the information and communication technologies in order to enhance all of the Government's procedures and processes since E-governance can make a change in the manner of how the relationship is between citizens and Government [67] in such a world where a huge revolution is occurring. The use of the internet, computers, and mobile phones has become a fundamental issue for living. It is affecting our lifestyle. Governments around the world are recognizing the value of E-Governance, thanks to its many privileges like improving the quality and availability of public services, increasing democratic participation, significant cost reduction, and greater transparency of the institutions also reducing the execution time[68]. With the aim of providing efficient dissemination and management of information to the citizen, a better service delivery, and pushing the citizens to contribute to public and policy decision-making, E-governance is a wider concept that defines and assesses the impacts of technologies on the practice of government administrations and their relationship between the public servants and the society.

Modernization of the administration also involves the use of new technologies to facilitate citizen's access to basic services and reduce administrative expenses for the administration. In Morocco, public sector expenditures represent a significant share of the state budget. Through the implementation of e-government services that streamline and automate information processing, this area is expected to achieve significant efficiencies.

Moreover, with the same context of making the public services more closely to citizens, we find a set of programs of E-governance launched by the Government of Morocco:

- The E-government program in 2009;
- Digital Morocco Plan in 2013;
- Digital Morocco Plan in 2020.

Those programs were launched with the aim of providing new requirements of availability, simplicity, and efficiency of the different services presented by the public administrations for the benefit of the citizens. Furthermore, the Agency for Digital Development (ADD) was founded in 2007, with the objective of fostering the digitalization process by creating an ecosystem and facilitating the necessary conditions.

At the same time, the world is doing much to mitigate the impacts of the pandemic coronavirus. It has upset the work patterns, organizational structures, and decision-making support tools. It pushed public administrations to strengthen their investment in Information System (IT) to digitalize their systems. These are therefore new challenges for management controllers to cope with the emergency caused by the pandemic of COVID-19, to provide the appropriate tools for ensuring continuity of work through teleworking. Thus indirectly participating in the digitalization of public administrations.

The Ministry of Justice in Morocco was among the first government organizations to adopt this digital transformation program. This participation of the said sector plays a key role in achieving the most desired goals. Improving the services provided by the ministry and its various entities, not only the judicial services such as jurisprudence, providing the service of downloading digital court decisions, improving the efficiency of the judiciary sector, enhancing the judicial services, facilitating the judicial access and streamlining the judiciary's time management. But also by initiating many researches to improve the social services provided by the ministry and its entities to its staff, an example, managing the operation of reservation of stay of the ministry staff in the summer resorts, which is affiliated with the Mohammedia Foundation for the social works of judges and justice officials in Morocco[69].

To achieve these goals, the Ministry has set up an emergent information system to manage the communications and the information sharing between all the users and the

stakeholders such as citizens, lawyers, notaries, experts, and the security sector. In parallel with the Ministry of Justice, we find the Supreme Council of the Judicial Power (SCJP) and the Presidency of the Public Prosecution (PPP), which seem of being connected to each other while they represent the most frequented government organizations by citizens and comprise the most complex system. They are directly related to the Ministry of Justice. All of those entities are considered to be a key Moroccan component of the e-Governance initiative.

Prior to 2017, both the SCJP and the PPP operated under the Ministry of Justice as sub-departments, and they shared a data center that relied on the Ministry of Justice. Essentially, the Minister of Justice was in charge of these departments.

Historically, the journey of the jury file followed this sequence: it starts with the SCJP, which initiates a claim or a judicial file. After the SCJP concludes its investigative procedures concerning the file, it transfers the file to the appropriate court to proceed with its legal proceedings. In certain cases, the SCJP may intervene. The advantage of having these departments interconnected and sharing a common data center is that it makes the management of court files exceptionally flexible.

Since October 2017, the Ministry of Justice, the Supreme Council of the Judicial Power, and the Presidency of the Public Prosecution were separated. Following the separation of departments, both SCJP and PPP are no longer under the direct command of the Minister of Justice. The power and authority have been distributed, and each entity now operates independently, managing its own affairs. In this situation, they function autonomously. However, they continue to collaborate on the same cases simultaneously. Under those circumstances, it has become vital to address one of the system's primary issues: data management and data interoperability.

The file-sharing process between those entities becomes more difficult and complex due to the many steps involved, which represents a significant issue for such a system; therefore, it affects the interaction between those principal organizations and consequently reduces the performance of the system. In reality, it decreases the quality of the decision-making process. Furthermore, the system becomes incapable of managing the file sharing between those entities, consequently, the time process of the judicial cases is increasing

day after day, which represents a noticeable trouble for the E-governance initiative.

Authors in [70] confirmed that Data Interoperability affects an organization's performance and is a major concern for Moroccan judicial entities utilizing big data technologies. The variety of data they manage the heterogeneity of E-Government development, the large amount of data, the interactions between different datasets, and the dynamic nature of the data all add to the challenge of creating seamless interoperability. The solution proposed is a data interoperability framework for e-governance based on warehousing technology. The case of the justice system is to help establish legal and judicial security by providing an easy-to-use database (centralized system) of jurisprudence and various legislative texts.

The goal of this study is to propose a new decentralized file-sharing system architecture based on Blockchain technology, IPFS, and smart contracts, to fix the issues mentioned above, by improving the flexibility, data interoperability, data security, and availability of the file-sharing process between the different users, especially after the separation of those three entities.

4.2 State of the Art

This section discusses existing systems that use Blockchain technology,IPFS, and smart contracts to secure data exchange between multiple parties.
The "Governance" word refers to the process by which the government operates itself. Using digital technologies, which are involved indirectly in our lifestyle in the communication between the citizens and the state, has given rise to what we call "E-Governance"[71].

So assessing good governance within a country involves analyzing indicators that enable the assessment of its primary manifestations, the existing structure and institutional arrangements, as well as the implementation processes. For this reason, and to ensure the country's successful entry into the digital era, the Moroccan government has identified three key challenges that aim to ensure the integrated development of digital encompassing both social and economic aspects. The essence of these three keys can be summarized as follows:

- Improving the quality of interactions between users and administrations (Smart

Government);

- The creation of a digital ecosystem that promotes innovation in the digital sector and the competitiveness of companies;
- Social inclusion and reduction of social inequalities[72].

Currently, at the operational level, Morocco possesses several electronic platforms, some of them has been developed during the Covid-19 pandemic period and the closure of public spaces during the lockdown, which helped to highlight the importance of electronic equipment and remote work applications. In this context, some examples include:

- the Ministry of Justice website and the courts' portal "mahakim.ma";
- the creation of a national system for digital administration "idarati.ma";
- Creation of a public services portal "service-public.ma";
- the platform "Chikaya" for receiving grievances from citizens;
- the national window of foreign trade procedures "PortNet";
- A platform for digitizing transactions, such as filing declarations and payments of tax "tax.gov.ma";
- the platform "Liqahcorona", for making appointments and monitoring the operation of vaccination against the Covid19;
- The platform "TelmidTICE" and the platform "SoutienSco" offer study support and e-learning opportunities for students.

The pandemic (covid-19) has also enhanced the challenges of digitization of public services[73]. Taking everything into account, Morocco has experienced a gradual improvement in its international e-governance ranking. In the Digital Commitment Report (DCR), it secured the fourth position in the Middle East and North Africa region, while in the Digital Developement Index (DEI), it attained the second position among all African countries. In the UN E-Government Development Index (EGDI), Morocco has shown notable progress in its ranking. In 2008, it held the 140th position with a score of 40.29, but by 2022, it had advanced to the 101st position with an improved score of 0.591[74] The remarkable advancement can be attributed to substantial growth across various indices contributing to e-governance. Specifically, the Online Services Index (OSI) experienced a notable increase, surging from 0.207 to 0.472 during the same period. Simi-

Table 4.1 – Evolution of e-government indices in Morocco for the last 10 years, source: The author, based on UN reports 2012-2022

	2012	2014	2016	2018	2020	2022
HCI	0.443	0.49	0.473	0.527	0.527	0.635
EGD	0.42	0.505	0.518	0.521	0.572	0.591
TII	0.277	0.334	0.342	0.369	0.58	0.667
OSI	0.542	0.692	0.739	0.666	0.523	0.472
Ranking	120	82	85	110	106	101

lar improvements were observed in other crucial areas like the Telecommunication Infrastructure Index (TII) and Human Capital Index (HCI). A short view of this improvement is summarized in Table 4.1 .

When we say E-governance, we say a digital administration, where individuals and organizations are interacting directly or indirectly with the government. This communication includes document sharing via different platforms. Those documents may belong to the government or citizens, also the platforms could be unsecured, they may be shared with all kinds of users or limited to a certain segment of society.

The integrity and immutability of documents are essential to maintaining their goals. However, today's digital era presents new and urgent challenges to this immutability and confidence. Digital documents are produced in great volume. Their inviolability leaves them open to modification not only to tampering but also to degradation over longitudinal periods. For example, file formats become obsolete and documents are transcoded. How can we ensure that meaning is not lost? That was the general issue studied on the approach of ARCHANGEL Trusted Archives of Digital Public Documents [75]. The existence of DLT back in the 90's years, known for their potential in the provenance and integrity of data in a distributed network, they consolidate the Blockchain Technology Approach [76]. The Blockchain technology is dedicated to supporting information exchange and transactions that require authentication and trust [77].

The authors in [3] confirmed that Blockchain technology would lead to innovation and transformation of governmental processes and that the use of Blockchain technology in information sharing is more efficient. Storing information on the transactions in different nodes called, distributed ledgers, reduces the dependency on a central actor and the

risk of manipulation or system failure. In a similar project to our study, the authors in [78] presented an approach of a Blockchain-based file-sharing system for academic Paper Review that relies on Blockchain technology combined with IPFS to store large files in a distributed manner in order to reduce storage requirements in the user side, also that's guarantee data decentralization, immutability, and auditability.

In[79] authors confirmed that using a P2P file-sharing system contributes to reducing the cost of files stored and protected in a decentralized environment. The use of smart contracts plays a significant role in managing a Blockchain-based file-sharing system in a decentralized environment and deploying it in the Ethereum network[80].

Alternative methods suggest storing information regarding the authors or the shared dataset on the Blockchain. For instance, in [81], the authors choose to store dataset metadata to enhance traceability. Another research[82] proposed using a Blockchain-based approach to collect, validate, and track the metadata in a secure, immutable, and transparent infrastructure.

As a work extension, authors in [83] suggested a novel architecture for secure data sharing among untrusted actors without the need for a third-party authority. It utilizes a public Blockchain and Distributed File system (DFS) network (IPFS and Swarm) for storage to achieve complete decentralization, and to guarantee dataset access, integrity, and traceability.

We conclude that all these researchers head down on the same goal: using Blockchain technology combined with IPFS and SC in a file-sharing system is the best solution for the digitalization of public administrations taking into consideration the number of its benefits.

The aim of this research is to introduce a new architecture for a decentralized file-sharing system for the Ministry of Justice. This architecture uses three key technologies: Blockchain, IPFS, and SC. The proposed architecture aims to address the issues mentioned earlier. These issues could be related to the existing file-sharing system's limitations, such as centralized systems, lack of data interoperability, security vulnerabilities, and challenges in painting availability.

The study emphasizes that these improvements are particularly relevant following the

separation of the Supreme Council of the Judicial Power and the Presidency of the Public Prosecution from the main data center relevant to the Ministry of Justice, which likely refers to cases where traditional centralized systems involving middlemen or intermediaries are dismantled. In such cases, a decentralized approach becomes even more crucial to maintain a robust and efficient file-sharing system.

4.3 Background

With the successful trial of e-services provided by the Ministry of Justice during the sanitary emergency, an outstanding social demand for digital technology is occurring through software applications, e-services, and video conferencing courts... to improve the quality of these services provided by the ministry in an age where the number of users is increasing daily.

Figure 4.1 describes the different types of consumers in this sector.



Figure 4.1 – Users and stakeholders of the judiciary system

Our study focuses on information sharing and file sharing via the ministry's information system, especially between the three entities: the Ministry of Justice, the PPP, and SCJP before and after the separation of these entities.

Figure 4.2 represents the old architecture of the file-sharing system.

Since the independence of the country of Morocco, the judicial field has been under the

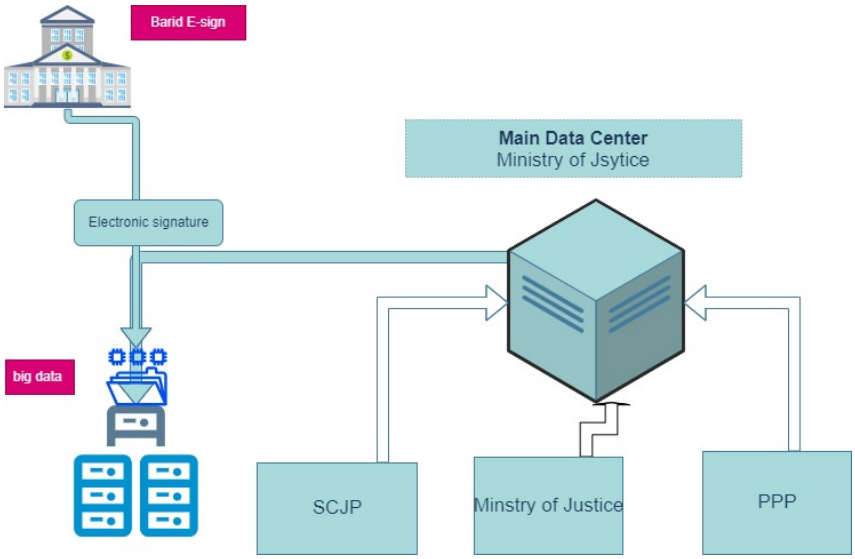

Figure 4.2 – Concept of old system's architecture (traditional architecture)

Ministry of Justice's authority, with all its departments. The main data center was the Ministry of Justice data center, and SCJP and the Presidency of the Public Prosecutor PPP were sub-departments that relay to the Ministry. Since we had a sole data center, all the data, or the big data was managed on it. Therefore, the problem is when those entities are separated from the ministry, the process of sharing information and files with the other entities that are: the PPP and the SCJP has become a big issue that makes the process of file treatment and judgment more difficult and consumes a lot of energy.

After the separation, how the data could be communicated between those three entities, noting that all these departments have a contribution to the data process or the decision-making? With attention to the huge number of users that have access to the current system and their different types: of employees or citizens, we found the ministry staff, (judges, clerks, and court clerks employees) and the external users like lawyers, notaries, and experts.

As shown in Figure 4.2, we found this external organization (Barid eSign), which represents the organization that contributes the electronic signature for the different governmental organizations among them, the Ministry of Justice. It's the one and only organization have the legal right to create certificates for electronic signatures and sell them to other organizations. To put it differently, the digital signature is the signature applied to all electronic documents as well as the handwritten signature on paper docu-

Table 4.2 – Number of electronic signature users

Function	number of users
Judges	4045
Employees	14179
Lawyers	12230
Training lawyers	1328
Notaries	4 679
Experts	3343
Qualified translators	287
Judicial commissioners	1654
Total	41745

ments. It must make it possible to authenticate the signatory and guarantee the integrity of a document. This signature is obtained using asymmetric encryption or hashing procedure. In our case, the Ministry of Justice, by using the electronic signature, aims to enhance the digital trust, by giving a legal authenticity to electronic documents issued by the different ministry departments, as well as facilitating the document's e-exchange in a secure and confidential environment.

To achieve these goals, a segment of users would need to possess those signatures. They will be applied in many use cases in the administrative process like signing a decision, adjudication, correspondence, and all the electronic shared files and data, between the employees of this domain. While this organization provides this service with money, due to the number of users for this signature whereof finding it very costly.

Table 4.2 describes the real number of users for electronic signatures.

According to Barid eSign, the price of the electronic signatures is specified at 150 dollars, considering the number of users mentioned in the table (table 4.2), we find the total cost for this service is an average of 6 261 750 dollars. As well as considering the lifetime of the talking service (it depends on the conditions of the selling contract) 3 months or 1 year on one hand, and annual users augmentation on the other hand.

In that case, we conclude that the use of this service is very costly for such a department of Government. Accordingly, the proposed architecture comes to resolve all of the mentioned issues, a decentralized sharing-files system based on Blockchain technology, IPFS, and smart contracts in order to ensure:

— data availability;

— data integrity (data is accessible at where and any time);

— data security (through hashing algorithms);

— zero-trust network (any need for a third party, no entity is empowered than the other);

— every node in the network has the same rights;

— no more need for an external organization to provide electronic signature service;

— data traceability;

4.4 Proposed Model

In this section, we describe the new solution proposed to improve the Ministry of Justice by proposing a new architecture for the file-sharing system based on Blockchain technology, IPFS protocol, and Smart Contracts under the Blockchain Ethereum environment.

Figure 4.3 represents the file storage and system-access processes. The proposed architecture is designed especially for the file-sharing system between the Ministry of Justice, the Supreme Council of the Judicial Power SCJP, and the Presidency of the Public Prosecution PPP.

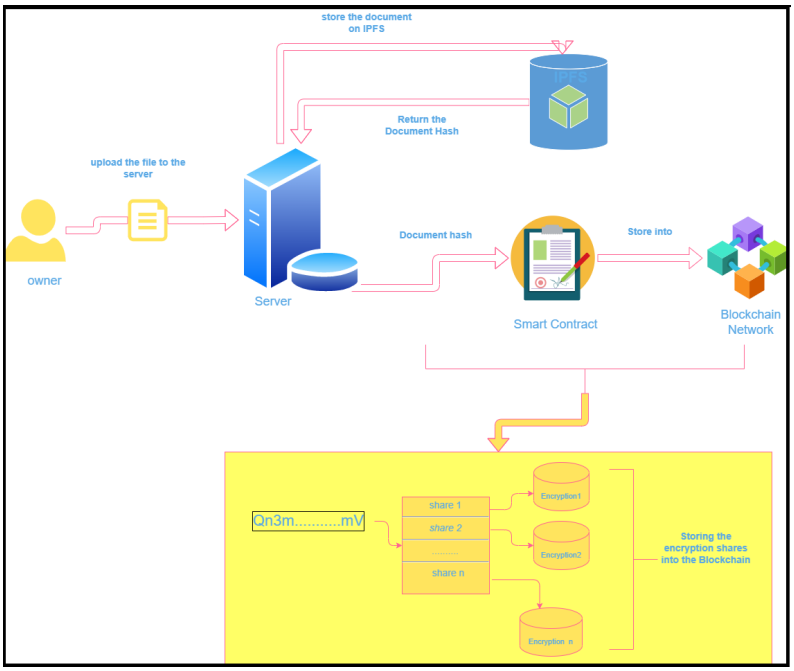

Figure 4.3 – New File sharing system Architecture

As presented in Figure 4.3, the user loads the document on the server. The document is stored on IPFS(whatever the document's type), and then the document's hash is generated. This one represents the key for document location on addressable content. The IPFS guarantees non-duplication of a document, addressed content (unique ID, as it is cryptographically generated), and a tamper-proof document. When the document's hash is generated, it will be stored on the Blockchain network (Figure 4.4) using a Smart Contract to allow traceability and authenticity. In that case, we can have access to documents using the hash generated. If a user changes one letter or character in that document a new hash will be generated and shows that the original document has been altered. All of these functionalities will be described in the rest of this section.

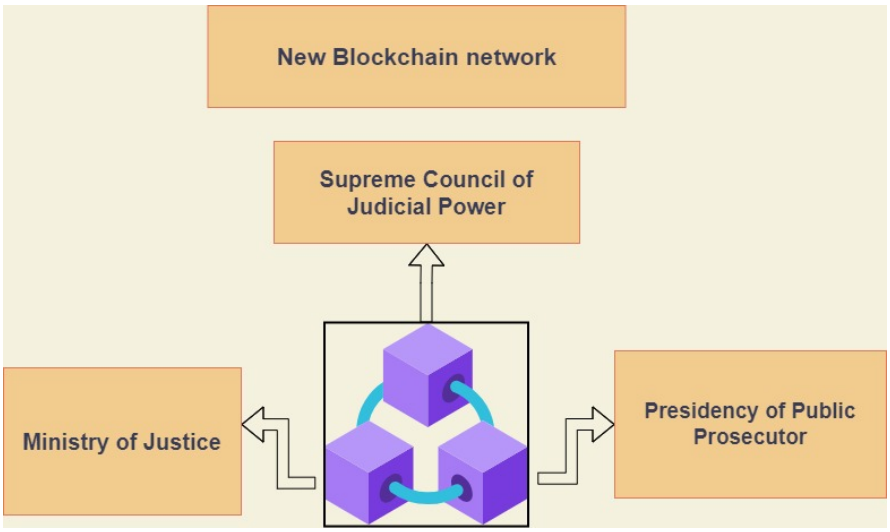

Figure 4.4 – Blockchain network (Blockchain-based architecture)

Figure 4.4 represents the Blockchain Network where the three entities (the Ministry of Justice, the Supreme Council of Judiciary Power, and the Presidency of the Public Prosecution) will be connected. Each entity represents a node on the network, for this reason, the data will be shared between users simultaneously, since Blockchain technology ensures the data distribution on all nodes at the same time. In that case, every user on the network will have access to data in (read/ write mode), as long as saving time process and ensuring transparency in data sharing.

4.5 Implementation and Challenges

4.5.1 System Design and Implementation

In Figure 4.5, we represent the scenario of the file uploading, described in Figure 4.3 . The user initiates a system connection uploads the document to the server, then the server stores the document in the IPFS node, which distributes it to the other nodes. After that, the document hash is generated, and then the user signs the transaction in order to store the document hash on the Blockchain Network using a smart contract. A transaction ID and a transaction hash are returned to the user.

The transaction ID and the document hash are used when the receiver wants to download the file. The receiver uses the transaction ID to get the data transaction from the network, the data contains the document hash, and this hash is used as a link to download the document from IPFS.

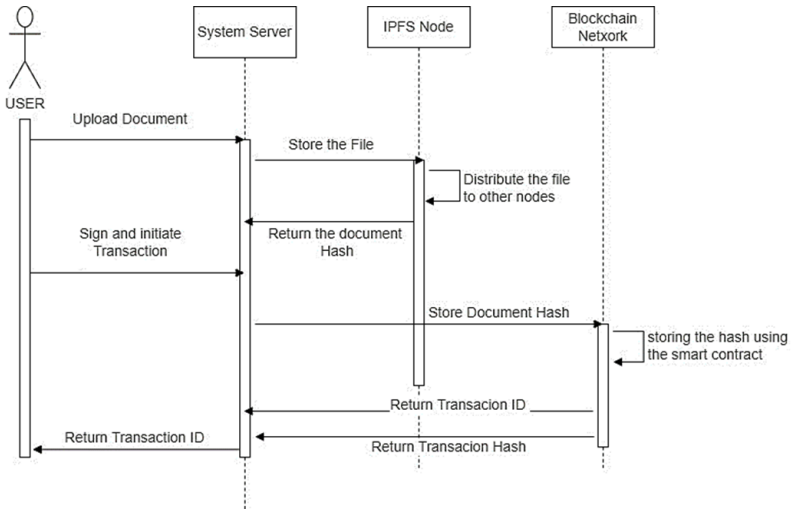

Figure 4.5 – Sequence Diagram of the file uploading process

To implement the architectures proposed, we have used the tools presented in Chapter 3.

First, we install Ganache-cli and then create a new workspace. A new workspace provides a list of 10 accounts for training, each of them containing 100 ETH in Balance for the smart contract's execution (Figure 4.6 is an illustration).

Figure 4.7 gives an overview of the latest blocks mined.

Figure 4.8 describes the details of smart contracts recently executed.

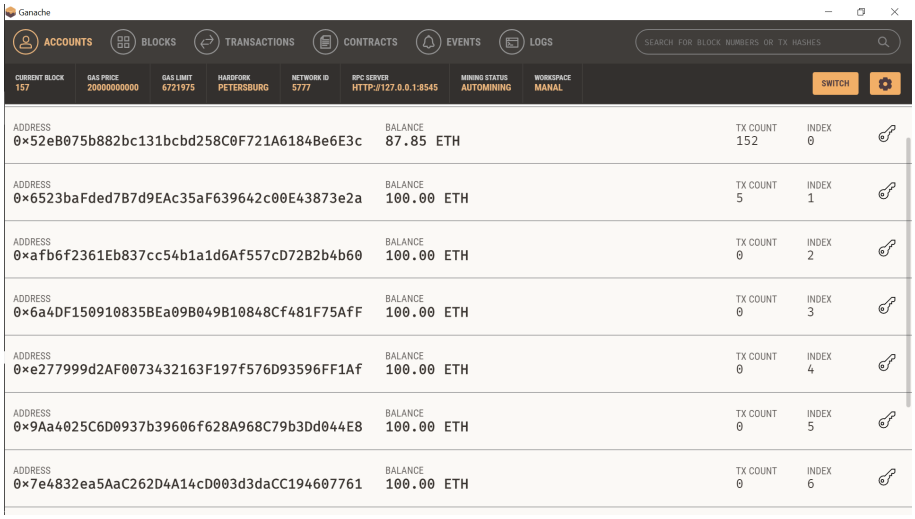

Figure 4.6 – List of Accounts provided automatically in ganache environment

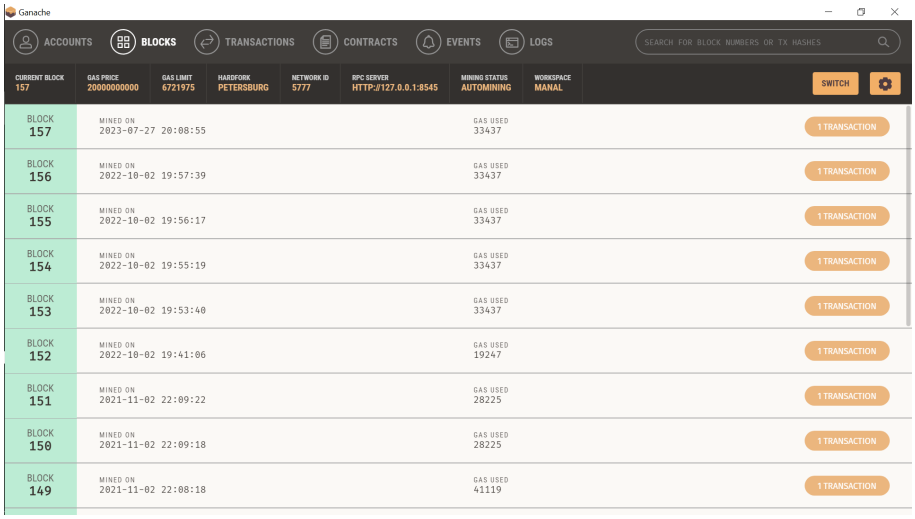

Figure 4.7 – List of Recent Block Mined

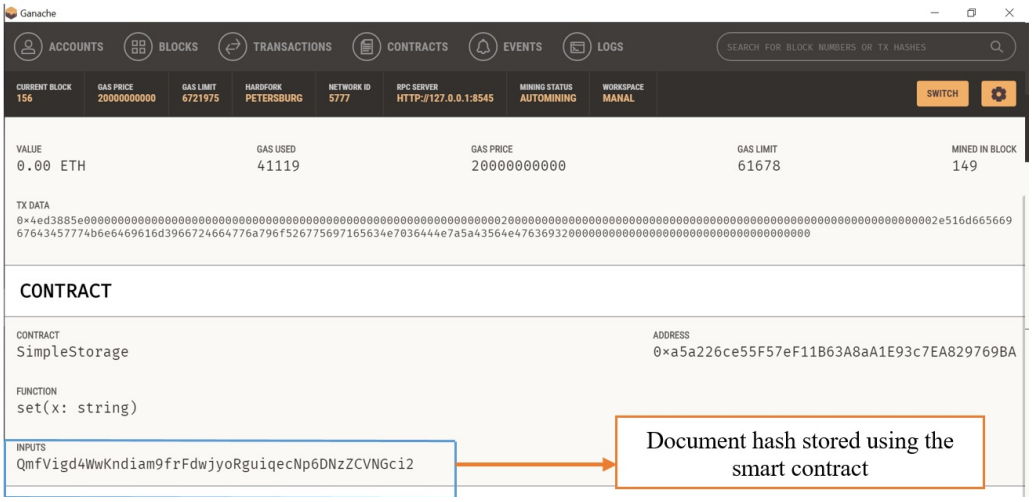

Figure 4.8 – Information about the Smart Contract executed and its related transaction

Concerning the development of the smart contract, as described before, the Remix IDE was used to write and test the smart contract code (Figure 4.9 is an illustration).

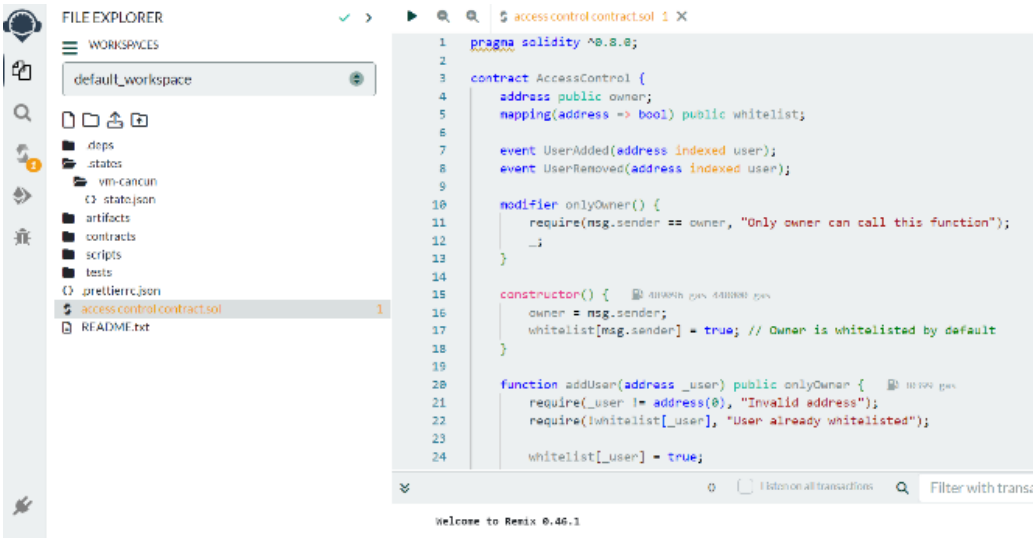

Figure 4.9 – Writing the smart contract code using the Remix IDE

The next figures (Figure 4.10 and Figure 4.11) describe the process of deployment and migration of the smart contracts using Truffle.

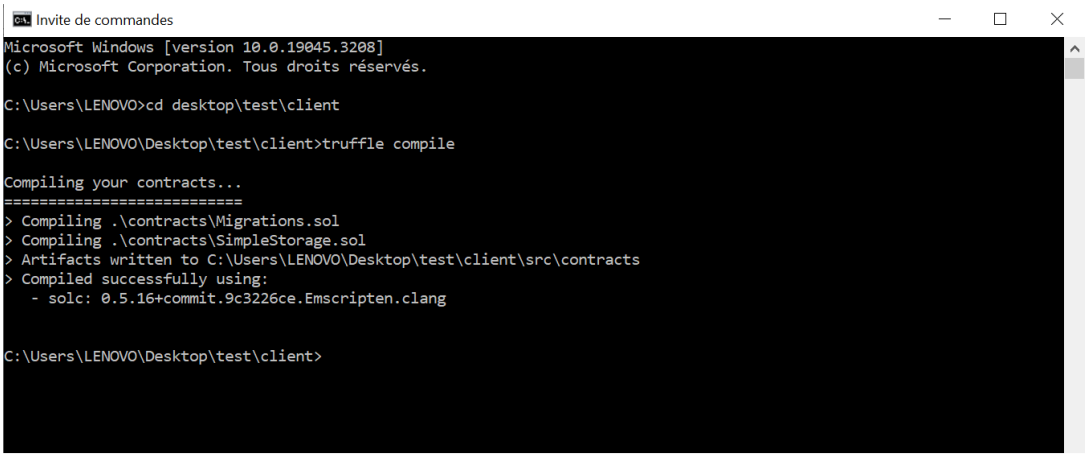

Figure 4.10 – Compiling the SC using truffle

To validate the transaction of the smart contract execution, and In this use case study, the Metamask tool is connected to our Dapp (Decentralized Application) via the link (https://127.0.0.1:8545) as presented in Figures 4.12 and 4.13 .

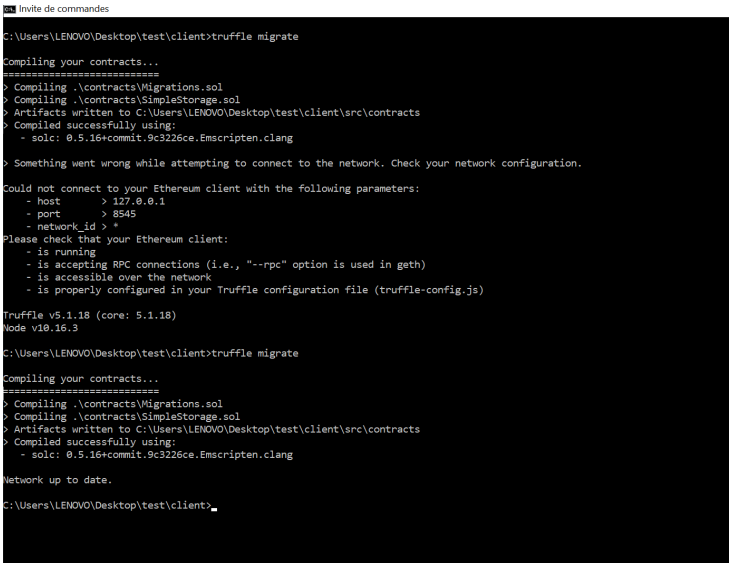

Figure 4.11 – Migration of the Smart Contract

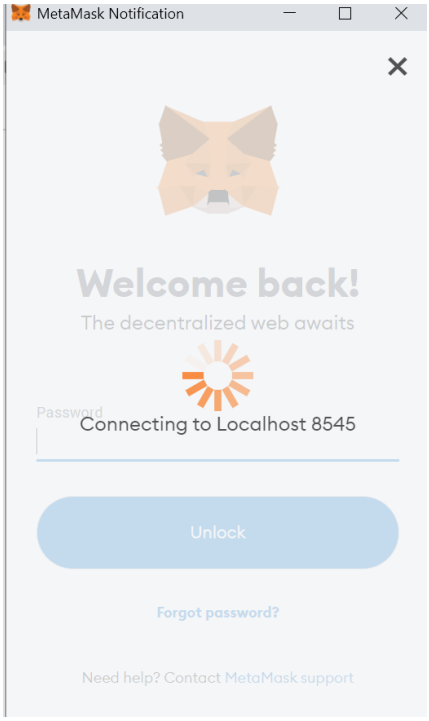

Figure 4.12 – Connecting Metamask to the application

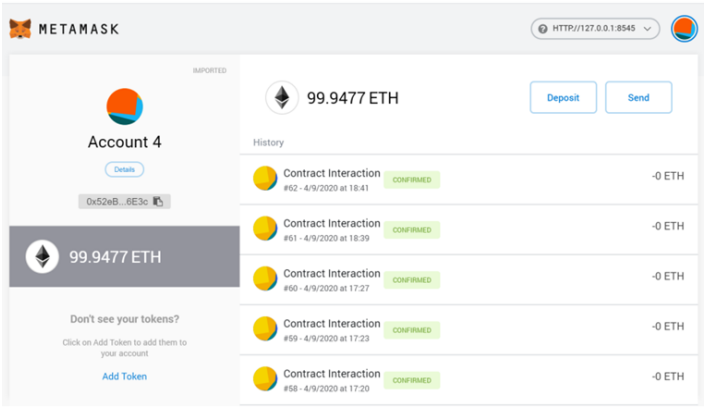

Figure 4.13 – Metamask home interface

Figure 4.14 represents the home Interface of the Decentralized application for data sharing between the different stakeholders in the Judicial system. This interface allows users to upload the document that they want to send.

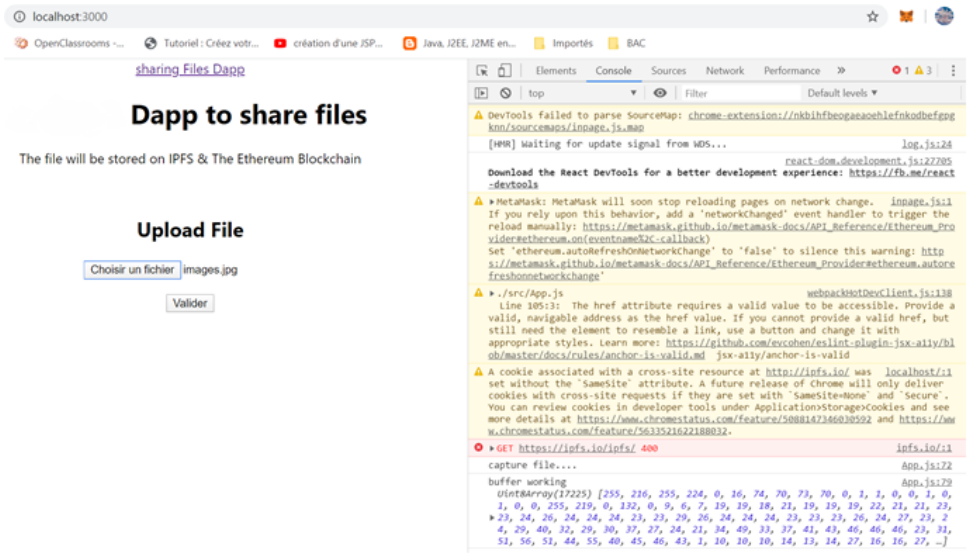

Figure 4.14 – The User uploads the document into the Dapp

After choosing the document, we click on the submit button, then the hash of the document is generated and at the same time the file is stored on IPFS, and the transaction is stored, then, on the Blockchain network (Figure 4.15).

To verify the document's existence on IPFS, we go to the link "https://ipfs.io/ipfs/DocHash " example in (Figure 4.16).

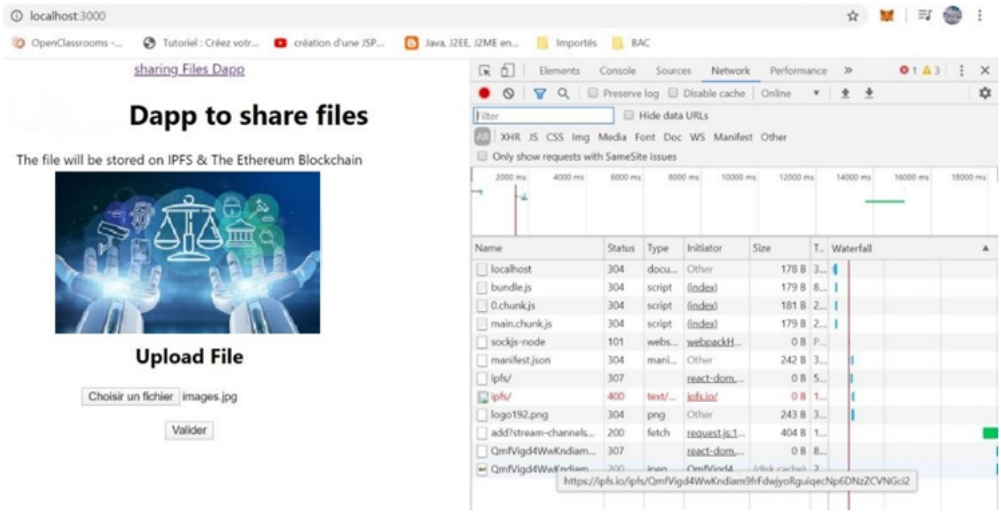

Figure 4.15 – The hash of the document is generated

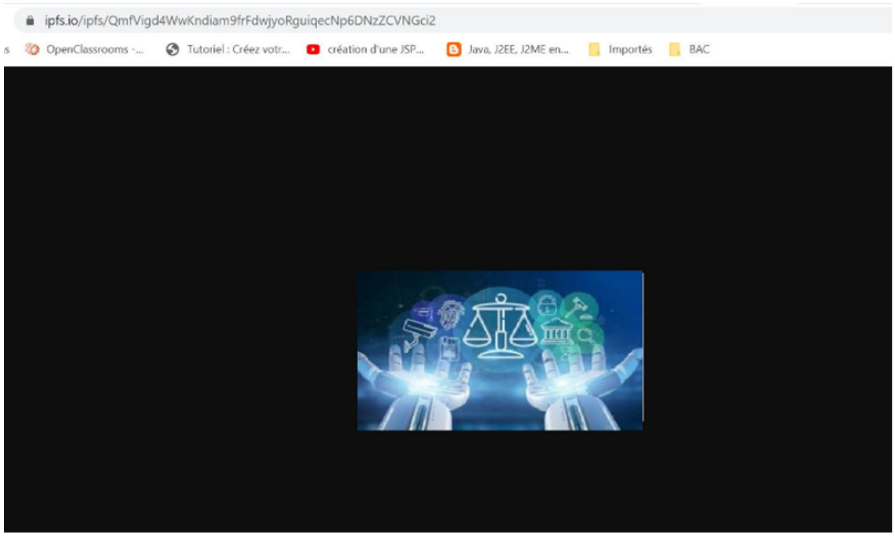

Figure 4.16 – Document verification using the hash generated

4.5.2 Implementation challenges

The digital transformation in the public administration process faces several obstacles that hinder its progress and prevent it from achieving its intended goals. Reference[84]. The use of Blockchain technology with IPFS just got over the traditional problems of centralized systems (unavailability, vulnerability, data integrity, and confidentiality) [85].

It is important to realize that those systems “decentralized systems” contribute to decreasing the use of paper in the ministry, as long as the sector uses paper in all procedures. Additionally, digital signatures provided by hashing algorithms, make the system faster and more efficient[28] than relying on a third-party organization.

For better implementation of the proposed architecture in the public sector, several challenges are faced in the adoption process. The most important entry point for e-governance success in the judicial field is the flexible access to judicial services by different users[86].In reality, the Ministry of Justice’s staff is manifold (almost 40,000 employees), and + 200 newly graduated Judges every year. For that reason, to put in place such a system we need a huge investment in multiple areas.

Management failure: Limited program coordination and a lack of control over project implementation, the absence of a joint governmental mechanism for overseeing the digital transition are e-governance issues. To address these challenges specialized bodies must be empowered with adequate resources to ensure the execution.

Infrastructure limitations: Since this project will be implemented for the benefit of the ministry and its external entities such as the courts which are distributed throughout the Moroccan territory, it should be noted that there are regions called "white areas" that lack adequate Internet infrastructure and the central administration has monopolized most of the equipment and information solutions, leading to limited resources and poor digitization of the local authorities[87].

Software and hardware challenges: Certainly providing equipment for the huge number of employees in the judicial sector and putting them in place is very hard and difficult especially, when we are talking about the equipment installation in different

justice courts in Morocco.

When we talk about software, it is almost the same thing, in addition, to implementing a blockchain-based file-sharing system that requires more types of equipment than a centralized file-sharing system.

Financial challenges: Financial challenges concern all of the hardware and software challenges, so implementing such a system for a governmental administration and its external entities is very challenging in terms of cost, as well as the cost to buy ethers for the users in the system. The choice of token is very crucial too, especially when designing a decentralized application for a governmental organization. The token chosen in this trial implementation is "Ether" which is the native Ethereum's blockchain cryptocurrency. This token could be acquired via a purchase from cryptocurrency exchanges platforms, or by receiving them as payments. However, using this token for a government application is critical, while this token is not scalable and stable. So then, using stablecoins like USDC, which is available in Metamask is more suitable for such use cases.

Concerning user education and training, offering support and assistance to the users of the system could be very costly for such a system which represents the first implementation for the benefit of the government of Morocco.

In such cases, it's very recommended to collaborate with other government sectors (other ministries) to succeed in this mission.

4.6 Evaluation and Discussion

4.6.1 Use case Experimentation

The suggested approach is based on Blockchain technology and IPFS protocol. The metrics used for the platform's evaluation are mainly based on download/upload time. The IPFS emerges as the most suitable choice for storing files in a decentralized environment if compared with other protocols[83].

For this reason, we used a dataset that comprises a set of judicial files with different extensions and formats(Text, images) and different sizes. we examined a list of 10 files of

different sizes: 1M, 2M, 4M, 8M, 16M, 32M, 64M, 128M, 256M, and 500M. Table 4 describes the measured time taken to upload/download these files on the IPFS. This measure helped us to understand the system's responsiveness concerning the file upload/download to ensure seamless in real-world usage scenarios. We noticed that the uploading time in a decentralized environment (IPFS) is relatively short, taking less than 1 second for files under 4MB. However, as the file size increases, the uploading time gradually extends.

Concerning file downloading, we employed the hash of the document to retrieve files from the IPFS storage. The downloading time from IPFS is summarized in Table 4.3 .

Table 4.3 – Upload and download time for the IPFS storage

File size	uploading time (s)	downloading time (s)
1 Mo	0,55	0,24
2 Mo	0,71	0,45
4 Mo	1,02	0,75
8 Mo	1,45	0,89
16 Mo	3,62	2.11
32 Mo	6,54	4,45
64 Mo	15,14	5,01
128 Mo	28,87	7,33
256 Mo	55,45	8,98
500 Mo	100,3	11,05

The results clearly demonstrate that the process of downloading files is faster compared to the time taken for uploading them.
Figure 4.17 confirms that downloading files is significantly faster than uploading them.

To summarize, IPFS has a lot of benefits as a decentralized file storage and distribution protocol. Its advantages include complete decentralization and content addressing using cryptographic hashes, as well as quick and easy access to content. These features make it a suitable choice to combine with Blockchain for Decentralized application's development.

4.6.2 Security Analysis

In Blockchain technology transactions are validated through the efforts of miners who dedicate significant power and energy to mine a block. As each block's hash is calculated using the previous block's hash, attempting to manipulate data on the Blockchain would

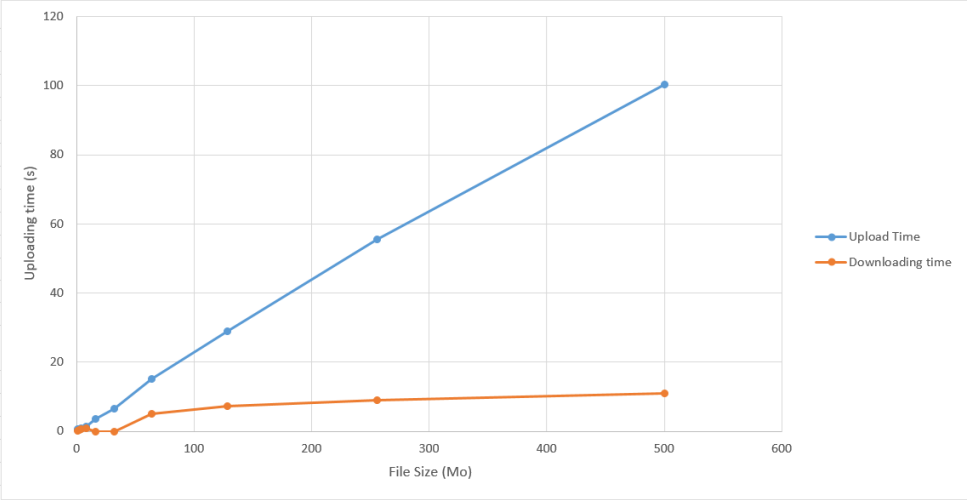

Figure 4.17 – Upload/download time's average using IPFS

require an enormous amount of computing power for the attack to succeed. The high costs associated with such an attack outweigh any potential gains, making it impractical and effectively preventing unauthorized access to data circulating in the network [88].

The files will be distributed in a decentralized network using smart contracts. In that case, Ensuring the smart contract's implementation is bug-free, devoid of vulnerabilities, and fortified against attacks is of utmost importance. Furthermore, it is important to safeguard the code and the information on the network, as they may be vulnerable to attacks[89].

Solidity code vulnerabilities pose significant threats and risks, as they can expose the system and network to cyberattacks, potentially leading to unauthorized access and exploitation [90]. Evaluating smart contracts for vulnerabilities has become a crucial aspect of building trust in the solidity and reliability of the contract.

In our use case study, smart contacts were developed using Remix IDE, this tool could help in compiling errors. Thus we used SolidityScan, which is a cloud-based smart contract vulnerability scanner, to discover vulnerabilities and help publish audit reports after vulnerability mitigations.

However, SolidityScan examines all of your smart contract code for potential security flaws and anti-patterns. The solution is designed to sit in your development pipeline, execute a scan of the code in your contract, and highlight known vulnerabilities. The product's final output is an audit report of your code that includes information on whether areas of

your code may lead to potential security issues. Our smart contracts code was analyzed using this SolidityScan tool.

Figures 4.18 and 4.19 show an overview of the security analysis of our smart contracts.



Figure 4.18 – Security Analysis of the first smart contract using SolidityScan



Figure 4.19 – Security Analysis of the second smart contract using SolidityScan

4.6.3 Discussion

Certainly, the results of this study show that adopting this architecture for the Ministry system will be a prominent revolution for the judicial sector in Morocco, in various aspects:

— A cost-effective judicial system;

— A modern and efficient system;

— Easy access to services that contribute to the improvement of the “digital court” approach;

— Improving the quality of services in order to accelerate the judicial decisions;

— This file-sharing system supplies the minimization of paper usage, then the promotion of environmental standards;

— Establishing a smart court that puts the new technologies at the judicial security service;

— Enhancing the “remote litigation” approach for time and cost reduction.

4.7 Conclusion

In the governmental sector, processes, and procedures are so complex and slow, so the use of centralized systems leads to a set of issues, especially a lack of trust, transparency, security, and confidentiality of data. The use of Blockchain technology, IPFS, and smart contracts in decentralized systems allows us to fix the mentioned issues and provide potential benefits and promises in different categories:

— Strategic:

like transparency, reduction of corruption, unauthorized changes;

— Informational:

high level of security due to hashing algorithms, data integrity, and privacy is guaranteed, storing data in multiple nodes enhances the easy access to data;

— Organizational:

by increasing control and trust due to data verification by multiple nodes and immutable record-keeping ledgers;

— Economical:

reducing cost while data verification and transaction validation are ensured automatically since no need for human contribution.

— Technological:

An implicit digital signature insured (public/private key encryption) mechanisms as well as reducing energy consumption.

The next Chapter presents the second use case study to design a new platform for criminal record management based on Blockchain technology.

CHAPTER

5

BLOCKCHAIN AND SMART CONTRACTS BASED SYSTEM FOR CRIMINAL RECORD MANAGEMENT

In this Chapter, 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.

5.1 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 [91]. The judicial sector represents a crucial department for government organizations globally. This frequently visited department encompasses a majority of tasks related to the security of a nation. 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 significantly improve efficiency in this area.

The information management could 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 [92]. Notably, within legal records,

court records stand out as a significant category[93]. One of the records produced by the courts is the criminal record. A criminal record is a crucial legal document that contains an individual's criminal history, aiding in law enforcement, courts, and employers in making informed decisions [94] [95]. 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 confidentiality 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 395724 offenses reported to the courts, and the crime rate will be 1086 offenses for every 100,000 citizens. In 2022, the number of reported sexual assaults exceeded 2182 cases, indicating a 2.3% rise over 2021 [96]. 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 [97], 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 [98]. 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 [99]. Despite advancements in centralized database systems, issues like data inconsistencies, inefficient storage space, and insufficient control over data management [100] [101] persist. Furthermore, centralized systems are more vulnerable to electronic attacks. The 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 study 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:

1. Offering a new solution for better criminal record management by enhancing: decentralization, data security, transparency, data integrity, and trust (benefits of Blockchain technology).
2. Designing a new platform including various entities and assigning respective roles using smart contracts, to avoid unauthorized access to the system.

3. Handling the issues of transparency and authenticity for citizens and stakeholders.
4. Using smart contracts for managing transactions.
5. Enhancing traceability and reducing the risk of fraud.

5.2 Literature Review

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 [102]. 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 [103]. 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 [104]. Research presented in [105] 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 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 [106]. Accordingly, the study presented in [3], 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.

In [107], the research 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. The paper proposed on [108] highlights 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. In [109], the study 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.

The research presented in [110] 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. In [111] the paper 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. Research paper in [112] 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 citizen's data by ensuring security, and integrity and improving information management openness. The study in [113] 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 this study is to propose a new solution for a criminal record management

system in profit to the Moroccan Ministry of Justice; this system will automate the process of storing and managing 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, lack of data security, data integrity, and traceability without the need of a trusted third party, or a system administrator.

5.3 Background

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 relies on "papers" exchange. An illustration of the current process management is presented in Figure 5.1 .

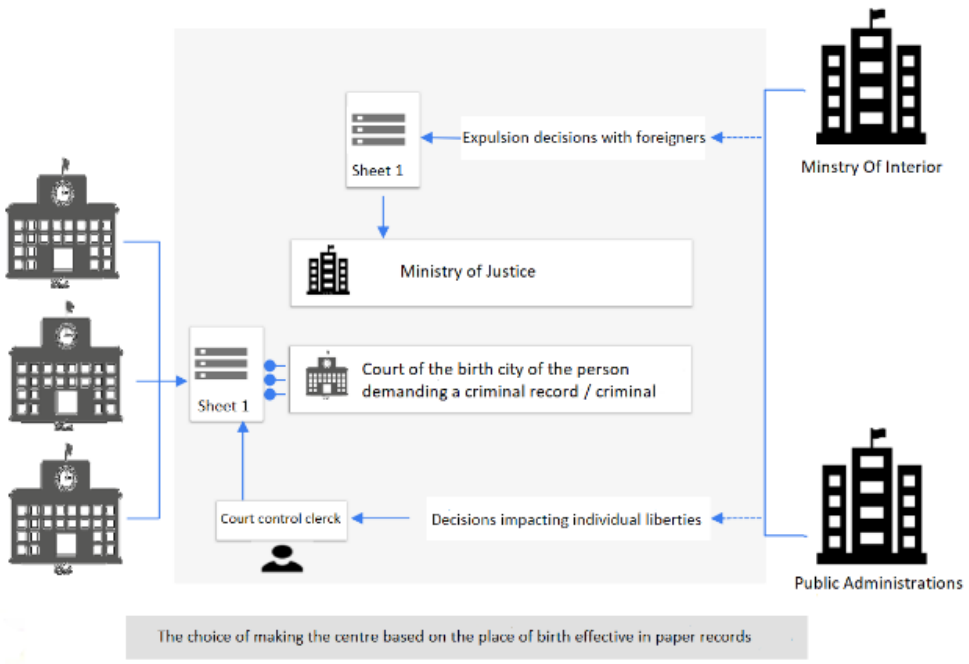

Figure 5.1 – The current process to get a criminal record

As shown in Figure 5.1, 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.

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 5.2 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

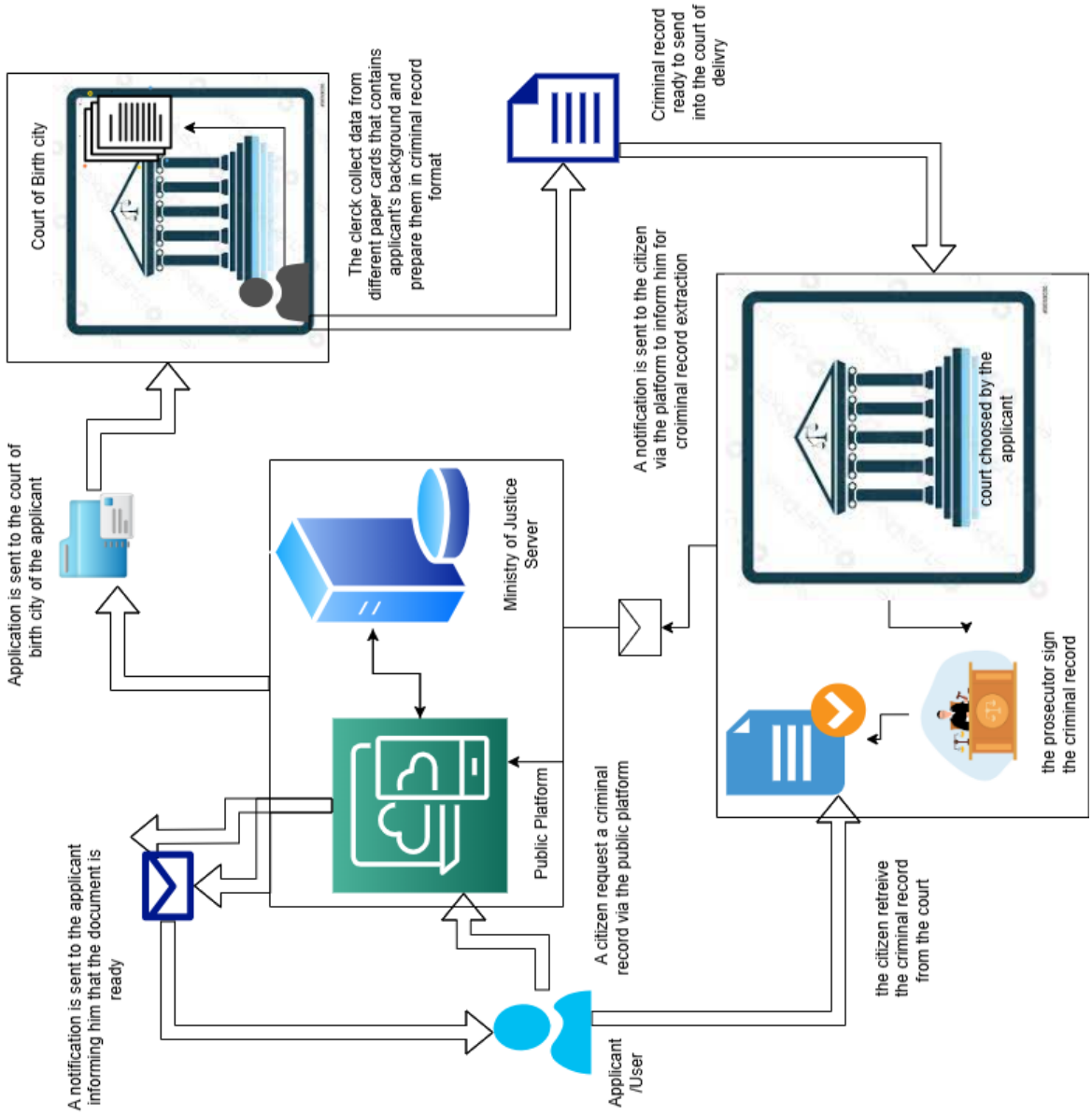

Figure 5.2 – The architecture of the public platform for criminal record application developed by the ministry of Justice in Morocco

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 retrival court signs it, to ensure its authenticity.

Figure 5.3 presents the proposed approach 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.

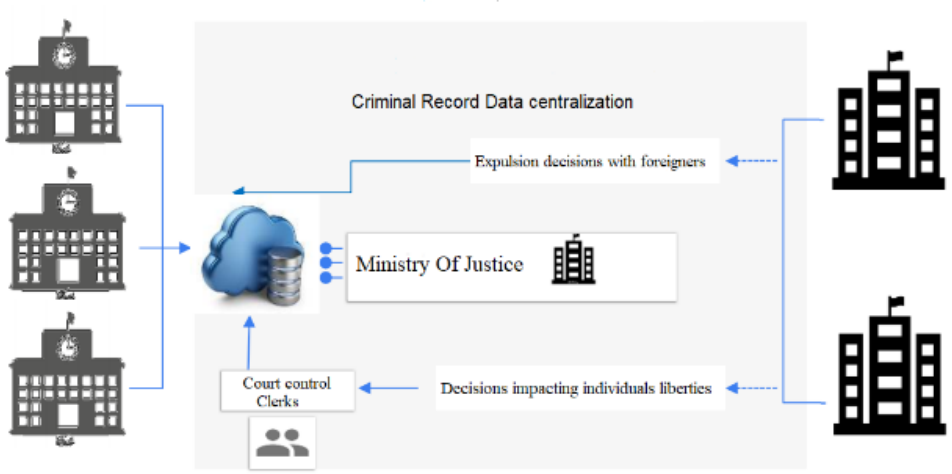

Figure 5.3 – Criminal Record Data Centralization

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.

5.3.1 Proposed System

In this part, 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 systems based on Blockchain technology and smart contracts.

Figure 5.4 illustrates the new 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.

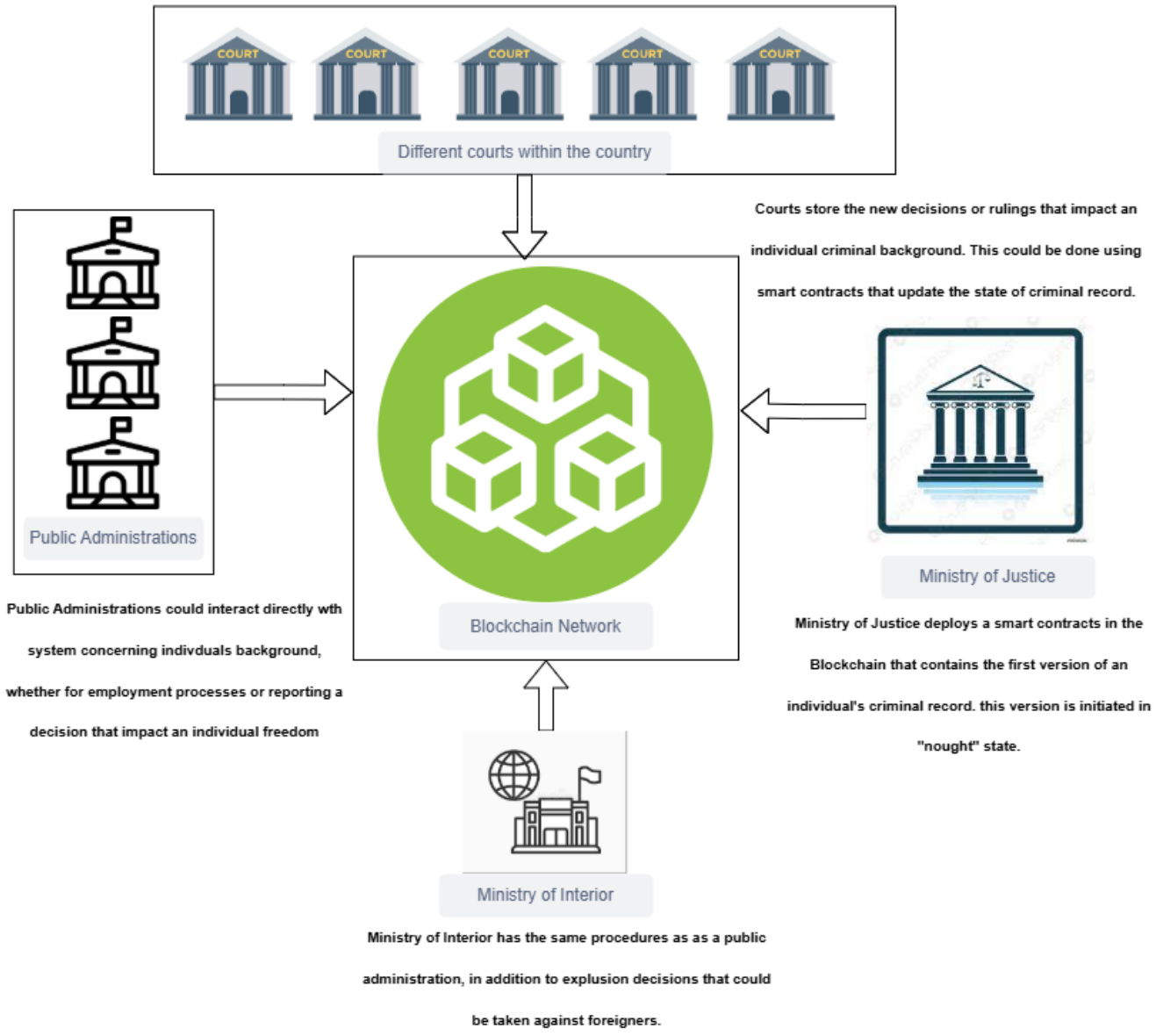

Figure 5.4 – Blockchain-based system for criminal record management

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 5.5 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.

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's 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.

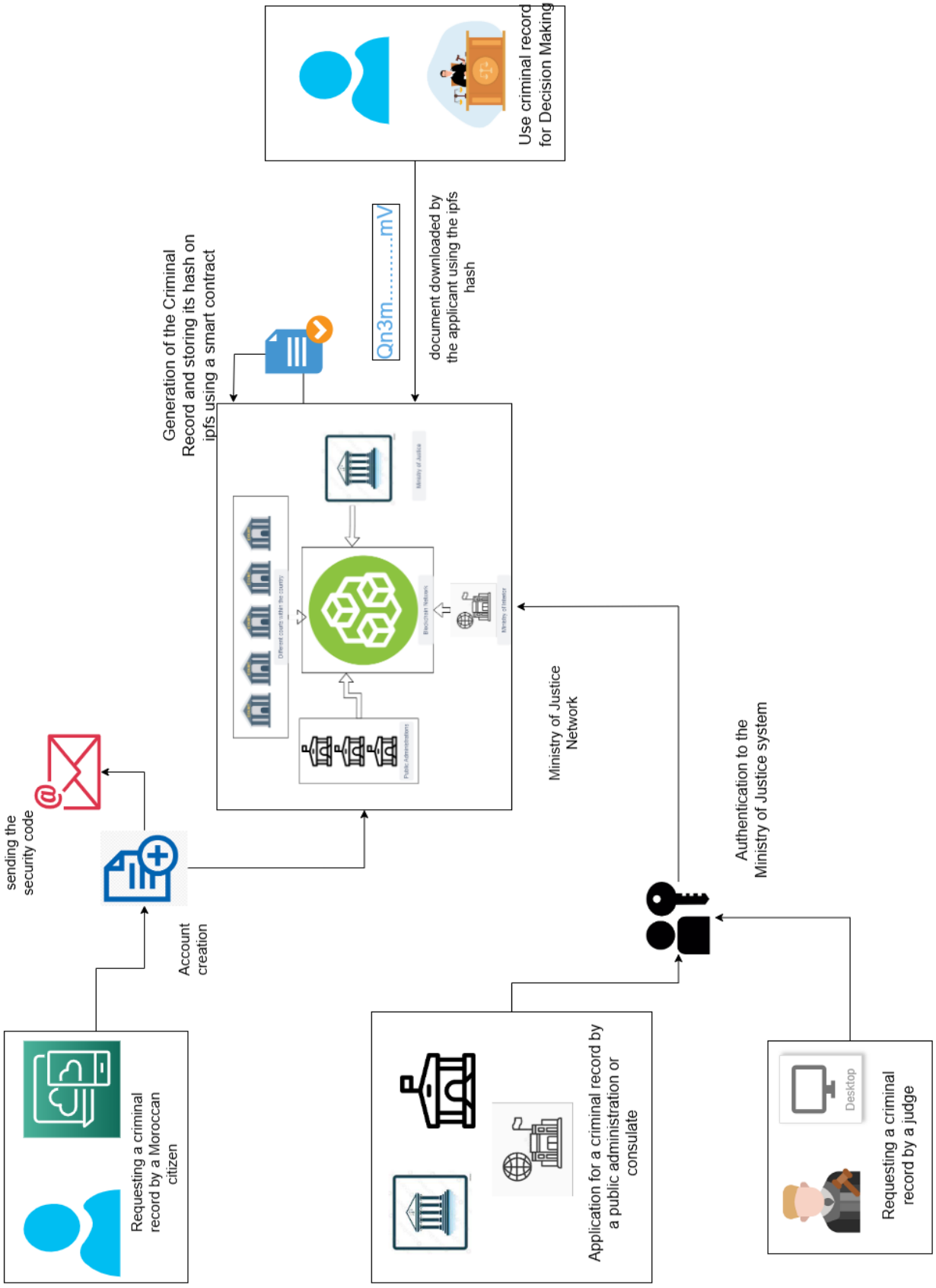

Figure 5.5 – The new process of getting a criminal record

5.3.2 System Design

The following is a description of various scenarios, using sequence diagrams to detail steps for designing the new proposed system.

Figure 5.6, 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 an email verification. After the email verification, the account is created and the corresponding ID is sent to the user.

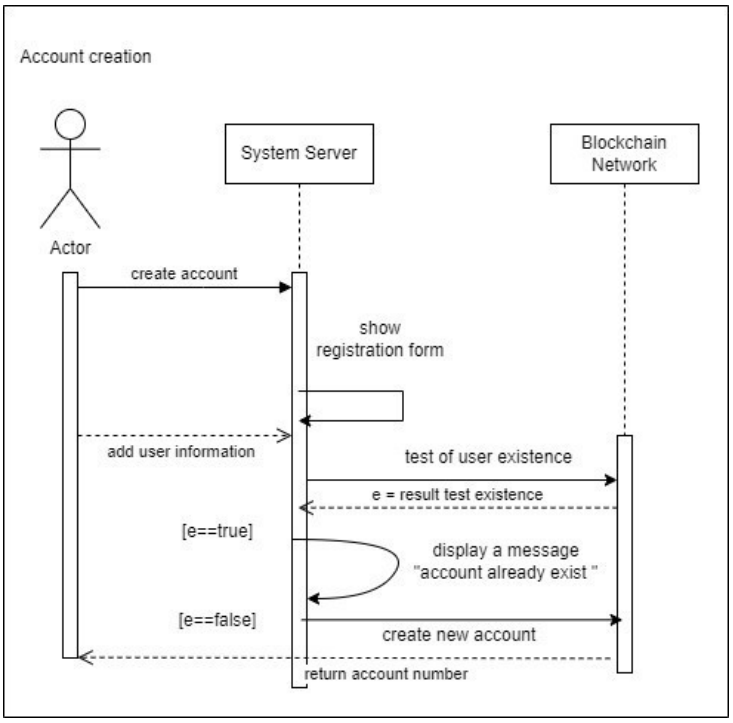

Figure 5.6 – Diagram of sequence for the account creation process

This next figure (Figure 5.7), 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.

The diagram in Figure 5.8, describes the process of adding for a criminal record.

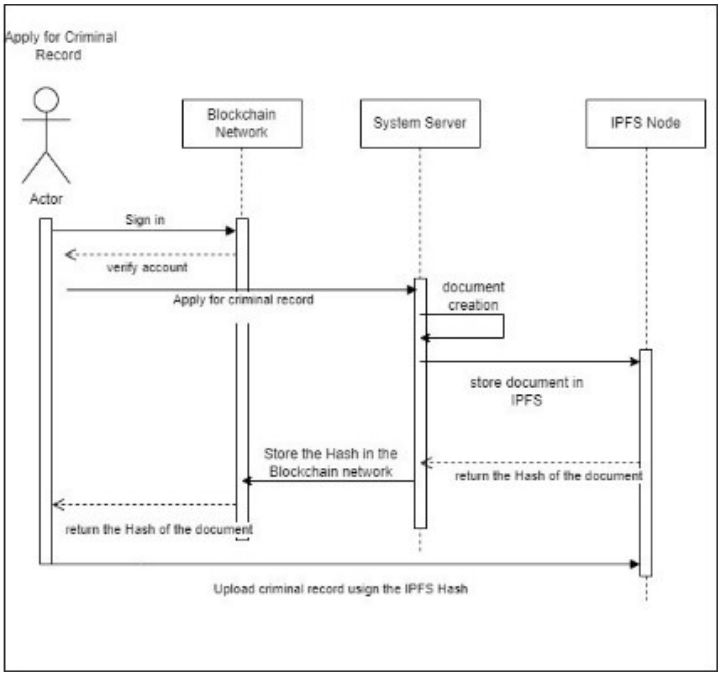

Figure 5.7 – Diagram of sequence for applying for a criminal record

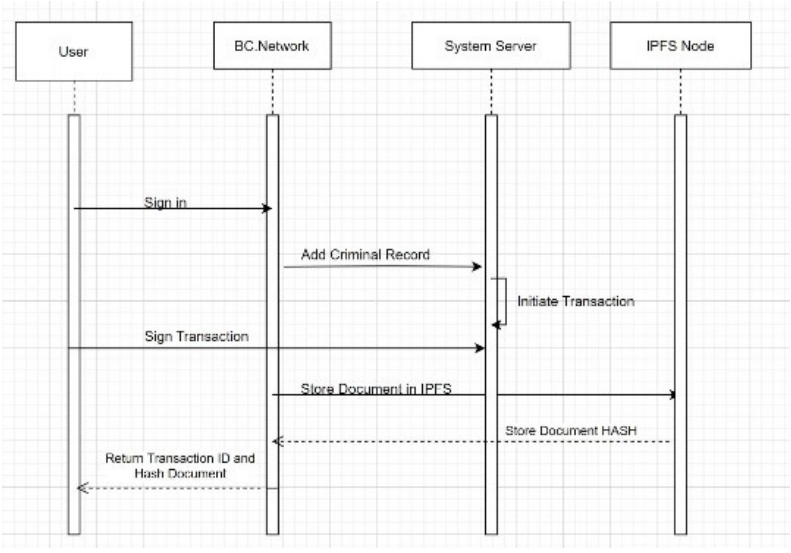

Figure 5.8 – Diagram of sequence for adding a criminal record

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.

5.3.3 Implementation

The tools used to implement the architecture proposed, have been defined in Chapter 2. Figure 5.9 describes the history of transactions in Ganache.

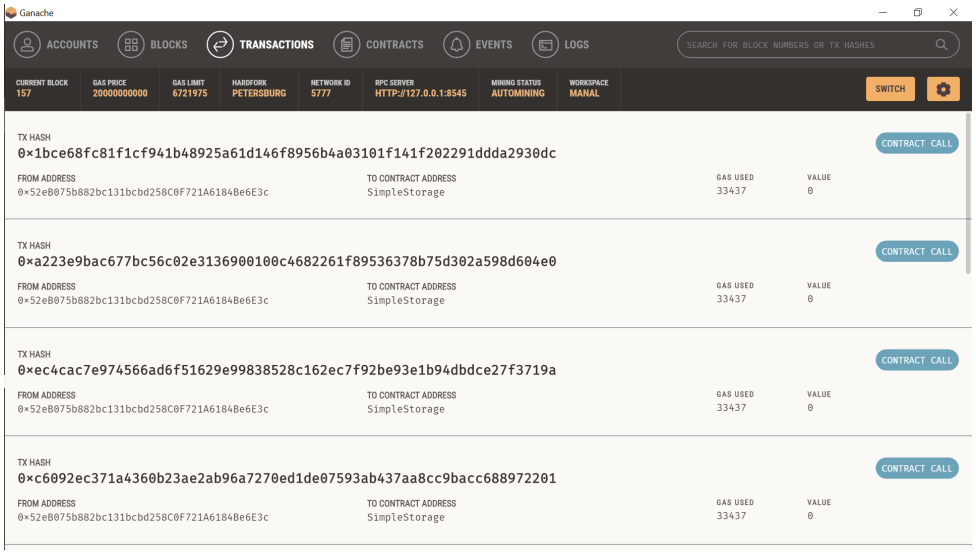

Figure 5.9 – Transactions History

Concerning user access control, we developed a smart contract specifically to handle this task. The smart contract was coded using Remix IDE, which encompasses a comprehensive set of development and deployment tools, providing an all-in-one solution for the creation and management of smart contracts [114]. The code for this contract is presented in Figure 5.10 .

As described before, Node js was used for the DApps development, Figure 5.11 represents the code of the DApps writing in javascript.



Figure 5.10 – The smart contract code for controlling the user access into the system

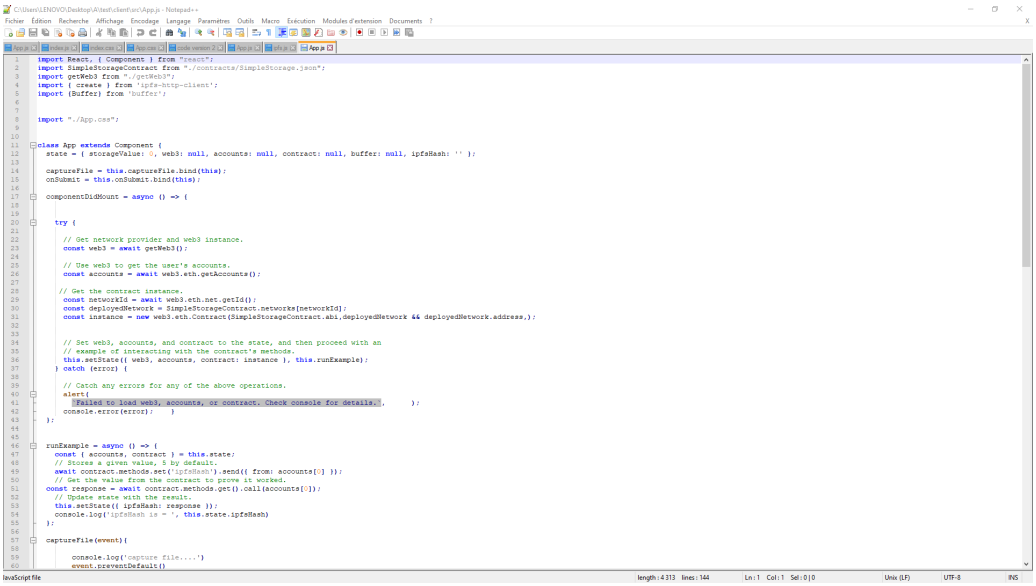

Figure 5.11 – Javascript code illustration of the Dapp

5.3.4 Scenario of the designed solution

In this part, an illustration of the application scenario is presented.

The First step of the process is to log into the network (Figure 5.12). If the user is a new applicant, an account creation is required. Consequently, the applicant needs to select his “user type” (Figure 5.13).

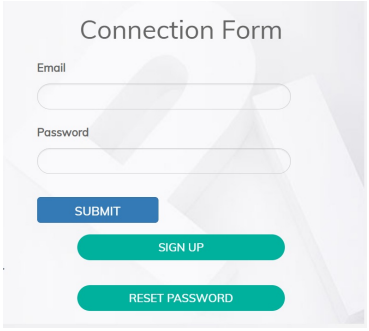

Figure 5.12 – Connection Form

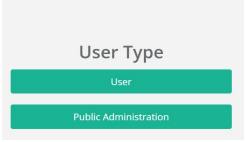

Figure 5.13 – User type selection

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

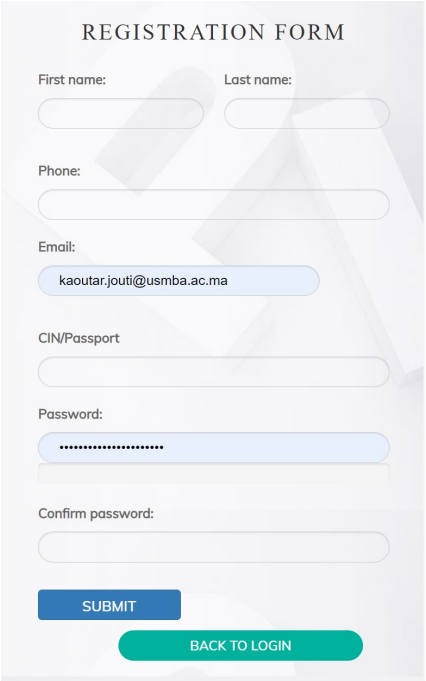

Figure 5.14 – Registration form when the user type is "Citizen"

5.14).

When the applicant is a “public administration”, an ID of the organization is requested (Figure 5.15).

After the account is created, the user has the right to log into the network.

Figures 5.16 and 5.17 illustrate these options. As presented in the following figures, and depending on the user’s role, we have two options:

— For citizens:

the ability to apply for a criminal record;

— For public administration, the ability of:

- Apply for a criminal record;
- Add a criminal record.

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 following interface (Figure 5.18) describes the process.

In this step, the user is required to fill 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 file is uploaded to the system server,

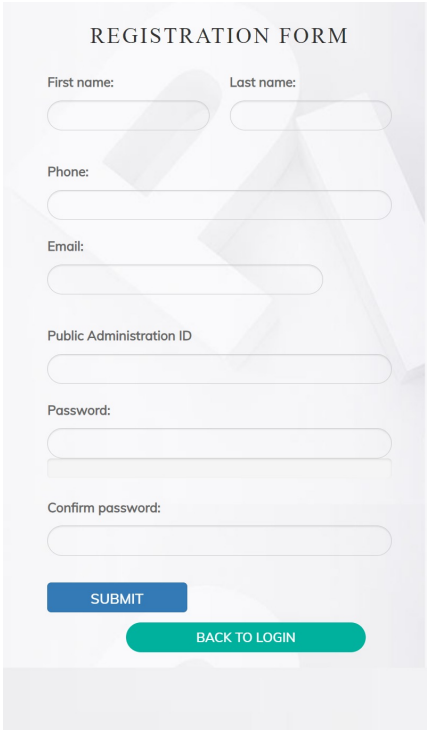

Figure 5.15 – Registration form when the user type is "Public Administration"

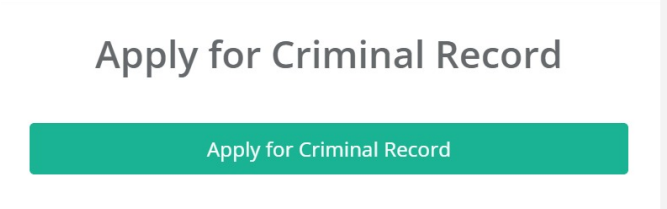

Figure 5.16 – The options for user type ="citizen"



Figure 5.17 – Options for user type ="public administration"

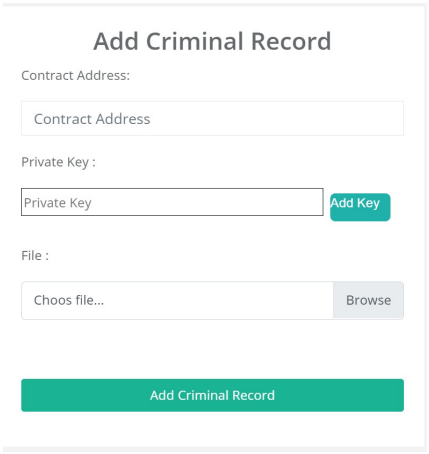

Figure 5.18 – Interface of adding a criminal record by "Public Administration"

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.

5.4 Evaluation and Discussion

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 falsification, 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 fortified 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 [115].

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 5.1 provides an overview of the security analysis of the smart contract’s “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.

Table 5.1 – 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 5.2 – 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

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 5.2 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.

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.

5.5 Conclusion

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.

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.

In the following Chapter, a detailed description of the proposed architecture to manage traffic accident reports using a Blockchain-based mobile application.

CHAPTER

6

BLOCKCHAIN-BASED SYSTEM FOR TRAFFIC ACCIDENT REPORT'S MANAGEMENT

This Chapter provides an innovative solution. It's a use case study of developing a Blockchain and interplanetary file system (IPFS) protocol-based system for traffic report management, using a mobile application. This application could be used at the time of the traffic accident. By using the application, road users can fill out the accident report at the same time as the accident while maintaining data authenticity, integrity, and reliability, and without the need for a third trusted party. Furthermore, the application reflects the safety performance of insurance companies and allows them to put an end to oversights, inaccuracies, or incorrect information when completing the amicable accident report. A better understanding and streamlining the process of handling accident reports is an essential component to enhance emergency response, promote road safety, and mitigate the economic impacts of traffic incidents, for both users and insurance companies.

6.1 Introduction

Traffic accidents present significant challenges worldwide, necessitating efficient and reliable management systems to streamline the reporting process. As a result, individuals frequently obtain car insurance to minimize their financial losses and receive compensation[116]. Despite that, the current process for filling traffic accident reports presents several issues, including instances of insurance fraud, challenges in efficiently tracking and transmitting insurance data, and complex procedures. In the case of traffic accidents, where there is no bodily harm, most of insurance companies rely on traditional processes of reporting. These methods present different problems such as delays, inconsistencies, and vulnerabilities that lead to inefficiencies in emergency response and insurance claim processing.

The basic solution to resolve this problem is the use of an information system to manage the accident report. However, centralized systems present several limitations, some of which are a lack of data security, integrity, and traceability without the need for a trusted third party. With this objective in mind, decentralized technologies like Blockchain have been recognized as a promising framework for enhancing the reliability, security, and transparency of data exchange within decentralized networks[117].

Numerous studies have suggested using Blockchain technology to collect, validate, and

track metadata within a secure, immutable, and transparent infrastructure. An example is presented in [118]. As a work extension, authors in [119] suggested a novel architecture for secure data sharing among untrusted actors without the need for a third-party authority.

By creating transparency and trust, blockchain technology eliminates third parties and builds trust models[120]. It also allows people to share data simultaneously while recording blocks that must be validated by everyone on the network [83].

The goal of this study is to develop a mobile application based on Blockchain technology and IPFS (Interplanetary file system) to manage traffic accident reports. The main goal of the proposed solution is to motivate road users to fill out the report from the accident zone, without the need for a trusted third party to enhance the management of accident reports, and finally to ensure that the data entered will not be altered by another person.

6.2 Literature Review

Several studies have investigated the application of Blockchain in different domains, such as supply chain management, healthcare, and finance, demonstrating its potential to revolutionize data management practices. Below is a brief description of prior researches that has explored various methodologies for improving traffic accident information management, including decentralized architecture, mobile applications for accident detection, also Blockchain, smart contracts, and IPFS-based systems.

Authors in[91] implemented a Blockchain-based vehicle insurance management system that facilitates the exchange of policy details among stakeholders in the network. In[121], the authors proposed an approach that uses modern technology to develop a road accident detection and notification system that can detect accidents and notify emergency services immediately. Another research presented in[122] describes a new Blockchain-enabled certificate-based authentication scheme for vehicle accident detection and notification in Intelligent Transportation Systems (ITS). Authors in[123] presented a study to design and develop a new Blockchain-based system for decentralized monitoring and management of accident/incident information in the construction industry.

In a study presented in [124] the authors introduced an approach of a Blockchain-based

file-sharing system for academic Paper Review that relies on Blockchain technology combined with IPFS to store large files in a distributed manner, in order to reduce storage requirements in the user side, also that's guarantee data decentralization, immutability, and auditability. In[125] authors confirmed that using a P2P file-sharing system contributes to reducing the cost of files stored and protected in a decentralized environment. The use of smart contracts plays a significant role in managing a Blockchain-based file-sharing system in a decentralized environment and deploying it in the Ethereum network[126].

With the growth of using smartphone devices, the mobile applications market is always changing, with new developments and trends emerging frequently[127] [128]. Intending to create safe, decentralized, and effective payment solutions, Blockchain technology has significantly impacted mobile applications especially, the applications designated for payment futures[129].

Furthermore, blockchain technology seamlessly integrates with IoT devices to address IoT-related challenges, including data security, trust, interoperability, and data provenance[130] [131].

Hence, Blockchain technology combined with IPFS and Smart Contracts has emerged as a promising solution to address the issues mentioned earlier, by providing a decentralized and tamper-proof ledger for recording and sharing accident-related information as well as a guarantee of data security, authenticity, and integrity.

6.3 Problem Statement

The proposed Blockchain-based mobile application for traffic accident report's management focuses on revolutionizing the current process of managing paper accident reports (Figure 6.1).

As presented in Figure 6.1, the current model is a paper-based report. As shown in the figure the document contains a lot of information to fill in and seems too complicated especially, in the case where the driver is a beginner in addition to that the risk of making mistakes is very high.

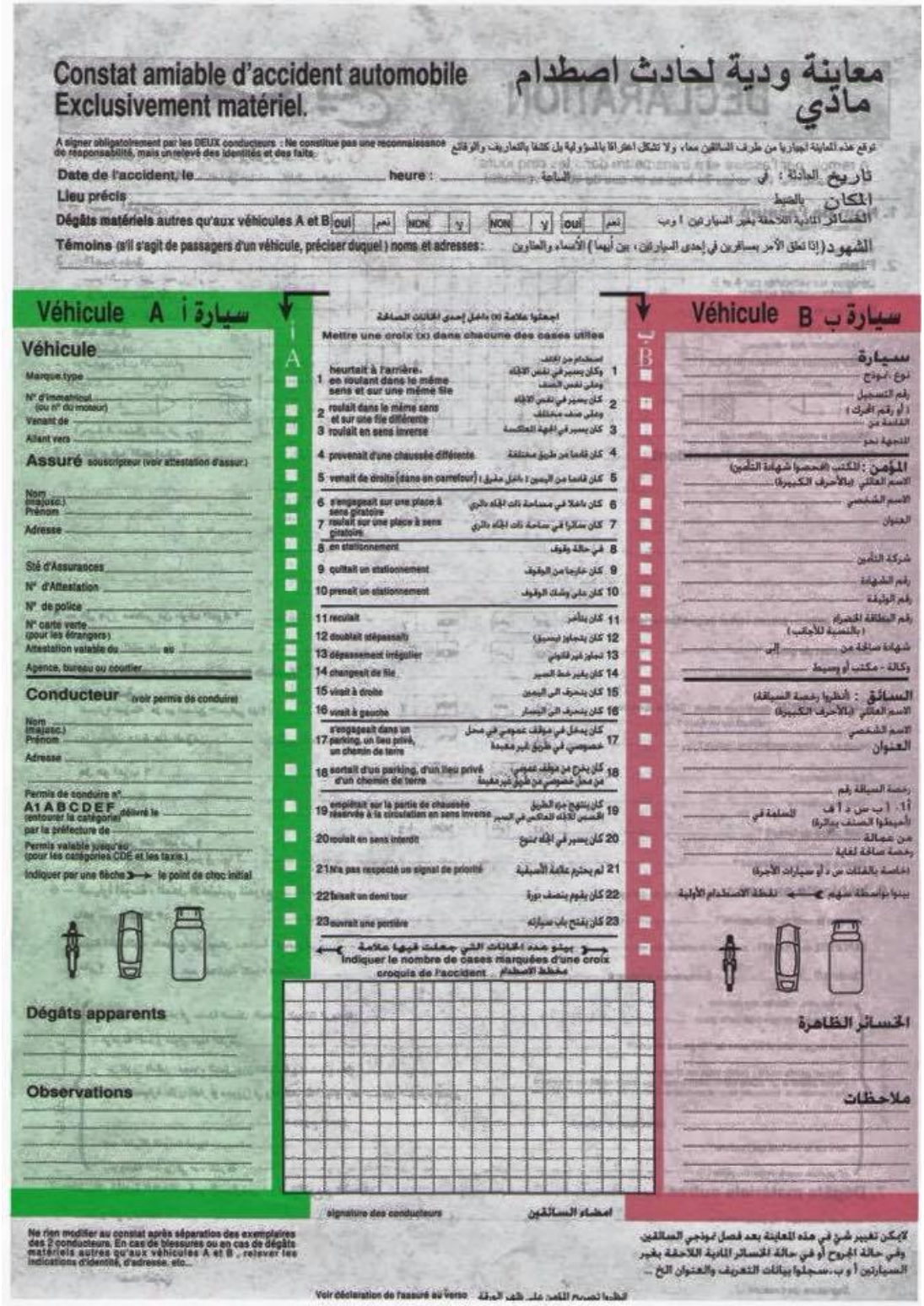

Figure 6.1 – Example of amicable traffic accident report used in case of car crash in the Moroccan country.

Moreover, written reports present several limitations such as:

— Error-prone:

paper reports are susceptible to human error, including illegible handwriting, incomplete information, and data entry mistakes;

— Limited accessibility:

paper reports may not be readily accessible to all relevant parties, such as insurance companies and law enforcement agencies, especially, if they are stored in physical files;

— Storage and retrieval challenges:

storing and retrieving paper reports can be space-consuming, particularly when dealing with large amounts of reports over time;

— Susceptible to damage:

paper reports are vulnerable to damage from environmental factors or even from loss, which can compromise the integrity and availability of the data;

— Lack of data security:

Paper-based reporting is weak in terms of protecting sensitive information from unauthorized access, tampering, or theft;

— Time processing:

Generally, manual reporting leads to delays in data entry that could affect the time of response and resolution in emergency cases.

After all, the integration of Blockchain technology and IPFS into a mobile application will introduce a decentralized and immutable system that ensures trust, data integrity, data accountability, and data traceability, besides reducing the time of processing the accident report.

6.4 Proposed Solution

Figure 6.2 describes the new proposed solution. As illustrated in Figure 6.2, when a traffic accident occurs, the driver can easily complete the amicable accident report using the user interfaces of the mobile application. Once the necessary information is filled out and photos of the accident are taken and uploaded into the application, the driver can

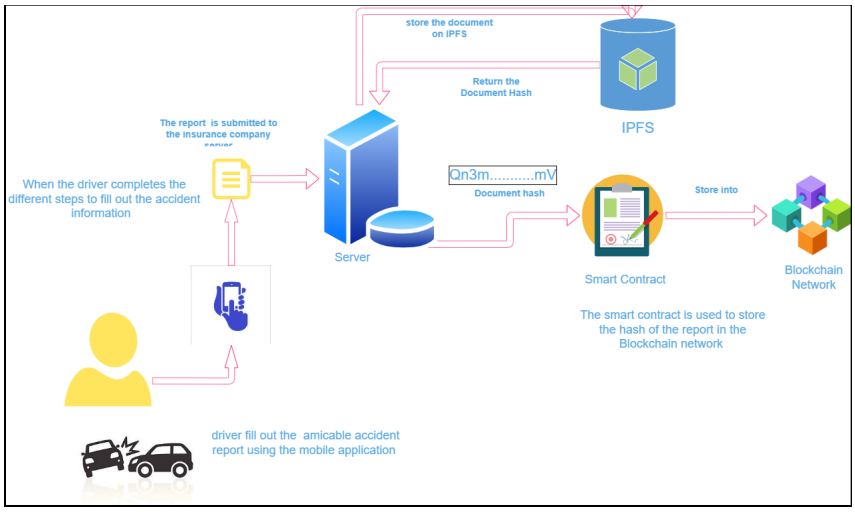

Figure 6.2 – Proposed architecture

promptly submit the report to the insurance company.

The document is stored on IPFS, and then the document's hash is generated. The hash of the document is the key for document location on addressable content.

The IPFS guarantees non-duplication of a document, (unique ID, as it is cryptographically generated), and a tamper-proof document. When the document's hash is generated, it will be stored on the Blockchain network using a Smart Contract to allow traceability and authenticity.

In that case, we can have access to documents using the hash generated. If a user changes, one letter or character in that document a new hash will be generated and show that the original document has been altered.

6.5 Evaluation and Discussion

The Proposed mobile application is, ultimately, simplifying the accident report process. When an accident occurs, the driver can simply use the mobile application, and complete the steps for filling out the report of the accident.

The following is a scenario describing the different steps of using the application for report generation.

The first step is completing a form with essential information about the drivers and the vehicle ID (Figure 6.3). The same Interface will be used for driver B.

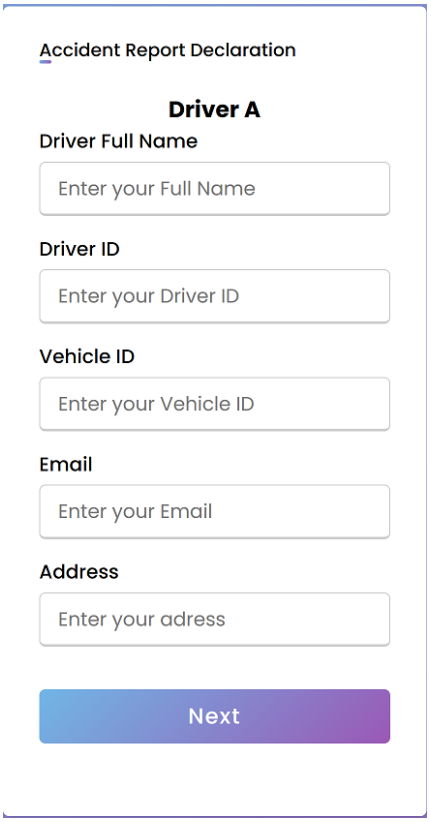

Figure 6.3 – The driver information form

The next Figures 6.4 and 6.5 present the step of selecting the car type from the existing list of cars.

After that a checklist that includes details about the traffic accident, the position of the vehicles at the time of the crash, the various damages caused as well as determining the at-fault driver. The Drivers can easily select options from the list (Figure 6.6).

The next step is taking photos of the accident (Figure 6.7).

For more accuracy, the application gives the opportunity to include photos of the accident to be inserted into the report. Finally, the report is generated with all the necessary information for user verification and signing, and it can be submitted to the insurance company system (Figure 6.8).

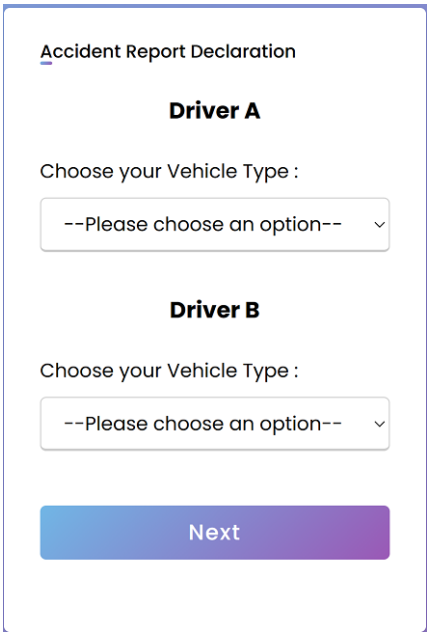

Figure 6.4 – Checking the vehicle type -1

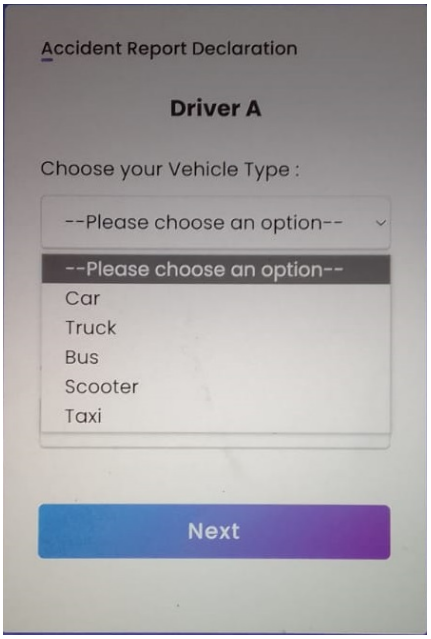

Figure 6.5 – Checking the vehicle type -2

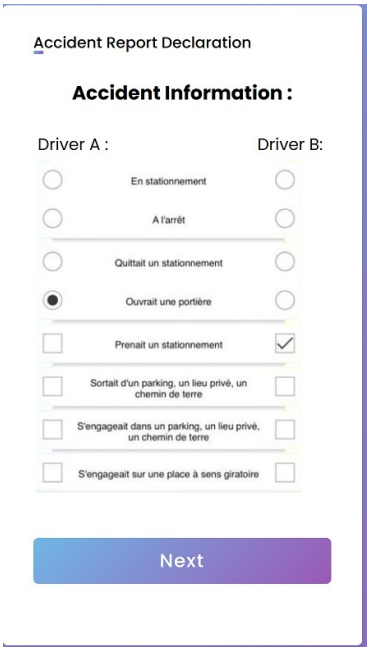

Figure 6.6 – Checking the accident information

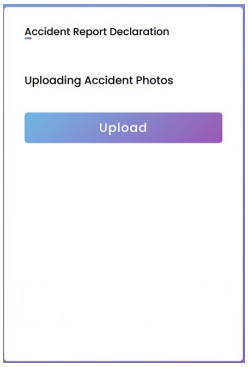

Figure 6.7 – Uploading real photos of the accident

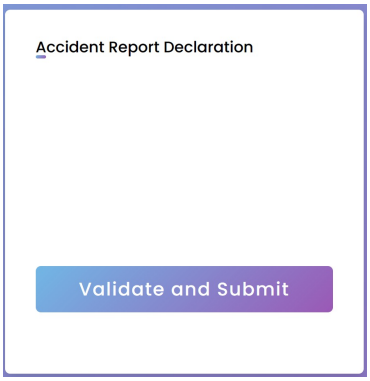

Figure 6.8 – Submitting the accident report

As a result, data-sharing processes are often complex and lack trust, particularly when managing documents manually. So, the use of centralized systems leads to a set of issues, especially a lack of trust, transparency, security, and confidentiality of data.

The use of Blockchain technology, IPFS, and smart contracts in decentralized systems allows us to fix the mentioned issues and provide potential benefits and promises in different categories such as :

— transparency;

— reduction of corruption;

— unauthorized changes;

— data security;

— data privacy;

— easy data retrieval.

Certainly, the results of this study show that adopting this Blockchain-based application for accident report's management will be a prominent revolution for the insurance sector.

6.6 Conclusion

In conclusion, a Blockchain-based mobile application is used to manage the traffic accident report in this paper. The integration of Blockchain technology into a mobile application combined with IPFS and Smart Contracts offers a promising solution for improving traffic accident report management. By leveraging Blockchain's decentralized architecture and cryptographic principles, the proposed system enhances data integrity, transparency, and efficiency in accident-related processes.

CHAPTER

7

CONCLUSION

7.1 Overview

In conclusion, Morocco's commitment to using technology for national development is exemplified by its journey toward digitalization and efficient data-sharing systems. Even though there are still challenges, the progress made so far shows the possibility of even more advancements. In order to fully benefit from digitalization in public administration, more funding investment in infrastructure, capacity building, and regulatory support will be essential.

This thesis explored the potential of Blockchain technology to revolutionize data sharing within E-government ecosystems. By decentralizing control, ensuring data integrity, and enhancing transparency, Blockchain offers a compelling solution to security, efficiency, and trust challenges.

Firstly, we presented a general overview of the concept of E-government and data-sharing systems in E-government. Then a description of the development of this concept in the Moroccan country. After that, a detailed description of Blockchain technology, its operating principles, technologies that constitute the Blockchain, and some use case applications were presented, followed by a presentation of the technologies, software, and platforms used in the deployment of the new architectures proposed in this thesis.
In addition, a detailed description of the use of Blockchain technology in E-government.

The next Chapters were dedicated to representing the proposed solutions to the research problems of the thesis.

The research works presented in this thesis led to many contributions. In our first contribution, we have designed a new architecture to improve traceability in E-governance file-sharing systems, taking as a use case study the Ministry of Justice in Morocco. This research aims to establish a file-sharing system to share data instantly between the Ministry of Justice, the Supreme Council of Justice, and the Presidency of the General Prosecutor's office in Morocco. This architecture is based on the Blockchain technology (Ethereum Blockchain) and IPFS protocol to solve the problem of the current system (centralized system) with all its issues and to enhance the security, immutability confidentiality, and availability of the process of sharing files between different users of judicial field.

The results of this study show that the users of the system could Share files in a

high-secured environment. The document is uploaded into the system, then the hash of the document is generated, and this hash will be stored on the Blockchain network using a smart contract for timestamp and document owner recording. Since the transactions are recorded in immutable ledgers, any fraud or corruption could be detected, and it is thanks to the power of Blockchain technology coupled with IPFS, that the files will be distributed in a decentralized network, in that case, all of the participants on the network have access to data in the same time.

The second contribution is to design a new platform for criminal record management. The new platform is a Blockchain and smart contracts-based system, with the aim of digitizing the process of getting a criminal record for the benefit of the Ministry of Justice in Morocco.

To implement the system, Blockchain technology was used to ensure integrity and transparency as well as secure exchange between different independent parties. The 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 role, and the document can be retrieved using its hash generated by the IPFS and stored in the Blockchain using the smart contract. In fact, the digitization of criminal record processes holds promise for modernizing law enforcement practices and facilitating more efficient justice administration in the digital age.

Regarding the third use case study, the contributions of this mobile application to traffic accident report's management will be a prominent revolution for the insurance sector. Certainly, The integration of Blockchain technology into a mobile application combined with IPFS and Smart Contracts offers a promising solution for improving the process of traffic accident report management.

Finally, By leveraging Blockchain's decentralized architecture and cryptographic principles, the proposed systems enhance data integrity, transparency, and efficiency, reducing costs and time processes. By adopting such systems in the governmental administrations will enhance the services provided by the government to citizens and improve the revolu-

tion of E-governance in Morocco.

7.2 Future perspectives

The perspective opens the door to exploring potential improvement of our proposed solutions. Concerning our first use case study, The main object that will constitute our future research axe is the enhancement of the system's security.

Techniques such as deploying smart contracts to manage access control and file-sharing rules, using a private IPFS network to restrict access to trusted nodes, or even integrating blockchain-based authentication mechanisms into the system can be used to enhance the system's security.

The future directions regarding the second use case study will focus on: 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 cases detection.

The primary focus that will shape our future research direction with reference to the third use case study, will concern the capability to check the status of the accident report, and facilitate interactions with the insurance company.

Additionally, we aim to expand the functionality of the mobile application to support automated data exchange with relevant stakeholders, such as law enforcement agencies, and healthcare providers in case of accidents with injuries.

Lastly, the integration of emerging technologies such as IoT, and Artificial Intelligence (AI) into our Blockchain-based applications could unlock new capabilities and respond to the changing needs in this field.

BIBLIOGRAPHY

[1] B. Narin, F. Fırat, D. Fırat, and B. Ayaz, "Büyük veri ve gazetecilik İlişkisi bağlamında veri gazeteciliği tt - data journalism in the context of big data and journalism," *AJIT-e: Academic Journal of Information Technology*, vol. 8, 2017.

[2] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer, D. Song, and R. Wattenhofer, *On Scaling Decentralized Blockchains*, 2016.

[3] S. Ølnesa, J. Ubachtb, and M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing," *Government Information Quarterly*, vol. 34, pp. 355–364, 2017.

[4] D. L. K. Chuen, *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*, 2015.

[5] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015*, 2015.

[6] N. United, *Department of Economic Social Affairs. UN e-government survey 2020*, 2020.

[7] R. Heeks, *Implementing and Managing eGovernment: An International Text.*, 2012.

[8] B. Aziza, "La digitalisation du service public : une priorité pour le développement économique et social au maroc," in *The International Congress in Innovation in Quantitative and Qualitative Research,.* hal-04520899, 2024. [Online]. Available: https://hal.science/hal-04520899v1

[9] R. Saad., F. AZIZI, and H. BADDIH, "Comparative analysis morocco-south korea in the context of e6administration and the digital transition of the state," *International Journal of Accounting, Finance, Auditing, Management and Economics*, vol. 5, pp. 312–331, 2024.

[10] M. Janssen, Y. Charalabidis, and A. Zuiderwijk, "Benefits, adoption barriers and myths of open data and open government," *Information Systems Management*, vol. 29, 2012.

[11] E. Cairns and A. Dawes, "Children: Ethnic and political violence-a commentary," *Child Development*, vol. 67, 1996.

[12] Y. Charalabidis, A. Zuiderwijk, C. Alexopoulos, M. Janssen, T. Lampoltshammer, and E. Ferro, *Open government data: Areas and directions for research*, 2018, vol. 28.

[13] J. C. Bertot, P. T. Jaeger, and J. M. Grimes, "Using icts to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies," *Government Information Quarterly*, vol. 27, 2010.

[14] P. T. Jaeger, J. Lin, and J. M. Grimes, "Cloud computing and information policy: Computing in a policy cloud?" *Journal of Information Technology and Politics*, vol. 5, 2008.

[15] J. R. Gil-Garcia, A. Guler, T. A. Pardo, and G. B. Burke, "Trust in government cross-boundary information sharing initiatives: Identifying the determinants," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2010.

[16] F. Karlsson, M. Frostenson, F. Prenkert, E. Kolkowska, and S. Helin, "Inter-organisational information sharing in the public sector: A longitudinal case study on the reshaping of success factors," *Government Information Quarterly*, vol. 34, 2017.

[17] I. Mergel, "The use of social media to dissolve knowledge silos in government." *The Future of Public Administration, Public Management and Public Service Around the World: The Minnowbrook Perspective*, 2011.

[18] OECD, "Society at a glance 2019," *Society at a Glance*, 2019.

[19] T. Martens, "Electronic identity management in estonia between market and state governance," *Identity in the Information Society*, vol. 3, 2010.

[20] B. Obama, "Memorandum on transparency and open government," *Federal Register*, 2009.

[21] C. European, "Isa² - interoperability solutions for public administrations, businesses and citizens," *The New European Interoperability Framework*, 2017.

[22] A. D. D. E. I. INDIRECTS, *ADMINISTRATION DES DOUANES ET IMPÔTS INDIRECTS 2023 « Rapportd'activité 2022 »*, 2022.

[23] M. BELHASSANI, "Digitalization of public administration and attracting investments in morocco," *International Journal of Accounting, Finance, Auditing, Management and Economics,*, vol. 4, pp. 426–440, 2023.

[24] S. Laghmari, *DEVELOPING A NATIONAL "INTEGRATED" AND "CITIZEN-CENTRIC" DIGITAL STRATEGY IN THE MOROCCAN PUBLIC ADMINISTRATION*, 2017.

[25] H. Radoine, "Digital morocco 2020: A strategy for digital transformation," *Journal of Digital Innovation*, 2019.

[26] S. Benabdelkader, "Digital transformation in the moroccan customs administration," *Journal of Customs and Trade*, 2018.

[27] A. Bouy, "Challenges in implementing data sharing systems in morocco," *Journal of Information Systems*, 2020.

[28] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system, october 2008," *Cited on*, 2008.

[29] A. A. A. Saveen, "Blockchain ready manufacturing supply chain using distributed ledger," *International Journal of Research in Engineering and Technology*, vol. 05, 2016.

[30] Y. Guo and C. Liang, "Blockchain application and outlook in the banking industry," *Financial Innovation*, vol. 2, 2016.

[31] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016*, 2016.

[32] XAYA, "The ultimate blockchain gaming platform," *[Online].Available*, 2017.

[33] "Blockchain gaming : The good, the bad, the ugly, and all their intersections | hacker noon." *[Online]. Available.*

[34] M. Swan, *Blockchain: Blueprint for a new economy*, 2013.

[35] D. Bhowmik and T. Feng, "The multimedia blockchain: A distributed and tamper-proof media transaction framework," in *International Conference on Digital Signal Processing, DSP*, vol. 2017-August, 2017.

[36] H.-N. D. X. C. Z. Zheng, S. Xie and H. Wang, "Blockchain challenges and opportunities: a survey„" *Int. J. Web and Grid Services*, vol. 14, no 4, 2018.

[37] A. M. Antonopoulos and G. Wood, *astering ethereum : building smart contracts and dapps*, 2019.

[38] U. A.-S. A. Khan, S. Amin, "P2p energy trading of evs using blockchain technology in centralized and decentralized networks: A review," *Energies*, 2024.

[39] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, 2017.

[40] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," *Journal of Cryptology*, vol. 3, 1991.

[41] R. Katarya and A. Mustafa, "Blockchain and consensus algorithms," *SSRN Electronic Journal*, 2020.

[42] D. I. C. Kroll, J. A. and E. W. Felten, "The economic and technological limits of bitcoin mining," in *Proceedings of the 2013 ACM Conference on Electronic Commerce*, 2013.

[43] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, 1997.

[44] V. Buterin, "A next-generation smart contract and decentralized application platform," *Etherum*, 2014.

[45] E. Androulaki, A. Barger, V. Bortnikov, S. Muralidharan, C. Cachin, K. Christidis, A. D. Caro, D. Enyeart, C. Murthy, C. Ferris, G. Laventman, Y. Manevich, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, and J. Yellick, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proceedings of the 13th EuroSys Conference, EuroSys 2018*, vol. 2018-January, 2018.

[46] N. E. Ioini and C. Pahl, "A review of distributed ledger technologies," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11230 LNCS, 2018.

[47] A. M. Antonopoulos and O. Media, "Mastering bitcoin," *CA*, vol. 95472, 2014.

[48] H. young Paik, X. Xu, H. D. Bandara, S. U. Lee, and S. Kuang, "Lo, analysis of data management in blockchain-based systems: From architecture to governance," *IEEE Access*, vol. 10, no. 1109, p. 4, 2019.

[49] A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, and J. Clark, *Bitcoin and Cryptocurrency Technologies Introduction to the book*, 2016.

[50] M. Pors. (2023) Understanding the ipfs white paper part 2. [Online]. Available: https://decentralized.blog/understanding-the-ipfs-white-paper-part-2.html

[51] N. Nizamuddin, H. R. Hasan, and K. Salah, *IPFS-Blockchain-Based Authenticity of Online Publications*. 10.1007, p. 199–212: Springer, 2018.

[52] A. Tuladhar, M. Rogerson, J. Engelhart, G. C. Parry, and B. Altrichter, "Blockchain for compliance: an information processing case study of mandatory supply chain transparency in conflict minerals sourcing," *Supply Chain Management*, 2024.

[53] P. Maya and P. A. Salam, "Implementation of a blockchain-based dapp for p2p electricity trading," in *IEEE, 2024*. 5th International Conference on Energy, Power and Environment: Towards Flexible Green Energy Technologies (ICEPE, 2024.

[54] S. M. Jain, *Introduction to Remix IDE*, Berkeley, CA, 2023, edited by A. Brief Introduction to Web3. Apress and Berkeley, C. A..

[55] R. Bahadure, R. Khasare, S. Mahure, L. Rathod, and S. Junghare, "Thr3ebay: E-commerce dapp using blockchain," *International Journal for Research in Applied Science and Engineering Technology*, vol. 11, p. 5, 2023.

[56] S. D. Hemani and R. K. Dwivedi, "Designing blockchain based secure autonomous vehicular internet of things (iot) architecture with efficient smart contracts," *International Journal of Information Technology*, 2024.

[57] J. I. Sihotang, Y. R. Simanjuntak, and A. F. Pakpahan, "Membership information system using node jsabstract," in *Proceedings International Scholars Conference*. Vol. 7, 2019.

[58] R. Böhme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, technology, and governance," *Journal of Economic Perspectives*, vol. 29, 2015.

[59] P. Noizat, *Blockchain Electronic Vote*, 2015.

[60] J. M. Graglia and C. Mellon, "Blockchain and property in 2018: At the end of the beginning," *Innovations: Technology, Governance, Globalization*, vol. 12, 2018.

[61] J. F. Galvez, J. C. Mejuto, and J. Simal-Gandara, "Future challenges on the use of blockchain for food traceability analysis," *TrAC - Trends in Analytical Chemistry*, vol. 107, 2018.

[62] S. R. Zambrano R. and S. C., "Using blockchain for a more transparent and inclusive government," *Inter-American Development Bank*, 2017.

[63] S. Leekha, "Book review: Don tapscott and alex tapscott, blockchain revolution: How the technology behind bitcoin is changing money, business, and the world," *FIIB Business Review*, vol. 7, 2018.

[64] S. Dubai, "Dubai blockchain strategy," *Smart Dubai*, 2016.

[65] W. Mougayar, "The business blockchain: Promise, practice, and application of the next internet technology," *John Wiley and Sons*, 2016.

[66] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services, Healthcom 2016*, 2016.

[67] O. Singore, F. Chesi, and M. Pallotti, "E-government: challenges and opportunities," in *CMG Italy - XIX Annual Conference*, 2005.

[68] G. Ntulo and J. Otike, *E-government: its Role, Importance and Challenges*. Academia, 2013.

[69] S. Majdoub and C. Loqman, "A new integer model for the management of booking stays at summer resorts," *Computers and Industrial Engineering*, vol. 107214, p. 154, 2021.

[70] C. L. O. A. Barakat Oumkaltoum El, beqqali Omar, "Hybrid e-government framework based on datawarehousing and mas for data interoperability," *IJACSA,12*, p. 10, 2021.

[71] Comnet-It, *Country Profiles Of E-Governance*, 2002.

[72] Z. B. Nechba, A. Boujibar, and A. Alj, "Good governance and digitalization in morocco: State of the art," *International Journal of Business and Technology Studies and Research*, vol. 4, no. 1, 2022.

[73] T. Abdelkhalek *et al.*, "How can the digital economy benefit morocco and all moroccans?" The Economic Research Forum, Working Paper N, 2021.

[74] U. Nations and E.-G. Survey, "The future of digital government," *New York*, vol. 2022, p. 63, 2022.

[75] J. Collomosse, T. Bui, A. Brown, J. Sheridan, A. Green, M. Bell, J. Fawcett, and J. Higgins, "Archangel: Trusted archives of digital public documents."

[76] T. Bui, D. Cooper, J. Collomosse, M. Bell, A. Green, J. Sheridan, J. Higgins, A. Das, J. Keller, O. Thereaux, and A. Brown, "Archangel: Tamper-proofing video archives using temporal content hashes on the blockchain, (2019)."

[77] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—a systematic review," *PLoS ONE*, vol. 11, no. 10, p. e0163477, 2016.

[78] I. Zhou, I. Makhdoom, M. Abolhasan, J. Lipman, and N. Shariati, "A blockchain-based file-sharing system for academic paper review," (2019).

[79] A.-M. Isaac, I. O. Agyemang, C. Sey, and A. A. Salako, "Securing music sharing platforms: A blockchain-based approach," (2022).

[80] I. Permatasari, M. Essaid, H. Kim, and H. Ju, *Blockchain Implementation to Verify Archives Integrity on Cilegon E-Archive, applied sciences.* MDPI, 2020.

[81] E. Nyaletey, R. M. Parizi, Q. Zhang, and K. K. R. Choo, "Blockipfs-blockchain-enabled interplanetary file system for forensic and trusted data traceability," in *Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta*, 2019, pp. 18–25.

[82] M. Pincheira, E. Donini, R. Giaffreda, and M. Vecchio, "A blockchain-based approach to enable remote sensing trusted data," in *Proceedings of the 2020 IEEE Latin American GRSS and ISPRS Remote Sensing Conference (LAGIRS), Santiago, Chile*, 2020, pp. 652–657.

[83] M. Pincheira, E. Donini, M. Vecchio, and S. A. Kanhere, "Decentralized architecture for trusted dataset sharing using smart contracts and distributed storage," *Sensors, MDPI*, vol. 22, p. 9118, 2022.

[84] A. Antonio-Hernandez, H. Ferreira-Medina, C. Torres-Millarez, and J. C. Olivares-Rojas, "Management of digital documents with encrypted signature, through the use of centralized pki, and distributed using blockchain for a secure exchange," *Journal of Research and Development*, vol. 5 N 15, pp. 26–37, 2019.

[85] Y. shaher Alslman and A. A. Taleb, "Exchanging digital documents using blockchain technology." the 3rd International Conference on Electrical, Communication and Computer Engineering (ICECCE), 2021.

[86] A. Zaanoun, *Morocco: The Impact of the Digitization of Public Services.* Arab Reform Initiative, 2023.

[87] C. Elhilali, "Public administration reform and development stakes in morocco," *Journal of Legal, Ethical and Regulatory Issues*, vol. 25, p. 4, 2022.

[88] T. Bult, *Security analysis of blockchain technology.* Business Information Technology, 2019.

[89] N. Nizamuddina, K. Salaha, M. A. Azadb, J. Arshadc, and M. H. Rehmand, "Decentralized document version control using ethereum blockchain and ipfs," *Computers and Electrical Engineering*, pp. 183–197, 2019.

[90] Y. I. R. J. S. P. Hasan H.R., Salah K. and O. M., "Trustworthy iot data streaming using blockchain and ipfs," *IEEE Access*, 2022.

[91] G. Ntulo and J. Otike, *E-government: its role, importance and challenges*. Academia, 2013.

[92] S. Idhiarhi, *Improving record management and security of exhibits: the role of judicial administrators. Workshop organised for Chief Registrars*. Abuja, 2016.

[93] A. Abiola, "Court records management and efficient administration of justice in nigeria," *African Journal of Library, Archives and Information Science*, vol. 24, pp. 795–4778, 2014.

[94] M. Denever, J. T. Pickett, and S. D. Bushway, "Criminal records and employment: A survey of experiences and attitudes in the united states," *07418825.2017.1340502*, 2018.

[95] D. N. Lee, *The Effect of Online Criminal Records on Crime*. COLUMBIA, 2011.

[96] T. Morocco, *High Commission for planing report*, 2021.

[97] S. Ali, S. A. Alvi, and A. U. Rehman, "The usual suspects: Machine learning based predictive policing for criminal identification." Lahore, Pakistan, doi: 10.1109/ICOSST48232.2019.9043925: ICOSST, 2019.

[98] 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.

[99] A. Haque and T. Mannan, "Upgradation and maintenance of crime data management system (cdms) and personnel information management system (pims)," *PHQ-CDMS-RS-001*, 2017.

[100] A. Sharma and M. Shahnawaz, "Crime records management system," *3rd International Conference on System Modeling Advancement in Research Trends (SMART*, 2014.

[101] 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, pp. 2549–9610, 2019.

[102] S. Cheng, M. Daub, A. Domeyer, and M. Lundqvist, "Using blockchain to improve data management in the public sector," 2017.

[103] A. A. Omar and S. Rahman, "Crab: Blockchain based criminal record management system. the 11th international conference on security, privacy and anonymity in computation, communication and storageat," 2018.

[104] a. D. A. S. A. S. P. A. B. A. Magar Shivani, Magar Harshad R. and M. R. S. Kakade, "Crime record management system," *International Journal of Advanced Research in Science, Communication and Technology*, vol. 4, 2024.

[105] I. A. T. R. D. Suseno 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, p. pp. 1759–1769, 2024.

[106] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology beyond bitcoin," *Inno*, vol. 2, pp. 6–10, 2016.

[107] M. Alghazwi, F. Turkmen, J. V. Velde, and D. Karastoyanova, "Blockchain for genomics:a systematic literature review," *Distributed Ledger Technologies: Research and Practice*, vol. 1, p. pp. 1–28, 2022.

[108] P. Shukla, R. Tyagi, and A. Tyagi, "Implementation of blockchain on criminality," *International Journal of Engineering Research and Technologies*, vol. 9, p. 4, 2020.

[109] 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*, pp. 2736–5492, 2023.

[110] P. Makwana and D. P. Sharma, "Criminal record keeping with blockchain,"," *Journal of Emerging Technologies and InnovativeResearch*, vol. 6, p. 4, 2019.

[111] Y. Borse, D. Patole, G. Chawhan, G. Kukreja, H. Parekh, and R. Jain, "Advantages of blockchain in digital forensic evidence management," in *Proceedings of the 4th*

International Conference on Advances in Science and Technology (ICAST2021), 2021.

[112] R. Z. Fathiyana, S. N. Yutia, and D. J. Hidayat, "Prototype of integrated national identity storage security system in indonesia usning blockchain technology," *JOIV: International Journal on Informatics Visualization.*, vol. 6, p. 1, 2022.

[113] M. B. R. C. Mullegowda, N. Hiremani 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, pp. pp. 617–630,, 2023.

[114] S. M. Jain, ""introduction to remix ide," in a brief introduction to web3," *Berkeley, CA: Apress*, p. pp. 89–126, 2023.

[115] N. Nizamuddina, K. Salaha, M. A. Azadb, J. Arshadc, and M. H. Rehmand, "Decentralized document version control using ethereum blockchain and ipfs," *Computers and Electrical Engineering*, pp. 183–197, 2019.

[116] C.-L. Chen, Y.-M. Zheng, D.-C. Huang, L.-C. Liu, and H.-C. Chen, "A blockchain and ipfs-based anticounterfeit traceable functionality of car insurance claims system," *Sensors*, vol. 23, p. 9577, 2023.

[117] F. A. Pujol, M. Higinio, R. Tamai, R. Carlos, and B. Arturo, "Blockchain-based framework for traffc event verifcation in smart vehicles," *"in press.*

[118] M. Pincheira, E. Donini, R. Giaffreda, and M. Vecchio, "A blockchain-based approach to enable remote sensing trusted data," in *Proceedings of the 2020 IEEE Latin American GRSS and ISPRS Remote Sensing Conference (LAGIRS), Santiago, Chile*, 2020, pp. 652–657.

[119] M. Pincheira, E. Donini, M. Vecchio, and S. A. Kanhere, "Decentralized architecture for trusted dataset sharing using smart contracts and distributed storage," *Sensors, MDPI*, vol. 22, p. 9118, 2022.

[120] N. Muqaddas, A. Fahad, K. Rabiya, J. Nadeem, M. Ali, K. Muhammad, and S. Muhammad, "A secure data sharing platform using blockchain and interplanetary file system, sustainability."

[121] S. . Abinesh Kannan, M. . Akash, B. . Brajesh Choudhary, M. . Maheswari, and K. Amsavalli, "Road accident detection and notification for speed recovery," *Inter-*

national Journal of Advanced Research in Computer and Communication Engineering. ., vol. 12, no. 4, April 2023.

[122] V. Anusha, B. Basudeb, S. Sourav, and K. Ashok, "Blockchain-enabled certificate-based authentication for vehicle accident detection and notification in intelligent transportation systems. ieee sensors journal, july 15," vol. 21, no. 14, 2021.

[123] A. . Salar, A. Saman, S. Rifat, and U. Furkan, "A transformative solution for construction safety: Blockchain-based system for accident information management," *Journal of Industrial Information Integration*, vol. 35, p. 100491, 2023.

[124] Z. Ian, M. Imran, A. Mehran, L. Justin, and S. Negin, *A Blockchain-based File-sharing System for Academic Paper Review, (2019), p.* DOI: 10, 2019.

[125] I. Adjei-Mensah, O. Isaac, S. Collins, and A. Abdulhaq, "Securing music sharing platforms: A blockchain-based approach," (2022), 2110.05949.

[126] P. Intan, E. Meryam, K. Hyeonwoo, and J. Hongtaek, *Blockchain Implementation to Verify Archives Integrity on Cilegon E-Archive, Applied Sciences.* MDPI, 2020.

[127] G. A. Oliveira, O. d. F. Oliveira, S. de Abreu, R. W. de Bettio, and A. P. Freire, "Opportunities and accessibility challenges for open-source general-purpose home automation mobile applications for visually disabled users," *Multimed. Tools Appl.*, vol. 81, pp. 10 695–10 722, 2022.

[128] M. Krichen, "Anomalies detection through smartphone sensors: A review," *IEEE Sens. J.*, vol. 21, pp. 7207–7217, 2021.

[129] H. S. Musa, M. Krichen, A. A. Altun, and M. Ammi, "Survey on blockchain-based data storage security for android mobile applications," *Sensors*, vol. 23, p. 8749, 2023.

[130] M. A. Krichen, "Survey on formal verification and validation techniques for internet of things," *Appl. Sci.*, vol. 13, p. 8122, 2023.

[131] M. Krichen, M. Lahami, O. Cheikhrouhou, R. Alroobaea, and A. J. Maâlej, "Security testing of internet of things for smart city applications: A formal approach," pp. 629–653, 2020.