الجمهورية الجزائرية الديمقراطية الشعبية

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE DR. YAHIA FARES DE MEDEA

FACULTE DE SCIENCE

Département de mathématiques et d'informatique



Mémoire de Fin d'Études

Présenté pour l'obtention du Diplôme
De Master en informatique

Option : Ingénierie des systèmes et technologies du web

THEME

Implémentation d'un système de validation de signature numérique par l'utilisation du protocole de Blockchain

(Réseaux des mineurs internes)

Proposé et dirigé par:

Mr. Tassalit Ahmed ‹‹ Voisinage PC ››

Mr. Toubal El bahi ‹‹ Faculté des sciences ››

Préparé et présenté par,

Mr. Abdelbasset Hamma

Mr. Abderrahmane Benkreira

Année Universitaire 2018-2019

Dédicaces

À ma famille qui m'a toujours témoigné son affection et apportée

réconfort et aide à tout moment.

À la prunelle de mes yeux, mes parents à qui

je leur dois mon éducation, « je prie Dieu pour les protéger et les garde pour moi. »

À mes frères :

Mohamed, Abdelkarim, Abdelkader, Noureddine, Redouane

À mes ami(e)s :

Abdelbasset, Tarek, Kamel, Hocine

À la fleur et la joie de notre maison Amina

À mes oncles et mes tantes

À mes cousins et cousines

À touts ceux qui ont contribué de près ou de loin pour la réalisation de mon travail.

BENKREIRA Abderrahmane

À ma famille qui m'a toujours témoigné son affection et apportée

Réconfort et aide à tout moment.

À la prunelle de mes yeux, mes parents à qui

je leur dois mon éducation, « je prie Dieu pour les protéger et les garde pour moi. »

À ma chère fiancée, qui m'a soutenue dans mes bons et mes mauvais moments, merci Beaucoup

À mes frères :

Mohamed, Salah eddine, Abdelaziz, Fatima Zohra, Nabila

À mes ami(e)s :

Abderrahmane, Tarek, Kamel, Khaled

Un merci spécial à ma sœur Fatima Zohra

À touts ceux qui ont contribué de près ou de loin pour la réalisation de mon travail.

Hamma Abdelbasset

Remerciement

Nous tenons, tout d'abord, à remercier Dieu qui nous a porté aide pour réaliser ce travail.

Nous tenons également à remercier et à exprimer notre profonde gratitude, nos reconnaissances et nos vifs remerciements à nos encadreurs d'avoir accepté de diriger notre travail et pour toutes les informations et les conseils qu'ils nous ont donnés.

Nos remerciements vont aussi aux membres du jury qui ont accepté de lire et d'évaluer ce travail.

À tous, Merci.

Résumé́

Une blockchain « ou chaîne de blocs » est un réseau permettant d'opérer des transactions en toute sécurité́ et sans l'intervention d'une partie tierce. Il s'agit d'un grand livre comptable public consignant les transactions de manière incontestable.

La blockchain a des différentes applications, elle a été premièrement utilisée dans le secteur de la crypto-monnaie, ou le majeur avantage de la technologie de blockchain est la protection des données dites critiques ainsi qu'assurer la propriété des biens.

Dans ce travail on s'intéressait à l'utilisation du Blockchain pour la validation des signatures numériques des transactions effectuées par et entre entités à travers des documents numériques, ainsi que protéger l'identité contre le vol on se basons sur des transactions similaires à la transaction du bitcoin.

Mots-clés : Blockchain, crypto-monnaie, bitcoin, transaction, Signature numérique.

Abstract

A blockchain "or chain of blocks" is a network to operate transactions safely and without the intervention of a third party. It is a large public accounting book recording transaction in an indisputable way.

The blockchain has different applications, it was first used in the cryptocurrency sector, where the major advantage of blockchain technology is the protection of so-called critical data as well as the property ownership.

In this work we are interested in the use of the Blockchain for the validation of the digital signatures of the transactions carried out by and between entities through digital documents, as well as protecting the identity against theft, basing on transactions similar to the Bitcoin transactions.

Keywords: Blockchain, Cryptocurrency, Bitcoin, Transaction, Digital Signature.

ملخص

إن البلوك تشين "أو سلسلة الكتل" عبارة عن شبكة لتشغيل المعاملات بأمان وبدون تدخل طرف ثالث.

إنه دفتر محاسبة عام كبير يسجل المعاملات بطريقة لا جدال فيها.

تطبيقات البلوك تشين مختلفه ، تم استخدامه لأول مرة في قطاع العملة المشفرة ، حيث تتمثل الميزة الرئيسية لتكنولوجيا البلوك تشين في حماية ما يسمى بالبيانات الهامة وكذلك ملكية البضائع.

في هذا العمل، نحن مهتمون باستخدام البلوك تشين للتحقق من صحة التوقيعات الرقمية للمعاملات التي تنفذها أطراف لوحدها او بينها من خلال الوثائق الرقمية ، وكذلك حماية الهوية ضد السرقة ، بالاستناد إلى معاملات مشابهة لمعاملات البيتكوين.

الكلمات الدلالية: بلوك تشين، العملات الرقمية، البيتكوين، المعاملات، التوقيع الرقمي.

Liste des abréviations

- **RSA:** **R**ivest–**S**hamir–**A**dleman. - AES : Advanced **E**ncryption **S**tandard

- **ASCII** : **A**merican **S**tandard **C**ode for **I**nformation **I**nterchange.

- **NIST** : **N**ational **I**nstitue of **S**tandards and **T**echnology. - **SSL** : **S**ecure **S**ockets **L**ayer

- **MAC** : **M**essage **A**uthentication **C**ode. - **NSA** : **N**ational **S**ecurity **A**gency.

- **MD2**, **MD4**, **MD5** : **M**essage **D**igest - **SHA** : **S**ecure **H**ash **A**lgorithm.

- **MITM** : **M**an **I**n **T**he **M**iddle. - **PKI** : **P**ublic **K**ey **I**nfrastructure

- **CA** : **C**ertification **A**uthority - **VPN** : **V**irtual **P**rivate **N**etwork,

- ECDSA : **E**lliptic **C**urve **D**igital **S**ignature **A**lgorithm - **P2P : P**eer **T**o **P**eer

- **PoA : P**roof **O**f **A**uthority - **SQL** : **S**tructured **Q**uery **L**anguage

- **PoS : P**roof **O**f **S**take **PoW : P**roof **O**f **W**ork - **RA** : **R**egistration **A**uthority

- **TH** : **T**erra **H**achages **IoT** : **I**nternet Of Things - **DES** : **D**ata **E**ncryption **S**tandard.

- **UML** : **U**nified **M**odeling **L**anguage

- **ACID**: (**A**tomicity, **C**onsistency, **I**solation, **D**urability

Liste des figures

Figure.1 fonctionnement du Chiffrement symétrique.....6
Figure 2 fonctionnement du Chiffrement asymétrique.....8
Figure 3. La fonction de hachage.....11
Figure 4. La signature numérique et la vérification.....13
Figure 5. L'attaque Man in the middle.....14
Figure 6. Architecture du PKI.....18
Figure 7. Schéma de chaîne des bloc.....25
Figure 8. Le réseau poste à poste (P2P).....27
Figure 9. Les types de blockchain.....28
Figure 10. Le Fonctionnement de blockchain.....29
Figure 11. Structure des blocs dans la Blockchain ….....30
Figure 12. Minage de blocs par tentatives successives.....31
Figure 13. Résolution du cas du bloc contradictoire.....33
Figure 14 exemples de transaction blockchain 35
Figure 15. Un smart contrat dans la blockchain.....37
Figure 17. Le réseau Blockchain.....41
Figure 18. Confidentialité de blockchain.....42
Figue 19. Une transaction crypto-monnaie en Bitcoin.....47
Figure 20 . Nombre estimé de terra hachages par seconde exécutés par le réseau Bitcoin.....49
Figure 21. Plateformes de minage du bitcoin.....50
Figure 22. La connexion entre le client et le mineur.....61
Figure 23. La connexion entre le client et le mineur.....61
Figue 24. La connexion entre les Mineurs entre eux.....62
Figue 24. La connexion entre les Mineurs entre eux.....63
Figure 26. Diagramme d'activités ‹‹création de l'identité ››.....65
Figure 27. Diagramme d'activités ‹‹ l'authentification ››.....68
Figure 28. Diagramme d'activités ‹‹signature individuelle››.....71
Figure 29. La signature collective(partie1).....74
Figure 30. La signature collective(partie 2) 75
Figure 31. La création des blocs 78
Figure 32. La validation des blocs reçus.....81
Fgure 33 : Architecture de fonctionnement d'application.....88

Figure 34 : interface d'accueil.....91
Figure 35 : interface Ajouter un Client.....92
Figure 36. interface d'accueil du Mineur Central.....93
Figure 37. interface d'accueil du Mineur.....94
Figure38 : interface du Connexion.....95
Figure 39 : Interface de Portefeuille.....96
Figure 40 . Interface de la signature individuelle.....97
Figure 41. Interface de la signature collective.....98
Figure 42 : Interface de l'invitation.....99

Liste des abréviations

Liste des figures.

Résumé.

Introduction Générale …….....…….……02

Chapitre I : La Cryptographie

I.1 Introduction …….....……05

I.2 La cryptographie …….....…….....…….……05

I.2.1 Définition ……....……..05

I.2.2 L'usage de la cryptographie …….....……...05

I.3 Le chiffrement symétrique …….....……06

I.3.1 Principe…….....…….... 06

I.3.2 Principe de fonctionnement …….....……06

I.4 Le chiffrement AES …….....……07

I.6.1 Fonctionnement du chiffrement AES…….....….07

I.5 Chiffrement asymétrique…….....……07

I.4.1 Principe…….....…….... 08

I.4.2 Principe de fonctionnement …….....……08

I.6 Le chiffrement RSA …….....……09

I.5.1 Principe de fonctionnement …….....……09

I.7 Fonction de Hachage …….....…..11

I.7.1 Propriétés…….....…..…11

I.7.2 Utilisation — Authentification et intégrité …….....……12

I.7.3 Principaux algorithmes …….....……...12

I.8 La signature numérique …….....……12

I.8.1 Définition …….....….12

I.8.2 Principe de la signature numérique …….....…...…13

I.9 Le certificat numérique …….....……..14

I.9.1 L'attaque Man in the Middle …….....…..14

I.9.2 Définition du certificat numérique …….....14

I.9.3 Structure d'un certificat X.509 …….....15

I.10 PKI (Infrastructure à clés publiques) …….…….....16
I.10.1 Définition ……..…….....14
I.10.2 Fonctionnalités d'une PKI …….....15
I.10.3 La gestion des clés …….....16
I.10.4 Acteurs d'une PKI …….....17
I.11 Le certificat et la signature numérique dans la loi algérienne ……..…….....18
I.11.1 Quelques lois sur le certificat et la signature numérique dans la loi algérienne.....18
I.12 Conclusion ……..……...22

Chapitre II : La Blockchain

II.1 Introduction..... .24
II.2 Historique..... 24
II.3 Définition..... 24
II.4 Valeurs principales des chaines de blocs..... 26
II.5 Typologie de la Blockchain..... 27
II.5.1. Blockchain publique..... 27
II.5.2. Blockchain Privée..... 28
II.5.3 Blockchain Consortium (Hybride) 28
II.6 Fonctionnement..... 28
II.7 Concepts de la Blockchain..... 29
II.7.1 Le bloc..... 29
II.7.2 La preuve de travail (NONCE) 30
II.7.3 Vérification de bloc 31
II.7.3 .1. Le cas des entrées des données contradictoires 32
II.7.3 .1. Le cas du bloc contradictoire 32
II.7.4 Transaction..... 33
II.7.4.1 La Sérialisation 33
II.7.4.2. Le Hash d'une transaction : 34
II.7.4.3. Identifiant de transaction : 34
II.7.4.4. Les clés cryptographiques 34
II.7.5 Messages 35
II.7.6 Le minage (La création du bloc) 35

II.7.7 Les contrats intelligentes..... 36
II.7.8 DApp (Decentralized Application) 37
II.7.9 le consensus..... 38
II.8 Fraude à double dépense 39
II.8.1 Principe 39
II.8.2 La prévention 40
II.9 . Le réseau blockchain..... 40
II.10 Confidentialité : 41
II.11 Conclusion : 42

Chapitre III : Les applications de Blockchain

III.1 INTRODUCTION …….. 44
III.2 La Crypto-monnaie ……..…….. 44
III.2.1 Définition ……...…….. 44
III.2.2 Avantages des crypto-monnaies ……..…….. 44
III.2.3 Inconvénients des crypto-monnaies …….. 44
III.3 Bitcoin ……...…… 45
III.3.1 Définition ……...…….…… 45
III.3.2 Caractéristiques de la monnaie Bitcoin ……...……..... 45
III.3.3 Concepts et mécanismes nécessaires ……...…….... 46
III.3.4 Outils technologiques nécessaires ……...…….... 46
III.3.5 Transactions ……...…….... 46
III.3.6 Le portefeuille électronique..... 46
III.3.7 Validation ……...…….…….... 47
III.3.8 La difficulté du réseau bitcoin ……...…….... 47
III.3.9 le minage dans le bitcoin……..…….. 49
III.4 Internet des objets (Iot) ……..…… …… 50
III4.1. Cas d'utilisation de la blockchain on Iot ……..…… 51
III.5 Services Gouvernementaux ……...…….…….... 52
III.6 Services d'Identité ……...…….……..... 53

III.8 Conclusion ……..…….……...……...……..... 54

Chapitre IV : Conception du système

IV.1 Introduction ……..…….. .. 56
VI.2 Présentation du projet……...…….……..... 56
VI.2.1 : Objectif.…….…….……..……..…….. 56
IV.3 : Modélisation du système … ……...…….……..... 56
IV.3.1 : Introduction ……...…….……..... 56
IV.3.2 : Identification des acteurs……...…….……..... 57
IV.3.3 : identification des entités du système……...…….…… ….... 57
IV.4. Les spécifications du système ……...…….……..... ... 59
IV.4.1 : Les spécifications fonctionnelles ……...…….……..... 59
IV.4.2 : Les besoins non fonctionnels ……...…….……..... 60
IV.5 : Fonctionnement du système ……...…….……..... 60
IV.5.1 : La connexion réseau entre les composants du système ……...…….…..... 60
IV.6 : Modélisation des spécifications fonctionnelle ……...…….……..... 62
IV.6.1 Diagramme de classes ……...…….……. . 62
IV.6.1.1. Diagramme de classe des entités du systèmes ….....…….....62
IV.6.2 : Diagramme d'activités ……...…….……... 64
IV.6.2.1 : Diagramme d'activités ‹‹création de l'identité ›› ……...…….... 64
IV.6.2.2 : Description textuelle ‹‹création de l'identité ›› ……...…….…….... 66
IV.6.3 : Connexion au portefeuille ‹‹ l'authentification›› ……...…….... 67
IV.6.3.1 : Diagramme d'activités ‹‹ l'authentification›› ……...…….…….... 67
IV.6.3.2 : Description textuelle ‹‹ l'authentification›› .. …….…….…..... 69
IV.6.4 : La signature des fichiers …… .. 70
IV.6.4.1 : La signature individuelle …… .. 70
IV.6.4.1.1 : Diagramme d'activités ‹‹signature individuelle›› 70
IV.6.4.1.2 : Description textuelle ‹‹signature individuelle›› 72
IV.6.4.2 : La signature collective des documents 72

IV.6.4.2.1 : Diagramme d'activités ‹‹ La signature collective ››..... 73
IV.6.4.2.2 Description textuelle‹‹ La signature collective›› 76
IV.6.5 : La création des blocs 77
IV.6.5.1. Diagramme d'activités < Création du bloc > 77
IV.6.5.2. Description textuelle ‹‹ La création du bloc ››..... 79
IV.6.6 : La validation des blocs reçus……...…… .. 80
IV.6.6.1. Diagramme d'activités ‹‹ La validation des blocs reçus ››..... 80
IV.6.6.2. Description textuelle‹‹ La validation des blocs reçus ›› 82
IV.7 : Conclusion …….....……...…… 83

Chapitre V : Implémentation du système

V.1 Introduction 85
V.2 Les technologies utilisées 85
V.2.1.Le Langage de programmation PYTHON 85
V.2.2. Le SQL 85
V.3 Les outils utilisés 86
V.4 Prototypes 87
V.4.1 Architecture de fonctionnement d'application..... 87
V.4.2 Description textuelle 89
V.4.2.1. Coté Autorité 89
V.4.2.2 Coté Client 89
V.4.2.3 Coté Mineur Central 89
V.4.2.4. Coté Mineurs 89
V.5.Présentation des interfaces de l'application 90
V.5.1 Introduction 90
V.5.2 Application de l'Autorité 90
V.5.2.1 Interface d'accueil 90
V.5.2.2 Interface Ajouter un Client..... 91
V.5.3 Application Mineur Central 92
V.5.3.1 Interface d'accueil 92

V.5.4 Application Mineur 93
V.5.4.1 Interface d'accueil..... 93
V.5.5 Application Client 94
V.5.5.1 Interface de Connexion 94
V.5.5.2 Interface de Portefeuille..... 95
V.5.5.3 Interface la signature individuelle 96
V.5.5.4 Interface de la signature collective 97
V.5.5.5 Interface de l'invitation ..... .98
V.6 Conclusion..... 99

Conclusion Générale 101

INTRODUCTION GENERALE

Aujourd'hui, la gestion et le suivi des données administratives sont devenus de plus en plus difficiles même pour les pays développés, le secteur des transactions commerciales ou administratives est un des secteurs critiques qui demande une bonne gestion et un bon suivi où la gestion de ce secteur n'aurait pas possible sans la faculté de noter et de mémoriser les faits et les choses dont nous voulons garder trace, l'Algérie comme État, ainsi que la majorité des entreprises et malgré les tentatives de numériser ce secteur, elle reste loin de garantir la bonne gestion du secteur.

Une numérisation des transactions sans une identité numérique qui garantit et protège l'identité des parties des transactions peut être considérée comme un archivage classique par documents où le vol d'identités est toujours possible et qui peut provoquer des conséquences graves.

Les certificats numériques sont un des outils efficaces pour prouver l'identité numérique des entités (personne, organisme ou entreprise), cet outil peut donner un bon suivi du secteur des transactions.

Un autre point faible dans la gestion du secteur des transactions est la centralisation des données et l'utilisation des bases de données traditionnelles, où un accès à la base de données centrale peut causer des modifications, des additions fraudeuses ou des suppressions des données critiques.

La blockchain est une technologie qui peut garantir l'intégrité et la sécurité des données, cette technologie distribuée permet en effet le stockage d'informations de manière sécurisée sous un registre numérique codé et stocké sur plusieurs ordinateurs dans un réseau public ou privé.

La blockchain est restée longtemps associée à la monnaie électronique, ou grâce à laquelle elle a été introduite, la blockchain a de nombreux autres usages et participe notamment à rendre les entreprises plus efficientes.

L'Algérie a l'opportunité de se positionner en précurseur par l'application de cette technologie dans les différents domaines, et il est indispensable de sensibiliser les sociétés et les entreprises algériennes de cette technologie, et pour cela et dans la continuité de la transformation numérique en Algérie que nous avons essayé dans ce projet de fin d'études d'effectuer une recherche sur la blockchain.

Dans ce contexte nous allons créer un système de validation des transactions signées numériquement grâce à des identités numériques uniques basées sur la technologie blockchain pour le but de faciliter et sécuriser les transactions commerciales ou administratives ainsi que protéger les identités des entités ou notre travail sera organisé de la façon suivante :

Dans le chapitre I, nous allons parler sur la cryptographie, ou nous allons voir qu'est-ce qu'une cryptographie, quels sont les types de la cryptographie, comment fonctionne et quels sont les outils utilisés dans la cryptographie ainsi que le certificat et la signature numérique et leur place dans la loi algérienne.

Le chapitre II inclut le concept du blockchain, ou nous allons voir sa définition, ces caractéristiques, ces composants, son fonctionnement, et son architecture, après on va donner une vision sur la notion fondamentale d'une transaction dans la blockchain et sa preuve de travail.

Dans le chapitre III, nous allons essayer d'exprimer les différents domaines d'application du blockchain ainsi que présenter un exemple d'utilisation dans la monnaie électronique.

Le chapitre IV sera destiné à la conception de notre système ou nous allons présenter notre objectif, les spécifications et les entités du système ainsi que ces différents cas d'utilisations, avec la modélisation de ces cas d'utilisation avec une présentation UML.

Le cinquième et dernier chapitre portera sur la réalisation de notre système, ou nous allons présenter l'architecture de notre système ainsi que l'environnement de développement avec la représentation et l'explication de quelques interfaces de ces différentes applications.

Nous clôturerons ce rapport par une conclusion générale dans laquelle nous présentons une conclusion sur tous les parties du rapport.

CHAPITRE I

LA CRYPTOGRAPHIE

I.1. Introduction :

Depuis le début des civilisations, le besoin de dissimuler préoccupe l'humanité. La confidentialité apparaissait notamment nécessaire lors des luttes pour l'accès au pouvoir.

Puis elle a été énormément développée pour les besoins militaires et diplomatiques, aujourd'hui, de plus en plus d'applications dites civiles nécessitent la sécurité des données transitant entre deux interlocuteurs via un vecteur d'information comme les réseaux de télécommunications actuels et futurs.

Ainsi les banques l'utilisent pour assurer la confidentialité des opérations avec leurs clients, les laboratoires de recherche s'en servent pour échanger des informations dans le cadre d'un projet d'étude commun, les chefs militaires pour donner leurs ordres de bataille, etc.

Le but de ce chapitre est de présenter les fondements et le fonctionnement de la cryptographie. Il intéressera le lecteur qui connait peu ou pas le domaine et qui souhaiterait comprendre le fonctionnement et les mécanismes mis en œuvre en cryptographie. Un minimum de culture mathématique sera parfois nécessaire lors de la lecture de certains paragraphes.[1].

I.2. La cryptographie :

I.2.1. Définition :

La cryptographie, ou l'art de chiffrer est devenu aujourd'hui une science à part entière. Au croisement des mathématiques, de l'informatique, et parfois même de la physique, elle permet ce dont les civilisations ont besoin depuis qu'elles existent : le maintien du secret. Pour éviter une guerre, protéger un peuple, il est parfois nécessaire de cacher des choses.[2]

I.2.2. L'usage de la cryptographie :

La cryptographie est traditionnellement utilisée pour dissimuler des messages aux yeux de certains utilisateurs. Cette utilisation a aujourd'hui un intérêt d'autant plus grand que les communications via internet circulent dans des infrastructures dont on ne peut garantir la fiabilité et la confidentialité.

Désormais, la cryptographie sert non seulement à préserver la confidentialité des données, mais aussi à garantir leur intégrité et leur authenticité.[3]

- **La confidentialité :** La confidentialité est le caractère réservé d'une information ou d'un traitement dont l'accès est limité aux seules personnes admises à la (le) connaitre pour les besoins du service, ou aux entités ou processus autorisés.

- **L'intégrité :** L'intégrité est la propriété assurant qu'une information ou un traitement n'a pas été modifié ou détruit de façon non autorisée.
- **L'authentification :** consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées.
- **La non-répudiation :** de l'information est de garantir qu'aucun des concernés ne pourra nier cette information.[4]

I.3. Le chiffrement symétrique :

Le chiffrement symétrique, que l'on nomme couramment chiffrement conventionnel, basé sur des fonctions mathématiques réversibles. Le chiffrement symétrique repose sur un principe de clé unique pour chiffrer et déchiffrer.[5]

I.3.1. Principe :

Le principe du cryptage à clé symétrique (ou secrète) est que la même clé doit être employée pour chiffrer ou déchiffrer le message.

I.3.2. Principe de fonctionnement :

Le chiffrement consiste alors à effectuer des opérations de chiffrement entre la clé privée et les données à chiffrer, le déchiffrement se fait à l'aide de cette même clé secrète.

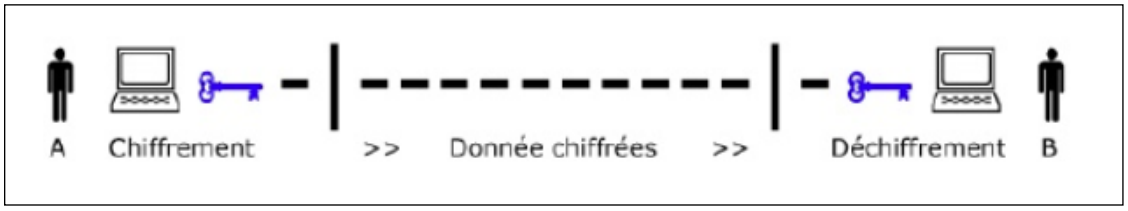


Figure.1 fonctionnement du Chiffrement symétrique.

- **Remarques :**

La qualité d'un cryptosystème symétrique se mesure par rapport :

- À des propriétés statistiques des textes chiffrés.
- À la résistance aux classes d'attaques connues.

En pratique : Un crypte système est bon tant qu'il n'est pas cassé.

I.4. Le chiffrement AES :

L'AES (Advanced Encryption Standard) est comme son nom l'indique, un standard de cryptage symétrique destiné à remplacer le DES (Data Encryption Standard) qui est devenu trop faible au regard des attaques actuelles. Historiquement, le développement de l'AES a été instigué par le NIST (National Institue of Standards and Technology). Il est également approuvé par la NSA (National Security Agency) pour le cryptage des informations dites très sensibles. Cet algorithme suit les spécifications suivantes :

- L'AES est un standard, donc libre d'utilisation, sans restriction d'usage ni brevet.
- C'est un algorithme de type symétrique
- C'est un algorithme de chiffrement par blocs
- Il supporte différentes combinaisons [longueur de clé] — [longueur de bloc] : 128-128, 192-128 et 256-128 bits (en fait, l'AES supporte également des tailles de blocs variables, mais cela n'est pas retenu dans le standard). [9].

I.4.1 : Fonctionnement du chiffrement AES :

AES comprend trois algorithmes de chiffrement par blocs : AES-128, AES-192 et AES-256, chaque code chiffre et déchiffre les données par blocs de 128 bits au moyen de clés cryptographiques de 128, 192 et 256 bits, respectivement.

Les codes symétriques ou à clé secrète utilisent la même clé pour le chiffrement et le déchiffrement. L'expéditeur et le destinataire doivent donc connaitre et utiliser la même clé secrète. Toutes les longueurs de clé sont jugées suffisantes pour protéger des informations classées jusqu'au niveau « Secret ». En revanche, des informations de niveau « Top Secret » nécessitent des clés de 192 ou 256 bits. Il faut 10 tours pour une clé de 128 bits, 12 pour une clé de 192 bits et 14 pour une clé de 256 bits. Un tour comprend plusieurs étapes de traitement : la substitution, la transposition et la combinaison du texte en clair en entrée avant sa transformation finale en cryptogramme.

Le chiffrement AES est fiable. Les seules attaques réussies se sont produites au niveau du canal auxiliaire sur des failles d'implémentation ou de gestion des clés de certains produits de chiffrement AES.

I.5. Chiffrement asymétrique :

La distribution des clés a été le point faible des systèmes de cryptographie symétrique.

En 1976, Whitfield Diffie et Martin Hellman proposent une nouvelle façon de procéder, qui contourne cet écueil, dans la cryptographie asymétrique, aussi appelée cryptographie à clé publique on utilise une paire de clés asymétriques, une clé publique et une clé privée correspondante, pour chiffrer et déchiffrer les données.

Dans un système cryptographique à clé publique, les utilisateurs possèdent deux clés relatives et complémentaires, l'une pouvant être révélée publiquement, l'autre devant rester secrète, la cryptographie asymétrique permet donc d'assurer que le message envoyé demeure confidentiel, et ce sans être contraint d'utiliser auparavant une voie sure afin de s'échanger les clés.

La première clé demeure privée et secrète et n'est généralement connue que par son détenteur, l'autre est publique et figure habituellement dans un répertoire électronique.

Si l'on utilise la clé publique pour chiffrer un message, la clé privée permet alors de le déchiffrer.

La cryptographie asymétrique rend aussi possible l'utilisation de la signature numérique qui permet de corroborer l'origine d'un message.[6]

I.5.1. Principe :

- Une clé publique connue par tous.
- Une clé privée connue seulement du destinataire du cryptogramme.

I.5.2. Principe de fonctionnement :

Expliquons le procédé de façon imagée :

Alice doit recevoir un message de Bob, mais elle ne fait pas confiance au facteur qui pourrait ouvrir sa lettre. Comment peut-elle être sure de recevoir ce message sans qu'il soit lu ? Alice va d'abord envoyer à Bob un cadenas ouvert, dont elle seule possède la clé. Ensuite, Bob va placer son message dans une boite, qu'il fermera à l'aide de ce cadenas, avant de l'envoyer à Alice. Le facteur ne pourra donc pas ouvrir la boite, puisque seule Alice possède la clé !

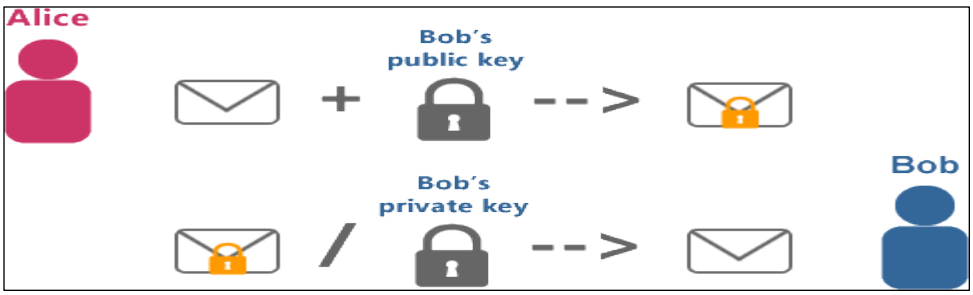


Figure 2 fonctionnement du Chiffrement asymétrique.

Ainsi, un système cryptographie à clé publique est en fait basé sur **deux clés** :

- Une clé publique, pouvant être distribuée librement, *c'est le cadenas ouvert*
- Une clé secrète, connue uniquement du receveur, *c'est la clé*

En résumé, on dispose d'une fonction P sur les entiers, qui possède un inverse S. On suppose qu'on peut fabriquer un tel couple (P, S), mais que connaissant uniquement P, il est impossible (ou au moins très difficile) de retrouver S. Autrement dit, il faut déterminer mathématiquement des fonctions difficilement inversibles, ou « à sens unique ».

Trouver de telles fonctions semblait ardu aux mathématiciens. En effet, comment imaginer une fonction qui soit à sens unique pour tout le monde, excepté pour son créateur qui peut l'inverser grâce à la connaissance d'une information particulière (la clé) ?

Bien sûr, il reste une difficulté : comment trouver de telles fonctions P et S ?
En 1977, Ronald Rivest, Adi Shamir et Leonard Adleman trouvent une solution possible, la meilleure et la plus utilisée à ce jour, c'est l'algorithme de chiffrement RSA.[7]

I.6. Le chiffrement RSA :

Le RSA est l'un des plus connus algorithmes de chiffrement asymétriques. C'est-à-dire qu'il est basé sur le principe des clés privées et publiques, dont seul le destinataire du message est censé la connaitre afin de décrypter le message. Ce qui est important avec ce système, c'est qu'on ne peut pas retrouver la clé privée à partir de la clé publique. Il a été inventé en 1978 par Ronald Rivest, Adi Shamir et Leonard Adleman, des chercheurs au MIT (Massachusetts Institute of Technology).

Cette méthode est très utilisée de nos jours par exemple, dans les navigateurs Internet afin de garantir la sécurité de certains sites ou encore pour chiffrer des données. Il est aussi le standard de chiffrement du secteur bancaire de plusieurs pays. Afin de crypter, nous avons besoin d'un message codé. Le RSA utilise l'arithmétique des congruences modulo n, c'est-à-dire qu'il utilise les restes des divisions. Il est alors possible, pour certains nombres, de trouver deux autres entiers qui nous permettent, par le calcul de puissance, de retomber sur le reste de départ (ainsi un premier calcul crypte et un second nous ramène sur ce chiffre de départ, donc décrypte).

Un des principaux avantages du RSA, c'est qu'il crypte par blocs de caractères, donc il ne conserve pas la fréquence d'apparition des lettres.[5]

I.6.1. Principe de fonctionnement :

❖ **Le Cryptage :**

On travaille principalement avec des nombres premiers. À priori, il est assez facile de dire si un petit nombre est premier ou non. Cependant, dès que ce nombre devient plus conséquent, il est très difficile de dire s'il s'agit d'un premier ou non. Voici un atout principal du RSA :

- On choisit donc deux nombres premiers très grand p et q qui serviront à former les clés publiques et privées.
- On calcule n le module de chiffrement, qui est un constituant de la clé publique et de la clé privée en faisant : n = p*q.
- ensuite on calcule e, qui fait partie de la clé publique, avec e : un nombre premier avec (p-1)*(q-1).
- La couple (n, e) forme ainsi la clé publique de chiffrement.

On peut commencer le cryptage. On va se servir de la clé publique de chiffrement. Tout d'abord, il faut un message préalablement codé. On doit donc transformer en nombres le message d'origine (en utilisant la valeur ASCII de chaque lettre ou encore en remplaçant chaque lettre par son rang dans l'alphabet par exemple) et qui sera M.

afin de crypter M on calcule $C = M^{e}$ ***mod*** n qui est le message chiffré.

❖ **Le Décryptage :**

Il s'agit désormais de calculer, à partir de p et q, la clé privée d. Pour cela, il faut satisfaire l'équation : ***e*d mod ([p-1]*[q-1]) = 1.***

Avec la clé ***d*** générée, on peut décrypter le message crypté C. On retrouve alors le message M ou : $M = c^{d}$ ***mod*** *n*. [8]

I.7. Fonction de Hachage :

Les fonctions de hachages sont des fonctions à sens uniques « sans collision », générant une sortie de taille fixe (appelée condensa ou empreinte) caractérise des données fournies en entrée. Ces fonctions sont dites à sens unique, car il est impossible de retrouver les données initiales à partir de l'empreinte. Une fonction est dite « sans collision » ou « injective » lorsqu'il est réputé très difficile de trouver deux sources différentes conduisant à un même résultat.[4]

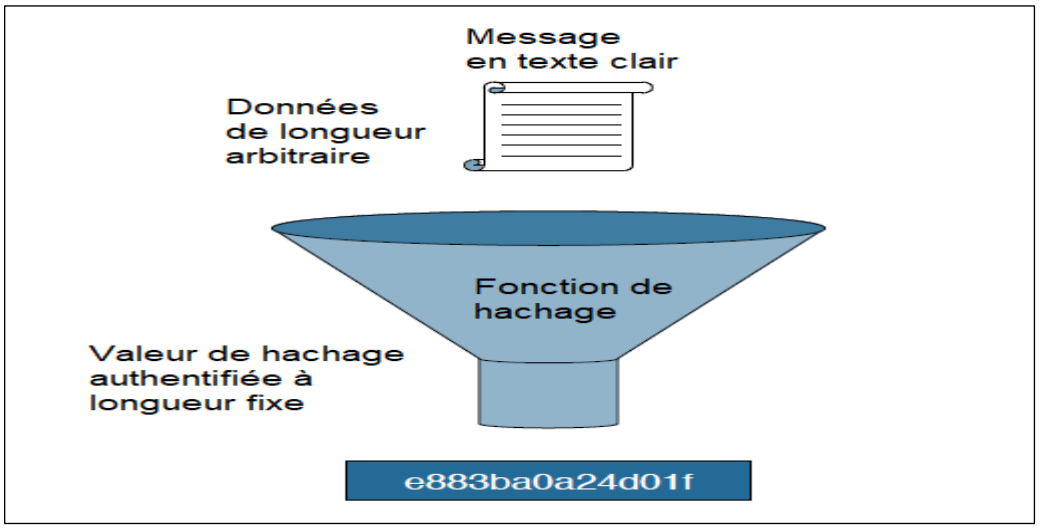


Figure 3. La fonction de hachage

Une bonne fonction de hachage doit garantir les propriétés suivantes :

- Elle doit être telle qu'elle associe un et un seul message ou une donnée en clair (cela signifie que la moindre modification du document entraîne la modification de son résumé), c-à-d « sans collision » par définition.
- Être une fonction à sens unique afin qu'il soit impossible de retrouver le message original à partir du hasch trouvé : Y = F (x), mais il est impossible de retrouver x à partir de Y.
- Il est par définition, impossible de trouver deux messages différents ayant la même valeur de hachage.

I.7.1. Propriétés :

Une fonction de hachage « H » transforme une entrée de données d'une dimension variable « m » et donne comme résultat une sortie de données inférieure et fixe « h » (h = H(m)).

- l'entrée peut être de dimension variable.
- La sortie doit être de dimension fixe.
- H(m) doit être relativement facile à calculer.
- H(m) doit être une fonction à sens unique.
- H(m) doit être « sans collision ».[4]

I.7.2. Utilisation — Authentification et intégrité :

Les algorithmes de hachage sont utilisés :

- Dans la génération des signatures numériques, dans ce cas, le résultat « h » est appelé « empreinte ».
- Pour la vérification de l'intégrité d'un document (le changement d'une partie du document change son empreinte).
- Vérifier l'intégrité de tous types de données transmis d'une source vers une destination.
- Pour la construction du MAC ‹‹Message Authentication Code››, ou code d'authentification de message, il permet de joindre l'empreinte du message chiffré avec une clé secrète ce qui protège contre toute modification du message (si l'intrus modifie le message et son empreinte, il est incapable de chiffrer celle-ci pour la remplacer dans le message).

I.7.3. Principaux algorithmes :

Il existe différents algorithmes réalisant de traitement :

- **MD2**, **MD4** et **MD5** (MD signifiant Message Digest) développé par Ron Rivest (société RSA Security), créant une empreinte digitale de 128 bits pour MD5. Il est courant de voir des documents en téléchargement sur Internet accompagnés d'un fichier MD5, il s'agit du résumé du document permettant de vérifier l'intégrité de ce dernier.
- **SHA** (Secure Hash Algorithm, pouvant être traduit par Algorithme de hachage sécurisé) développé par le NIST en 1995. Il crée des empreintes d'une longueur de 160 bits. C'est un standard SHA0 et SHA1 (devenu le standard SHS).
- **Tiger** développé par Ross Anderson et Eli Biham, plus rapide que MD5 (132 Mb/s contre 37 Mb/s sur une même machine, optimisé pour processeur 64 bits).[11]

I.8. La signature numérique :

I.8.1. Définition :

Comme la signature manuscrite, la signature électronique est un terme générique qui indique tout simplement un mécanisme permettant de lier une donnée signée à un signataire.

Dans les deux cas, les signatures peuvent être vérifiées publiquement. Donc elle permet de garantir l'intégrité de la donnée une fois signée et d'en authentifier le signataire.

Les schémas de signature électronique sont donc fondamentalement asymétriques : la clé privée du signataire intervient dans l'algorithme de signature, et la clé publique correspondant sert à la vérification.

La primitive RSA peut également être utilisée pour des applications de signatures. [12]

I.8.2. Principe de la signature numérique :

- **La signature :**
  1. Lorsqu'on signe, une empreinte numérique unique se crée (appelée un hachage) grâce à un algorithme mathématique. Ce hachage est spécifique à la donnée signée (document, médias, logiciel.), ce qui signifie que la moindre modification créera un hachage différent.
  2. Le hachage est chiffré avec la clé privée du signataire. Le hachage chiffré et la clé publique du signataire sont ensuite réunis dans une signature numérique qui est annexée au document.
- **Vérification de la signature :**
  1. Lorsqu'on ouvre le document avec un programme qui supporte la fonction de signature numérique (par ex. : Adobe Reader, Microsoft Office), celui-ci utilise automatiquement la clé publique du signataire (qui faisait partie de la signature numérique du document) pour déchiffrer le hachage du document.
  2. Le programme calcule un nouveau hachage pour le document. Si ce nouveau hachage correspond au hachage déchiffré de l'étape 1, le programme saura que le document n'a pas été modifié et affiche un message similaire à celui-ci : « Le document n'a pas été modifié depuis la signature. »

Le programme valide également que la clé publique utilisée pour signer appartient bien au signataire et affiche son nom.[4

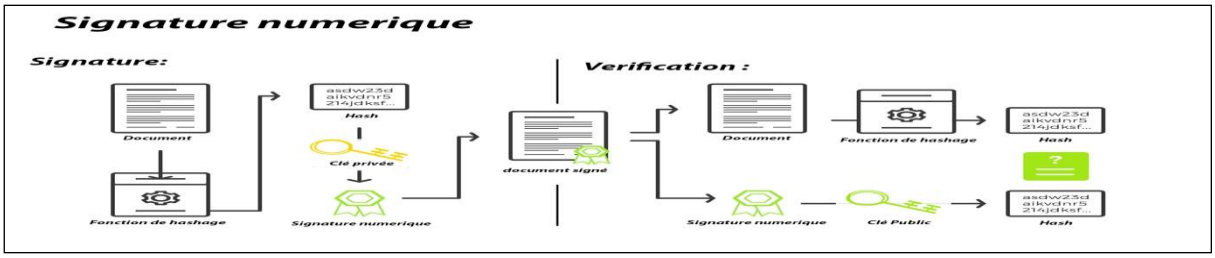


Figure 4. La signature numérique et la vérification

I.9. Le certificat numérique :

I.9.1. L'attaque Man in the Middle :

L'attaque de l'homme du milieu (**HDM**) ou man in the middle attack (**MITM**) est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis. Le canal le plus courant est une connexion à Internet d'un internaute. L'attaquant doit d'abord être capable d'observer et d'intercepter les messages d'une victime à l'autre. L'attaque « homme du milieu » est particulièrement applicable dans le protocole original d'échange de clés Diffie-Hellman, quand il est utilisé sans authentification. Avec authentification, Diffie-Hellman est en revanche invulnérable aux écoutes du canal, et est d'ailleurs conçue pour cela. [13]

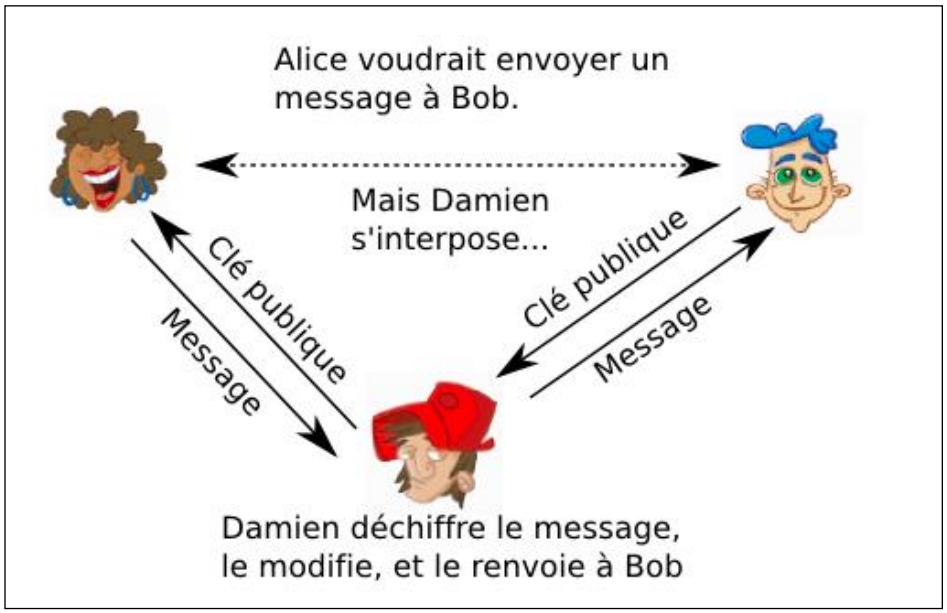


Figure 5. L'attaque Man in the middle

I.9.2. Définition du certificat numérique :

La solution qui peut éliminer l'attaque man in the middle est l'utilisation des certificats numériques. Un certificat numérique est une sorte de passeport électronique qui permet à une personne, un ordinateur ou une organisation d'échanger de manière sure des informations sur Internet en s'appuyant sur une infrastructure à clé publique (PKI).

À l'instar d'un passeport, un certificat numérique fournit des informations d'identité, se veut résistant aux tentatives de réalisation de faux, et peut être vérifié parce qu'il est émis par une agence officielle de confiance. Le certificat contient le nom de son porteur, un numéro de série,

des dates de validité, une copie de clé publique de son porteur utilisée pour chiffrer des messages et produire des signatures électroniques et la signature électronique de l'autorité qui l'a émis (CA) afin de permettre au destinataire d'en vérifier l'authenticité.

Pour prouver son authenticité et sa validité, un certificat est signé numériquement par un certificat racine appartenant à une autorité de certification de confiance. Les systèmes d'exploitation et les navigateurs Web tiennent à jour des listes de certificats racines afin de pouvoir vérifier aisément les certificats émis et signés par les autorités de certification. Dans le cadre d'un déploiement interne de PKI, les certificats peuvent être auto-signés.[4]

I.9.3. Structure d'un certificat X.509 :

Le X.509 est une norme des certificats numériques créée en 1988 ou le certificat numérique contient des éléments d'information spécifiques sur l'identité du propriétaire du certificat et sur l'autorité de certification qui sont :

1. Version
2. Numéro de série
3. Algorithme de signature du certificat
4. Signataire du certificat
5. Validité (dates limite)
6. Pas avant
7. Pas après
8. Détenteur du certificat
9. Informations sur la clé publique
10. Algorithme de la clé publique
11. Clé publique
12. Identifiant unique du signataire (facultatif)
13. Identifiant unique du détenteur du certificat (facultatif)
14. Extensions (facultatif)[4]

I.10. PKI (Infrastructure à clés publiques):

I.10.1. Définition :

PKI (Public Key Infrastructure) : est un système de gestion des clés publiques qui permet de gérer des listes importantes de clés publiques et d'en assurer la fiabilité, pour des entités généralement dans un réseau. Elle offre un cadre global permettant d'installer des éléments de

sécurité tels que la confidentialité, l'authentification, l'intégrité et la non-répudiation tant au sein de l'entreprise que lors d'échanges d'information avec l'extérieur. [4]

I.10.2. Fonctionnalités d'une PKI :

❖ **Création d'une paire de clés et demande de certificat :**

Une entité physique crée une paire de clés privée/publique. Elle crée ensuite une demande de certification (un certificat qui n'est pas encore signé) le certificat contient toutes les informations identifiant cette entité, ainsi que la clé publique de l'entité.

❖ **Signature du certificat :**

L'entité envoie son certificat à une autorité d'enregistrement (RA). Cette autorité approuve ou désapprouve la certification. Si elle est approuvée, le certificat est envoyé à l'autorité de certification (CA) et signé, il est ensuite stocké sur le serveur de la CA pour annoncer que cette clé publique est certifiée.[4]

❖ **Utilisation typique du cryptage par clé publique :**

Disposant de la clé publique certifiée de l'autre partie, les interlocuteurs peuvent communiquer entre eux en toute sécurité. Ils peuvent crypter des données et utiliser les signatures digitales. Pour la partie cryptage, la cryptographie par clé publique est trop lente pour permettre le transfert de grandes quantités des données. Un cryptage symétrique est plus approprié. Dans ce cas, une clé de cryptage symétrique est cryptée par clé publique et envoyée à l'autre partie. L'échange peut alors se poursuivre en cryptage/décryptage symétrique classique.[4]

I.10.3. La gestion des clés :

La gestion des clés de l'infrastructure doit être rigoureuse. En effet, il a été démontré dans les faits qu'il est beaucoup plus facile de s'introduire dans un système et de se procurer illicitement les clés plutôt que de casser un algorithme. Et le moment le plus propice pour espérer se procurer les clés est sans conteste le moment où l'échange des clés a lieu. C'est pourquoi l'échange des clés doit être fait avec la plus grande prudence, car il représente le point de vulnérabilité de tout le système.

La gestion des clés proprement dite se compose des opérations suivantes :

- **Génération** : Les clés doivent être générées de manière aléatoirement.
- **Distribution** : La distribution est l'action de déplacer une clé de cryptage. Un exemple de distribution est la clé de session.

- **Stockage** : La clé doit être protégée et doit garder à tout prix son intégrité et sa confidentialité.
- **Suppression** : La suppression de clés intervient quand la clé a atteint sa fin de validité ou lorsqu'un doute subsiste sur sa confidentialité. La suppression signifie la destruction de toutes les copies de la clé symétrique ou de la clé publique.
- **Archivage** : L'archivage des clés permet de conserver une copie des clés même si elles ne sont plus utilisées, une clé archivée ne peut pas être remise en service dans un environnement d'application.
- **Recouvrement** : Le recouvrement des clés est une procédure délicate qui permet de retrouver la clé privée d'un client. Par exemple lorsqu'un utilisateur a perdu sa clé privée. Ce principe permet aussi le recouvrement des données chiffrées par cette clé.

Toutes ces étapes doivent être minutieusement effectuées et contrôlées pour que la PKI ne soit pas sujette à diverses attaques. [4]

I.10.4. Acteurs d'une PKI :

On distingue différentes entités au sein d'une PKI :

- **Le détecteur d'un certificat :** c'est une entité qui possède une clé privée et le sujet de certificat numérique contenant la clé publique correspondante. Il peut s'agir d'une personne physique (certificat client), un serveur web (certificat serveur), un équipement réseau (certificat VPN).
- **L'utilisateur d'un certificat :** celui-ci récupère le certificat et utilise la clé publique qu'il contient dans sa transaction avec le détecteur du certificat.
- **L'autorité de certification CA :** c'est un ensemble de ressource et de personnels défini par son nom et sa clé publique qui génère, distribuer des certificats et maintient les archives concernant les certificats expirés et révoqués
- **L'autorité d'enregistrement RA :** intermédiaire entre le détecteur et la clé et le CA il a comme rôle d'enregistrer et vérifier les demandes de certificats.
- **L'émetteur de CRL :** l'émission de liste de révocation peut être déléguée hors du CA à une entité spécialisée.
- **Dépôt de certificats (Annuaire) :** qui se charge :
  - De distribuer les certificats et les CRL.
  - D'accepter les certificats et les CRL d'autre CA et les rendre disponibles aux utilisateurs.

En résumé, voici les différents composants d'une PKI :[4]

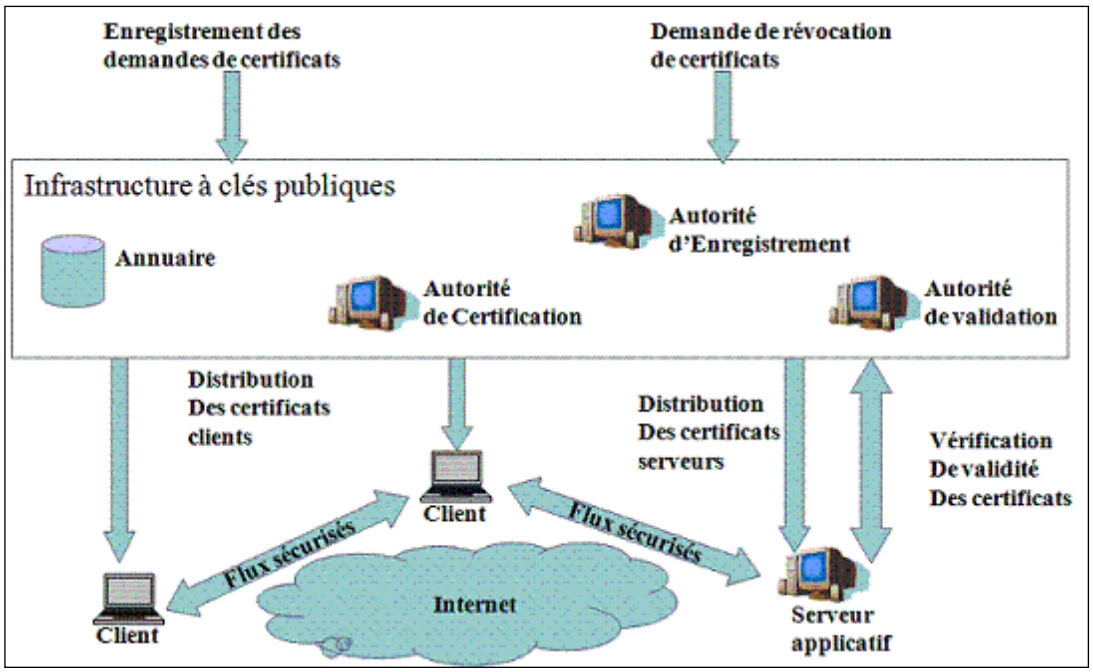


Figure 6. Architecture du PKI.

I.11. Le certificat et la signature numérique dans la loi algérienne :

En 1er février 2015 et après un avis du Conseil d'État, après l'adoption par le Parlement algérien, le président algérien Abdelaziz BOUTEFLIKA a signé un décret de 82 titres relié à la définition, la création et l'utilisation des certificats et signatures numériques en Algérie.

Ou l'Algérie a autorisé la signature numérique pour la signature de tous types de documents « transactions commerciales ou administratives… » et considéré la signature numérique comme une signature sur papier, dans le titre 323 du Code civil dans le chapitre des preuves :

« Art. 323 ter. (Nouveau) : l'écrit sous forme électronique est admis en tant que preuve au même titre que l'écrit sur support papier, à la condition que puisse être dument identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ».[14]

I.11.1. quelques lois sur le certificat et la signature numérique dans la loi algérienne :

Ici quelques articles du code algérien sur le certificat et la signature électronique dans la loi algérienne :

Article 2 : Il est entendu par :

1— Signature électronique : Données sous forme électronique, jointes ou liées logiquement à d'autres données électroniques, servant de méthode d'authentification.

2— Signataire : personne physique qui détient des données de création de signature électronique, agissant pour son propre compte ou pour celui de la personne physique ou morale qu'elle représente.

3 –Données de création de signature électronique : Données uniques, telles que des codes ou des clés cryptographiques privés, que le signataire utilise pour créer une signature électronique.

4 –Dispositif de création de signature électronique : Matériel ou logiciel destiné à mettre en application les données de création de signature électronique.

5— Données de vérification de signature électronique : Des codes, des clés cryptographiques publiques ou d'autres types de données, qui sont utilisées pour vérifier une signature électronique.

6— Dispositif de vérification de signature électronique : Matériel ou logiciel destiné à mettre en application les données de vérification de signature électronique.

7— Certificat électronique : Document sous forme électronique attestant du lien entre les données de vérification de signature électronique et le signataire.

8— Clé cryptographique privée : Chaîne de chiffres détenus exclusivement par le signataire et utilisée pour créer une signature électronique, cette clé est liée à une clé cryptographique publique.

9— Clé cryptographique publique : Chaîne de chiffres mise à la disposition du public afin de lui permettre de revérifier la signature électronique, elle est insérée dans le certificat électronique.

10— Autorisation : Désigne le régime d'exploitation desservies de certification électronique et se matérialise parle document officiel délivré au prestataire de manière personnelle lui permettant de commencer la fourniture effective de ses services.

11— Tiers de confiance : Personne morale qui délivre certificats électroniques qualifiés ou éventuellement fournit d'autres services en matière de certification électronique au profit des intervenants dans la branche gouvernementale.

12— Prestataire de services de certification électronique : Personne physique ou morale qui délivre les certificats électroniques qualifiés et fournissant éventuellement d'autres services en matière de certification électronique.

13— Intervenants dans la branche gouvernementale : Institutions et administrations publiques, établissements publics tels que définis par la législation en vigueur, institutions nationales autonomes, autorités de régulation, intervenants dans les échanges interbancaires, ainsi que toute personne ou entité qui de par sa nature ou mission fait partie de la branche gouvernementale.

14— Titulaire de certificat électronique : Personne physique ou morale à laquelle un prestataire de services de certification ou un tiers de confiance a délivré un certificat électronique.

15— Politique de certification électronique : Ensemble des règles et procédures organisationnelles et techniques liées à la signature et à la certification électroniques.

16— Audit : Vérification de la conformité par rapport à un référentiel

Article 4 : Le document signé électroniquement est conservé dans sa forme d'origine. Les modalités de conservation du document signé électroniquement sont définies par voie réglementaire.

Article 6 : Une signature électronique a pour fonction d'authentifier l'identité du signataire et de manifester l'adhésion de ce dernier au contenu de l'écrit sous forme électronique.
Article 7 : La signature électronique qualifiée est une signature électronique qui satisfait aux exigences suivantes :

1 — Etre réalisée sur la base d'un certificat électronique qualifié,

2 — Etre liée uniquement au signataire.

3 –Permettre l'identification du signataire.

4 –Etre conçue au moyen d'un dispositif sécurisé de création de signature électronique,

5 — Etre créée par des moyens que le signataire puisse garder sous son contrôle exclusif,

6 — Etre liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectée.

Article 15 : Le certificat électronique qualifié est un certificat électronique qui satisfait aux exigences suivantes :

1. Être délivré par un tiers de confiance ou un prestataire de services de certification électronique conformément à la politique de certification électronique approuvée.

2. Ne peut être délivré qu'au signataire.

3. Doit comporter notamment :

a. Une mention indiquant que le certificat électronique est délivré à titre de certificat électronique qualifié.

b. L'identification du tiers de confiance ou du prestataire des services de certification électronique autorisé émetteur du certificat électronique ainsi que le pays dans lequel il est établi.

c. Le nom du signataire ou un pseudonyme permettant d'identifier le dit signataire.

d. La possibilité d'inclure, le cas échéant, une qualité spécifique du signataire, en fonction de l'usage auquel le certificat électronique est destiné,

e. Des données de vérification de signature qui correspondent aux données de création de signature électronique,

f. L'indication du début et de la fin de la période de validité du certificat électronique,

g. Le code d'identité du certificat électronique,

h. La signature électronique qualifiée du prestataire de services de certification électronique ou du tiers de confiance, qui délivre le certificat électronique,

i. Les limites à l'utilisation du certificat électronique, le cas échéant,

j. Les limites à la valeur des transactions pour lesquelles le certificat électronique peut être utilisé, le cas échéant et,

k. Une référence au document certifiant la représentation d'une autre personne physique ou morale, le cas échéant.

Article 61 : Dès la signature de son certificat électronique, le titulaire est seul responsable de la confidentialité des données de création de sa signature. [15]

I.12.Conclusion :

Dans ce chapitre nous avons expliqué et présenter les généralités dans le domaine de la cryptographie qui est basé sur plusieurs méthodes de chiffrements.

Aujourd'hui, le domaine de la cryptographie devient une science très importante, car cette science est la base de la plupart des technologies, aussi utilisée généralement aux problèmes de sécurité des communications.

Les systèmes de cryptographie Symétrique et asymétrique permettent donc de s'assurer à la fois un certain nombre de sécurité de base : Confidentialité, Intégrité et Authentification des données transmises, ainsi que l'authentification des tiers et la Non répudiation.

Pour signe et vérifier la signature d'un document, la meilleure méthode utilisée pour éviter les problèmes de la longueur du message signé et le temps prenne est l'utilisation de fonction de hachage (ou de compression) sécurisées. Au lieu de signer le message tout entier, il suffit de ne signer qu'une empreinte numérique plus courte.

Toutefois, les méthodes expliquées feront dans une ou plusieurs machines, et la communication entre plusieurs machines et l'échange des clés produites le problème de l'attaque (l'homme de milieu), bute d'intercepter les communications entre deux parties, particulièrement applicables dans le protocole original d'échange de clés Diffie-Hellman, quand il est utilisé sans authentification et pour faire une communication parfaite et augmenter le niveau de sécurité Une méthode de protection a été développée pour identifier les deux parties, est l'utilisation des certificats numérique.

CHAPITRE II

LA BLOCKCHAIN

II.1 Introduction :

La protection des données sur internet est le sujet le plus important et un problème qui inquiète les utilisateurs et les propriétaires, nous entendons tous les jours parler de piratage des sites et des banques, malgré la protection extrême mais insuffisante dans la mesure requise.
C'est pourquoi les chercheurs se concentrent aujourd'hui sur les technologies de cryptage et de sécurisation des données comme la blockchain.

II.2 Historique :

Selon Marley Gray, directeur de la stratégie technologique pour les services financiers chez Microsoft, en 2008, une personne ou un groupe de personnes connu sous le nom de **Satoshi Nakamoto** a publié un article décrivant le bitcoin et comment il pourrait être utilisé pour la numérisation et l'envoie des paiements entre deux entités consentantes sans avoir besoin d'une institution financière tierce. Chaque transaction a été enregistrée sur le registre blockchain, le bloc le plus récent lié à ceux précédant par l'utilisation d'une signature numérique. Pour assurer la confiance dans le grand livre, les participants du réseau doivent exécuter des algorithmes compliqués pour vérifier ces signatures numériques avant d'ajouter des transactions à la chaîne de blocs.

Les prochaines années pour le bitcoin ont été tumultueuses, y compris l'effondrement de l'échange de bitcoin de premier plan, Mt. Gox, est une réputation de plus en plus aigrie comme la monnaie alimentant le bazar de drogue en ligne. Mais beaucoup d'entreprises ont vu une opportunité dans la technologie sous-jacente - la blockchain - qui a rendu possible l'existence de bitcoin. [16]

II.3 Définition :

Pour les profanes, on peut définir les chaînes de blocs comme étant une feuille de calcul qui enregistre dans l'ordre les transactions entre les utilisateurs d'un même réseau poste à poste.
Par défaut, la feuille de calcul est publique : tous les utilisateurs et les nœuds du réseau ont un accès complet en temps réel aux données enregistrées dans la base de données. Il n'est pas nécessaire d'obtenir l'autorisation préalable de tiers ou d'une autorité centrale.
La feuille de calcul est également répartie.

Une copie des données à jour est stockée dans chaque nœud du réseau. De la même manière, les données mises à jour sont automatiquement diffusées dans le réseau chaque fois

qu'une nouvelle rangée est ajoutée. Aucun ordinateur ou serveur central n'est donc requis pour gérer ou diriger le trafic.

Une des grandes innovations des chaînes de blocs est la manière dont les écritures sont liées entre elles. Chaque écriture dans la base de données est constituée d'un bloc de transactions et comporte un identificateur unique. Chaque bloc de transactions est lié au bloc précédent.

En langage informatique, on dit que le nouveau bloc est l'enfant du bloc précédent, ce qui crée une chaîne logique entre les blocs. Comment cela est-il accompli ? L'identificateur unique est utilisé pour générer l'identificateur unique du bloc suivant. Cela crée une chaîne de blocs liés entre eux. Il est donc pratiquement impossible de modifier le contenu ou l'ordre des rangées. Un bloc est donc l'enfant mathématique du bloc qui le précède. La seule exception est ce que l'on appelle le « bloc de genèse », c'est-à-dire le premier bloc, ou la première rangée de données, qui est orphelin, puisqu'il n'a pas de parents.

La figure sous-dessus fournit une représentation schématique des blocs aléatoires d'une chaîne de blocs fictifs. Par exemple, le bloc a son propre identificateur unique et comprend sa propre série de transactions. Il comprend aussi l'identificateur unique du bloc précédent et un horodateur unique qui enregistre la date et l'heure auxquelles l'écriture a été ajoutée à la chaîne de blocs. [17]

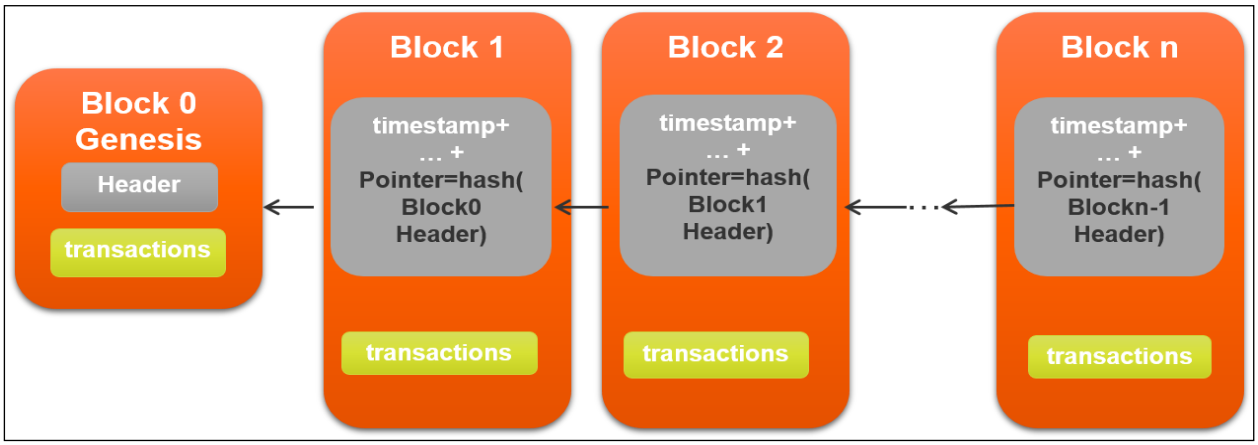


Figure 7. Schéma de chaîne des blocs

Les chaînes de blocs sont évidemment beaucoup plus complexes que des feuilles de calcul ordinaires. Cela est sans doute particulièrement bien illustré dans la manière dont les écritures sont ajoutées à une chaîne de blocs.

Une blockchain présente plusieurs intérêts majeurs :

- **Transparente** : bien que les échanges demeurent anonymes, n'importe qui peut les consulter.

- **Sécurisée** : les transactions sont infalsifiables et sécurisées par des protocoles basés sur la cryptographie asymétrique.
- **Indépendante** : de tout tiers de confiance : c'est l'ensemble du réseau qui se charge d'authentifier les transactions grâce à la cryptographie employée. Il existe de nombreux domaines d'application tels que signer un contrat de mariage, voter électroniquement ou encore envoyer de l'argent à l'autre bout du monde. En s'affranchissant de tout tiers de confiance extérieur, une blockchain assure des coûts et un délai considérablement réduit pour l'utilisateur.

II.4 Valeurs principales des chaînes de blocs :

❖ **Données immuables :**

Les chaînes de blocs garantissent l'intégrité des données et des utilisateurs. Premièrement, il est pratiquement impossible de modifier ou de falsifier les blocs d'une chaîne, ce qui offre un niveau élevé d'intégrité ou d'immuabilité des données. Deuxièmement, les métadonnées relatives aux transactions effectuées par un nœud ou un utilisateur final sont enregistrées dans la chaîne de blocs et peuvent être liées à l'utilisateur qui les effectue, cela signifie que les utilisateurs ne peuvent pas tromper le réseau ou tenter d'effectuer une transaction invalide. Bien que l'anonymat complet soit impossible, les chaînes de blocs ne contiennent aucun renseignement personnel et utilisent un chiffrement privé/public pour authentifier les utilisateurs qui effectuent les transactions. Les nœuds et les utilisateurs n'ont pas besoin de fournir de noms ou de renseignements personnels pour faire partie du réseau, et le minage de chaînes de blocs pour obtenir des renseignements personnels en vue de les vendre à des tiers pour réaliser un profit est impossible.

❖ **Confiance répartie :**

La chaîne de blocs permet de contourner la nécessité d'une autorité centrale digne de confiance. La confiance est plutôt répartie entre les éléments du réseau. Il en va de même pour les mécanismes de gouvernance ; en principe, les différents types d'utilisateurs et de nœuds ont le même poids politique.

❖ **Acteurs principaux :**

Les principaux développeurs ont un accès en écriture au code source.

Les nœuds complets contiennent des copies à jour de la chaîne de blocs, valident les nouveaux blocs puis les diffusent dans le réseau. Les mineurs se consacrent à la preuve de travail. Les utilisateurs finaux se servent du réseau pour effectuer leurs transactions au moyen d'un

logiciel client ou d'un logiciel de portefeuille. Les nœuds de service comme les portefeuilles, le stockage, les échanges et les Services infonuagiques.

❖ **Technologie poste à poste (P2P) :**

Dans un réseau d'égal à égal, tous les nœuds interconnectés sont en principe égaux. Comme il n'y a pas de serveur central, il n'y a pas de point de défaillance central. Si un nœud tombe en panne, tous les autres nœuds demeurent interconnectés ; les données et l'information qui circulent dans le réseau sont ainsi préservées.

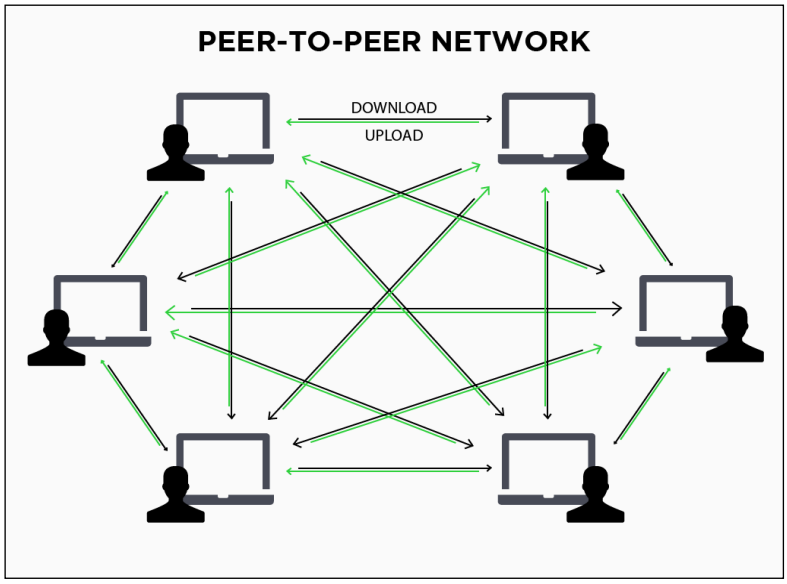


Figure 8. Le réseau poste à poste (P2P)

❖ **Cryptographie :**

La chaîne de blocs utilise une cryptographie à clés publique : une clé privée qui n'est connue que de son propriétaire, et une clé publique qui est partagée avec le reste du monde. Une clé privée est d'abord générée de manière aléatoire pour être ensuite utilisée pour créer une clé publique. La clé privée est utilisée pour chiffrer la transaction qui peut ensuite être déchiffrée par le destinataire visé au moyen de la clé publique de l'expéditeur. Il est mathématiquement impossible d'utiliser une clé publique pour déchiffrer une clé privée. [18]

II.5 Typologie de la Blockchain :

Il existe trois types de blockchain. Chacune correspondant à un périmètre précis :

II.5.1. Blockchain publique :

Il s'agit d'une blockchain accessible à n'importe qui dans le monde. Aucune permission n'est à demander pour effectuer des transactions ou pour participer au processus de consensus.

Tous les acteurs sont en situation égalitaire dans leur participation au réseau. Bitcoin et Ethereum sont les deux principales Blockchain publiques.

II.5.2. Blockchain Privée :

Il s'agit d'une blockchain tournant sur un réseau privé, dans lesquelles tous les participants sont connus et pour lesquelles la gouvernance est assurée par une organisation. Personne ne peut y accéder et y participer sans y être autorisé.

II.5.3 Blockchain Consortium (Hybride):

Il s'agit de blockchain dans lesquelles le processus de consensus (validation des transactions/blocs) est contrôlé par un nombre connu et restreint de nœuds. Certains nœuds peuvent être rendus publics (accès autorisé en lecture seule) tandis que d'autres restent privés. Elles sont plus adaptées aux contextes régulés. [19]

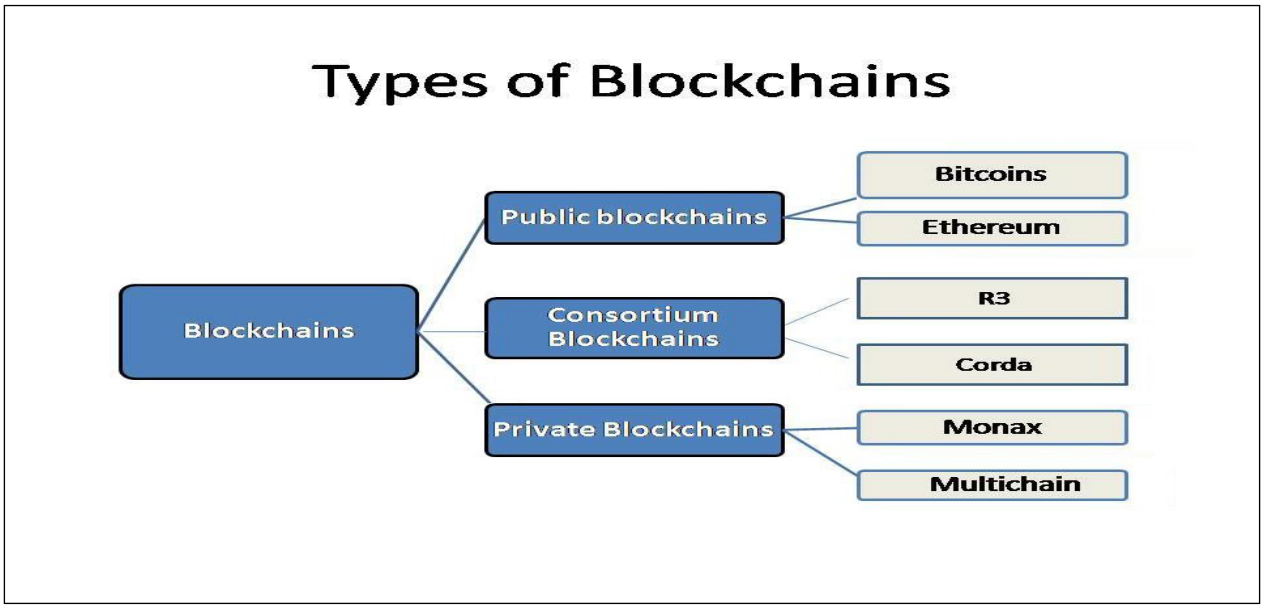


Figure 9. Les types de blockchain

II.6 Fonctionnement :

Les transactions effectuées entre les utilisateurs du réseau sont regroupées dans une structure de données appelée bloc. Les blocs sont ordonnés et hiérarchisés dans une seule et unique chaîne. Chaque bloc pointe sur le dernier bloc précédent valide. Cette chaîne est « distribuée » et « répliquée » sur tous les nœuds du réseau. Chaque nouvelle transaction et/ou Smart Contrat, « en attente », sont groupés dans un nouveau bloc. Pour que ce bloc puisse être ajouté à la Blockchain, il faut qu'il soit validé. Cette validation est réalisée au travers de certains nœuds spécifiques du réseau appelés « mineurs ». Le rôle de ces nœuds consiste à répondre à un

Casse-tête crypto mathématique complexe. Chaque réponse trouvée est propre à un et à un seul bloc interdisant ainsi, sa réutilisation pour la validation d'un nouveau bloc. Le problème crypto/mathématique, propre à chaque bloc, est très difficile à résoudre. Il demande d'importantes ressources de calcul et donc de ressources financières (électricité, coût de maintenance matérielle, coût du personnel, etc.). Pour encourager les mineurs, essentiels au bon fonctionnement et à la viabilité du réseau, une rémunération leur est attribuée en récompense de leur travail. La complexité du problème de validation est liée à une difficulté associée au bloc.

Afin de maintenir constant, le temps de production d'un bloc, le niveau de difficulté est automatiquement ajusté par le réseau. Extrêmement difficile à calculer, la validation de la solution est, à l'inverse, très facile. Il existe plusieurs solutions valides pour un bloc donné. Il suffit d'en trouver au moins une pour que le bloc soit validé au travers du processus de consensus. Une fois que le bloc est validé par un « miner » et approuvé par les autres nœuds du réseau, il est horodaté et ajouté, en tête de la chaîne de blocs (dernier bloc valide créé) et tous les nœuds du réseau l'ajoutent dans leurs copies de la chaîne. La figure ci-dessous illustre le fonctionnement d'une Blockchain.

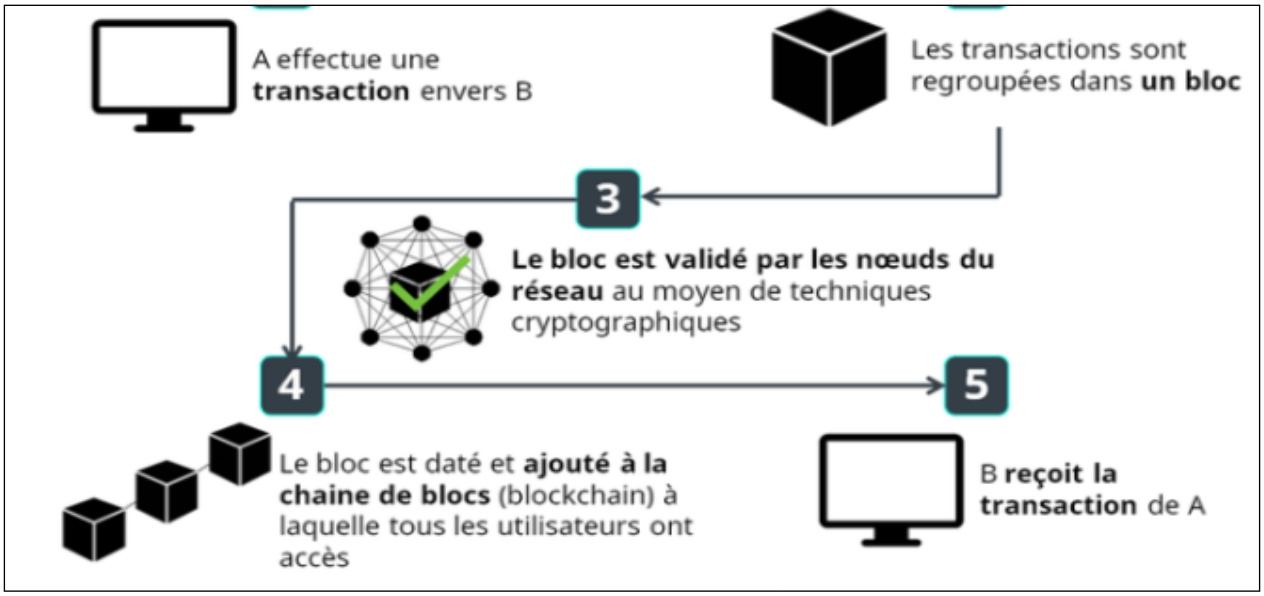


Figure 10. Le Fonctionnement de blockchain

II.7 Concepts de la Blockchain :

II.7.1 Le bloc :

Une blockchain est une chaîne de blocs contenants chacun plusieurs transactions, et qui vont être inscrits au fur et à mesure dans la blockchain par des nœuds du réseau.

L'implémentation peut différer d'une blockchain à l'autre, mais les principaux éléments d'un bloc sont les suivants :

- **Un index :** c'est le numéro do bloc.
- **Un hash servant à identifier le bloc** : la valeur du hash associé au bloc.
- **Le hash du bloc précédent** : la valeur du hash associé au bloc précédent.
- **Un timestamp :** l'instant de création du bloc.
- **Un ensemble de transactions** : l'ensemble de transactions effectuées.

Le premier bloc d'une blockchain est appelé le "Genesis Block". [16]

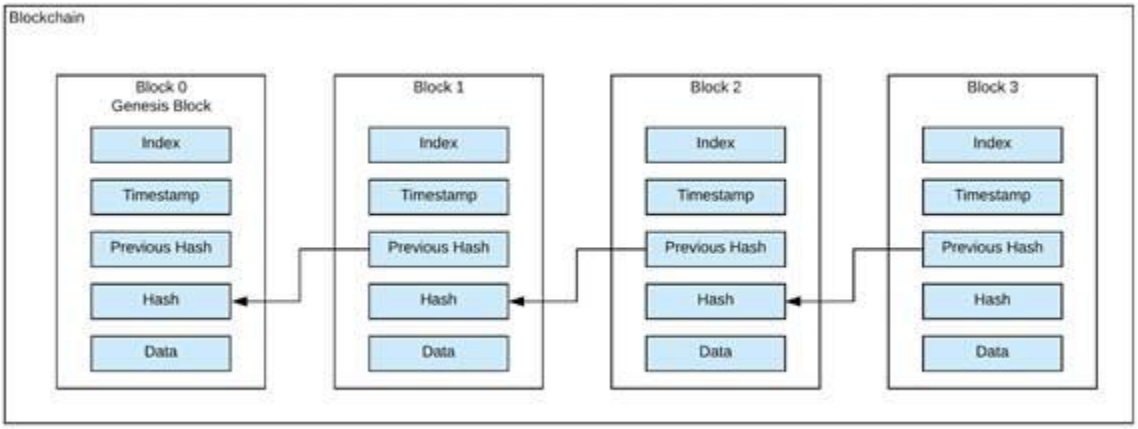


Figure 11. Structure des blocs dans la Blockchain

II.7.2 La preuve de travail (NONCE) :

Un nonce est un nombre aléatoire créé par un générateur de nombre pseudo-aléatoire et qui a pour propriété d'être unique dans un système.

Concernant en-tête. Pour le moment, On n'attardera pas sur les 4 premiers éléments (On suppose qu'ils sont facilement identifiables). Restent la difficulté et le nonce. C'est sur ces deux éléments que va s'effectuer la preuve de travail. L'idée est la suivante : le hash de l'en-tête du bloc doit, pour que la preuve de travail soit valide, être inférieur à un certain nombre que l'on nomme seuil et qui est défini par la difficulté. Comme les 4 premières informations changent à chaque bloc et qu'il est impossible de prédire la valeur du hash sans appliquer la fonction SHA-256, la seule manière d'obtenir un hash valide est de tester différents nonces jusqu'à obtenir un hash correspondant au niveau de difficulté.

On comprend ici que plus le seuil est bas, plus le nombre de 0 requis en début de hash est important, et donc plus il est difficile de trouver un nonce valide.

Dans le cadre de la blockchain Bitcoin, les transactions (adresses, montant, signature) sont regroupées dans des blocs toutes les 10 minutes. Pour qu'un bloc soit non-répudiable, il faut qu'un mineur l'ait validé et transmis par le réseau. La validation d'un bloc s'effectue de la manière suivante :

Des listes de transactions sont en attente dans les nœuds.

Les mineurs doivent calculer la somme cryptographique (un hash) de cette liste associée à d'autres éléments : horodatage, identifiant du bloc précédant ainsi qu'un nonce du bloc précédent.

- La valeur du hash doit débuter par un certain nombre de zéros déterminé par le réseau.

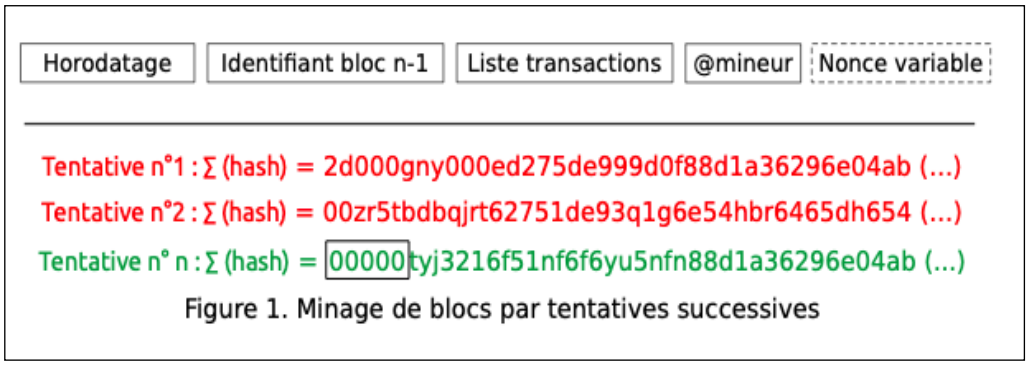


Figure 12. Minage de blocs par tentatives successives.

Des nonces successifs sont essayés pour arriver à ce résultat. Lorsqu'un résultat valide est trouvé (i.e. respectant le nombre de premiers bits à 0), il est transmis aux autres nœuds qui peuvent vérifier facilement la somme à l'aide du nonce qui a servi à réaliser l'opération. Plus le nombre de zéros requis augmente, plus la probabilité de générer une somme débutant par ceux-ci est faible et donc plus il faudra de puissance de calcul pour parvenir à ce résultat. Ce nombre de zéros correspond à la notion de preuve de travail. Plus la taille du réseau augmente, plus la puissance de calcul est importante et plus il faut augmenter le nombre de zéros afin de rester sur une production d'un bloc toutes les 10 minutes. [20]

II.7.3 Vérification de bloc :

Dès qu'un mineur a trouvé un bloc valide, il le transmet au réseau. Chaque nœud qui reçoit ce bloc vérifie sa validité grâce à l'algorithme suivant :

1- Vérifier que le bloc précédent existe et est valide (revient à vérifier que le hash du dernier bloc correspond bien à l'élément « hash du bloc précédent » référencé en en-tête du bloc en cours de vérification).
2- Vérifier que la date du bloc est supérieure à la date du bloc précédent.
3- Vérifier que la preuve de travail est valide (i.e. le hash de l'en-tête du bloc est inférieur au seuil).
4- Vérifier l'ensemble des transactions. Si l'une d'entre elles retourne une erreur, stopper et retourner FAUX.
5- Mettre à jour l'ensemble des transactions non vérifiées et retourner VRAI, Si l'algorithme retourne vrai, le bloc est considéré valide et le nœud l'ajoute à la blockchain. Dans le cas où ce nœud est un mineur, il se met alors à la recherche du prochain bloc : il collecte un nouveau ensemble de transactions dans l'ensemble des transactions non vérifiées et recommence la preuve de travail pour cet ensemble. [21]

II.7.3.1. Le cas des entrées des données contradictoires :

Un nœud peut recevoir deux éléments de données mutuellement incompatibles. Par exemple, A est « Je vends toutes mes actions à Alice » et B est « Je vends toutes mes actions à Bob ». Chaque nœud devra en garder un et en rejeter un car ils ne peuvent pas coexister logiquement. Une solution intuitive est que les nœuds agissent sur la priorité temporelle, en gardant le premier et en rejetant le second. Cependant, différents nœuds peuvent entendre les messages dans différents ordres. Les messages se propageront et une partie du réseau pensera que A est arrivé (et B ne l'a pas fait) et le reste du réseau pensera que B est arrivé (et A ne l'a pas fait). Le réseau est dans un état instable. La solution proposée est que chaque nœud travaille sur sa propre version de la vérité. Quel que soit le nœud qui arrive à ajouter le bloc suivant, il propagera sa version des événements, et tous les nœuds liront ceci et agiront sur la nouvelle 'vérité'.

II.7.3.2. Le cas du bloc contradictoire :

Sur un réseau, il est possible que deux blocs différents soient ajoutés en même temps par différents nœuds, créant ainsi une fourchette dans la chaîne. Dans ce cas, il existe une « règle de consensus » qui aide les nœuds à déterminer quel bloc ils doivent croire. Dans Bitcoin, la règle est appelée la « règle de la plus longue chaîne » - chaque nœud reconnaît la légitimité des deux blocs concurrents et la situation se résout lorsque le bloc suivant est construit sur l'un des prétendants. La chaîne plus longue devient une partie de la blockchain. [21]

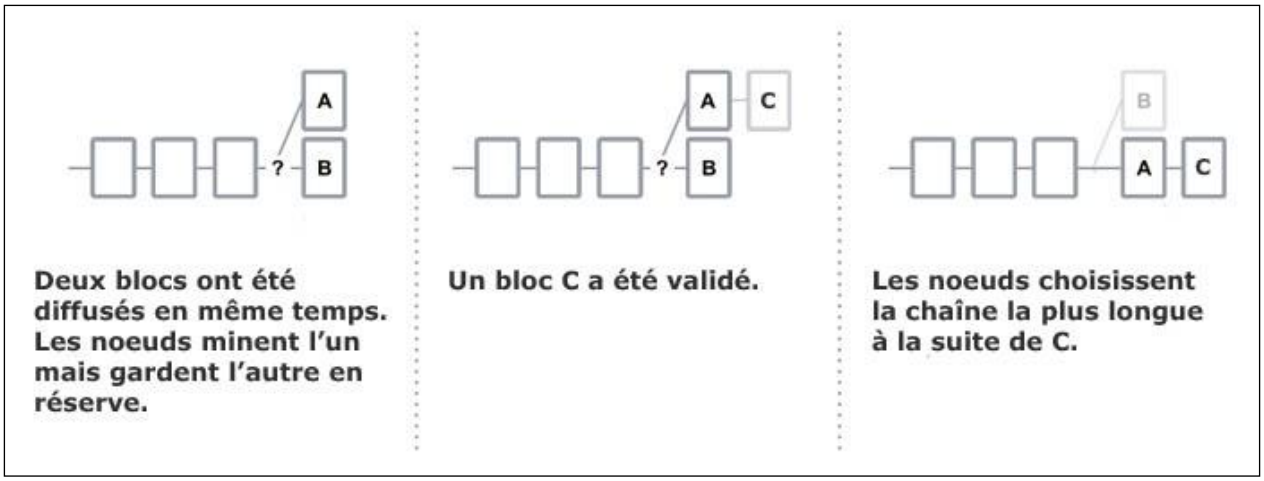


Figure 13. Résolution du cas du bloc contradictoire.

II.7.4 Transaction :

Une transaction est un transfert de valeur (monnaie virtuelle, token, etc.) entre deux comptes, chaque transaction est signée avec la clé privée du compte émetteur, fournissant ainsi la preuve « mathématique » qu'elle provient bien du propriétaire du compte émetteur.

La signature empêche également toutes modifications de la transaction après son émission. Une fois signée, la transaction est « placée/déployée » sur un nœud quelconque du réseau qui la diffuse à son tour, de proche en proche, sur tous les nœuds du réseau.

À présent, tout le monde sur le réseau peut utiliser la clé publique de l'émetteur pour vérifier et s'assurer que la demande de transaction provient bien du propriétaire légitime du compte. Si la transaction est valide, elle est alors incluse, avec d'autres transactions en « attente », dans un bloc de la Blockchain, à son tour « exploité » par les mineurs.

Une fois le bloc validé, le destinataire peut voir l'objet obtenu dans son compte.

La transaction est un message structuré. Ce message structuré a 2 représentations :

- Un format binaire, utilisé pour le calcul de hachage, la signature et le transfert réseau.
- Un format source arbitraire.

II.7.4.1 La Sérialisation :

LA sérialisation est le processus de transformation d'un format source en format binaire. Le format binaire est le seul format "officiel". En effet, le format source est hors de portée de la spécification du protocole. Par conséquent, tout processus applicable à une transaction sera appliqué à ce format binaire. Les règles de conversion pour sérialiser un format source dans un format binaire sont les suivantes :

- La plupart des nombres sont codés avec la convention de Little-Endian sur 32 bits.
- Un code de hachage est considéré comme un grand nombre sur 256 bits, codé avec la convention de Little-Endian,
- Une quantité est un nombre entier sur 64 bits, codé avec la convention de Little-Endian,
- Un tableau commence par le nombre d'entrées, codé sur un octet, suivi d'une séquence de toutes les entrées,
- Toute autre donnée commence par la taille des données codées sur un octet.

II.7.4.2. Le Hash d'une transaction :

Un hachage d'une transaction est un double hachage du format binaire de la transaction. L'algorithme SHA-256 est appliqué pour des raisons historiques, et pour augmenter la sécurité.

II.7.4.3. Identifiant de transaction :

Le code de hachage d'une transaction est appelé le « txid » généralement noté « Tx ». Cet identifiant de transaction est utilisé pour référencer une transaction.

II.7.4.4. Les clés cryptographiques :

Une signature numérique d'une transaction est un cryptage du hachage de transaction calculé avec une clé secrète. Cette clé secrète est appelée clé privée. La signature de la transaction peut être vérifiée avec une clé publique associée.

La signature numérique prouve que la transaction n'a pas été modifiée et que cette transaction a été émise par le propriétaire de la clé privée. L'algorithme secp256k1, basé sur des courbes elliptiques (également appelé 'ECDSA' : Elliptic Curve Digital Signature Algorithm), est utilisé pour la signature numérique des transactions.

Cet algorithme permet de générer une nouvelle paire de clés de chiffrement :

Une clé privée et une clé publique. La clé privée est un nombre de 256 bits généré de manière aléatoire. Et la clé publique est calculée à partir de cette clé privée. [16]

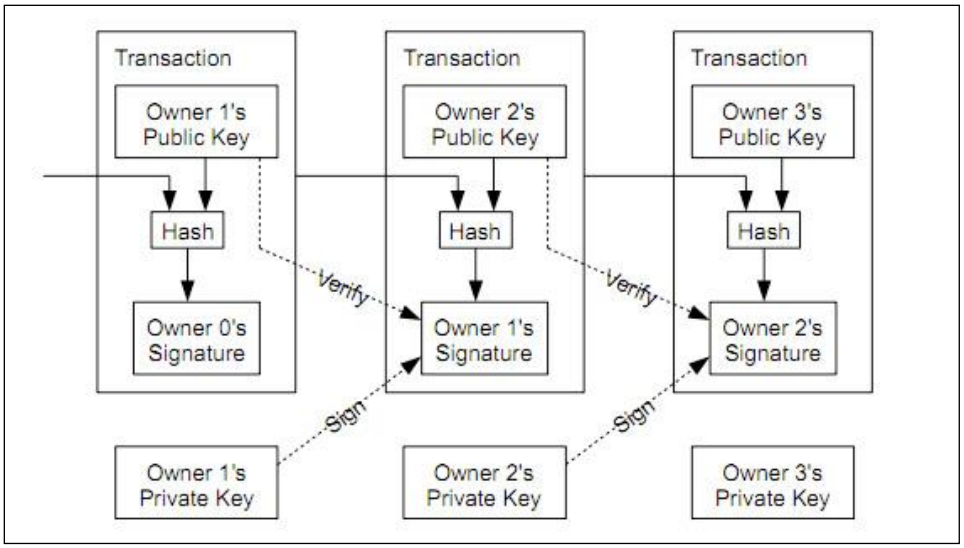


Figure 14 exemples de transaction blockchain

II.7.5 Les messages :

Deux types principaux des messages sont diffusés le plus largement possible sur Internet :

- La transaction, qui représente un paiement,
- Le bloc, qui enregistre une collection de transactions.

Lorsqu'une nouvelle transaction est signée, elle est diffusée sur le réseau blockchain. Il sera ensuite collecté et enregistré dans un bloc. Chaque bloc, une fois constitué, sera à son tour diffusé.

Tous ces messages sont publics et vérifiables. Ils permettent de notifier et donc de prendre à témoin tous les participants du réseau blockchain sur toute nouvelle information qui enrichit la blockchain.

Les messages sont transférés sur le réseau dans un format binaire, codant des nombres sur 32 bits ou 256 bits en utilisant la convention de Little-Endian.

II.7.6 Minage (La création du bloc) :

Chaque transaction nouvellement créée donne lieu à une « écriture » dans une Blockchain. Cette écriture entre dans le réseau par un nœud du système, qui vérifie et contrôle que sa structure est correcte au regard des spécifications du protocole implémenté et qu'elle est légitime par rapport aux écritures déjà enregistrées.

Si la validation de l'écriture est satisfaite, elle est alors « mise en attente » dans une liste locale et diffusée via le réseau P2P à tous les nœuds du réseau. Dans le cas contraire, elle est rejetée.

N'importe quel utilisateur peut être un mineur du réseau et tous travaillent simultanément. Ils sont libres de choisir quelles écritures ils incorporent dans leur bloc en construction. Ce bloc est

ensuite complété par un en-tête, qui contient en particulier son hash et l'identifiant du bloc précédent.

Étant donné que le minage est (souvent) rémunéré, la validation d'un nouveau bloc conduit (mais pas forcément) à une « compétition » des mineurs entre eux. Il est alors possible, que la chaîne de blocs ait des splits (deux versions simultanées coexistant) qui surviennent. C'est le cas par exemple lorsque deux mineurs arrivent à deux solutions valides différentes pour le même bloc en même temps et à l'un de l'autre. Ce cas peut également se produire lors de la « mise à jour de l'ensemble des copies décentralisées » car la réplication des nouveaux blocs ne prend pas nécessairement le même temps sur l'ensemble des nœuds (latence réseau par exemple). Il est alors possible qu'un des nœuds ne soit pas encore « synchronisé » alors qu'un nouveau bloc vient d'être validé et ajouté.

Le réseau est conçu pour résoudre ces splits et ce dans un court laps de temps, de sorte qu'une seule branche de la chaîne survit. C'est la chaîne valide « la plus longue » qui est retenue. La « longueur » de la chaîne ne se réfère pas à son nombre de blocs mais à la difficulté la plus combinée. C'est une sécurité conçue pour empêcher les forks.

Comme les calculs nécessaires à la résolution d'un bloc sont volontairement énergivores et nécessitent de plus en plus de ressources à mesure que le réseau croit, la plupart des mineurs sont regroupés en coopératives. Ils forment alors une importante « puissance » de calcul et augmentent, par conséquent, leurs chances de voir leurs blocs acceptés et inclus dans la blockchain et être rémunérés.

Dès qu'un mineur reçoit un bloc d'un autre mineur, il arrête de construire le bloc en cours, qui n'a pratiquement plus aucune chance d'être accepté. Il l'élimine de sa liste d'attente locale toutes les transactions que contenait le bloc qu'il vient de recevoir, et commence à construire un nouveau bloc. C'est de cette façon que de nouveaux blocs sont produits et diffusés en continu à travers le réseau. [19]

II.7.7 Les contrats intelligents :

Un « contrat intelligent » est un programme informatique autonome dont le code contrôle et conditionne, sous certaines conditions, le transfert de devises ou d'actifs entre différentes parties. Ils définissent non seulement les règles et les pénalités d'un accord de la même façon qu'un contrat traditionnel ou qu'un engagement transactionnel. Mais ils peuvent également, lorsque tous les engagements préalables à son exécution ont été respectés, faire appliquer

automatiquement ces obligations sans qu'aucune des parties ne puisse s'y opposer. Conçus et écrits à l'aide d'un langage de programmation haut niveau, les Contrats intelligents peuvent être très complexes. Leur potentiel dépasse, de fait, largement le simple transfert d'actifs. Ils permettent de simplifier et d'automatiser les processus « lourds » et répétitifs pour lesquels aujourd'hui les gens paient des avocats et des banques à des frais considérables. Au vu de leur appellation, on a tendance à les assimiler à des contrats classiques. Cependant, ils n'ont pas en eux-mêmes d'autorité juridique. Un contrat intelligent n'est qu'une application technique d'un contrat juridique. [19]

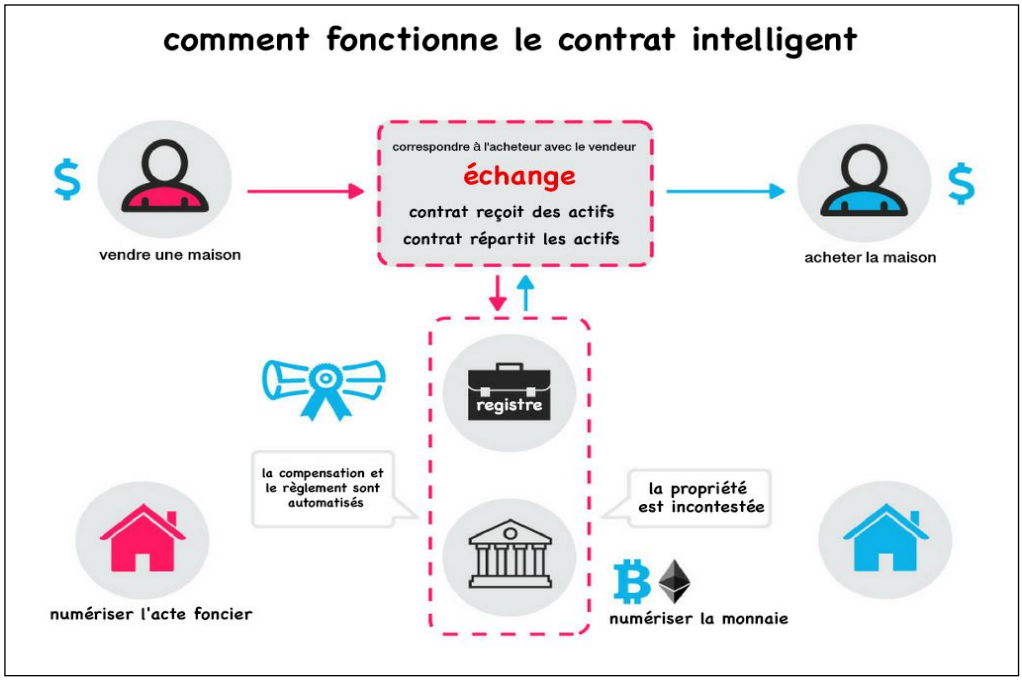


Figure 15. Un smart contrat dans la blockchain

II.7.8 DApp (Decentralized Application) :

Une application décentralisée est une application connectée à et utilisant une Blockchain. Elle satisfait aux critères suivants :

- L'application doit être complètement ouverte (Open Source). Elle doit fonctionner de manière autonome et sans entité qui contrôle la majorité de ses token. L'application doit pouvoir adapter son protocole en réponse aux améliorations proposées au niveau de la Blockchain qu'elle utilise. Malgré tout, tous les changements doivent être décidés par consensus de ses utilisateurs

- Les données d'application et les enregistrements d'opération doivent être stockés crypto graphiquement dans une chaîne de blocs (publique ou non) décentralisée afin d'éviter tout point central d'échec.
- L'utilisation d'un jeton cryptographique (crypto-monnaie : Bitcoin, Ethereum ou un Token natif de son système) est nécessaire pour accéder à l'application. [19]

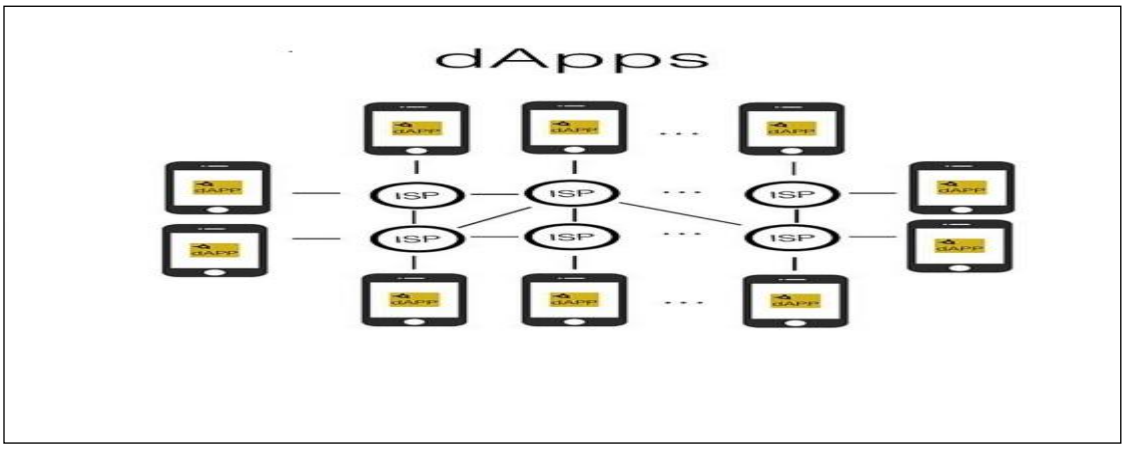


Figure 16. Decentralized Application

II.7.9 le consensus :

Il est parfaitement adapté pour traiter du « Problème des Généraux Byzantins ».

Dans le mode de la Blockchain, le consensus désigne le mécanisme qui consiste à garantir qu'une transaction n'est pas frauduleuse et qu'un bloc soit valide. Le seul moyen de faire émerger une validation globale au sein du réseau, c'est d'obtenir un « vote général » entre toutes les parties prenantes. L'hypothèse faite, c'est que les utilisateurs malveillants seront toujours moins nombreux que les utilisateurs honnêtes.

Il est donc important pour la sécurité du réseau, qu'il existe des mécanismes et/ou des règles reconnus, partagés et validés par tous, qui permettent de valider une transaction puis un bloc avant qu'il soit ajouté dans la chaîne de blocs, il existe de nombreuses méthodes d'obtention du consensus sur une blockchain. Les principales sont :

- **Proof Of Authority (PoA) :**

  Une preuve d'autorité est le mécanisme de consensus d'une chaîne de blocs privés qui donne essentiellement à un utilisateur ou à un nombre spécifique d'utilisateurs, le droit de miner tous les blocs de la Blockchain.

- **Proof Of Stake (PoS) :**

Proof of Stake ou preuve d'enjeu en français est un mécanisme qui se base sur le montant de crypto-monnaie mis, à dessein, en dépôt par un utilisateur. Ce processus est appelé minting et on parle alors de forgeurs, le principe est le suivant :

- Un certain nombre de possesseurs de crypto-monnaie mettent en dépôt une partie de leurs « avoirs » dans le cadre du mécanisme de preuve d'enjeu. Ils deviennent alors des « valideurs ».
- Lorsqu'un nouveau bloc est proposé à l'ajout de la blockchain, un valideur est sélectionné, « aléatoirement » parmi tous les valideurs identifiés et se voit attribuer le droit de créer le prochain bloc et donc d'être rémunéré.
- La sélection d'un valideur est pondérée en fonction du montant total de cryptomonnaie (ou token) qu'il a mis en dépôt. Ainsi par exemple, un valideur avec 10 000 « unités » aura dix fois plus de chance d'être sélectionné qu'un valideur avec 1 000 « unités ».
- Si ce valideur ne crée pas le bloc dans un intervalle de temps donné, il est alors « abandonné » et un deuxième valideur est sélectionné, puis un troisième et ainsi de suite.

- **Proof Of work (PoW) :**

Proof of Work ou preuve de travail en français est un mécanisme de validation d'un bloc qui repose sur la résolution « d'un problème crypto-mathématique complexe ». Le processus de résolution est appelé minage et on parle de mineurs. Comme expliqué, il existe une grande diversité de méthodes, chacune avec ses avantages et ses inconvénients, son niveau de maturité et sa qualité d'implémentation. Leur compréhension est « primordiale » car elles sont une composante essentielle au bon fonctionnement du réseau.

Citons-en encore quelques-uns :

- Pratical Bizantine Fault tolerance » (PBFT)
- Proof of Hold » PoH)
- Proof of Use » PoU)
- Proof of Stake/Time » PoST)
- Proof of Minimum Aged Stake » PoMAS). [19]

II.8 Fraude à double dépense :

II.8.1 Principe :

La fraude double dépense consiste à émettre deux transactions qui dépensent le même actif : la première transaction est émise pour payer un premier bénéficiaire, la seconde est émise

pour payer un complice ou l'attaquant lui-même, afin de récupérer la somme dépensée. Pour que la fraude ne soit pas immédiatement découverte, ces deux transactions doivent coexister dans deux instances concurrentes de la blockchain. La seconde instance doit devenir la plus longue blockchain pour que la fraude réussisse. Dans ce cas, la première transaction sera considérée comme invalide car elle est incompatible avec la seconde transaction et sera finalement rejetée. Si, entre les deux transactions, le premier bénéficiaire a accepté le paiement, il découvrira par la suite que cette transaction a été rejetée. Puisque les participants sont anonymes, ils ne peuvent pas se retourner contre l'attaquant.

II.8.2 La prévention :

Pour éviter toute fraude, le bénéficiaire doit s'assurer que la transaction émise par le payeur est correctement enregistrée dans un bloc de la plus longue instance de blockchain et que cette instance est durable. Par conséquent, il doit attendre qu'un nombre suffisant de blocs réussisse le bloc qui enregistre cette transaction, avant d'accepter le paiement.

La structure en arbre de Merkel d'un bloc permet de restaurer un bloc allégé. Le bénéficiaire peut ainsi vérifier une transaction sans avoir à télécharger le contenu intégral des blocs. Si le nombre de blocs successeurs est suffisamment élevé et que l'attaquant ne possède pas plus de 51 % du pouvoir de calcul total, alors le risque de double dépense tend vers zéro. [22]

II.9. Le réseau blockchain :

Le réseau Blockchain est le réseau Internet utilisé en tant que réseau peer-to-peer. Tous les participants du réseau ont le même statut ; aucun participant ne peut prétendre à une plus grande légitimité. Chaque participant est considéré comme un pair avec les autres. Les étapes pour exécuter le réseau sont les suivantes :

- Diffusion de toutes les nouvelles transactions à l'ensemble des nœuds pour faire la vérification de l’historique pour soyer sûr que les transactions ne sont pas utilisées avant et cette opération fait par les mineurs.
- Regroupement des nouvelles transactions dans un bloc de chaque nœud
- Chaque mineur qui inclut la transaction dans son bloc, Tentative de résoudre de preuve de travail avec son bloc.
- On diffuse la preuve de travail à l’ensemble des nœuds du réseau et chaque nœud de jonction apprendre d’autres nœuds en demandent à leurs voisins pour connus.

- Une fois connectée, les nœuds n'acceptent le bloc que si toutes les transactions qu'il contient sont valides et n'ont pas déjà été passées. Les nœuds expriment leur acceptation du bloc en travaillant sur :
- La création du nouveau bloc suivant dans la chaîne, en utilisant le hash du bloc accepté comme hash précédent.

Les nœuds considèrent toujours que la chaîne la plus longue est le plus sécurit et continueront à l'étendre. Si deux nœuds diffusent simultanément différentes versions du bloc suivant, certains nœuds peuvent recevoir l'un ou l'autre en premier. Dans ce cas, les mineurs travaillent sur le premier qu'ils ont reçu, mais sauvez l'autre branche au cas où elle deviendrait plus longue. La cravate sera brisée lorsque la prochaine preuve de travail sera trouvée et qu'une branche deviendra plus longue ; les nœuds qui travaillaient sur l'autre branche passeront alors au plus long. Les nouvelles diffusions de transactions n'ont pas nécessairement besoin d'atteindre tous les nœuds. Tant qu'ils atteignent de nombreux nœuds, ils vont entrer dans un bloc avant longtemps. Les diffusions de blocs sont également tolérantes aux messages abandonnés. Si un nœud ne reçoit pas de bloc, il le demande lorsqu'il reçoit le bloc suivant et comprend qu'il en a manqué un Bloc. [23]

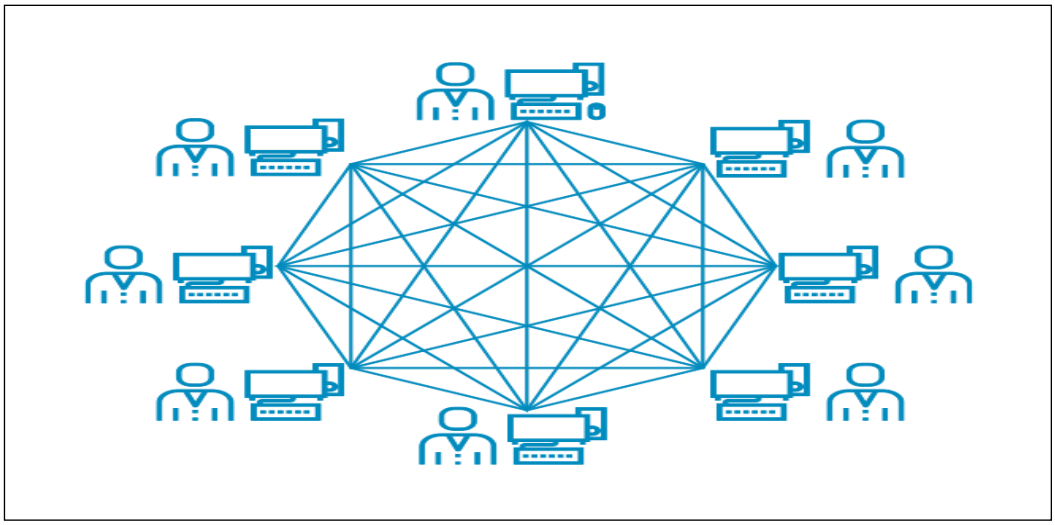


Figure 17. Le réseau Blockchain

II.10 Confidentialité :

Les identités des personnes réalisant les transactions sont gardées secrètes, malgré une diffusion publique des transactions elles-mêmes. [24]

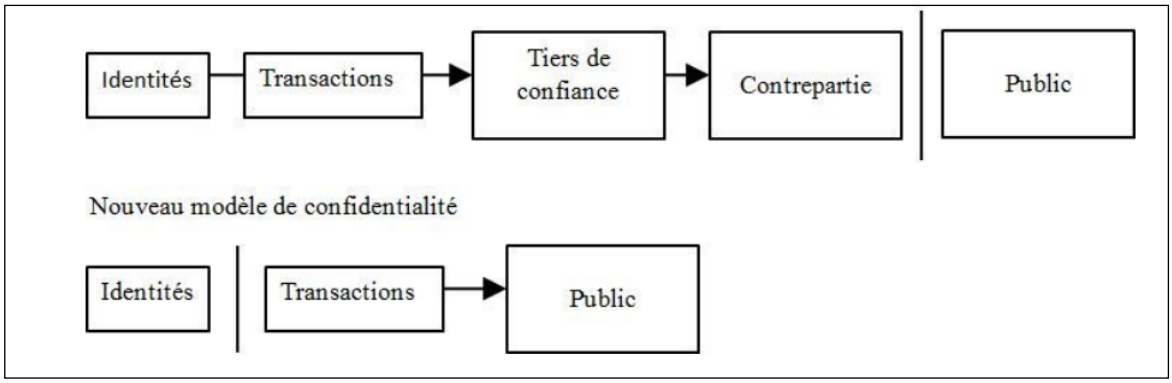


Figure 18. Confidentialité de blockchain

II.11 Conclusion :

Dans ce chapitre, nous avons étudié différentes étapes et le procédé technique sur lequel repose la Blockchain.

Cette étude permet d'organiser les échanges de données sur un réseau distribué (peer to peer), et sécurisé les données par chiffrement, et faisant participer les nœuds du réseau pour la création de nouveaux blocs de la chaîne.

Le principe de base d'une chaîne de blocs repose sur la notion de preuve de travail, et a recours aux techniques de la cryptographie pour vérifier les détenteurs distincts d'un système d'enregistrement collectif.

CHAPITRE III

APPLICATIONS DE BLOCKCHAIN

III.1 INTRODUCTION :

Tous que nous avons expliqués dans le chapitre précédent sont des études abstraites sur la blockchain, pour une meilleure explication on peut présenter un certain nombre de cas d'usage destinés à illustrer le potentiel de cette technologie complexe et des exemples concrets offert par cette technologie.

La première utilisation du blockchain était dans le secteur de la crypto-monnaie, mais après l'utilisation de blockchain a été développée dans d'autre domaine

Dans ce chapitre nous allons présenter un exemple d'utilisation de la blockchain dans le domaine de la crypto-monnaie, ainsi que définir d'autres domaines d'utilisation de la blockchain.

III.2 La Crypto-monnaie :

III.2.1 Définition :

La crypto-monnaie ou monnaie cryptographique est une monnaie 100 % électronique et magnétique. Sa valeur est la même que les monnaies que nous utilisons au quotidien mais celle-ci est virtuelle, c'est-à-dire sans billet ni pièce.

La crypto-monnaie s'échange de personne à personne (particulier ou entreprise) sur internet contre d'autres devises monétaires (euro, dollar) c'est-à-dire en dehors des réseaux bancaires traditionnels.

La crypto-monnaie a été créée à partir de la technologie informatique blockchain.

Elle s'apparente à un immense registre virtuel public et anonyme regroupant toutes les transactions effectuées par des utilisateurs. [25]

III.2.2 Avantages des crypto-monnaies :

- Elles limitent les intermédiaires comme les banques et donc permettent une réduction des frais.
- Elles sont universelles et donc peuvent être utilisées dans le monde entier.
- Elles permettent l'anonymat des transactions.

III.2.3 Inconvénients des crypto-monnaies :

- Elles sont proscrites dans certains pays.
- Leur valeur n'est pas régulée par une banque centrale.
- Elles sont dépourvues de cadre juridique.
- Elles font face à un lobby bancaire et financier qui ne les soutient pas et les attaquent. [24]

Il existe un grand nombre de crypto monnaies dans le monde tels que : Le Bitcoin. L'Ethereum. Le : Bitcoin Cash, Le Ripple, Le Dash, Le Litecoin, L'Ethereum Classic., mais la crypto-monnaie la plus connue et la plus utilisée est le bitcoin.

III.3 Bitcoin :

III.3.1 Définition :

Le bitcoin est une monnaie virtuelle créée en 2009 par une personne non identifiée dont le pseudonyme est Satoshi Nakamoto. Le bitcoin n'est pas émis et administré par une autorité bancaire. Il est émis sur le protocole blockchain. Cette technologie permet de stocker et transmettre des informations de manière transparente, sécurisée et sans organe central de contrôle. Le bitcoin, comme beaucoup d'autres crypto-monnaies, est mis en circulation via le minage. Les "mineurs", des personnes réparties partout dans le monde,

L'émission de bitcoins est limitée à 21 millions d'unités, comme il a été prévu dans le code initial. Ce montant devrait être atteint en 2140. Début 2018, le nombre de bitcoin émis a passé la barre des 17 millions, soit 80 % du total. En raison de la difficulté croissance de calculs, le bitcoin se crée à un rythme décroissant : 12,5 bitcoins toutes les dix minutes aujourd'hui (contre 50 bitcoins en 2009), Sa capitalisation boursière, ou plus précisément, le nombre de Bitcoin en circulation est d'une valeur de 42 milliards de dollars le 5 juin 2017.

Il n'existe pas de valeur officielle du bitcoin. Cet indicateur est seulement une moyenne des cours du bitcoin sur l'ensemble des plateformes d'échange de crypto-monnaies du monde, Tout simplement sa valeur est définie par la loi de l'offre et la demande. Le 1er juin 2019, le cours du bitcoin s'élevait à 7 640 euros. [27]

III.3.2 Caractéristiques de la monnaie Bitcoin :

- Une monnaie « déflation aire » : la récompense décroît avec le temps.
- Divisible en très petites unités.
- Frais de transactions payés au réseau I Le même coût pour une transaction de $0.01 ou de $1 000 000.
- Basé sur le consensus : sans autorité centrale.
- Difficile à contrefaire.
- Processus de création bien défini.
- Ne peut se dépenser plusieurs fois. [26]

III.3.3 Concepts et mécanismes nécessaires :

- Le réseau Internet : pour les communications entre les participants
- Un moyen de vérifier la validité des transactions et de les inscrire dans un fichier public sans autorité centrale.
- Une chaîne de signatures électroniques qui certifie les transferts de fonds (transactions)
- Un moyen d'éviter la double utilisation d'un bitcoin Un registre de transactions horodaté. [28]

III.3.4 Outils technologiques nécessaires :

- Réseau pair-à-pair (P2P).
- Signature électronique.
- Hachage cryptographique.
- Horodatage.
- Mécanisme de preuve de travail. [26]

III.3.5 Transactions :

Pour envoyer une certaine somme de bitcoin, vous devez publier votre intention de transférer une certaine somme. Les nœuds de vérification vont ensuite venir scanner l'entièreté du réseau afin de s'assurer que :

1) vous possédez bien la somme que vous souhaitez envoyer

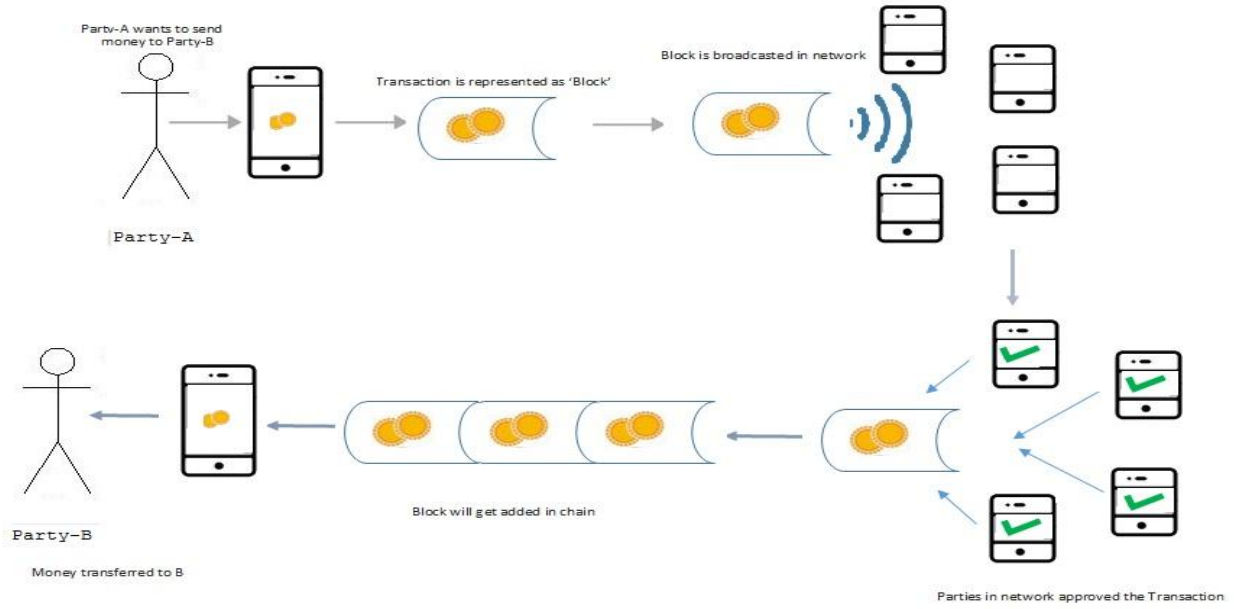
2) vous ne l'avez pas déjà envoyée à quelqu'un d'autre.

Une fois que ces informations ont été confirmées, alors votre transaction est inclue dans un « bloc ». Ce bloc se rattache au bloc précédent. [27]

III.3.6 Le portefeuille électronique

Une fois que vous avez acheté des bitcoins, il est possible de les conserver dans un wallet, un portefeuille électronique physique ou numérique. Il permet d'éviter les risques de piratage dont peuvent être victimes les plateformes de crypto-monnaies. En réalité, votre portefeuille bitcoin ne détient pas réellement vos bitcoins. Ce qu'il contient, mais c'est votre adresse bitcoin, qui elle, détient l'enregistrement de toutes vos transactions passées, et donc votre solde. Et ce qu'on l'appelle la « clé publique ». Elle est donc, comme son nom l'indique, publique. Tout un chacun peut la connaître sans vous faire courir de risque. Toute clé publique a pour corollaire une « clé privée » qui lui correspond. Et il est très important que vous la gardiez confidentielle pour protéger vos bitcoins.

Toute transaction que vous effectuez depuis votre adresse doit être « signée » de votre clé privée. C'est ce qui prouve que vous êtes bien à l'origine de la transaction. Pour ce faire, vous entrez votre clé privée ainsi que les détails de la transaction (combien vous souhaitez envoyer, et à qui) sur votre logiciel de bitcoin. Avec ces informations, le programme crée une signature digitale, qui est envoyée au réseau pour validation. À aucun moment votre clé privée n'apparaît publiquement. Ce n'est que la signature digitale qui apparaît. [27]



Figue 19. Une transaction crypto-monnaie en Bitcoin

III.3.7 La Validation :

Pour faire la validation, Bitcoin utilise un langage de scriptage minimaliste qui automatise les vérifications.

Le langage est non Turing-complet afin d'éviter les boucles infinies.

1. Lors de la validation d'une transaction, les scripts de chaque input sont exécutés.
2. La transaction n'est validée que si le résultat est « vrai » pour tous les inputs.

III.3.8. La difficulté du réseau bitcoin :

Les mineurs effectuent des hashs cryptographiques (deux *SHA256* successifs) sur ce qu'on appelle un *en-tête de bloc*. Pour chaque nouveau hash, le logiciel de minage utilise un nombre aléatoire différent qu'on appelle le *nonce*. Le nonce est une valeur entière avec 32 bits de mémoire qui lui sont alloués. Cela signifie qu'il est limité à environ 4 milliards de possibilités

seulement, ce qui, avec la puissance de hachage actuel du réseau, est largement insuffisant. On ajoute donc dans le hash l'horodatage du bloc en heure Posix, constamment actualisée.
Le hash produit ressemblera à ceci :

```
93ef6f358fbb998c60802496863052290d4c63735b7fe5bdaac821de96a53a9a
```

Afin de rendre le minage difficile, il y a ce qu'on appelle la *difficulté cible*. Afin de créer un bloc valide, un mineur doit trouver un hash qui est inférieur à la difficulté cible. Par exemple, si la difficulté est de :

```
1000000000000000000000000000000000000000000000000000000000000000
```

N'importe quel nombre qui débute par un zéro serait accepté et considéré comme inférieur à la cible. Exemple :

```
0787a6fd6e0782f7f8058fbef45f5c17fe89086ad4e78a1520d06505acb4522f
```

Si nous diminuons la cible à :

```
0100000000000000000000000000000000000000000000000000000000000000
```

Nous avons maintenant besoin d'un nombre débutant par deux zéros :

```
00db27957bd0ba06a5af9e6c81226d74312a7028cf9a08fa125e49f15cae4979
```

Une puissance de hachage de 1 TH/s signifie que 1,000,000,000,000 *hash* sont "essayés" chaque seconde.
La figure suivante présente la difficulté le minage du bitcoin entre juillet 2018 et juin 2019 ou le la difficulté a atteint un niveau très difficile qui a arrivé a plus de 66 millions terra hash par seconde ce qui demande une puissance de calcul très énorme. [30]

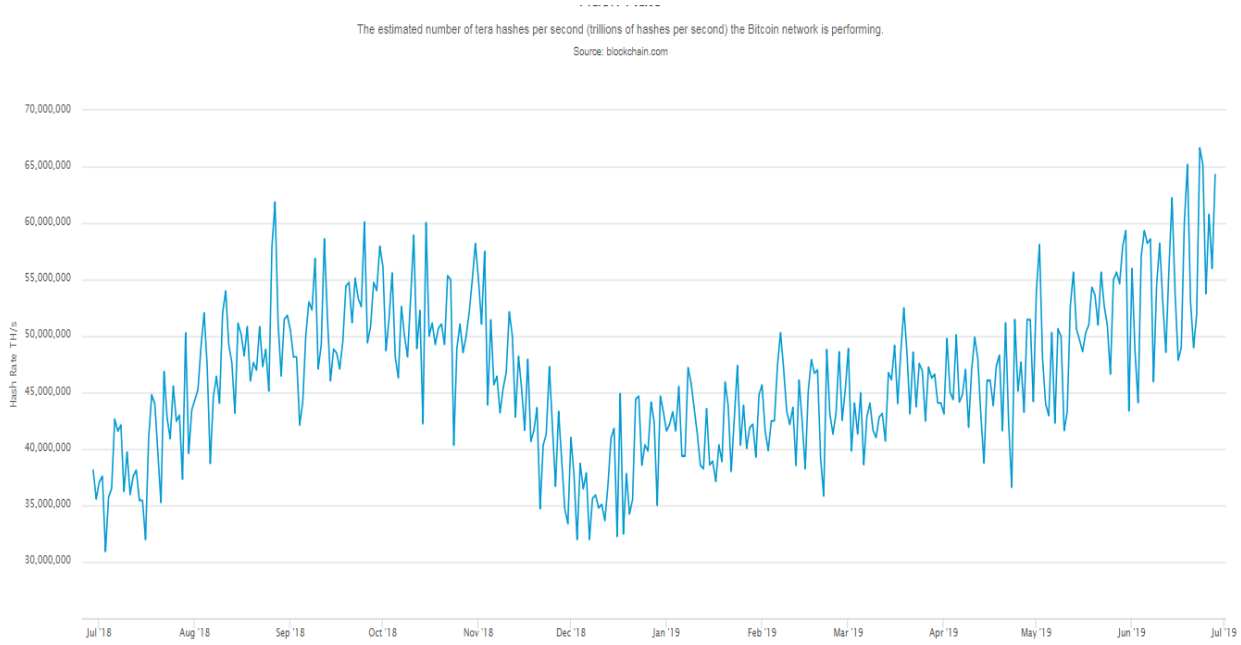


Figure 20 . Nombre estimé de terra hachages par seconde exécutés par le réseau Bitcoin.

III.3.9. Le minage dans le bitcoin :

Aux débuts du Bitcoin, les problèmes mathématiques que l'on devait résoudre étaient relativement simples. Un ordinateur de bureau suffisait à réaliser des opérations et à procurer des revenus à son propriétaire. Mais, au fur et à mesure que le réseau s'est mis à grandir, les problèmes mathématiques sont devenus de plus en plus complexes. Les acteurs du minage dotés d'une puissance de calcul de plus en plus importante.

Aujourd'hui et avec l'augmentation de difficulté du réseau le minage de bitcoin nécessite une puissance de calcul ou il existe des machines spécialisées et optimisées juste pour miner du bitcoin. On les appelle des « ASICs Bitcoin Miner »

La figure suivante montre des centres spécialisés juste dans le minage de bitcoin ou un grand matériel est exploité pour résoudre la fonction cryptographique pour la validation des blocs ce qui augment la sécurité du bitcoin ou la validation des blocs n'est pas disponible pour tout le monde ce qui diminue les essaies de fraudes. [31]



Figure 21. Plateformes de minage du bitcoin

III.4 Internet des objets (Iot) :

La Blockchain repose essentiellement sur un grand livre distribué sécurisé par cryptographie qui permet le transfert sécurisé des données entre les parties.

Les systèmes IoT traditionnels dépendent d'une architecture centralisée. Les informations sont envoyées de l'appareil vers le Cloud où les données sont traitées à l'aide d'analyses, puis renvoyées aux appareils connectés, Avec des milliards d'appareils devant rejoindre les réseaux IoT dans les années à venir, ce type de système centralisé a une évolutivité très limitée, expose des milliards de points faibles compromettant la sécurité du réseau et deviendra incroyablement coûteux et lent si des tiers doivent constamment vérifier et s'authentifier chaque micro-transaction entre les appareils.

Les contrats intelligents dans les réseaux de chaînes de blocs permettront aux appareils de fonctionner de manière sécurisée et autonome en créant des accords qui ne sont exécutés qu'une fois que des exigences spécifiques ont été remplies. Cela permet non seulement une plus grande

automatisation, une plus grande évolutivité et des transferts moins coûteux (aucune tierce partie n'est nécessaire pour superviser les transactions), mais ces contrats intelligents peuvent également empêcher les personnes qui souhaitent utiliser les données à leur avantage, de passer outre aux exigences. Les informations sont partagées sur un réseau décentralisé, sécurisé par cryptographie, ce qui signifie qu'il devient très difficile de compromettre la sécurité du réseau.

Enfin, avec un réseau centralisé, le risque qu'un seul point de défaillance désactive tout un réseau est une possibilité très réelle. Un réseau de blockchain décentralisé atténue ce risque avec des millions de nœuds individuels qui transfèrent des données sur une base Peer-to-Peer (p2p) afin de garantir le bon fonctionnement du reste du réseau IoT[32].

III4.1. Cas d'utilisation du blockchain on Iot :

Les applications IoT dans les chaînes de blocs ont le potentiel de pénétrer presque tous les aspects de la vie quotidienne. À mesure que nous devenons de plus en plus dépendants d'appareils, nous devenons plus dépendants de l'Iot.

Au fur et à mesure que l'IoT évolue vers de futures applications de blockchain. La création de bases de données sécurisées sur le plan cryptographique pour ces concentrateurs de connectivité de périphériques sera au centre des cas d'utilisation de l'IoT.

Ici quelques domaines ou on peut appliquer la blockchain :

- **Véhicules**

  Le secteur de l'automobile a de nombreux cas d'utilisation de la blockchain car il s'agit d'un secteur à forte intensité de main-d'œuvre. La chaîne d'approvisionnement centralisée et la distribution basée sur la confiance constituent le modèle actuel pour la fabrication et l'obtention de véhicules à usage quotidien.

  L'Iot pourrait être utilisé pour mettre à jour automatiquement les grands livres basés sur les chaînes de blocs afin de conserver un enregistrement de véhicule transparent et immuable. Cela contribuerait à accroître la transparence de l'industrie. Les pièces proviennent de tant de fournisseurs différents et implémentent des applications

blockchain et l'IoT pour permettre de suivre ces pièces en mouvement dans un système inviolable et authentifié, ce qui améliorerait la façon dont les véhicules sont achetés, vendus, fabriqués et distribués.

- **Appareils intelligents**

Les appareils intelligents sont la vague du futur. Les maisons et les bâtiments récents ont tous des appareils pouvant se connecter à d'autres appareils, à des applications pour téléphone portable et à Internet. Plutôt que de stocker ces données dans un serveur central ou une solution de stockage dans le Cloud, les données de l'Appliance intelligente pourraient être stockées dans la blockchain. Cela aiderait à sécuriser les informations personnelles et à garder les sites Web IoT à la maison sécurisés. Les données pourraient être utilisées pour améliorer des coûts tels que les coûts énergétiques pour un réseau entier sans lier les informations à une personne ou à un domicile spécifique en utilisant une clé cryptographique à clé publique / privée pour analyser l'identité des données, tout en maintenant l'authenticité des données.

- **Marchés de l'énergie**

Les consommateurs pourraient avoir un accès direct aux places de marché de l'énergie via la plateforme blockchain. Les appareils pourraient être connectés à cette plate-forme, téléchargeant des données en temps réel et offrant des excédents de réseau énergétique permettant de réduire les déchets et de nouvelles sources de revenus, offrant ainsi des services publics plus économiques aux masses. [32]

III.5. Services Gouvernementaux :

En principe, les technologies de chaînes de blocs pourraient être utilisées pour fournir des services gouvernementaux qui nécessitent le traitement et la gestion de documents publics auxquels les personnes ont difficilement accès, dans les pays en développement du moins. De manière plus générale, on peut se servir des chaînes de blocs pour appuyer la prestation générale de la plupart des biens publics aux citoyens et aux parties prenantes, particulièrement ceux qui exigent une interaction personnelle et une identification individuelle. Il existe un lien implicite entre la technologie des chaînes de blocs et le gouvernement électronique, et ce lien est exploré par un petit groupe de jeunes entreprises du domaine des chaînes de blocs. Procivis, une jeune

entreprise suisse, lancera bientôt une boutique d'applications relatives aux chaînes de blocs pour la prestation de certains services gouvernementaux au public. L'entreprise offrira également des services d'identité à ses clients. L'Ukraine a récemment conclu une entente avec **BitFury** [34] pour le soutien de la prestation de services publics à ses citoyens, entre autres choses.

Dubai s'est aussi jointe à la vague des technologies de chaînes de blocs et a l'intention de devenir une ville de chaînes de blocs à part entière d'ici 2020 dans le cadre de l'initiative Smart Dubaï. Les services de santé, qui sont un secteur riche en information, pourraient particulièrement profiter des technologies de grand livre reparti. De nombreuses jeunes entreprises du domaine des chaînes de blocs soutiennent maintenant ces secteurs et travaillent dans des pays comme les Philippines et l'Estonie, pour ne nommer que ceux-là. Comme nous l'avons mentionné plus tôt, la santé est l'une des cibles principales d'Hyperledger. En revanche, le secteur de l'éducation n'est pas parvenu à susciter beaucoup d'intérêt de la part des jeunes entreprises et des consortiums du domaine des chaînes de blocs. [34]

III.6 Services d'Identité :

L'identité auto souveraine est non seulement une bonne idée. Mais peut mettre fin à de nombreux problèmes qui ont une incidence sur la vie privée des consommateurs, notamment le vol d'identité.

L'année dernière, 16,7 millions de personnes aux États-Unis ont été victimes d'une fraude d'identité. Mais ces chiffres ne montrent que la moitié de la réalité. Souvent, les individus n'ont aucune idée que leurs identités numériques ont été compromises jusqu'à ce qu'ils tentent d'acheter une maison ou de contracter un prêt et de retrouver leur vie financière en ruine.

L'utilisation d'un registre à chaînes multiples pour gérer les identités rendrait extrêmement difficile pour les fraudeurs de faire des ravages sans laisser de trace numérique évidente.

Voici comment cela fonctionne : chaque bloc de la blockchain repose sur son prédécesseur et la nature cryptographique de ces blocs rend difficile la modification des informations stockées dans les blocs existants. L'enregistrement résultant est immuable, ce qui signifie que les modifications apportées à chaque identificateur associé à une personne doivent être consignées. Ce système empêche les dépositaires de données de mener des actions malveillantes et rend finalement le vol d'identité plus difficile à exécuter. [33]

III.7. Conclusion :

La technologie de Blockchain est actuellement utilisée dans plusieurs domaines, tels que les services gouvernementaux, Services d'identité, les élections, Titre Fonciers, la médecine, et d'autres domaines et rendre la vie des individus organisée, à l'abri de toutes manipulations, et aussi préserve leurs droits et dicte leurs devoirs.

Malgré tout, la blockchain est en phase de pics d'espérances et a commencé à connaître quelques désillusions. Ainsi, on peut en conclure que la confiance en cette nouvelle technologie n'est pas entière, et qu'elle lui faut davantage d'expérience et d'initiatives afin de la rendre viable dans le monde de l'entreprise.

Les blockchains doivent respecter des normes afin de garantir un fonctionnement considéré comme normal. Ces normes ne sont pas encore totalement établies et une standardisation est nécessaire.

CHAPITRE IV

CONCEPTION DU SYSTEME

IV.1 Introduction:

L'une des étapes les plus importantes dans la réalisation d'un projet est l'étape de conception. Cette dernière est exprimée grâce à la modélisation qui fournit une vue globale du système sans s'approfondir dans les détails d'implémentation. Ce chapitre a pour objet de présenter la modélisation de notre système en utilisant le langage UML. Nous nous sommes basés principalement sur les diagrammes d'activités, ainsi que les diagrammes de classes.

VI.2 Présentation du projet

VI.2.1 : Objectif

Rappelons que l'objectif de ce projet est d'implanter un système de validation des signatures, ainsi que la possibilité de l'appliquer par l'État algérien, ce système qui est considéré comme une nécessité dans notre temps ou le vol de l'identité a augmenté et que notre état ne possède pas d'un système de sauvegarde des copies numériques du document signé numériquement pour assurer l'identité des signataires et la sécurité de ces documents.

Ou ce système pourra offrir de nouvelles solutions pour lutter contre la corruption, puisqu'il permet de créer et de stocker des enregistrements chiffrés qui peuvent être vérifiés, mais ne peuvent pas être modifiés ou supprimés, pour ces raisons on propose de déployer une blockchain pour gérer toutes les signatures et les documents signés dans les différentes utilisations, la blockchain garde les traces de toutes les opérations de chaque document, ce qui va permettre aux entités d'être à l'abri des fraudes et corruption on protégeant son identité ainsi que ces transactions commerciales ou administratives effectuées.

Une infrastructure des machines proposée dans une architecture distribuée, à travers un réseau point à point, les sections qui suivent vont décrire notre application sur un plan purement conceptuel.

IV.3 : Modélisation du système

IV.3.1 : Introduction :

Dans la phase de la modélisation, on cherche d'abord à bien comprendre quelles sont les parties du système, de quoi se compose chaque partie et quel est son rôle précis dans le système.

Nous allons essayer de clarifier le fonctionnement du système à l'aide d'une présentation par des diagrammes UML.

IV.3.2 : Identification des acteurs :

Les acteurs qui forment notre système sont les suivants :

- **L'autorité :** C'est l'organisme qui possède le système et le responsable de la création des fichiers d'identités et des clés cryptographiques, ainsi que de la gestion et de la maintenance du système.
- **Le Client :** c'est une personne physique ou morale identifiée dans le système, qui peut signer des documents individuellement ou collectivement avec d'autres personnes grâce à son fichier d'identité et sa clé cryptographique

IV.3.3 : identification des entités du système :

Le système est composé de plusieurs entités qui sont décrites comme suit :

- **Les mineurs :** Sont des machines puissantes et qui sont les membres principaux et les plus importantes dans un système de blockchain et qui sont tous connectés entre eux dans un système distribué par une connexion point à point et ceux qui garantissent la sécurité et l'intégrité des données, les fonctions principales des mineurs dans notre système sont :
  - La vérification des identités des clients signataires.
  - La vérification et la validation des signatures et des transactions
  - La création et la vérification des blocs de la chaîne
- **Le mineur central :** c'est un mineur dans le système mais avec des fonctions différentes de celles des autres mineurs dont le rôle de ce dernier est :
  - Gérer les transactions de création des identités et de signatures des documents
  - Diffusion la liste des mineurs connectés à tous les utilisateurs (Clients, mineurs)
  - La Gestion des signatures d'un document (Cas : plusieurs signataires).
- **La paire des clés cryptographique :** Chaque client dans le système possède une paire des clés cryptographiques, une clé privée personnelle et secrète et seul le client qui est responsable sur elle.

  Elle est utilisée pour l'authentification dans le système ainsi que la signature des documents, et une clé publique, lisible pour tout le monde et utilisée pour la vérification de l'identité et la vérification des signatures et des transactions.
- **Le fichier d'identité :** c'est un fichier qui contient les informations nécessaires du client et qui est créé par l'autorité, et crypté avec une clé du système.

  Le fichier contient les informations suivantes :

- Le nom et prénom du client.
- L'identification (id.) du client.
- Date de la naissance.
- Lieu de la naissance.
- Numéro du téléphone
- Adresse du Client
- Certificat SSL p12 du client.

- **Le Document signé :** c'est un fichier signé par un ou plusieurs clients, le format du fichier est .PDF
- **La transaction :** Une transaction est un ensemble d'informations structurées et qui identifient et contiennent les opérations de signatures des documents et de création des identités dans le système et qui est contenue dans les blocs de la chaîne.

  Ou nous avons deux catégories de transactions :

  1. Transaction pour les signatures des documents effectuées par les clients

  2. Transaction pour identifier les clients dans notre système.

  Chaque transaction a une syntaxe spécifique définie comme suit :

  - **La syntaxe de la transaction de signatures des documents :**
    - **Id._transaction :** par incrémentation
    - **Signataire :** liste des id des signataires.
    - **Document :** le document signé en format hexadécimal.
    - **Hash_document :** le Hash du document signé.
    - **Signatures :** dictionnaire {id Client : signature du **Hasch_document}**

  - **La syntaxe de la transaction d'identification des clients dans notre système :**
    - **Id._transaction :** par incrémentation
    - **Nom_prénom :** le nom et le prénom du client.
    - **Id._Client :** le id du client.
    - **Public_Key :** la clé publique du client.
    - **Hasch_identité :** le Hasch du fichier d'identité

- **Le bloc de la chaîne :** dans notre système il existe deux types de chaînes des blocs, une chaîne pour les transactions des signatures des documents effectués par les clients, et l'autre pour identifier les clients dans le système.
  - **La syntaxe du bloc :**
    - **Index** : par incrémentation.
    - **Timestamp** : le temps de création de bloc.
    - **Proof** : la preuve du travail.
    - **Previous_Hasch** : le Hasch du bloc précède.
    - **Transactions** : la transaction effectuée.

IV.4. Les spécifications du système

Une spécification est un ensemble explicite d'exigences à satisfaire par un matériau, produit ou service. Si un matériau, produit ou service ne parviennent pas à satisfaire à une ou plusieurs des spécifications applicables, il peut être désigné comme étant hors spécification [35].

IV.4.1 : Les spécifications fonctionnelles :

Rédigée par un analyste fonctionnel, les spécifications fonctionnelles décrites les processus métier dans lesquels le produit informatique devra intervenir. Les tâches prises en charge par le produit informatique, son interaction avec les autres intervenants ‹‹utilisateurs et autres produits›› et les règles des interactions[35].

Les spécifications fonctionnelles de notre système sont les suivants :

Le système doit permettre au client :

- Une opération d'authentification par un login sans transmettre aucun de ces fichiers d'identité ou de clé cryptographique dans le réseau et sans un mot de passe.
- La signature des documents individuellement ou collectivement à n'importe quel moment de la journée et sans être besoin de déplacer a un tiers de confiance pour confirmer son identité.
- Consulter son historique des documents signés ainsi que télécharger ces documents.

Le système doit permettre à l'autorité :

- La génération des clés cryptographique et la création des certificats numérique et des fichiers d'identité.
- L'ajout des clients dans la chaîne des blocs.
- La consultation de la chaîne des blocs
- La consultation de l'ensemble des transactions effectuées et les documents signés.

- L'activation et la désactivation des clients dans le système.

IV.4.2 : Les spécifications non fonctionnels :

Il s'agit des spécifications qui caractérisent le système. Ce sont des besoins en matière de performance, de type de matériel ou le type de conception. Ces besoins peuvent concerner les contraintes d'implémentation comme le langage de programmation, le type du SGBD et du système d'Exploitation.[35]

L'ensemble des extensions à réaliser doivent respecter les besoins suivants :

- **La simplicité :** le système doit être simple a utilisé parce qu'il sera utilisé par un ensemble de clients avec un niveau d'éducation différent et une difficulté de l'utilisation du système peut provoquer un ensemble de problèmes
- **Disponibilité :** Le système doit être disponible à tout moment pour être utilisée par n'importe quel utilisateur.
- **Sécurité :** le système comporte des informations personnelles, donc il doit respecter les règles relatives à la sécurité des systèmes informatiques.
- **La performance :** Le système doit être performant c'est-à-dire qu'il doit répond à toutes les exigences des usagers d'une manière optimale.

IV.5 : Fonctionnement du système :

IV.5.1 : La connexion réseau entre les composants du système :

Dans cette partie, nous allons clarifier la manière dont les composants du système communiquent les uns avec les autres.

- **La connexion entre le client et les mineurs :**

  Dans cette connexion, nous avons utilisé une connexion directe établie avec chaque un des mineurs en mode (client-serveur).figure[22], ou les clients ont besoin des mineurs pour s'identifier dans le système.

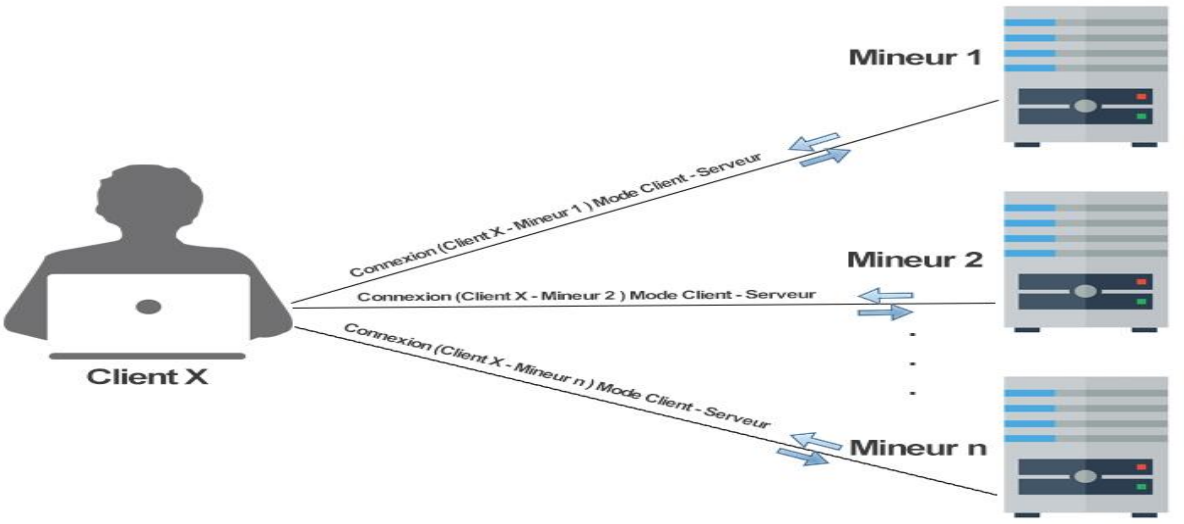


Figure 22. La connexion entre le client et le mineur

- **La connexion entre l'autorité et le mineur central :**

La connexion entre l'autorité et les mineurs est représentée dans la connexion entre l'autorité et le mineur central ou la connexion entre les deux est établi en mode client-serveur comme montré dans la figure[23].

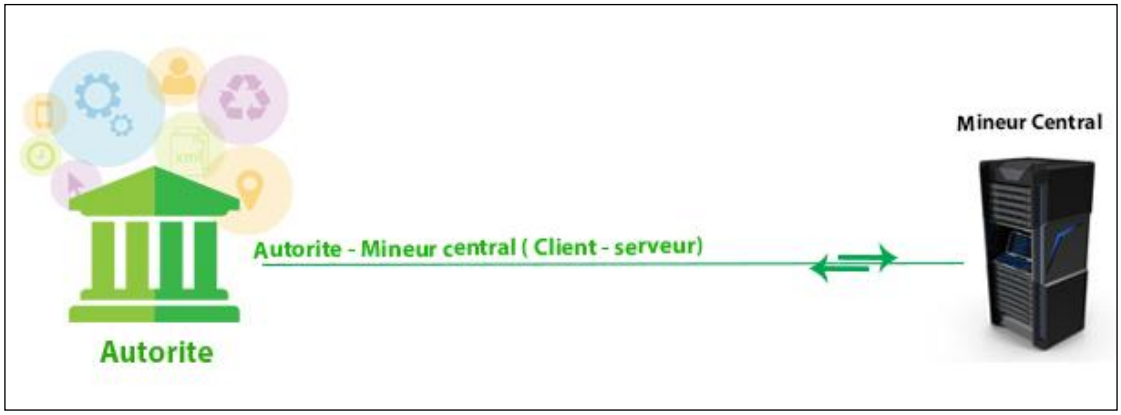
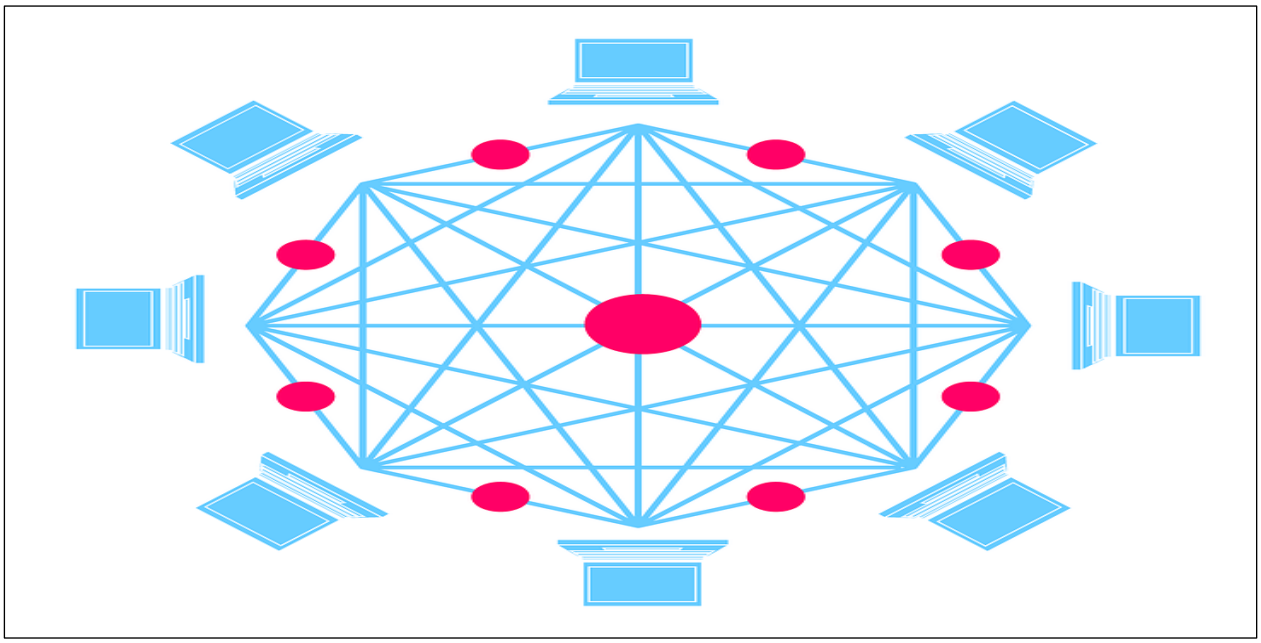


Figure 23. La connexion entre le client et le mineur

- **La connexion entre les mineurs :**

La connexion entre les mineurs est établie en mode point à point (P2P).figure[24], ou chaque client est un client et un serveur au même par rapport aux autres mineurs temps et qu'ils exécutent tous les mêmes actions et fonctionnalité sauf le mineur central qui a des fonctionnalités un peu différentes de l'ensemble des autres mineurs.



Figue 24. La connexion entre les Mineurs entre eux

IV.6 : Modélisation des spécifications fonctionnelle :

La représentation des spécifications fonctionnelles est considérée nécessaire avant d'entamer la réalisation de chaque de chaque projet afin d'obtenir une vue globale sur les exigences du système.

IV.6.1 Diagramme de classes:

Le diagramme de classe est un diagramme faisant partie des diagrammes structurels et est un des diagrammes d'UML le plus utilisés du fait de sa notation syntaxique riche. Il représente la structure d'une application orientée objet en montrant les classes et les relations qui s'établissent entre elles.[36]

IV.6.1.1. Diagramme de classe des entités du systèmes:

le diagramme suivant représente les entités du système de façon plus détaillée avec les avec ses composants et les associations entre eux:

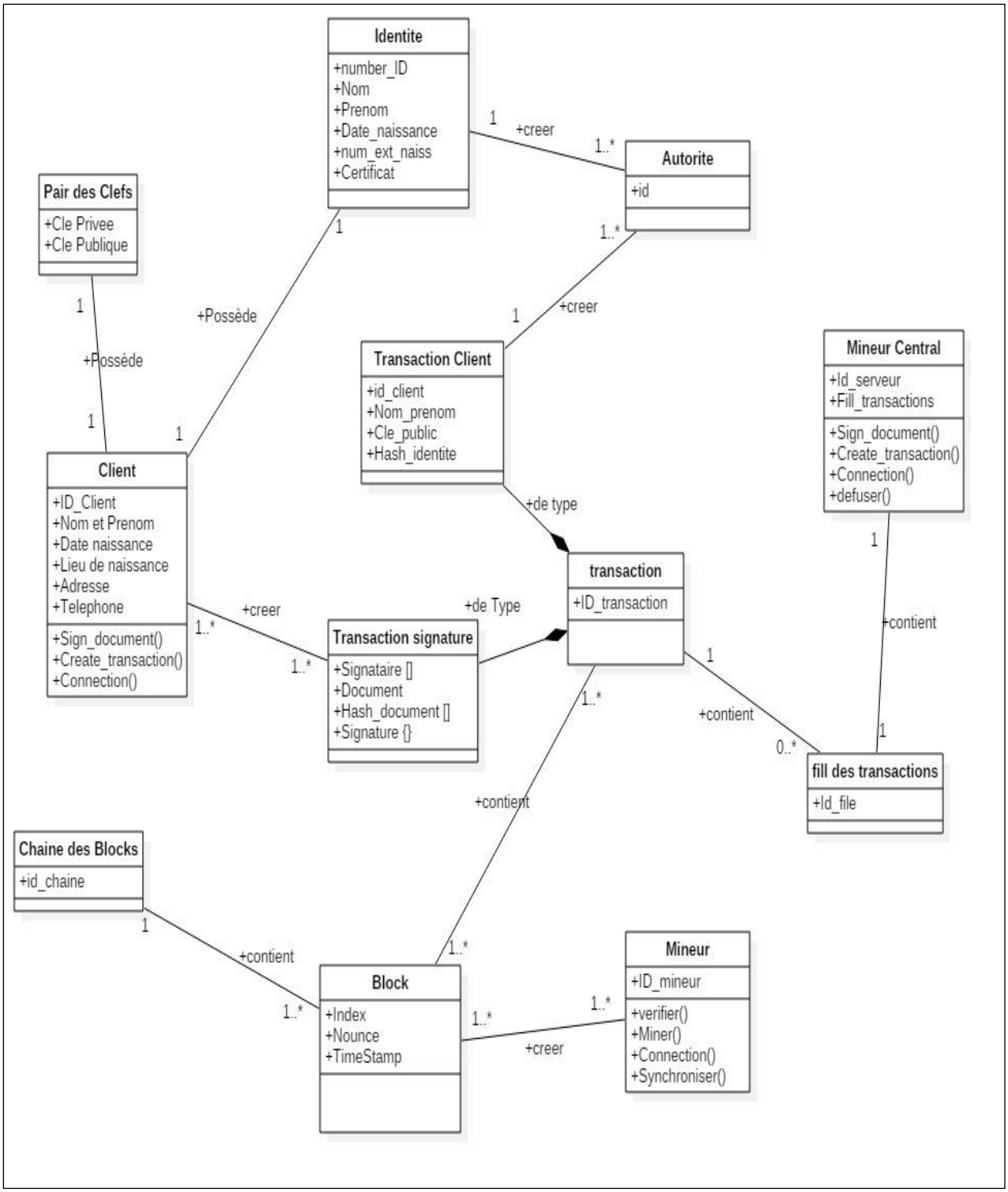


Figure 25. Diagramme de classe des entités du systèmes.

IV.6.2 : Diagramme d'activités :

Un diagramme d'activité fournit une vue du comportement d'un système en décrivant la séquence d'actions d'un processus. Les diagrammes d'activité sont similaires aux organigrammes de traitement de l'information, car ils montrent les flux entre les actions dans une activité. Les diagrammes d'activité peuvent, cependant, aussi montrer les flux parallèles simultanés et les flux de remplacement.[37]

Dans cette partie nous allons représenter les cas d'utilisation principaux dans le système à l'aide du diagramme d'activités.

IV.6.2 : La création de l'identité :

La création du fichier de l'identité est la première étape pour enregistrer dans le système, ou, le client se rapproche à l'autorité responsable que nous considérons comme un tiers de confiance du système avec les papiers nécessaires prouvant l'identité de la personne ou l'entité, et cette dernière qui va créer une paire de clés et un fichier d'identité et enregistrer le client dans le système, ou l'opération détaillée ce passe comme suit :

IV.6.2.1 : Diagramme d'activités ‹‹création de l'identité ›› :

La figure suivante représente le diagramme d'activités représentant les interactions du cas d'utilisation ‹‹création de l'identité››, ou il représente d'une façon plus claire comment ce processus se déroule :

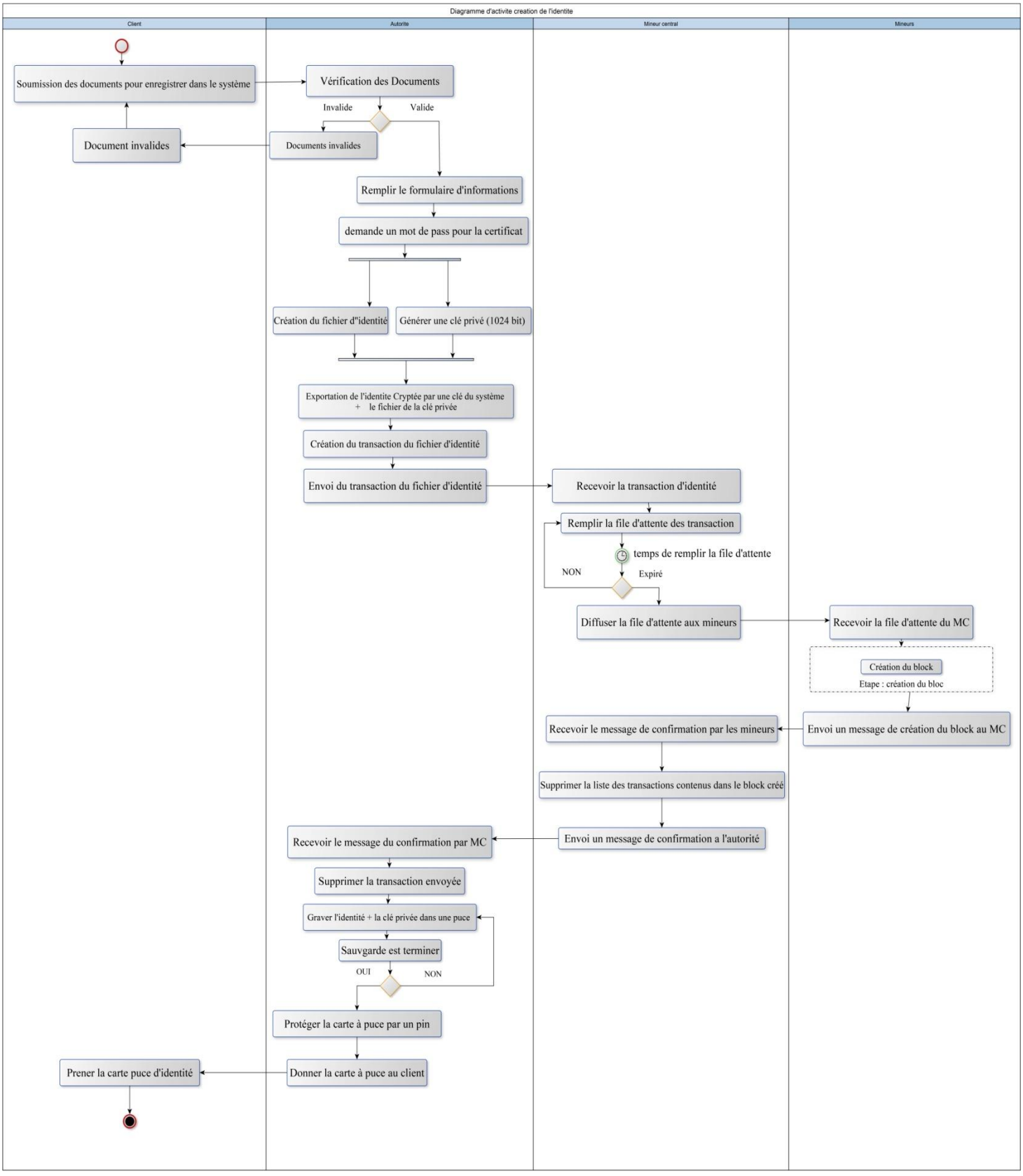


Figure 26. Diagramme d'activités ‹‹création de l'identité ››

IV.6.2.2 : Description textuelle ‹‹création de l'identité ›› :

Scénario normal :

Premièrement le client doit se rapprocher à l'autorité pour enregistrer dans le système, avec les documents nécessaires qui prouvant son identité, après la vérification des documents qu'ils sont valide, le processus suivant se passe.

1. L'agent commence par la vérification des documents prouvant l'identité du client.
2. Il doit remplir ensuite un formulaire des informations du client.
3. Il demande au client de choisi un mot de passe pour son certificat de signature.
4. Une génération d'une clé cryptographique se passe à travers l'application avec une longueur de 1024 bits.
5. Un ficher d'identité cryptée par une clé du système et un fichier contient la clé privée sont créées ensuite et sauvegarder dans la machine.
6. Une transaction d'enregistrement dans le système est créée ensuite et envoyée au mineur central.
7. Le mineur central reçoit cette nouvelle transaction et la stocker dans une file d'attente des transactions.
8. Après la fin du temps de remplir la file que nous avons défini par 10 minutes, le mineur central diffuse cette file de transactions sur l'ensemble des autres mineurs.
9. Les mineurs commencent le processus de la création du bloc.
10. Si le bloc des identités qui peuvent être plusieurs dans un même bloc est créé, un message de confirmation envoyé par les mineurs au mineur central,
11. Après que le reçoit la confirmation, le mineur central supprime la fille d'attente envoyée et renvoi un autre message de confirmation l'autorité pour confirmer la création d'un bloc contient l'identité envoyée, cette confirmation lance le processus final de la création de l’identité par graver cette identité dans une carte à puce.
12. Le client peut prendre alors sa carte à puce contient sont fichier d'identité et sa clé privée et serait ensuite le seul responsable de ses données.

Scénario alternatif :

1. Des documents non valides : le client doit apporter tous les documents nécessaires et valides.

2. En cas de problème de création du bloc ou la probabilité de ce cas est presque nulle ce cas au niveau du mineur il envoie un message d'échec et le mineur renvoi la liste des transactions à nouveau dans la prochaine opération d'envoi.

IV.6.3 : Connexion au portefeuille ‹‹ l'authentification›› :

L'opération de connexion du client a son portefeuille est effectuée sans aucune transmission d'une de ses clés privées ou de son fichier d'identité à travers le réseau, et cette opération d'authentification est effectué par après la participation de chaque un des nœuds (mineur) comme nous ne ferons confiance que dans le système complet, les mineurs vont tous participer alors dans l'opération de l'authentification des clients.

Le processus peut être expliqué comme suit :

IV.6.3.1 : Diagramme d'activités ‹‹ l'authentification››

La figure suivante représente le diagramme d'activités représentant les interactions du cas d'utilisation (connexion au port feuille), ou il représente d'une façon plus claire comment ce processus se déroule :

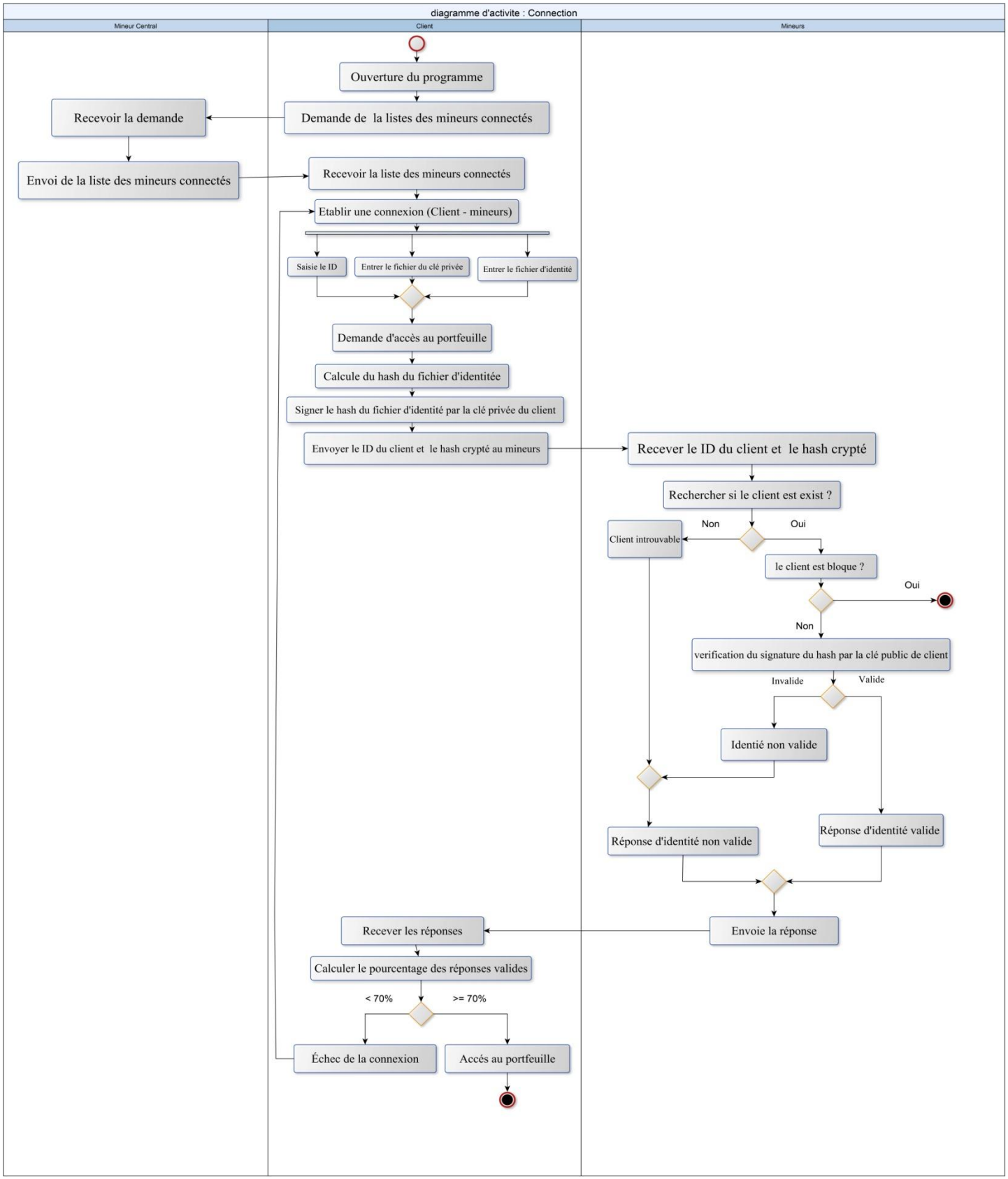


Figure 27. Diagramme d'activités ‹‹ l'authentification ››

IV.6.3.2 : Description textuelle ‹‹ l'authentification›› :

Scénario normal :

Les étapes sont décrites comme suit :

1. Pour accéder au portefeuille le client ouvre le programme du client, le programme connecte automatiquement avec le mineur central, demande la liste des mineurs connectés et établir une connexion avec chaque un de ces mineurs actifs dans le système.
2. Le client ensuite entre sa carte à puce dans un lecteur (dans notre application l'opération est faite manuellement par l'entrée du id, fichier de la clé privée et fichier d'identité).
3. L'application client calcule ensuite le hash du fichier d'identité, et le signer par la clé privée du client et l'envoie avec l'ID aux mineurs.
4. Les mineurs reçoivent les informations envoyées par le client, et commencent la recherche, si le id existe ou non ? :
5. Si l'ID existe : il vérifie encore si le client est en état actif ou désactivé dans le système.
6. Si le client est actif alors chaque mineur vérifie la signature de hash envoyé par la clé publique du client avec le hash contenu dans la transaction qui contienne les informations de ce client.
7. Le mineur renvoie une réponse au client du résultat de vérification d'identité.
8. Le client reçoit tous les messages d'identification des mineurs et calcule pourcentage du nombre de réponses positif par rapport au nombre des mineurs, si le pourcentage égal ou supérieur à 70 pourcents (notre proposition), l'accès au portefeuille du client est autorisé.
9. Le programme extraire ensuite automatiquement la clé privée et la certificat de signature et toutes les informations à partir des fichiers utilisés dans l'opération d'authentification ainsi qu'il envoie l'id du client au mineur central en tant qu'un client authentifié pour l'ajouter dans un dictionnaire avec son socket de connexion pour les utiliser ultérieurement dans les opérations de signatures.

Scénario alternatif :

Tout échec dans l'opération soit au calcul du hash, ou l'inexistence du client dans le système ou l'échec d'authentification, le client sera informé par un message spécifie le type de l'erreur.

IV.6.4 : La signature des fichiers :

La fonction principale du système est la signature des documents des transactions commerciales ou administratives, ou le système doit garantir l'intégrité des données pendant et après la fin de ces transactions.

Dans notre système il existe deux types de signatures des documents, la signature individuelle et la signature collective.

Le processus de déroulement des deux opérations et différent l'un de l'autre et c'est pour sa que nous allons représenter chaque un d'une façon individuelle :

IV.6.4.1 : La signature individuelle :

IV.6.4.1.1 : Diagramme d'activités ‹‹signature individuelle›› :

La figure suivante représente le diagramme d'activités représentant les interactions du cas d'utilisation (signature individuelle), ou le processus de déroulement de l'opération est représenté plus clairement.



Figure 28. Diagramme d'activités ‹‹signature individuelle››

IV.6.4.1.2 : Description textuelle ‹‹signature individuelle›› :

Le déroulement du processus d'opération se passe comme suit :

Scénario normal :

1. Le client commence l'opération par ouvrir la fenêtre de signature individuelle et mettre le fichier dans le dialogue de signature.
2. Le client demande la signature du document, le système lui demande d'entrer le mot de passe du certificat de signature.
3. Le système vérifie le mot de passe du certificat, s'il est valide : l'application client signe le document, et aussi signe le hash du document signé.
4. La transaction du fichier signé ensuite est créée et l'envoyée au mineur centrale.
5. Le mineur principal reçoit la nouvelle transaction reçue et la stocker dans la file d'attente des transactions.
6. Après la terminaison du temps du stockage des transactions dans la file d'attente où ce dernier est limité par 10 minutes, le mineur central diffuse la file des transactions sur tous les mineurs.
7. Les mineurs commencent le processus de création du bloc, si le bloc de la signature du document est créé, les transactions dans le bloc sont envoyées ensuite par les mineurs au mineur central, et ce dernier renvoi un autre message contient le fichier signé au client pour garder une copie signée et validée sur sa machine.

Scénario alternatif

1. Quand le client demande la signature du fichier, et après trois essaies incorrectes du mot de passe du certificat, un message de désactivation de l'identité est envoyé au mineur central, et ce dernier diffuse le message sur l'ensemble des autres mineurs pour ajouter l'identité dans une liste noire, le client ensuit ne peut pas utiliser son identité jusqu'à la réactivation à partir de l'autorité.
2. Toute erreur dans l'opération de signature ou de renvoi ou de création de la transaction, le client sera informé par le type d'erreur.

IV.6.4.2 : La signature collective des documents :

La signature collective est une opération faite par deux ou plusieurs signataires identifiés dans le système ou l'opération est effectuée localement chez chaque un des signataires sans transmettre son identité en réseau, avec la garantie de l'intégrité des données pendant l'opération

Le processus de l'opération se passe comme suit :

IV.6.4.2.1 : Diagramme d'activités ‹‹ La **signature collective ››**

La figure suivante représente le diagramme d'activités qui introduit une explication des interactions du cas d'utilisation ‹‹signature collective››, ou le processus de déroulement de l'opération est représenté plus clairement :

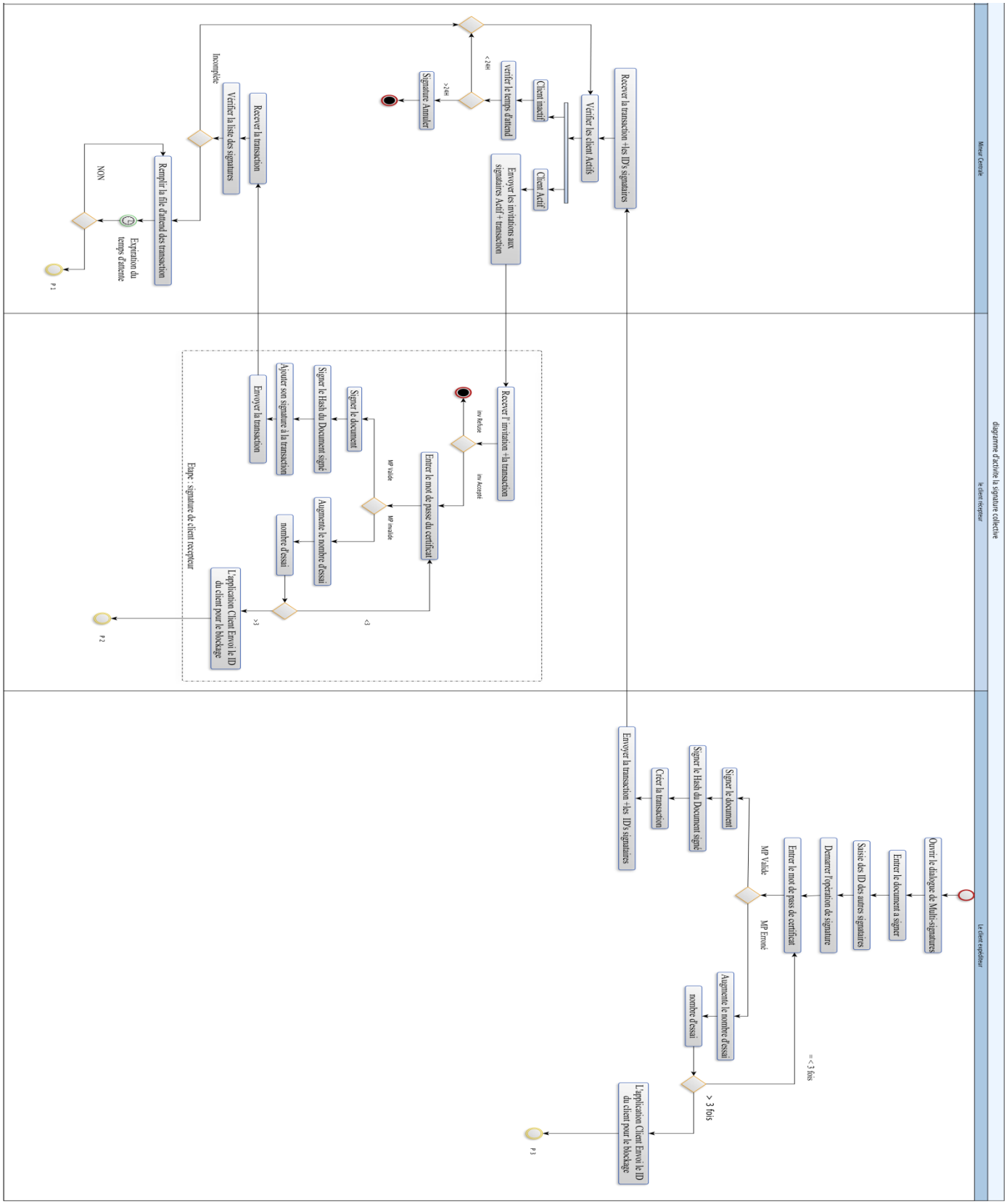


Figure 29. La signature collective (Partie1).

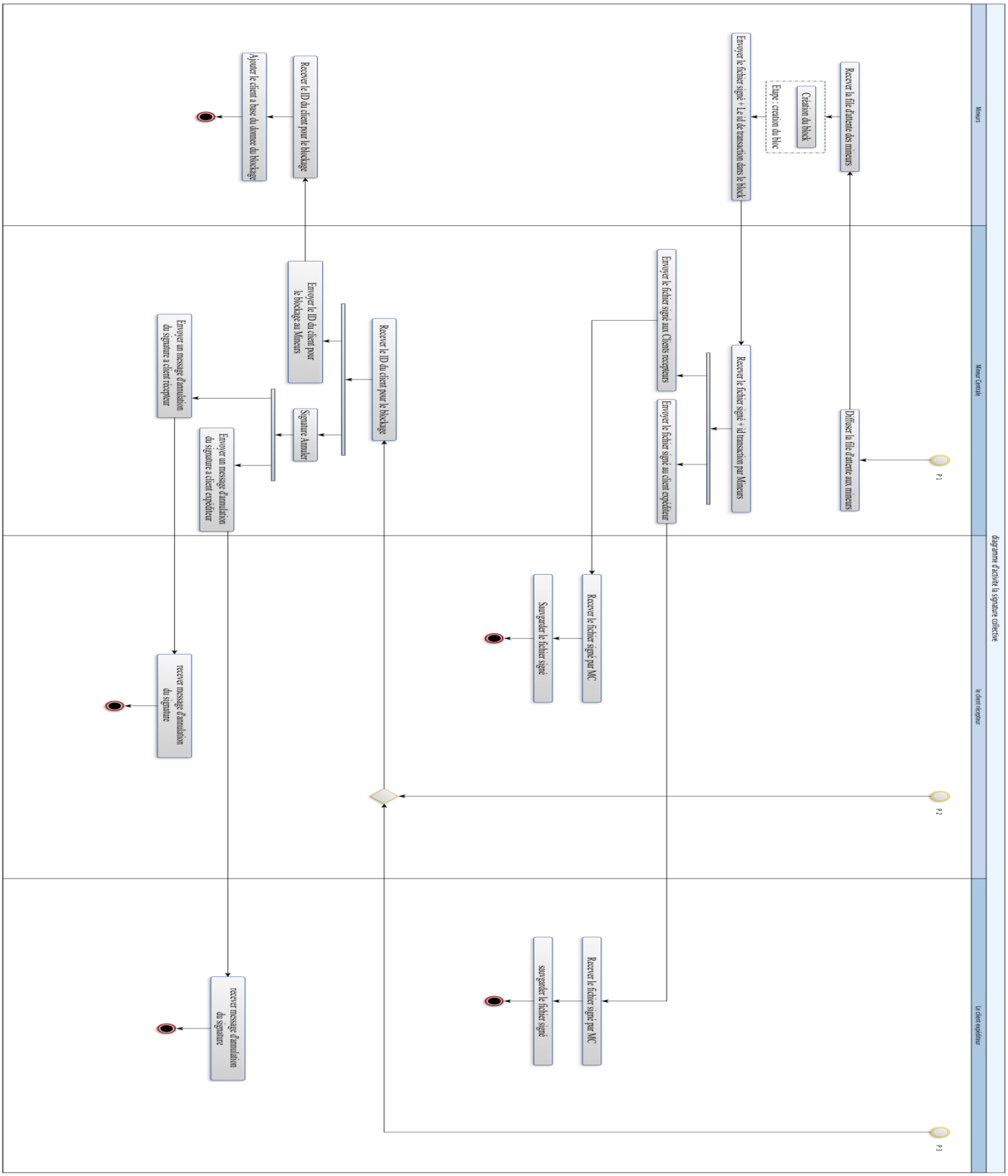


Figure 30. La signature collective (Partie2).

IV.6.4.2.1 Description textuelle‹‹ La signature collective ›› :

Scénario normal :

1. Le client expéditeur de l'invitation de signature et après ouvrir le dialogue de signature collective charge le fichier a signé et saisie les ID's d'autres clients qui vont signer avec lui.
2. Le client qui va inviter les autres clients de signer avec lui commence par signer le premier le document localement, ou il doit entrer son mot de passe du certificat.
3. Si le mot de passe du certificat est valide : l'application client signe le document, signe le hash du document signé, créer la transaction du fichier a signé et l'envoie au mineur central.
4. Le mineur central reçoit la transaction contienne la liste des ID des autres clients, effectue ensuite une opération de recherche si ces clients invités sont en ligne dans système, il envoie ensuite aux clients en lignes un par un la transaction signée par le client précédent et l'invitation à signer le document avec tous les ides des signataires qui vont signer, la nouvelle transaction contiennent le fichier signé, les id des signataires qui sont déjà signer le document du et leurs signatures de la transaction.
5. Dès que le client accepte l'invitation, sa signature est ajoutée ensuite dans le fichier ainsi que sa signature du hash du fichier est ajoutée à la liste des signatures dans la transaction.
6. Après que le document est signé par tous les clients concernés, le mineur principal reçoit la dernière transaction qui sera utilisée pour la création du bloc et l'ajouter dans la file d'attente des transactions.

7. Le reste de l'opération de création et validation du bloc est le même de celle d'une signature individuelle.

Scénario alternatif :

1. Si les clients ne sont pas tous en ligne et qu'un ou plusieurs signataires n'entrent pas dans le système pour signer le document, nous avons défini une durée de 24 heures pour l'opération, après l'expiration de la durée est que le fichier n'est pas signé par touts les signataires concernés l'opération sera annulée, et les autres clients qui ont signé seraient informés par l'annulation de l'opération.

2. Si un client entre trois fois un mot erroné du certificat, son identité sera désactivée du système, ainsi que la transaction sera annulée tous les clients seront informés par l'annulation de la transaction.
3. Si un client invité refuse l'invitation de signature, l'opération sera annulée immédiatement et les autres signataires seraient informés par l'annulation.
4. Toute autre erreur dans le processus, le client sera informé par un message de description de l'erreur.

IV.6.5 : La création des blocs :

Contrairement aux bases de données normales ou partagées dotées d'un gestionnaire de données central, les chaînes des blocs disposent d'un système de gestion spécifique et hautement sécurisé, qui dépend d'un consensus de tous les mineurs du système.

IV.6.5.1. Diagramme d'activités < Création du bloc > :

La figure suivante représente le diagramme d'activité représentant les interactions du cas d'utilisation (Création du bloc), ou le processus de déroulement de l'opération est représenté plus clairement :

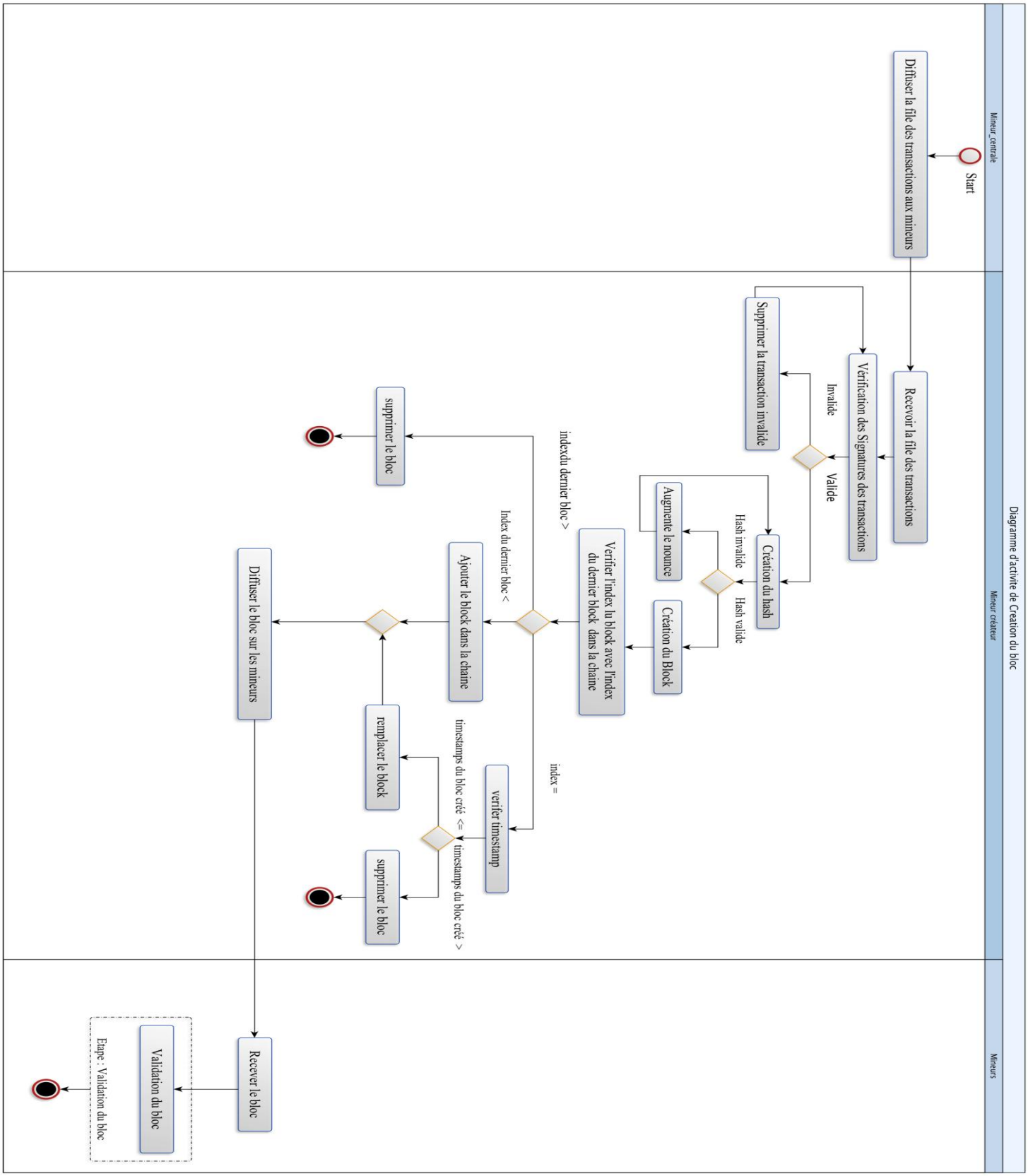


Figure 31. La création des blocs

IV.6.5.2. Description textuelle ‹‹ La création du bloc ›› **:**

Le déroulement du processus d'opération se passe comme suit :

Scénario normal :

1. Lorsque le Mineur central distribue la file d'attente des transactions aux autres mineurs, le mineur commence par vérifier la validité des transactions envoyées en vérifiant leurs signatures numériques de chaque client dans les transactions par l'utilisation de sa clé publique.
2. Après la vérification des transactions, le mineur commence le processus de création du bloc ou il doit retrouver un hash obtenu de la multiplication de la valeur du nonce du dernier bloc avec un nombre qui sera la valeur du nonce du bloc en cour de création a, ou ce hash doit commencer par "n" nombre de zéros définit par l'autorité du système et qui est appelé la difficulté du système, cette opération effectuée par le mineur est appelée la preuve du travail < cette technique est déjà expliquée dans le chapitre II
3. Dès que le mineur trouve le hash, il crée le bloc et le remplir avec les informations nécessaires.
4. Mais avant d'ajouter le bloc à la chaîne, un processus de vérification du bloc doit être effectué pour ne pas tomber dans des problèmes de différence des blocs dans les différents mineurs.
5. La méthode de vérification se passe comme suit :
   - Si le bloc créé est de même index avec le dernier bloc dans la chaîne, c'est-à-dire il existe un bloc reçu avant que le mineur termine la création du bloc, le mineur dans ce cas compare le temps de création du bloc, et choisi le bloc le plus moins temps.
   - Si le bloc créé à un index supérieur l'index du dernier bloc dans la chaîne le mineur ajoute le bloc directement à la chaîne.
   - Tout mineur qui termine l'opération de création du bloc diffuse ensuite le bloc créé sur l'ensemble des autres mineurs pour valider le bloc.
   - Il effectue ensuite une opération de vérification de la validité de la chaîne.

Scénario alternatif :

- Pendant la vérification toute transaction n'est pas valide sera supprimée.

IV.6.6. La validation des blocs reçus:

L'une des opérations les plus importantes qui garantissent l'intégrité et la sécurité des données est la validation des blocs, cette opération dépend d'un ensemble de tests qui déroulent comme suit :

IV.6.6.1. Diagramme d'activités ‹‹ La validation des blocs reçus ›› :

La figure suivante représente le diagramme d'activités représentant les interactions du cas d'utilisation ‹‹validation des blocs››, ou le processus de déroulement de l'opération est représenté plus clairement :

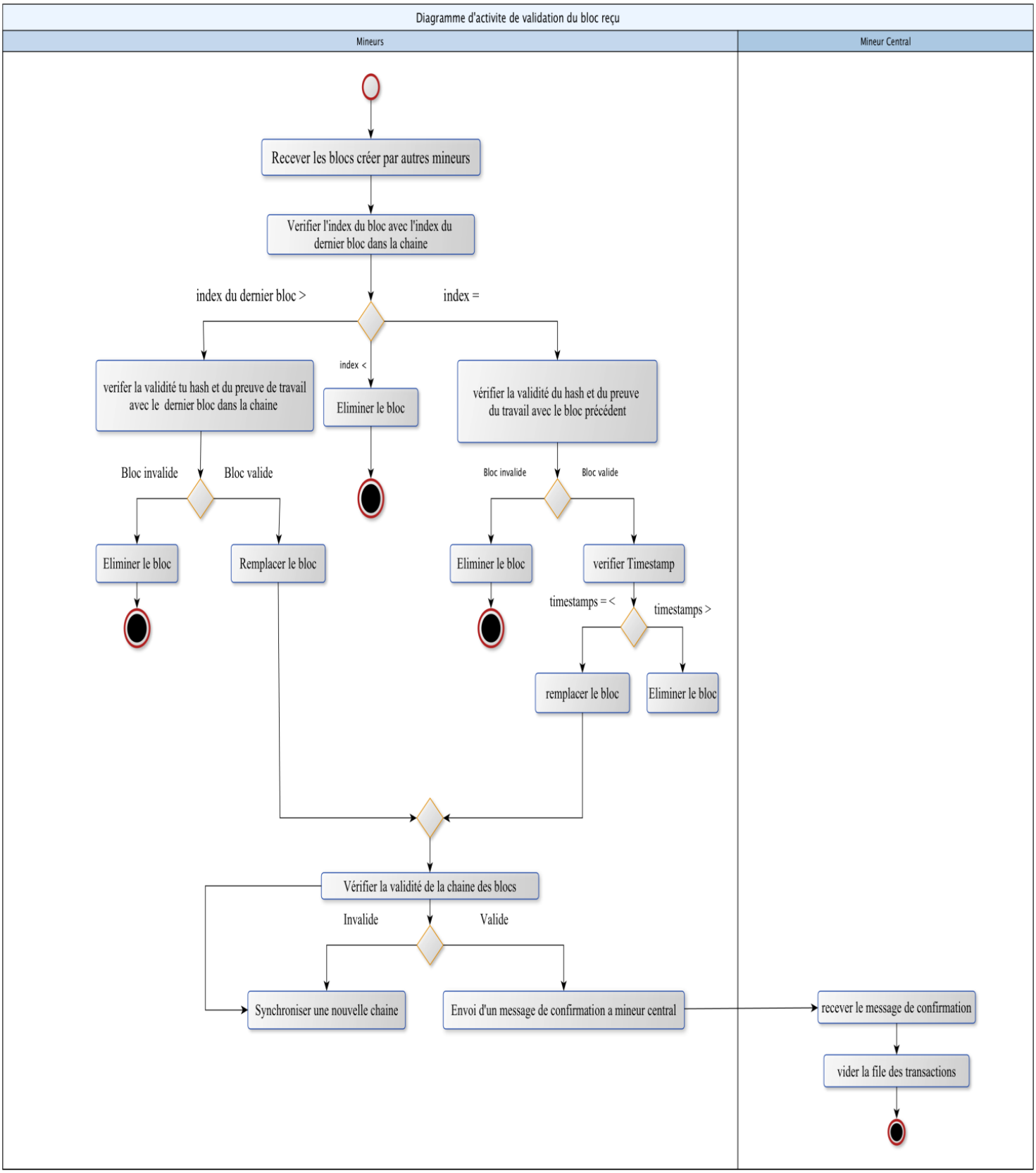


Figure 32. La validation des blocs reçus

IV.6.6.2. Description textuelle‹‹ La validation des blocs reçus ›› :

Le déroulement du processus d'opération se passe comme suit :

Scénario normal :

L'opération de validation du bloc ce passe lorsqu'un mineur reçoit un bloc créé d'un autre mineur, ou le mineur doit vérifier la validité du bloc et des transactions contenues dans le bloc avant de l'ajouter dans la chaîne ou le supprimer, ou les étapes sont décrites comme suit :

1. Dès que le mineur reçoit un bloc à partir d'un autre mineur il doit effectuer les opérations suivantes :
2. Si le bloc reçu est de mêmes index avec le dernier bloc dans la chaîne, c'est-à-dire il existe un bloc créé ou reçu avant ce bloc, le mineur dans ce cas commence par vérifier si le bloc est valide, en vérifiant le la valeur prévious_hash si c'est vrai que c'est la valeur du hash du bloc inférieur, il vérifie ensuite la valeur du nonce du hash si l'opération de multiplication de cette valeur avec celle du bloc inférieur forme donne un hash qui commence par les "n" zéros définit par l'autorité, ensuit le mineur effectue une vérification de toutes les transactions du bloc en vérifiant les signatures des clients dans les transactions.
3. Si le bloc est valide, il compare alors l'index du bloc avec le dernier bloc de la chaîne.
4. Si le bloc reçu à un index inférieur de l'index du dernier bloc dans la chaîne alors le mineur élimine le bloc reçu.
5. Si le bloc reçu à l'index suivant de l'index du dernier bloc dans la chaîne, le mineur alors l'ajoute dans la chaîne.
6. Si le bloc a le même index avec le dernier bloc de la chaîne alors il compare le temps de création du bloc, et choisi le bloc qui a été créé en premier.
7. Après la méthode de vérification du bloc, tous les mineurs exécutent une méthode de vérification de la validité de la chaîne des blocs, cette méthode permet de vérifier la chaîne de blocs en cas d'ajout d'un bloc invalide par une partie illégale ou une modification dans les blocs existe, ou cette opération se passe comme suit :

   Pour chaque bloc il multiplie la valeur du nonce avec celle du bloc précédent est calcul la hash du résultat s'il commence par les n zéros définis pas l'autorité, pour chaque bloc calcul le hash du bloc précédent est le compare avec la valeur previous_hash jusqu'à la fin de la chaîne.

Scénario alternatif :

1. Pendant la validation, une erreur dans la vérification de la valeur du nonce ou du hash précédent implique une ignorance directe du bloc.
2. Pendant la vérification de la chaîne toute petite modification dans la chaîne implique une modification dans le hash, et alors implique une non-validité de la chaîne le mineur ensuite supprime la chaîne de demande une synchronisation d'une nouvelle chaîne valide des autres mineurs

IV.7 : Conclusion :

Ce chapitre avait pour but de décrire le système globalement sans rentrer dans les détails d'implémentations. Le prochain chapitre sera consacré au développement de notre application en détaillant les différents éléments d'implémentation.

CHAPITRE V

IMPLEMENTATION DU SYSTEME

V.1 Introduction :

Après avoir présenté la conception de notre projet, nous allons dans ce chapitre décrire l'implémentation de note système. Nous allons tout particulièrement aborder les outils de développement, l'implémentation de la base de données et donnons un aperçu des interfaces de notre application.

V.2 Les technologies utilisées :

V.2.1.Le Langage de programmation PYTHON :



Python est un langage de programmation multi-paradigme. Il favorise la programmation impérative structurée, et orientée objet. Il est doté d'un typage dynamique fort, d'une gestion automatique de la mémoire par ramasse-miettes et d'un système de gestion d'exceptions ; il est ainsi similaire à Perl, Ruby, Scheme, Smalltalk et Tcl.

Le langage Python est placé sous une licence libre proche de la licence BSD et fonctionne sur la plupart des plates-formes informatiques, des supercalculateurs aux ordinateurs centraux, de Windows à Unix en passant par Linux et Mac OS, avec Java ou encore.NET. Il est conçu pour optimiser la productivité des programmeurs en offrant des outils de haut niveau et une syntaxe simple à utiliser. Il est également apprécié par les pédagogues qui y trouvent un langage où la syntaxe, clairement séparée des mécanismes de bas niveau, permet une initiation plus aisée aux concepts de base de la programmation [38].

V.2.2. Le SQL :



SQL est un langage de requête standardisé permettant de demander des informations à une base de données. La version originale appelée SEQUEL (structured English query language) a été conçue par un centre de recherche IBM en 1974 et 1975. SQL a été introduit pour la première fois en tant que système de base de données

commerciale en 1979 par Oracle Corporation.

Traditionnellement, SQL était le langage de requête préféré des systèmes de gestion de bases de données fonctionnant sur des mini-ordinateurs et des ordinateurs centraux. Cependant, SQL est de plus en plus pris en charge par les systèmes de base de données. Car il prend en charge des bases de données distribuées (bases de données réparties sur plusieurs systèmes informatiques). Cela permet à plusieurs utilisateurs d'un réseau local d'accéder simultanément à la même base de données.[39]

V.3 Les outils utilisés :

- **Pycharm :**



Pycharm est un environnement de développement intégré utilisé pour programmer en Python.

Il permet l'analyse de code et contient un débogueur graphique. Il permet également la gestion des tests unitaires, l'intégration de logiciel de gestion de versions, et supporte le développement web avec Django.

Développé par l'entreprise tchèque **JetBrains**, c'est un logiciel multiplateformes qui fonctionne sous Windows, Mac OS X et Linux. Il est décliné en édition professionnelle, diffusé sous licence propriétaire, et en édition communautaire diffusé sous licence Apache. [40]

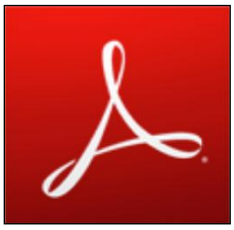
- **Adobe Photoshop :**



Est un logiciel de traitement d'image. Cette application permet de créer, de modifier des images.

Avec Photoshop, l'éditeur Adobe peut se targuer de proposer l'un des logiciels de création les plus courants dans la culture populaire. Cette solution est une référence en termes de création et de retouche photo et ne connaît pas de concurrence véritable tant ses fonctions s'adressent aux professionnels les plus exigeants. [41]

- **Adobe Acrobat Reader :**



Développé par l'entreprise Adobe, permettant de visualiser, de commenter, de signer et vérifier la signature en toute sécurité les documents PDF. [V.5

- **SQLite :**



SQLite est un système de gestion de base de données relationnelle. Ce moteur de base de données est connu pour implémenter une grande partie du standard SQL-92 et des propriétés ACID.

Cette bibliothèque écrite en C est directement intégrée au programme. Ce système et son code source sont entièrement dans le domaine public ce qui permet à tout à chacun d'utiliser et de participer à l'évolution de ce projet. [V.6

V.4 Prototypes :

V.4.1 Architecture de fonctionnement d'application :

La figure suivante résume l'architecture de notre application en montrant quelques fonctionnalités avec chacun de nos utilisateurs. Expliquant notre système en le divisant en quatre parties (Autorité, Le mineur central, Les mineurs et le Client) sachant que les applications sont toutes disponibles sous tous les systèmes d'exploitation (Windows, Linux et Mac os).

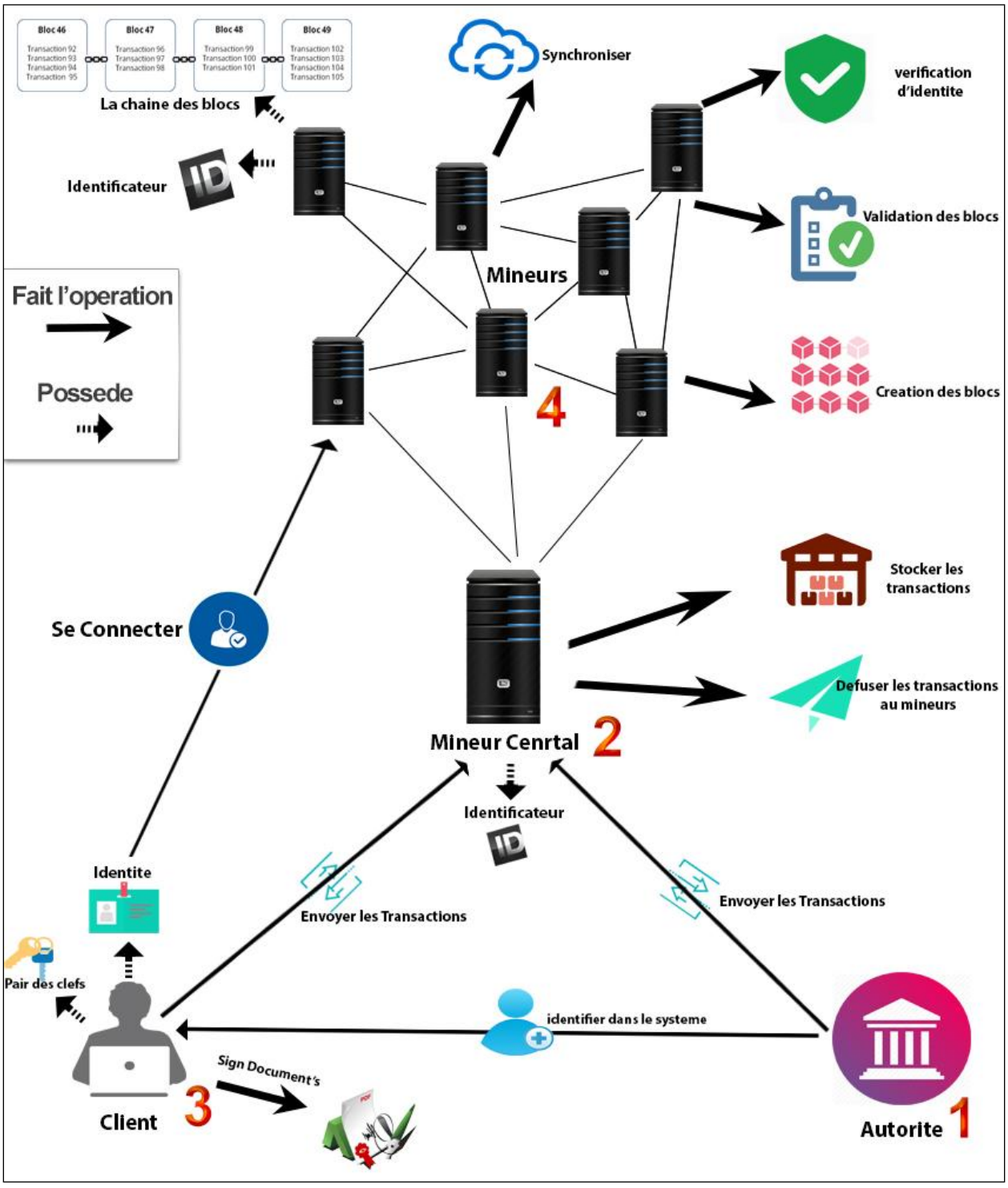


Figure 33: Architecture de fonctionnement d'application

V.4.2 Description textuelle :

V.4.2.1. Coté Autorité :

- **Identifier les clients dans le système :**

L'Autorité enregistre les clients dans le système pour leur permettre de signer des documents sous à travers des transactions avec le réseau de la Blockchain.

V.4.2.2 Coté Client :

Le client possède une identité pour l'identifier dans le système, et une clé privée pour crypter les messages échangés et la signature numérique ou il peut :

- **Se Connecter :**

Le client se connecte au système via les fichiers mentionnés ci-dessus.

- **Signer un document :**

Le client peut signer un document PDF individuellement ou avec un groupe des clients.

V.4.2.3 Coté Mineur Central :

Le mineur central est un mineur mais a un accès limité et un rôle différent des autres, il communique avec tous les composants du système, on peut le considérer comme un point de passage et d'observation, se communique avec les mineurs avec le mode point à point (Peer to Peer), et avec les autres avec le mode client-serveur, il possède un seul identifiant pour l'identifier dans notre système ou il peut :

- **Stocker les Transactions :**

Chaque opération, soit un ajout d'un nouveau client ou une signature d'un document est stockée dans une transaction, ses transactions sont créées par les clients ou par l'autorité. Elles sont Toutes stockées de façon temporaire dans le mineur central.

- **Diffuser la liste des transactions aux Mineurs :**

Après le stockage des transactions, le mineur central les regroupe dans une file d'attente. Une fois le délai d'attente est écoulé, le mineur central diffusera la file d'attente vers tous les mineurs.

V.4.2.4. Coté Mineurs :

Le mineur est le cœur du système, fait des opérations de la vérification d'informations et la validation des blocs créés ou reçus.

Se Communiquer avec les autres mineurs avec le mode point à point (Peer to Peer), et avec les clients en mode client-serveur, possède un identifiant pour l'identifier dans notre système et les deux chaînes des blocs (chaîne des clients et chaîne des documents signés) les fonctions de mineur sont :

- **La création des blocs :**

Après avoir reçu la file d'attente, le mineur crée le bloc contenant toutes les transactions reçues.

- **La validation des blocs :**

Chaque mineur crée, envoie et reçoit des blocs en même temps, il vérifie et valide le bloc reçu et le compare avec les blocs précédents pour l'ajouter à la chaîne ou l'ignorer.

- **La vérification d'identité :**

Il communique avec le client pour vérifier l'accès à son portefeuille.

- **La synchronisation des blocs :**

Si le mineur est absent ou si une erreur survient dans la chaîne, il synchronise la chaîne valide depuis les autres mineurs.

V.5.Présentation des interfaces de l'application :

V.5.1 Introduction :

Les interfaces graphiques sont devenues essentielles dans l'utilisation de toutes les applications, elles déterminent comment utiliser ses applications de manière simple et devenue un standard dans l'évaluation des applications.

Dans cette section on va présenter les principales interfaces de nos applications

V.5.2 Application de l'Autorité :

V.5.2.1 Interface d'accueil :

En tant qu'autorité capable de :

- Créer de nouveaux clients.
- Afficher les informations du client.
- Vérifier la signature d'un document.
- Afficher la chaîne stockée.
- Paramètres de l'application

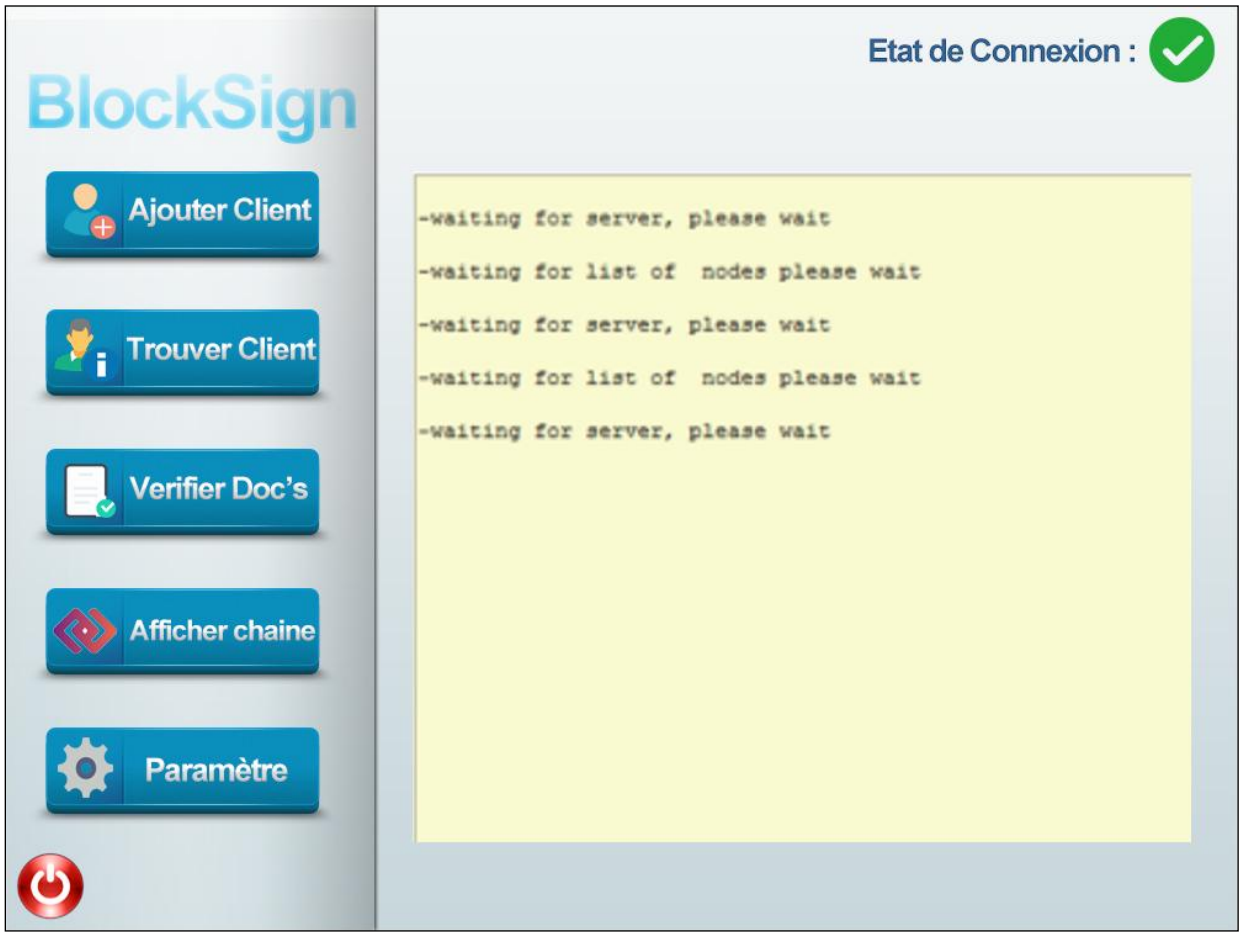


Figure 34: interface d'accueil

V.5.2.2 Interface Ajouter un Client :

Pour ajouter un nouveau client, l'Autorité remplira le formulaire indiqué dans l'interface suivante après vérification des données du client :



Figure 35 : interface Ajouter un Client.

V.5.3 Application Mineur Central :

V.5.3.1 Interface d'accueil :

Le mineur central possède une interface simple à utiliser, Il a trois boutons :

Le premier pour lancer le mineur dans le réseau en tant que client et serveur au même temps central, le second pour l'arrêter et le troisième pour ouvrir la fenêtre des paramètres de connexions avec un espace d'affichage comme un journal pour afficher les principaux événements effectués ou passées par le mineur.

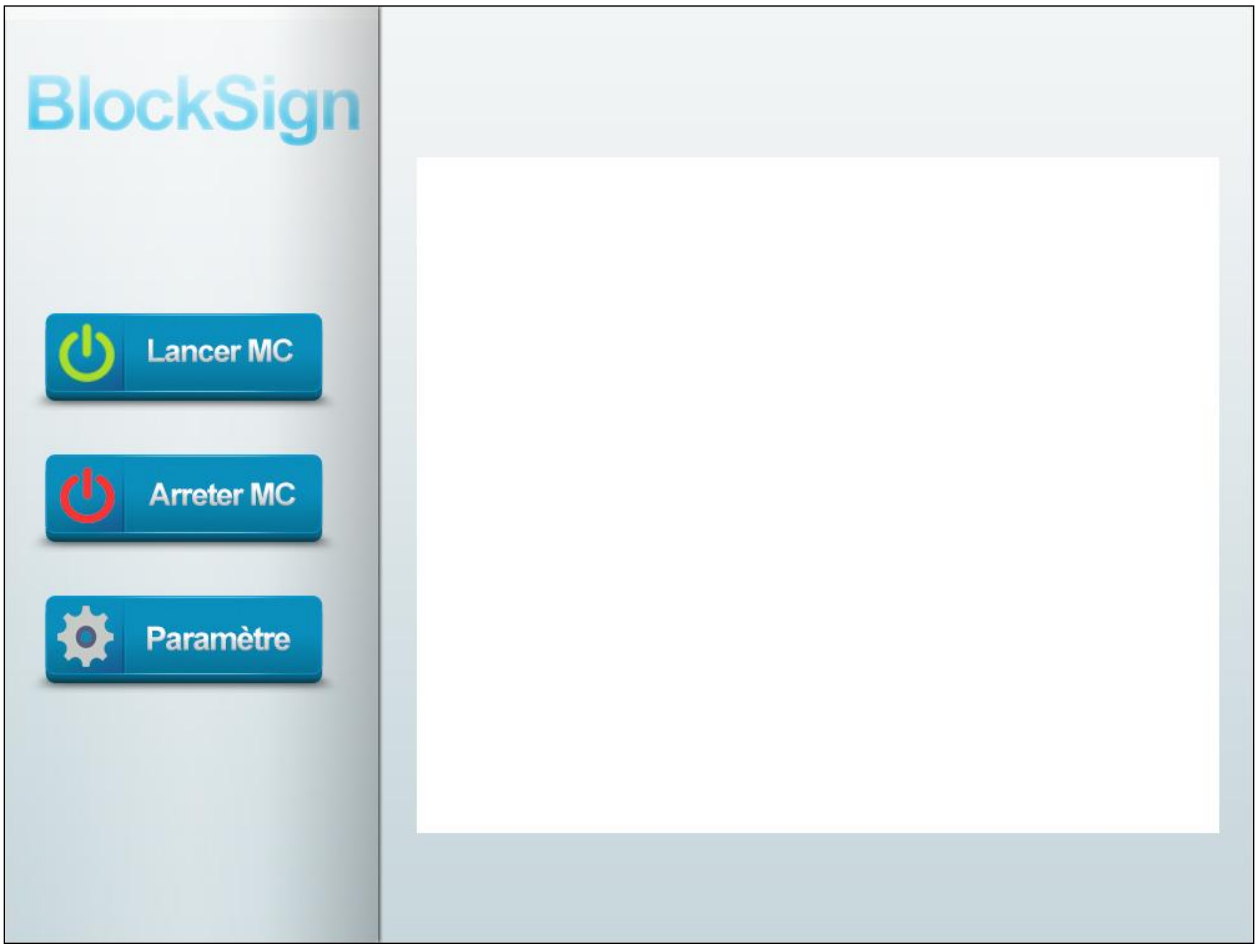


Figure 36: interface d'accueil du Mineur Central.

V.5.4 Application Mineur :

V.5.4.1 Interface d'accueil :

Le mineur central possède une interface simple à utiliser, Il a quatre boutons :

Le premier pour exécuter le Mineur dans et le lancer dans le réseau en tant qu'un client et serveur au même temps, le second pour l'arrêter et le troisième affiche les chaînes des blocs et le quatrième pour les paramètres de la connexion.



Figure 37: interface d'accueil du Mineur.

V.5.5 Application Client :

V.5.5.1 Interface de Connexion :

L'interface de connexion du client contient plusieurs champs, le premier permettant de saisir le numéro d'identification, le second permettant de charger le fichier d'Identité et le troisième permettant de charger le fichier de la clé privée, et finalement deux boutons pour se connecter ou pour annuler l'opération.



Figure 38: interface du Connexion**.**

V.5.5.2 Interface de Portefeuille :

L'interface du portefeuille possède trois boutons principaux, Le premier nous amène à l'interface de la signature individuelle, le deuxième nous amène à l'interface de la signature collective, et la troisième affiche les invitations reçues à partir des autres Clients.

Il possède aussi deux boutons :

Le premier pour se déconnecter du portefeuille, et le second pour les paramètres.



Figure 39: Interface de Portefeuille.

V.5.5.3 Interface la signature individuelle :

L'interface de la signature individuelle possède un champ pour charger le fichier à signer et un autre champ pour afficher le document à signer, et bouton pour signer le document.

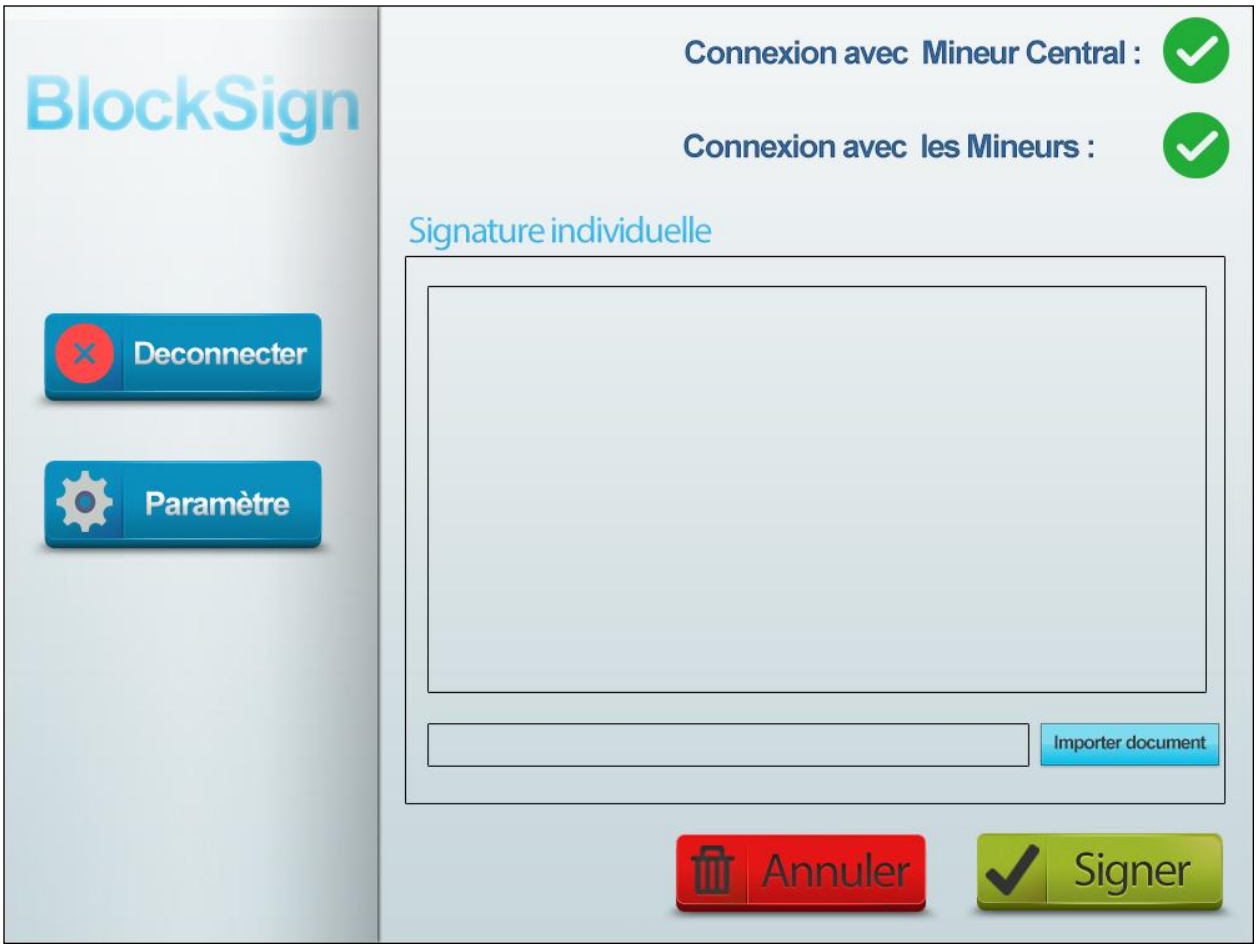


Figure 40: Interface de la signature individuelle.

V.5.5.4 Interface de la signature collective :

L'interface de signature collective contient un champ pour charger le fichier à signer, des autres champs pour saisir les numéros d'identification des clients signataires et pour afficher le document à signer, et deux boutons pour se signer le document ou pour annuler l'opération.

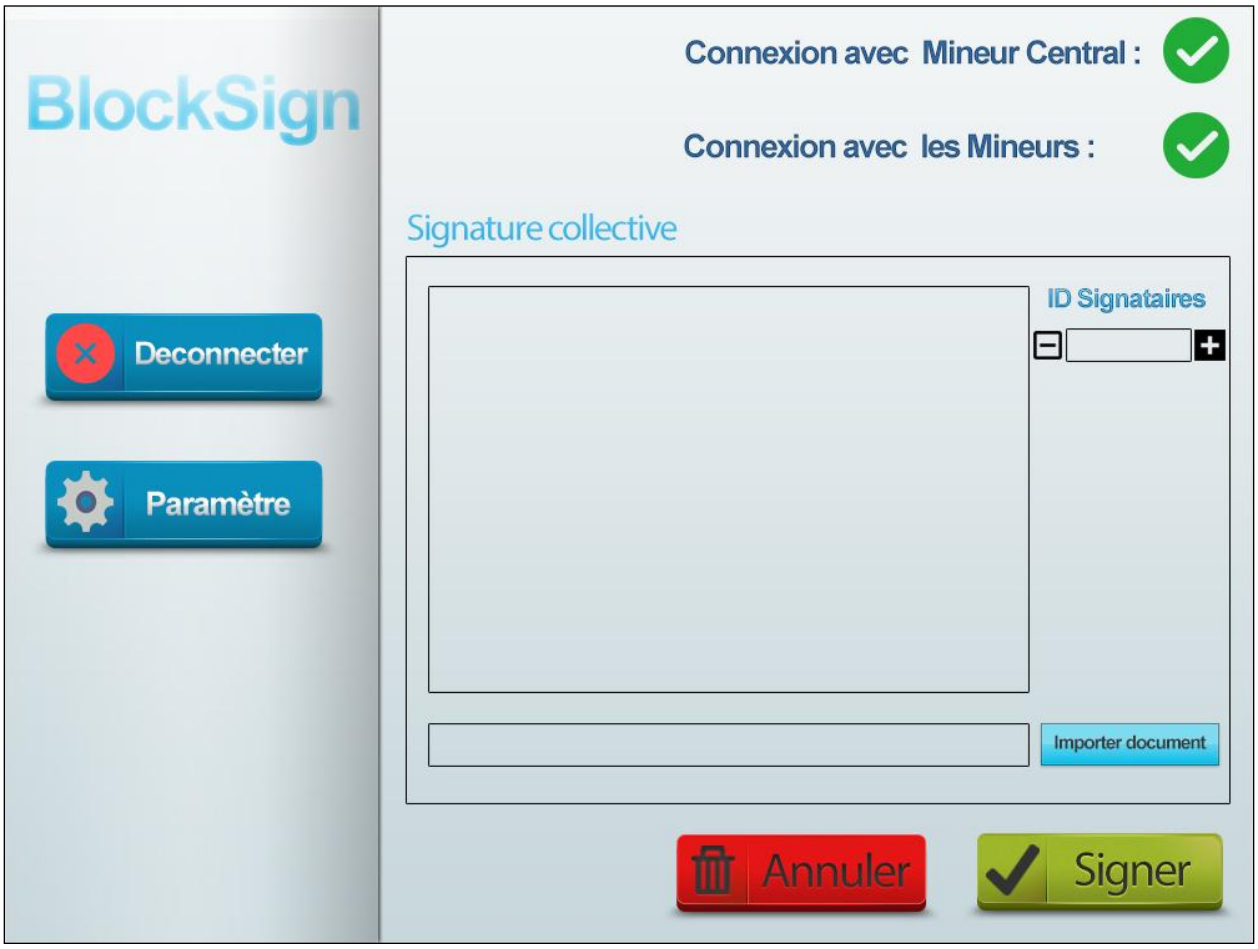


Figure 41 : Interface de la signature collective.

V.5.5.5 Interface de l'invitation :

L'interface d'invitation contient des informations sur le client expéditeur, et trois boutons, le premier pour afficher le document a signé, et les deux autres boutons l'un pour accepter l'invitation et continue l'opération, et l'autre pour refuser l'opération et arrêter la transaction de la signature définitivement.

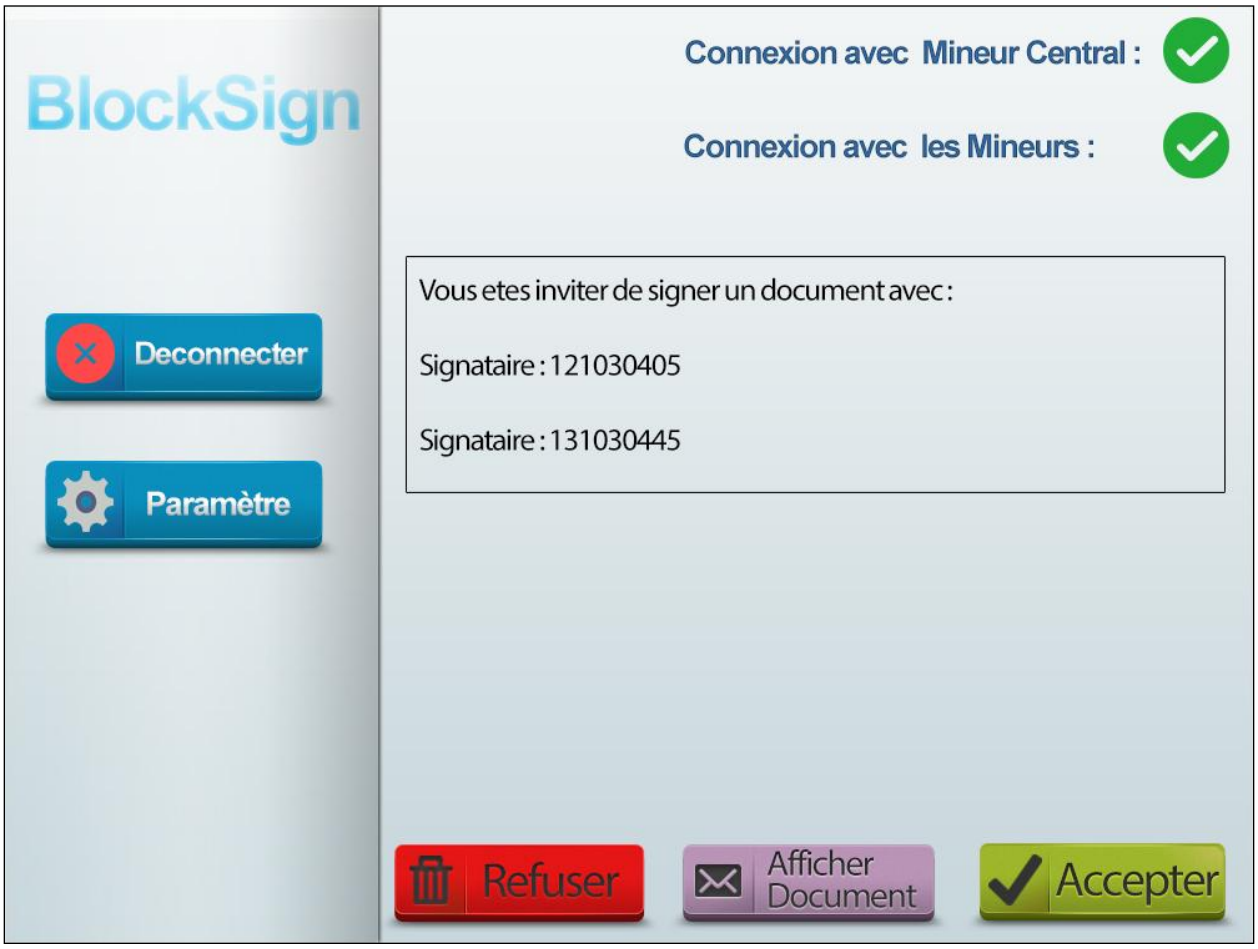


Figure 42: Interface de l'invitation**.**

V.6 Conclusion :

Dans ce chapitre, notre projet d'études atteint sa fin. Tout au long de ce chapitre, nous avons abordé notre environnement de travail. Par la suite, nous avons expliqué notre architecture d'applications afin de présenter finalement les différentes principales parties d'implémentations de notre application réalisées.

CONCLUSION GENERALE

CONCLUSION GENERALE

Ce rapport de projet de fin d'études avait le but de créer un système confiant pour la validation des signatures numériques des documents en se basant sur la technologie blockchain, ou le but nécessaire était de sécuriser au maximum les transactions effectuées ainsi que protéger les identités dans un système distribué et garantir l'intégrité des données.

Nous avons vu qu'est-ce qu'une technologie blockchain et que son utilisation n'est pas destinée juste pour la monnaie électronique et comment en peut l'appliquer sur notre système de validation des signatures.

Il est utile de comprendre le mécanisme du travail de la monnaie électronique, car c'est le premier à exploiter la technologie de la blockchain, et la première monnaie électronique c'est le Bitcoin.

Cette monnaie a grandement contribué au développement de cette technologie, mais tous les systèmes n'ont pas besoin des mécanismes de Bitcoin tels que la preuve de travail, la base de chaîne la plus longue et plusieurs autres mécanismes.

Chacune système peut déterminer ses fonctionnalités et ses mécanismes purs , tout en respectant les principes fondamentaux de la technologie Blockchain, la caractéristique principale la plus importante est le consensus dans la prise de décision, car le manque de confiance des participants entre eux dans le système génère une forte protection, Chaque processus est mené avec la participation de tous les éléments du système dont ses tâches est limitée à la validation des informations pour donner une réponse, tout en assurant les réponses de la majorité des éléments du système pour prendre une décision.

Il existe des avantages et des inconvénients pour chaque solution, et on doit les considérer individuellement pour chaque cas d'utilisation.

La technologie blockchain pourrait fournir un moyen de suivre l'historique unique de chaque périphérique, en enregistrant un registre des échanges de données entre celui-ci et d'autres périphériques, services Web et utilisateurs humains.

Dans des domaines aussi distincts que le système de validation des signatures électroniques. Cette évolution permettra également un contrôle plus aisé des opérations, menant à une très forte protection dans le système de signatures électroniques.

Finalement, même si notre solution n’est encore parfaite, mais l’adoption de technologies telles que Blockchain pour accroître la transparence des signatures électronique rendra l'ensemble du processus plus fiable. De plus, cela réduira les taches fastidieuses, manuelles et répétitives des clients, des autorités et de tous les autres intervenants à condition que les clés cryptographiques utilisées soient sous le contrôle de l’utilisateur.

[1] : Raymond,M (2011, Janvier 05). Introduction à la Cryptographie. Récupéré de: https://cours.toucharger.com/fiches/cours/introduction-a-la-cryptographie/1095.htm

[2] : INTRODUCTION. Récupéré de :http://www.cryptage.org/introduction.html

[3] : Introduction à la cryptographie. Récupéré de: https://web.maths.unsw.edu.au/~lafaye/CCM/crypto/crypto.htm

[4] : **SIDI AISSA Ikram** et **KEDDAR Souria** (2018, Juin 28). Proposition d'un système à base de blockchain pour la gestion des opérations sur les véhicules au niveau national. université de tlemcen.

[5] : LÉO G.(2014, Decembre 1). Chiffrement symétrique. Récupéré de: https://blog.devensys.com/chiffrement-symetrique/

[6]: cryptographie asymétrique.(2013, février 27). Récupéré de: https://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/terminologie_sec_informatique/cryptographie_asymetrique.html

[7] : LA CRYPTOGRAPHIE A CLE PUBLIQUE. Récupéré de: http://www.cryptage.org/cle-publique.html

[8] : La Cryptographie & Le RSA (Vincent S. – 9VSB 3) p09 < 'http://es-beausobre.ch/tp/concours_05/crypto.pdf' >

[9] : SoGoodToBe.(2001, Novembre 04). L'AES : Advanced Encryption Standard. Récupéré de: https://www.securiteinfo.com/cryptographie/aes.shtml

[10] : AES (Advanced Encryption Standard). (2016, juillet). Récupéré de: https://whatis.techtarget.com/fr/definition/AES-Advanced-Encryption-Standard

[11] : Cryptographie (2015, Mars 23) . Récupéré de: http://ista02.blogspot.com/2015/03/cryptographie.html

[12] : BOUCHAMA M.(2012, octobre 28). Exploitation des transformées paramétriques dans le cryptage des image fixes., Thèse magister communication, Université Ferhat Abbas de Sétif.

[13] : Attaque de l'homme du milieu .(2019, Janvier 20) Récupéré de: https://fr.wikipedia.org/wiki/Attaque_de_l%27homme_du_milieu

[14] : Code civil algérien (2007)

[15] : La signature et à la certification électroniques.(2015, Février 1). Récupéré de: https://www.algerianbanks.com/index.php/environnement-juridique/principaux-codes-juridiques/la-signature-et-a-la-certification-electroniques

[16] : **Kamal K. Block Chain Technology- An Insight into Future Global Business** (2016, aout 30). Récupéré de: http://cfdmaster.com/block-chain-technology-insight-future-global-business-20160830/

[17] : Libérer le potentiel révolutionnaire de la technologie des chaines de blocs pour le développement humain. Raúl Zambrano (Aout 2017). Page 22

[18] : Libérer le potentiel révolutionnaire de la technologie des chaines de blocs pour le développement humain. Raúl Zambrano (Aout 2017). Page 23-24

[19] : Blockchain la révolution de l'économie de partage. (Édition 2017 Open Source Solutions).

[20] : Blockchain : évolution ou révolution pour les contrats en France ? (Pierre-Marie Lore) Page 30.

[21] : Principes clés d'une application blockchain (GODEBARGE Ferréol - ROSSAT Romain EM Lyon Business School -15/12/2016).

[22] : Fraude à double dépense - La prévention Récupéré de: https://www.ethereum-france.com/

[23] : blockchain une opportunité pour les consommateurs d'énergie (version anglais).

[24] : Blockchains et smart contracts : des technologies de la confiance ? (une série des annales des mines , Publié l'Août 2017 dans ''RÉALITÉS INDUSTRIELLESS ''série trimestrielle '')

[25] : Définition de la semaine : la crypto monnaie.(2017, Septembre 12) .Récupéré de: https://www.btobmarketers.fr/lexique/definition-de-semaine-crypto-monnaie/

[26] : Raúl Zambrano < Libérer le potentiel révolutionnaire de la technologie des chaines de blocs pour le développement humain>

[27] : Charlie P. (2019, Juin 19). Bitcoin : définition, évolution du cours, comment en acheter Récupéré de: https://www.journaldunet.fr/patrimoine/guide-des-finances-personnelles/1210185-bitcoin-definition-evolution-du-cours-comment-en-acheter-juin-2019/

[28] : Guy Bégin. (2016, Novembre 30) **B n B: Bitcoin et Blockchain.**

[29] **Comment fonctionne une transaction en bitcoin ?.** Récupéré de: https://pouruneautreeconomie.fr/comment-fonctionne-transaction-bitcoin/:

[30]: Jean-Luc (2018, Septembre 20). Générer des bitcoins. Récupéré de: https://bitcoin.fr/minage/

[31]: ROMAIN B. (2018, Février 1) Comment miner des Bitcoins : matériel, techniques et rendement. Récupéré de: https://www.papergeek.fr/comment-miner-des-bitcoins-materiel-techniques-et-rendement-12014

[32] : Blockchain Applications in *Internet of Things (IoT)*. Récupéré de: https://www.blockchaintechnologies.com/applications/internet-of-things-iot/

[33] : FREDERIC K. (2018, Avril 20) . Commentary: How Blockchain Could Put an End to Identity Theft. Récupéré de: http://fortune.com/2018/04/20/blockchain-technology-identity-theft-data-privacy-protection/

[34] : Raúl Z. Libérer le potentiel révolutionnaire de la technologie des chaines de blocs pour le développement humain.

[35] Spécification (norme technique) . Récupéré de: https://fr.wikipedia.org/wiki/Sp%C3%A9cification_(norme_technique)

[36] Modélisation UML : Le diagramme de classes.(2019, Mai 12) Récupéré de : https://fr.wikiversity.org/wiki/Mod%C3%A9lisation_UML/Le_diagramme_de_classes

[37] : UML 2 :De l'apprentissage à la pratique. Récupéré de : https://laurent-audibert.developpez.com/Cours-UML/?page=diagramme-activites

[38] : PYTHON LANGAGE. Recupéré de : http://dictionnaire.sensagent.leparisien.fr/PYTHON%20LANGAGE/fr-fr/

[39] : Vangie Bea. SQL - structured query language, Récupéré de : https://www.webopedia.com/TERM/S/SQL.html

[40] : Pycharm, Récupéré de : https://fr.wikipedia.org/wiki/PyCharm

[41] : **François Verrier,** (2019, Février 11). Adobe Photoshop cc. récupéré de : https://www.clubic.com/telecharger-fiche9635-adobe-photoshop-cs6.html

[42] : **SQLite.** Récupéré de: https://sql.sh/sgbd/sqlite.