REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOHAMED BOUDIAF - M'SILA

FACULTE MATHEMATIQUES ET DE L'INFORMATIQUE

DEPARTEMENT D''INFORMATIQUE

N° :……..

DOMAINE : Mathématiques et Informatique

FILIERE : Informatique

OPTION : Réseaux et Technologies de l'Information et de la Communication

Mémoire présenté pour l'obtention

Du diplôme de Master Académique

Par: DOUCENE Walid

Intitulé

Infrastructures à Clés Publiques Basées sur la Technologie Blockchain

Soutenu devant le jury composé de :

GHRIBI Hayet	Université de M'sila	Président
CHIKOUCHE Noureddine	Université de M'sila	Rapporteur
BRAHIMI Belkacem	Université de M'sila	Examinateur

Année universitaire : 2018 /2019

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOHAMED BOUDIAF - M'SILA

FACULTE MATHEMATIQUES ET DE L'INFORMATIQUE

DEPARTEMENT D''INFORMATIQUE

N° :……..

DOMAINE : Mathématiques et Informatique

FILIERE : Informatique

OPTION : Réseaux et Technologies de l'Information et de la Communication

Mémoire présenté pour l'obtention

Du diplôme de Master Académique

Par: DOUCENE Walid

Intitulé

Infrastructures à Clés Publiques Basées sur la Technologie Blockchain

Soutenu devant le jury composé de :

GHRIBI Hayet	Université de M'sila	Président
CHIKOUCHE Noureddine	Université de M'sila	Rapporteur
BRAHIMI Belkacem	Université de M'sila	Examinateur

Année universitaire : 2018 /2019

Remerciement

Je tien à saisir cette occasion et adresser mes profonds remerciements et mes profondes reconnaissances à :

- Mon encadrant de mémoire de fin d'étude Dr CHIKOUCHE Noureddine, pour ses précieux conseils et son orientation ficelée tout au long de ma recherche.

- A mon prof Saoudi Lalia et ma famille et mes amis en particulier : Chaker Tayeb Rachid, Chenen Boubaker, qui par leurs prières et leurs encouragements, on a pu surmonter tous les obstacles.

- Je voudrais remercier aussi toutes les personnes qui ont participé de près ou de loin à mes recherches et à l'élaboration de ce mémoire.

À tous ces intervenants, je présente mes remerciements, mon respect et ma gratitude.

Table des matières

Chapitre 4: Implémentation et etude comparative

Liste des figures

Liste des tables

Introduction Gènèrale

Les communications Internet reposent sur la sécurité de l'infrastructure de clé publique (PKI), qui gère les clés utilisées par les entités pour établir des canaux de communication.

L'infrastructure à clé publique offre un moyen sécurisé de authentifier les identités sur Internet. Il définit les politiques et les procédures nécessaires pour émettre, gérer, valider et distribuer des certificats numériques afin d'utiliser le cryptage à clé publique de manière sécurisée.

La gestion des clés publiques par une infrastructure à clé publique repose généralement sur la norme de certification X.509, qui permet de vérifier la propriété d'une clé privée par une entité externe (autorité de certification). Le certificat X.509 est défini comme une structure de données qui lie les valeurs de clé publique aux sujets (par exemple, les noms de domaine).

La liaison est établie par les autorités de certification (AC) de confiance, signant numériquement chaque certificat.

L'approche conventionnelle de PKI est utilisé par les modèles de Web of-trust (WoT), qui sont des infrastructures à clé publique simple (SPKI). WoT et SPKI comportent des failles de sécurité.

Des événements très médiatisés, tels que le piratage de CA DigiNotar en 2011, ont encouragé les travaux visant à améliorer la sécurité de l'infrastructure à clé publique. Une solution émergente pour construire des infrastructures à clé publiques sécurisées est la blockchain, est une conception pour les grands livres publics distribués introduite en tant qu'enregistrement de transaction sous-jacente à la crypto-monnaie. En théorie, la blockchain répond aux des nombreuses exigences de la PKI et résout certains problèmes de sécurité des approches classiques: dans une PKI décentralisée basée sur la blockchain, les points de défaillance uniques que représentent les CA sont éliminés et un registre des événements de la PKI fiable est publié. La majorité des contributeurs de blockchain sont honnêtes.

La problématique étudiée dans ce mémoire est quelle est la différence entre le PKI conventionnelle et le PKI basée sur la blockchain ? dans quel domaine utilisé chaque catégorie?

Objectifs du travail :

Les objectifs de ce projet de fin d'études sont:

- ✓ Présenter les technologies de la Blockchain et de la PKI.
- ✓ Lier ces deux technologies pour obtenir une vision sur le PKI basé sur la blockchain.
- ✓ Implementer les deux technologies (PKI conventionnelle et le PKI basé sur la blockchain).
- ✓ Faire une étude comparative entre la PKI conventionnelle et la PKI basée sur la blockchain est connaitre les points d'efforts et les points de faiblesse de chaque technologie et les applications utilisèes ces technologies et quel est le meilleur choix et de connaitre la relation entre la blockchain et le PKI et qeul est l'addition de la blockchain pour le PKI .

Structure du mémoire

Notre mémoire est organisé comme suit:

Le chapitre 1 est consacré a la définition du blockchain en général et ses différents taches, et opérations ensuit on parle de ces types et ces modèles et ces éléments nécessaire , enfin on cite les avantages et les inconvénients.

Chapitre 2 : Dans ce chapitre on a présenté le pki en général et ces éléments ensuite on parle sur sa structure et son fonctionnement et comment utiliser les certificats et les champs de certificat et on va spécifier les certificats x.509 .

Le chapitre 3 est réservé a la description de la relation entre la blockchain et le pki avec le fonctionnement de pki base sur la blockchain ,ensuite, je parle de l'utilisation de cette technologie et comment la blockchain améliore le pki .

Chapitre 4 : dans ce chapitre on parle d'environnement matériel et logiciel, on parle aussi sur les fonctions et les méthodes utilisé et en fin on a faire une comparaison entre le PKI conventionnelle et le PKI basé sur la blockchain .

.

CHAPITRE 1

1.Introduction

En 2018 pas une semaine ne s'écoule sans que l'on entende parler de la blockchain dans les medias ou même au bistrot ! Il est vrai que le mot « blockchain » est sur toutes les lèvres mais pourtant peu de personnes comprennent véritablement l'enjeu de cette technologie et comment elle peut être utilisée pour réaliser [1] des transactions financières, faire des ICO (Initial coins offering), transférer des informations de manière fiable, vérifiée et sécurisée.

2. Définition

La Blockchain est fondamentalement une technologie de stockage et de transmission d'informations sécurisées, à l'image d'une base de données distribuée, en y intégrant en plus une protection cryptographique des données et en permettant la conservation de l'historique de tous les échanges effectués entre ses participants. Echange de valeurs, transfert de propriété, ou encore notarisation… ces transactions se réalisent grâce à une chaîne de blocs contenant les données, d'où le terme 'block' - 'chain'. Mais à la différence d'une base de données classique, la Blockchain introduit un nouveau type de gouvernance décentralisée, intégrée et gérée par la technologie, sans intermédiaire qui ne requiert pas la présence d'une tierce autorité de contrôle.

En remettant en cause l'utilité des acteurs de confiance traditionnelle (notaires, banques, chambres de compensation…), elle permet d'envisager une approche totalement nouvelle et disruptive de nos[2] organisations. En résumé, la technologie Blockchain repose sur trois grands principes techniques fondamentaux : Une architecture décentralisée ou architecture pair à pair pour assurer la résilience du système. L'utilisation de cryptographie asymétrique pour garantir la sécurité des informations. La mise en place d'un algorithme, appelé consensus, pour éliminer le risque de fraude et garantir la confiance au sein du système. Ci-dessous dans la figure 1 est présenté la blockchain.

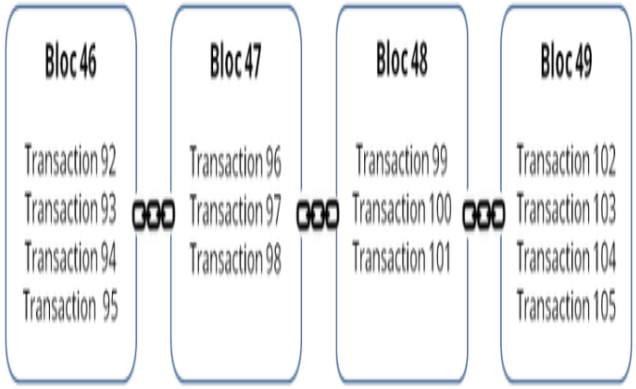

Figure 1.1 Exemple de Blockchain[2]

3. Historique

Bien avant l'invention du bitcoin, le premier système de certification décentralisé utilisait chaque semaine la rubrique « annonces et objets trouvés » du «New York Times » pour fonctionner si vous avez la chance de faire partie des personnes qui savent ce qu'est la blockchain, il est probable que vous vous la représentiez sous la forme d'un énorme fichier informatique contenant des millions de lignes, dupliqué sur des millions d'ordinateurs à travers le monde. Et vous auriez plutôt raison, puisque c'est ainsi que fonctionne la plus célèbre des blockchains, sur laquelle s'appuie la monnaie bitcoin depuis 2009.

Les confrères américains de Motherboardils invitent pourtant à reconsidérer la question, en relayant un tweet du[3] chercheur It tai Abraham qui affirme que le première blockchain remonte en réalité à 1995, et qu'elle est imprimée depuis lors sans discontinuer dans… le New York Times.

4. Les Types de la Blockchain

Il existe deux types fondamentaux de la blockchain dans lequel :

4.1. Blockchain publique: peut donc être assimilée à un grand livre comptable public, anonyme et infalsifiable.

4.2.Blockchains privées: dont l'accès et l'utilisation sont limités à un certain nombre d'acteurs.

Comparons maintenant les avantages et les inconvénients des blockchains privées à

ceux des blockchains publiques. Si la blockchain publique représente une solution de confiance décentralisée pour beaucoup, la complètement centralise entre un petit nombre d'acteurs, prenant le contrepied du rêve libertaire de la blockchain publique. Il est donc important de distinguer ces deux types de blockchain, qui diffèrent énormément sur le plan de la gouvernance. L'une des différences majeures entre blockchain privée et blockchain publique est lié à la confidentialité des smart contracts, des transactions et des données. Comme nous l'avons souligné précédemment, il est relativement facile de garantir la confidentialité des données stockées dans des blockchains privées, puisque seul un nombre limité d'acteurs peuvent y avoir accès, ce qui explique leur développement rapide. Les données stockées dans les blockchains publiques sont ,au contraire, accessibles à tous, puisqu'il s'agit de construire un registre public décentralisé.

Cela dit, il est possible d'obtenir certaines formes de confidentialité dans les blockchains publiques qui utilisent des pseudonymes (c'est le cas pour le réseau bitcoin). Par ailleurs, certaines solutions techniques sont développées sur des blockchains publiques pour protéger les données sensibles. Ainsi, le projet Enigma du MIT (Massachusetts Institute of Technology) propose une blockchain de données de santé dans laquelle un nœud du réseau ne peut accéder à l'ensemble des données en utilisant une infrastructure Secure Multiplatform Computation : ces données sont réparties sur les différents nœuds du réseau et ne peuvent pas[4] être entièrement révélées dans leur intégralité lors d'une requête. D'autres initiatives sont basées sur une technique de zeroknowledge proof qui permet de vérifier la validité des transactions dont les métadonnées sont ,peut-être, cryptées blockchain privées.

	Confidentialité	Rapidité	Confiance
Publique	-	-	-
Privée	+	+	+

Table1.1 Blockchain privée et publique

5.Consensus

Le consensus désigne le mécanisme de gouvernance qui permet à une architecture Blockchain de valider la validité d'une information. La Blockchain étant basée sur une

architecture décentralisée, il n'existe pas de nœud central ayant vocation à servir d'organe de contrôle pour vérifier et valider les informations stockées au sein du réseau. Cette étape de vérification est ,au contraire, distribuée sur l'ensemble des nœuds, l'objectif était de faire émerger une validation globale au [5] sein du réseau. Chacun de ces nœuds vérifie la validité de la nouvelle transaction en calculant divers algorithmes, on dit dans ce cas qu'ils minent la nouvelle transaction, les nœuds en charge du calcul étant les mineurs. Lorsqu'un mineur a validé une transaction, il l'insère dans un bloc et rajoute chronologiquement ce bloc à la liste des blocs existants : la transaction est enregistrée dans la Blockchain. Les blocs sont donc liés aux uns et aux autres de telle sorte que si on souhaite modifier un bloc, on est contraint de modifier toute la chaine.
La figure suivante illustre la structure de consensus.

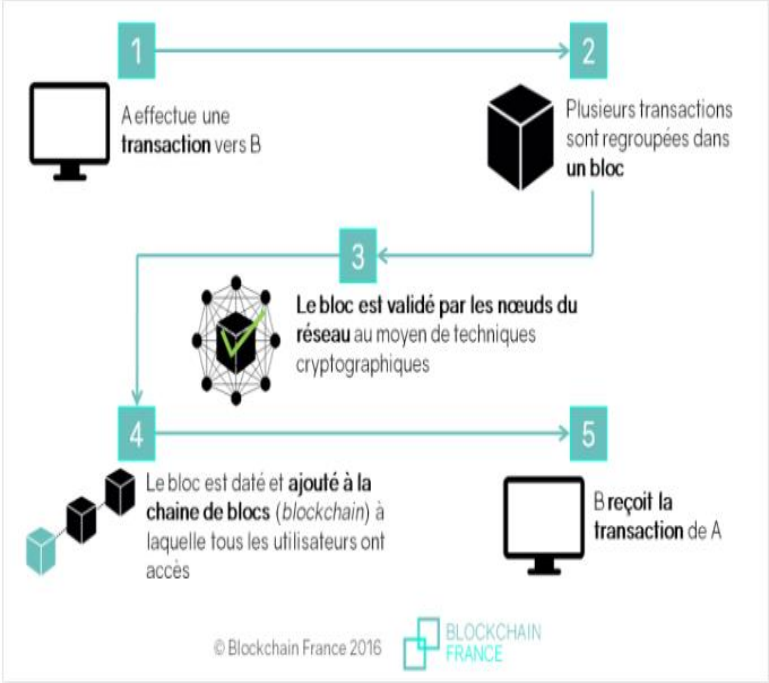

Figure 1.2 Transaction et Consensus **[6]**

6. Les Modèles de la blockchain

Il existe différents modèles de mise en œuvre de la technologie Blockchain. Historiquement

- les premières plates-formes Blockchain étaient accessibles à tout utilisateur sans restriction d'accès. Dans ce modèle public, chaque utilisateur est libre de consulter les informations enregistrées sur le registre et d'en publier de nouvelles qui seront elles-mêmes enregistrées tant que les règles de fonctionnement du réseau sont respectées le

réseau fonctionne de manière totalement décentralisée et autonome grâce au mécanisme de consensus L'implémentation la plus connue de ce modèle est la plate-forme Bitcoin. D'autres modèles existent toutefois. S'ils se basent sur les mêmes principes d'architecture technique (réseau distribué, organisation des informations par bloc), ils diffèrent toutefois du modèle public en restreignant l'accès au réseau et les droits des différents utilisateurs. On parle de modèles permissionnés et on distingue deux sous-types d'architecture au sein de cette catégorie.

- Dans le modèle consortium, l'accès au réseau est public mais une gestion des droits permet de restreindre l'accès et l'ajout d'informations. La gestion de ces droits implique l'existence d'un ou plusieurs utilisateurs ayant un rôle d'administration et de contrôle, c'est pourquoi on parle également de modèle partiellement décentralisé ou de modèle hybride. Dans le modèle privé, les droits d'accès et [6] d'écriture sont centralisés sous la responsabilité d'une seule organisation. Cette organisation contrôle également les règles de fonctionnement du réseau et peut décider de les modifier à tout moment. Les différents mécanismes de confiance introduits par la Blockchain publique (consensus...) ne sont pas ou plus nécessaires car la gestion et le contrôle du réseau sont assurés par l'organisation centrale.

7.Les Applications

7.1.Les smart contracts: ou contrats intelligents représentent un des cas d'usages les plus prometteurs de la Blockchain. Ce sont des programmes informatiques reposants sur la technologie Blockchain[2] et conçus pour exécuter automatiquement les termes d'un contrat dès lors que certaines conditions sont réunies. Ces programmes sont accessibles et audit ables par toutes les parties autorisées, leur exécution est donc contrôlée et vérifiable. Enfin, la Blockchain garantit la fiabilité et l'immuabilité de ces contrats.

7.2.Le stockage cloud ou l'art de partager son disque dur: La blockchain peut être utilisée pour décentraliser le stockage des données dans le cloud. L'idée est de mettre à disposition des autres utilisateurs l'espace de stockage dont vous disposez sur le serveur cloud mais que vous n'utilisez pas. Contre rémunération en crypto-monnaie.

7.3.L'automatisation du paiement des salaires : La blockchain a ses racines dans les crypto-monnaies. Utiliser cette[7] technologie pour gérer la paie des salariés fait donc totalement sens.

8. Les avantages et les inconvénients

Quand on a parlè sur une technologie on a besoin de connaître les avantages et les inconvénients.

8.1.Les Avantages

Parmi les avantages de cette technologie on a cité:

8.1.1.Absence d'intermédiaire

La blockchain pourrait révolutionner le système monétaire car elle ne nécessite plus l'intervention d'une structure bancaire. Avec les monnaies numériques qui utilisent la technologie blockchain, il est possible de faire des transactions directement de particulier à particulier sans intermédiaire. Plus besoin de banquier, d'une administration qui note et stocke[8] toutes les informations concernant vos échanges monétaires. Toutes ces informations seront reprises dans les blocs de la chaîne. La monnaie cryptée est en quelque sorte sa propre administration bancaire.

8.1.2. Economie de plusieurs milliards

Selon un rapport de la Goldman Sachs, la suppression de tous ces intermédiaires pourrait faire gagner chaque année plusieurs milliards de dollars aux institutions bancaires, aux marchés financiers et à de nombreuses industries. Le rapport parle de 2 milliards de dollars pour les États-Unis et de 6 milliards à l'échelle mondiale. Mais de nombreux autres secteurs pourraient également économiser de très importantes sommes monétaires en utilisant cette technologie.

8.1.3.Lutte contre la fraude

Puisque la fraude est souvent une affaire de manipulation de chiffres et de lettres sur des papiers, quoi de mieux qu'une technologie avec laquelle on pourrait stocker toutes sortes d'informations sans les modifier? La blockchain joue ce rôle. Vente de logements sociaux, arnaque au kilomètres sur véhicules d'occasion, sociétés offshores… toutes ces informations pourraient se retrouver de façon chronologique dans un fichier sécurisé et aisément consultable.

8.1.4.Recherche scientifique et médicale

La création de la série des robots Sophia est un bon exemple de l'utilité de la blockchain. La start-up *Singularity NET* a pu développer ces intelligences artificielles articulées à visage humain grâce à un système de blockchain. Aucune information n'a pu se perdre en chemin et les chercheurs ont pu travailler sur le projet depuis plusieurs coins du globe. Cette absence de fragmentation du travail propre à la chaîne de blocs a

également intéressé l'Union européenne qui y voit des applications dans le domaine de la santé, de la gestion des données personnelles ou encore dans le traitement des questions logistiques.

8.2.Les Inconvénients

Parmi les inconvénients de cette technologie

8.2.1.Lourdeur technologie

La transmission d'informations par la chaîne de blocs nécessite un support technologique assez important. De nombreux ordinateurs entrent en compétition pour résoudre une série de calculs qui, une fois résolus, permettent le transfert d'informations cryptées: c'est ce qu'on appelle le mining. L'ordinateur qui résout le problème est « récompensé » en monnaies numériques.

Mais ce procédé peut être lent. Une transaction en Bitcoin peut prendre jusqu'à plusieurs heures là où une simple transaction traditionnelle peut être instantanée (à condition de payer un supplément à la banque). Plus il y aura des demandes de dispositifs basés sur la blockchain, plus grand sera le nombre d'ordinateurs exploité. Ce qui aura pour conséquence de ralentir encore le système. Bien que de nouvelles approches technologiques plus rapides similaires à la Blockchain commencent à être développées, comme le Tangle, ce procédé reste encore très lent.

8.2.2.Inaccessibilité intellectuelle

Si, en théorie, l'utilité et le fonctionnement de la blockchain semble encore accessible au grand public, en pratique, c'est une autre histoire. Les adresses des blocs sont des hash, soit des suites de caractères comprenant des chiffres et des lettres qui, pour la majorité des individus, ne représentent pas une grande chose. Avant de se mettre à utiliser cette technologie complexe, il faut sacrifier pas mal de son temps pour en saisir la réelle utilité. Ceux qui comprennent comment les gérer auront un avantage sur les autres. Ils peuvent – et le font – créer des applications simplifiées permettant de gérer la blockchain. Des applications qu'ils feront payer à ceux qui souhaitent les utiliser.

8.2.3.Aval d'une autorité

Tous les processus administratifs ne peuvent pas être remplacés par une technologie blockchain. Certains nécessitent encore l'aval d'une autorité compétente. Certaines opérations qui seraient réalisées via la blockchain – sans intermédiaire donc – n'auraient ainsi aucune valeur. Le journal suisse Le Temps donne l'exemple des transferts de propriété. « Le contrat de transfert doit revêtir la forme authentique

(notaire) et être vérifié par le conservateur du registre foncier. Une transaction immobilière qui ne passe que par la blockchain n'a pas de valeur ».

8.2.4.Augmentation du chômage

De par sa simplicité et son automatisation, la blockchain pourrait remplacer de nombreux services defonds, de comptabilitéet d'administration et faire disparaître de nombreux métiers. La technologie de la chaîne de blocs pourrait envoyer plein d'employés au chômage: banquiers, comptables, assureurs, notaires et fonctionnaires.

Il y adonc autant d'avantages[9] que d'inconvénients à utilisé la blockchain. Certains pensent qu'elle va révolutionner le monde industriel et économique. D'autres pensent que c'est une perte de temps. L'avenir tranchera.

9.Conclusion

Cette technologie est encore jeune, complexe et reste limitée à certaines communautés ou à certains secteurs. nous avons tout d'abord pu étudier le procédé technique sur lequel repose la Blockchain. Cette innovation informatique permet ainsi d'organiser les échanges de données sur un réseau[10] distribué, assurant une sécurisation des données par chiffrement, et faisant participer les nœuds du réseau pour la création de nouveaux blocs de la chaîne.

CHAPITRE 2

2.1 Introduction

A l'heure actuelle, la sécurité des données informatiques est au centre des préoccupations de tout utilisateur. Pour se protéger des vols de données, il est important de les crypter afin que seuls ceux qui[11] sont autorisés à les manipuler puissent y avoir accès. La méthode de cryptographie la plus répandue est sans doute la cryptographie à clé publique. Et l'ensemble des solutions techniques basé sur cette méthode est appelé infrastructure à clé publique ou PKI (Public Key Infrastructure).

2.2 Définition

PKI (Public Key Infrastructure) est un système de gestion des clefs publiques qui permet de gérer des listes[12] importantes de clefs 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 [13]que lors d'échanges d'information avec l'extérieur.

Une infrastructure PKI fournit donc quatre services principaux:

- Fabrication de bi-clés.
- Certification de clé publique et publication de certificats.
- Révocation des certificats.
- Gestion la fonction de certification.

2.3 Certificat numérique

Un certificat numérique est une sorte de passeport électronique qui permet à une personne, un ordinateur ou une organisation d'échanger de manière sûre des informations sur Internet en s'appuyant sur une infrastructure à clé publique (PKI).A 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 celle 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[14]. 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.

2.4 Les Composants de PKI

L'infrastructure de gestion des clés est basée sur plusieurs composants qui sont indispensables à son fonctionnement. Parmi ces composants, nous répertorions comme principaux, les suivants:

2.4.1 Autorité de certification (CA)

On peut dire que c'est le composant le plus important de l'infrastructure PKI du fait de son rôle central dans les différentes cinématiques d'échanges à l'intérieur d'une PKI. La CA est chargée de délivrer et gérer les certificats. En effet, elle génère des certificats à clés publiques et assure l'intégrité et l'authenticité des informations contenues en les signant avec sa clé privée. Pour émettre des certificats, elle doit recevoir, au préalable, les requêtes de certification contenant la clé publique de l'entité qui le sollicite.

2.4.2 Autorité d'enregistrement (RA)

Elle joue le rôle d'intermédiaire entre l'utilisateur et la CA et dépend de cette dernière. Elle a comme responsabilité de vérifier tout ce qui concerne l'utilisateur, son identité, la concordance entre clés privées/publiques, de certifier et d'assurer qu'il possède les droits nécessaires pour demander des certificats. En résumé, cette autorité a pour tâche de gérer les requêtes de certificat qu'elle reçoit des différentes entités et de concevoir les paires de clés qui leur sont spécifiques.

2.4.3Annuaire électronique LDAP

L'annuaire est un rassemblement structuré des données sur des machines, des ressources, et des personnes.

Dans le domaine de sécurité, l'annuaire électronique peut être vu comme une base de données spécifique permettant de sauvegarder les clés publiques (chiffrement asymétrique) de chaque utilisateur et offrant la possibilité de recherche selon des critères prédéfinis. L'annuaire permet à stocker et diffuser des certificats dans une PKI. Le point faible de l'annuaire électronique se représente dans ce qui suit: un pirate peut corrompre la clé publique enregistrée dans l'annuaire en la remplaçant par sa clé

publique [6]. La plupart des annuaires existants au format LDAP (*Lightweight Directory Access Protocol*).

LDAP est un service d'annuaire dérivé de la norme X.500, il est un mécanisme permettant la[15] mise en œuvre, la publication et la distribution des certificats. L'architecture du PKI avec l'annuaire LDAP se compose quatre entités.
Dans la phase d'enregistrement de clé publique, une entité finale envoie son identité ainsi que sa clé publique à une autorité d'enregistrement (RA).
Si l'identité est validée par l'autorité d'enregistrement, l'autorité de certification (CA) publiera le certificat de l'entité finale, en l'enregistrant dans l'annuaire LDAP.

Le certificat publié peut être récupéré par tout client LDAP correctement authentifié. Si le certificat émis est révoqué pour une raison quelconque, l'autorité de certification est responsable de la révocation du certificat en publiant les listes de révocation des certificats dans l'annuaire LDAP.

Au niveau des annuaires LDAP, les entités finales (clients) peuvent non seulement télécharger des certificats d'autres personnes pour envoyer des messages cryptés ou vérifier des signatures numériques, mais aussi connaître les dernières informations de révocation des certificats en téléchargeant des listes CRL. La Figure 1 illustre l'architecture PKI avec LDAP.

Un annuaire électronique va centraliser des informations et les rendre disponibles, via le réseau, à des applications, des systèmes d'exploitation ou des utilisateurs. Il va généralement s'appuyer sur les éléments suivants :

- Un protocole : échange des données proprement dit et indication des opérations à effectuer sur ces dernières.
- Un modèle fonctionnel : description de la nature des opérations que l'on peut effectuer, comme par exemple une recherche, ou une modification. Un modèle de nommage : identification des données ; organisation des différentes entrées de l'annuaire.
- Un modèle d'information : nature des données pouvant être enregistrées (des chaînes de caractères, des nombres, des numéros de téléphone...).
- Un modèle de sécurité : description des services de sécurité permettant d'assurer par exemple le chiffrement des données transférées ou bien l'authentification du client vis-à-vis du serveur.

- Un modèle de distribution : création et gestion de serveurs secondaires dans un but de sauvegarde ou de répartition de charge, création et gestion de liens spéciaux (*referrals*, méta-annuaires) pointant vers des annuaires responsables d'une partie des données de l'entreprise ou vers des annuaires complètement différents.

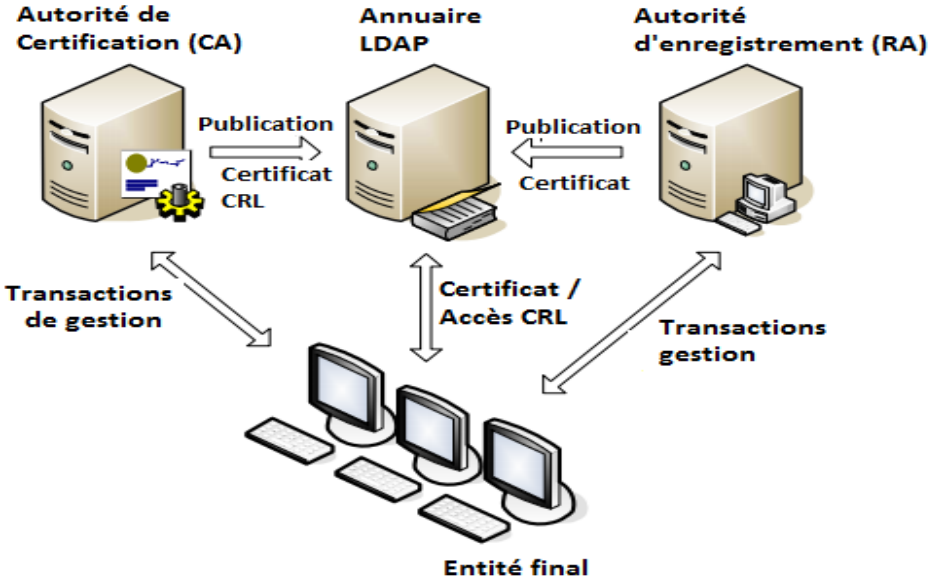

Figure2.1: Architecture PKI avec LDAP[15]

La structure de l'annuaire LDAP est basée sur la représentation hiérarchique des objets nommés. Il est un arbre, où chaque nœud comprend: un identifiant unique (*DN: Distinguished Name*), un ou plusieurs classes (*objectclass*) définissant les attributs possibles, et des attributs, couple nom et sa valeur. Voici quelques exemples sur les attributs les plus utilisés:

- **c**: pays,
- **cn** : Common Name ou nom commun
- **o**: nom d'organisation,

Pour accéder à un certificat, l'utilisateur envoie une requête LDAP (par exemple: "cn=Imad o=UMBM c=DZ") via une application implémentée pour chercher les certificats et consulter les CRL. La structure de l'annuaire permet la faciliter de recherche. Utilisant une méthode efficace et légère, le dépôt de certificat LDAP envoie le certificat correspondant à l'utilisateur.

Concernant l'implémentation de l'annuaire, le logiciel *OpenLDAP* qui a été développé par *The OpenLDAP Project*, il permet la publication des certificats et CRL.

2.4.4 Les certificats

Ils assurent la sécurité d'une clé publique afin d'éviter les failles de sécurité liées à l'usurpation d'identité et à la modification écrite.

2.4.5Les services d'archivage et de publication

L'archivage est un service qui permet le stockage des paires de clés pour une restitution en cas de perte de la clé privée. En effet, il a pour mission de stocker en toute sécurité les clés de chiffrement émis au sein de l'infrastructure. La publication est un service qui répertorie les différents certificats à clés publiques émis par la CA afin de les rendre disponibles aux éventuels futurs utilisateurs, c'est pourquoi on se réfère communément à lui par le terme de dépôt. Ainsi, un annuaire peut être utilisé (LDAP ou X500 par exemple), un serveur Web ou encore un outil de messagerie, etc.

Ce service est contraint par plusieurs exigences telles que, par exemple, le délai de mise à jour des listes de révocation ou la disponibilité de ces listes. Le dépôt est également responsable de la publication de la CRL (Liste de Révocation de Certificat).

2.4.6 Les utilisateurs

Ce sont les personnes ou entités organisationnelles ayant émis ou émettant des demandes de certificat, ou souhaitant simplement vérifier la validité et les informations sur l'identité d'un certificat préalablement reçu.

2.5Organisation d'une PKI

Ci-dessous dans la figure 2 est présenté l' Organisation d'une PKI

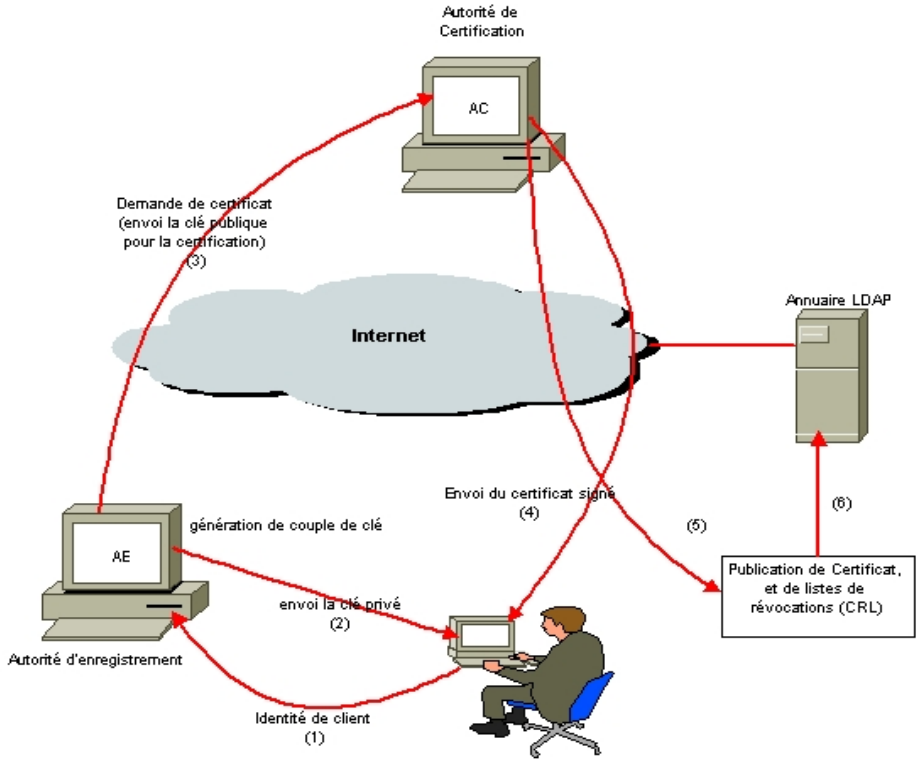

Figure 2.2 L'Organisation d'une PKI[16]

Les étapes

- le client envoie une demande a AE contient ces informations.
- AE renvoie la clé privée pour le client .
- AE envoie la clé publique a AC pour le certification de client.
- AC envoie deux certificats signée la première pour le client et la deuxième a LDAP pour la publication .

2.6 Fonctionnement de PKI.

Alice veut certifier que sa clé publique lui appartient.

Alice envoie sa clé à un CA, ainsi que différentes informations la concernant (nom, email, etc...).

Cet organisme vérifietouts les informations de Alice, et ajoute son nom, une date limitée de validité, et surtout une signature numériqueau certificat.

Cette signature est réalisée grâce à sa clé privée et à un algorithme de hachage (ex.RSA et le SHA).

- L'CA fournit un certificat tel que: $\mathbf{C_A = E_{KRauth}\,[T,ID_A\,,KUa\,]}$

On va expliquer les éléments de certification de clé:

- E_{KRauth} : signature apposée au certificat,
- T : timestamp,
- ID_A : l'ensemble des informations propres à l'entité A
- Kua: la clé publique de A.
- Lorsque Bob veut envoyer un message à Alice, il applique la clé publique de l'autorité de certification (CA).
- Cette action permet de vérifier que le certificat est bien authentique: $D_{KUauth}[C_A]$ =
- $[T,ID_A\,,KUa\,]$[15]

2.7 Norme X.509

X.509 est une norme de cryptographie de l'Union internationale des télécommunications[17] pour les infrastructures à clés publiques (PKI).

2.7.1 Génération de certificat X.509

Un certificat est généré après qu'une demande de certification a été initiée par une entité de l'infrastructure à clé publique .La demande est suivie d'un enregistrement, sous la responsabilité de l'AR, qui recueille et vérifie l'identité du propriétaire du certificat et toutes les autres informations utiles à la délivrance d'un certificat.

Le RA transmet ensuite ces informations à l'autorité de certification qui doit émettre un certificat. Avec les informations d'enregistrement et la clé publique du propriétaire du certificat, l'autorité de certification[18][19] peut émettre le certificat. Pour ce faire, vous devez signer numériquement le certificat à l'aide de la clé de signature privée de l'AC. Après que le certificat a été délivré et vérifié comme étant correct par le propriétaire du certificat, il peut être distribué et utilisé par d'autres entités**.**

2.7.2 Validation de certificat X.509

Lors de la vérification d'une signature numérique, non seulement la validité de la signature est importante, mais également celle du certificat correspondant et de toute sa chaîne des certificats**.**

Les étapes permettant de vérifier une signature numérique (lors de la signature des documents ou lors de l'authentification) peuvent être résumées comme suit:

1. Vérifiez la signature avec la clé publique dans le certificat.
2. Vérifiez la signature de l'émetteur du certificat.
3. Vérifiez la date de validité du certificat.
4. Vérifiez que le certificat n'a pas été révoqué.
5. Vérifier la validité des certificats d'émission dans la chaîne des certificats (vérifier la signature de [20] l'émetteur, la validité de la date et le statut de révocation).
6. Vérifiez que l'autorité de certification racine ou une autorité de certification intermédiaire est approuvée.

2.7.3 Révocation de certificat X.509

La révocation de certificat, l'invalidation de clés publiques, peut être effectuée de différentes manières. La distribution de listes de révocation de certificats (CRL) et l'offre d'un service en ligne avec le protocole OCSP (Online Certificat Statu Protocol) sont deux méthodes couramment utilisées.

Une liste de révocation de certificats est une liste d'identifiants de tous les certificats émis par une autorité de certification qui ont été révoqués . Pour prouver l'authenticité de la liste de révocation des certificats, celle-ci est numériquement similaire aux certificats X.509. Les listes de révocation des certificats peuvent être directement signées par l'autorité de certification qui a délivré les certificats révoqués ou indirectement par un émetteur nommé.

La liste de révocation de certificats doit être mise à la disposition de toutes les entités effectuant l'authentification et mise à jour périodiquement pour garantir qu'aucune entité ne fait confiance à un certificat révoqué.

Un vérificateur va télécharger la liste de révocation des certificats, vérifier la signature, puis vérifier si un certificat spécifique est présent dans la liste de révocation des certificats. Un inconvénient des listes de révocation des certificats est qu'elles augmentent de taille et peuvent devenir assez volumineuses si les certificats expirés ne sont pas supprimés.

Une solution à ce problème consiste à utiliser des listes CRL delta, contenant uniquement les identifiants des certificats révoqués depuis l'émission d'une certaine liste CRL complète, la liste CRL de base. Les listes CRL delta doivent être signées avec la même clé de signature que celle utilisée pour signer la liste CRL de base. En émettant des listes de révocation de certificats delta, il est possible d'émettre de plus

petites mises à jour vers les listes de révocation de certificats avec une fréquence plus élevée.

Une autorité de certification utilisant OCSP disposera d'un service en ligne que les entités peuvent interroger pour connaître l'état de révocation d'un certificat spécifique.

Toutes les réponses OCSP doivent être signées numériquement. Un des avantages de l'utilisation d'OCSP est qu'un vérificateur doit seulement extraire des informations sur le certificat [21][22] spécifique à vérifier (contrairement aux listes de révocation de certificats qui récupèrent des informations sur tous les certificats révoqués). De plus, les informations sur un certificat révoqué peuvent être récupérées presque immédiatement après sa révocation, au lieu de devoir attendez qu'une nouvelle liste de révocation de certificats soit publiée.

2.8 Structure d'un Certificat numérique selon la norme X509

La Figure 3 illustre Les champs exacts des certificats.

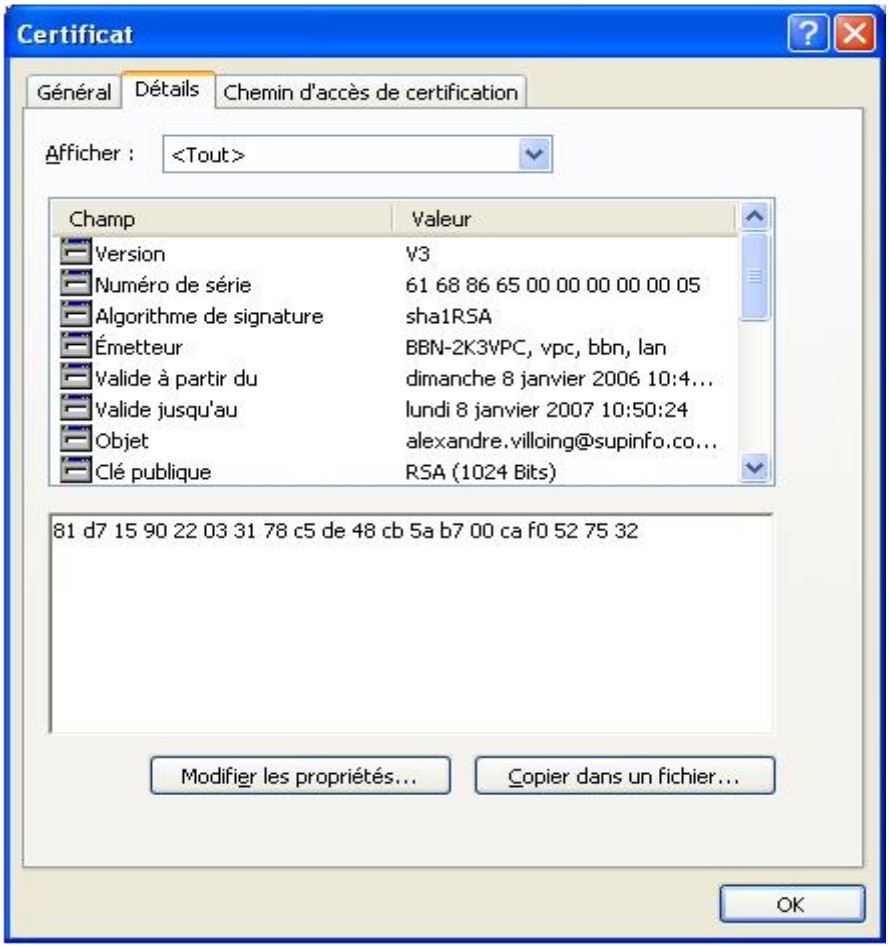

Figure 2.3 LaStructure d'un Certificat numérique selon la norme X509 [23]

Certificat format version

Ce champ donne la version du certificat : 1, 2 ou 3. Dans la pratique, il n'a en général pas d'implications pour l'interprétation.

Certificate serial number

Numéro de série unique, dans le domaine de confiance auquel appartient le certificat, qui l'identifie de façon unique.

C'est ce numéro de série qui sera posté dans la liste de révocation en cas de révocation.

Signature algorithmidentifier for CA

Désigne le procédé utilisé par l'AC pour signer le certificat : (norme ISO). Il s'agit d'un algorithme asymétrique et d'une fonction de condensation.

Un exemple est : RSA with SHA-1.

Cette information étant répétée dans le champ CA signature (le dernier), il n'est pas forcément d'une grande utilité.

Issuer X.500 name

Spécifie le DN (Distinguished Name) dans la norme X.500 de l'AC qui a généré le certificat.

Un exemple est : c=FR, o=Boite

Validityperiod

Donne les dates de début et de fin de la validité du certificat.

Un logiciel client utilisant les certificats doit impérativement vérifier ces dates avant l'utilisation, et rejeter le certificat s'il est expiré. Cela ne suffit cependant pas, car cela dépend de l'horloge de la machine cliente. On peut avoir recours à la consultation des CRL (ou LCR, Liste de Certificats Révoqués), où peut être mise l'information concernant l'expiration.

Subject X.500 name

Spécifie le DN dans la norme X.500 (... un reste -judicieux- des télécoms) de l'utilisateur possédant la partie privée de la clé publique contenue dans le certificat.

Un exemple est : c=FR, o=Jussieu, cn=Marie Curie

Subject public key information

C'est le cœur du certificat. Ce champ contient la valeur de la clé publique du détenteur du certificat et les algorithmes avec lesquels elle doit être utilisée RSA with MD5 par exemple [24]

2.9 Cycle de vie d'un certificat

Ci-dessous dans la figure 4 est présentée la Cycle de vie d'un certificat

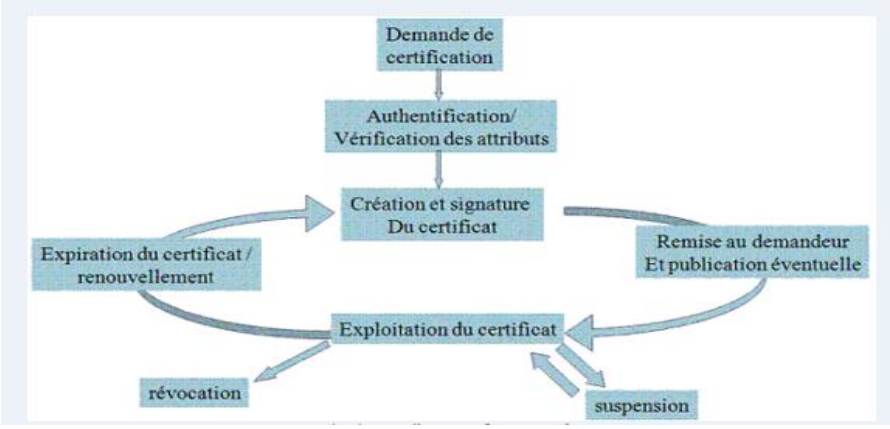

Figure 2.4 Cycle de vie d'un certificat[25]

2.10 Conclusion

Nous avons vu qu'une infrastructure de la gestion des clés publiques se construit, c'est donc une structure à la fois technique et administrative. Comme les PKI intègrent la cryptographie à clé publique et certificat numérique, elles peuvent se confier à des tierces parties de confiance et échanger des données en toute sécurité.
Il existe plusieurs solutions ou produits qui implémentent une PKI et qui offrent la possibilité de sécuriser les données. Le chapitre suivant sera consacré à la mise en place de l'un de ces produits.

CHAPITRE 3

1.Introduction

L'approche classique PKI est de nature centralisée et elle est mise en œuvre par le biais du modèle d'autorités de certification (AC) et du Web de confiance. Les autorités de certification sont des entités de confiance qui émettent un certificat signé (X.509) aux utilisateurs, Cette approche comporte des failles de sécurité[26].

Une solution efficace pour construire des infrastructures à clé publiques sécurisées est la blockchain, la blockchain répond à des nombreuses exigences de la PKI et résout certains problèmes de sécurité[27] **.**

Les solutions PKI proposées basées sur une chaîne de blocs fournissent des nouvelles propriétés de sécurité.

2. Pki Base sur la Blockchain

Blockchain est un grand livre permanent distribué au public dans lequel les événements de transaction sont postés et vérifiés par des pairs du même réseau avant d'être confirmés dans un système incité dans lequel les membres doivent se faire concurrence pour mener à bien un défi cryptographique de type preuve de travail. Les transactions Bitcoin sont extraites et construites sous forme de blocs sur la chaîne de blocs existante dans l'arborescence Merkle[28].

La nature décentralisée de la blockchain a déjà été explorée afin de concevoir une infrastructure à clé publique capable de fonctionner en configuration peer to peer.

Certcoin conçu sur Namecoin est une PKI décentralisée qui exécute presque toutes les fonctionnalités[29] d'une PKI conventionnelle.

Certcoin est immunisé contre les défaillances en un seul point et maintient la conservation de l'identité, ce qui empêche la réplication des certificats de clé publique pour mêmes utilisateurs. Il évite également la génération de certificats non autorisés en raison de la transparence de ses opérations.

Cependant, Certcoin n'a pas pu protéger la confidentialité des utilisateurs impliqués dans les transactions PKI. Certcoin a un rôle limité pour répondre aux besoins des DApps liés à la PKI par rapport à notre modèle. La Figure 3.1 illustre la structure de PKI base sur la blockchain.

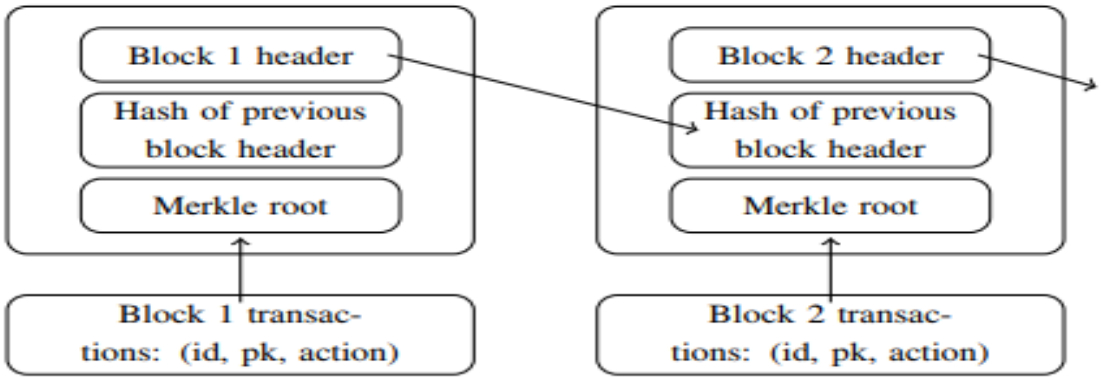

Figure 3.3 BlockchainPKI structure[30]

3. Racine de Merkle

Chaque transaction est associée à un hachage. Dans un bloc, tous les hachages de transaction du bloc sont eux-mêmes hachés (parfois plusieurs fois - le processus exact est complexe) et le résultat est la racine de Merkle. En d'autres termes, la racine de Merkle est le hachage de tous les hachages de toutes les transactions du bloc. La racine Merkle est incluse dans l'en-tête du bloc[31]. La Figure 2 illustre la racine de merkle.

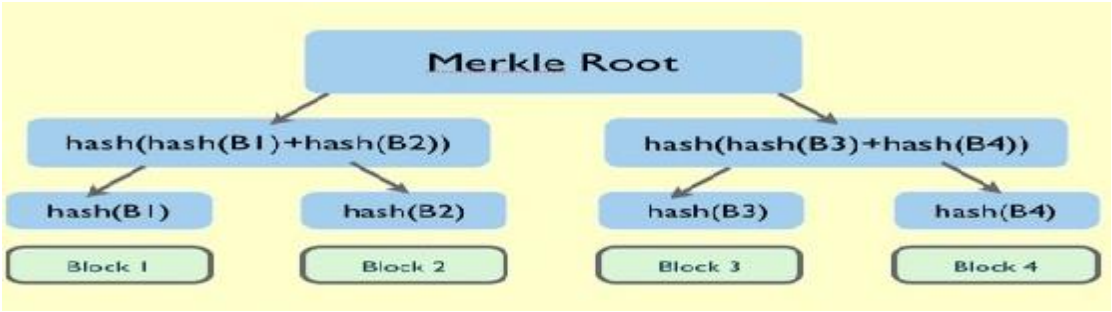

Figure 3.2 La racine de Merkle[32]

4.Le rôle de PKI sur la Blockchain

L'architecture de base d'une infrastructure à clé publique blockchain est la suivante. La blockchain a pour fonction, comme dans la confirmation des transactions Bitcoin, d'enregistrer la liaison d'une clé publique à une identité et de confirmer ce lien pour des actions ultérieures. Les fonctions PKI - enregistrement, mise à jour, révocation - sont exécutées en publiant l'identité et la clé publique avec une action requise dans la blockchain.

ils évaluent l'approche fondée sur la chaine des blocs pour construire une infrastructure à clé publique et en montrent les avantages, avant de poursuivre avec notre proposition concernant la protection de la vie privée. En comparant l'approche de la PKI basée sur

la blockchain avec les approches basées sur la AC et le WoT, nous[33] identifions les avantages de la PKI à la blockchain qui devraient être conservés. La Blockchain est bien adaptée à la PKI et fournit les propriétés souhaitables: transparence et révocation du certificat, suppression des points de défaillance centraux et enregistrement fiable des transactions. Nous commençons par comparer une infrastructure à clé publique basée sur une autorité de certification à une infrastructure à clé en bloc; en particulier, nous décrivons en détail les problèmes posés par une infrastructure à clé publique basée sur une autorité de certification et montrons que l'utilisation de la blockchain peut naturellement atténuer certains de ces problèmes .

L'infrastructure à clé publique basée sur une autorité de certification contient de nombreux points d'échec uniques. Le modèle de confiance centralisé d'une infrastructure à clé publique basée sur une autorité de certification signifie que la sécurité du système repose sur des points uniques: les autorités de certification elles-mêmes. De plus, la structure de la chaîne de certificats signifie que si une seule autorité de certification de la chaîne est malveillante ou subvertie, ce qui peut compromettre la sécurité de l'ensemble de la chaîne.

La création d'une infrastructure à clé publique sur la chaîne de blocs supprime les points de défaillance potentiels représentés par chaque autorité de certification.

Dans une infrastructure à clé publique basée sur une autorité de certification, la révocation est généralement gérée par le biais de listes de révocation de certificats (CRL) - listes de certificats révoqués. Il est bien établi que le traitement de la révocation de tels les processus peuvent être coûteux en termes de temps. La révocation d'une infrastructure à clé publique basée sur une chaîne de blocs peut être résolue efficacement à l'aide de tables de hachage distribuées.

Le projet de transparence des certificats de Google [34] cherche à faciliter la détection des autorités de certification et des certificats non autorisés. La transparence du certificat (CT) est donnée par l'enregistrement public des informations de certificat numérique où les utilisateurs peuvent consulter le journal et donc[34] vérifier les certificats numériques qu'ils utilisent - c'est de la transparence. L'utilisation de la blockchain pour l'infrastructure à clé publique donne une disposition naturelle de la propriété de transparence que Google cherche à atteindre dans ce projet: la blockchain fonctionne comme un journal public.) - tout en éliminant simultanément le besoin d'AC de confiance présentes dans CT.

Dans une infrastructure à clé publique basée sur WoT, les membres du réseau sont «approuvés» si leur «fiabilité» est attestée par un autre membre du réseau «approuvé». Afin de construire ces relations de «confiance», un nouveau réseau les membres doivent en quelque sorte gagner la confiance de certains membres du réseau, car c'est sur cette confiance que leur «fiabilité» peut être attestée par d'autres.

Ce besoin d'établir la confiance signifie qu'il existe une barrière élevée à l'entrée pour un nouveau membre dans un réseau de confiance; en particulier, la quantité de travail requise pour obtenir un site Web permettant de prouver la «fiabilité» à une large proportion utile du réseau est élevée.

L'infrastructure PKI basée sur une Blockchain n'a pas besoin de créer un réseau Web de membres «faisant confiance» pour chaque entité, de sorte que ce travail nécessaire avant d'être exécuté en tant que membre du réseau est supprimé.

Nous concluons que la décentralisation de pki donne des propriétés de sécurité souhaitables qui ne sont pas atteintes par les approches classiques de pki.

5.Méthodologie de conception

La conception de (PKI basée sur la chaîne de blocs) repose sur des Certificats X.509, comme illustré à la figure 3. Un certificat contient certaines informations sur l'environnement PKI dans les champs d'extension.

La valeur des champs d'extension est la suivante:

5.1. Identificateur le clé de sujet

Il contient l'identité du propriétaire du certificat.

5.2. Nom de la blockchain

Il contient le nom de la blockchain Plate-forme. Actuellement, nous utilisons la blockchain publique Ethereum mais nous envisageons de couvrir plus de plates-formes.

5.3Identifiant de clé de l'AC

Il contient l'adresse du contrat intelligent de l'autorité de certification actuelle, s'il s'agit d'un certificat d'autorité de certification. Pour les non-CA certificats ce champ est vide.

5.4 Identificateur de l'autorité de certification de l'émetteur

Il contient l'adresse du contrat intelligent de l'autorité de certification qui a délivré ce certificat. Il permet au validateur de rechercher le contrat intelligent de l'autorité de certification parent dans la blockchain et de vérifier si le certificat avec le hachage

correspondant a été publié et n'a pas été révoqué. Pour les certificats racine ceci le champ est vide.

5.5 Algorithme de hachage:il contient des informations sur le hachage algorithme utilisé dans le calcul de la valeur du certificat hachage chargé dans la blockchain.

La Figure 3 illustre les deux modèles de certificat hybird et standard.

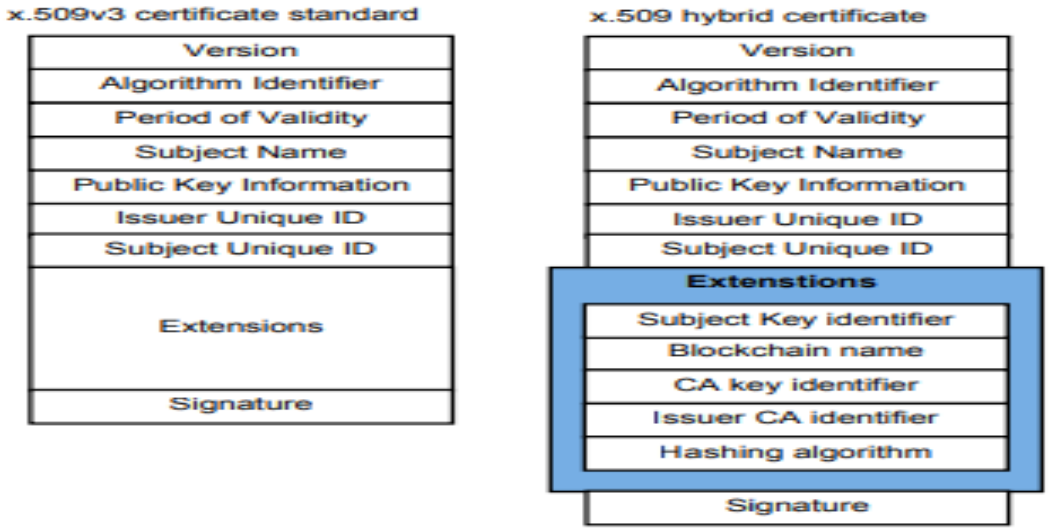

Figure 3.3 Standard vs Hybird[35]

6.Amélioration de la Blockchain dans la PKI

6.1Stockage de certificats de serveur

La première des trois manières dont blockchain peut améliorer la PKI consiste à stockerles certificats de serveur dans la blockchain.

Cela empêcherait une attaque de type homme du milieu par laquelle un pirate informatique fournit un faux certificat de serveur et incite le client à penser qu'il communique en toute sécurité avec le serveur.

Les attaques de[36] type «homme au milieu» risquent d'exposer des informationpersonnellement identifiables à des pirates.

6.2. Vèrification de révocation distribuée

La deuxième des trois manières dont blockchain peut améliorer la PKI est la vérification de la révocation.

La vérification de révocation est le processus d'un client ou d'un serveur vérifiant la validité d'un certificat.

La vérification de révocation est effectuée via CRL ou OCSP à un emplacement central.

Cela crée un point de blocage du réseau et un point de défaillance unique. De plus, étant donné que le certificat est envoyé au début de la négociation TLS, avant que tout cryptage ne soit défini, les informations qu'il contient sont envoyées en clair.

Si un pirate informatique est capable d'intercepter le certificat et de voir l'adresse de l'autorité de certification, il peut alors lancer une attaque par déni de service sur le répondeur OCSP et arrêter le réseau.

La vérification de la[36] révocation peut être plus rapide et plus sûre si elle est distribuée globalement dans une blockchain et à proximité du client ou duserveur qui effectue la vérification de la révocation.

6.3. Validation de chemin de certificat

La troisième des trois façons dont blockchain peut améliorer l'infrastructure à clé publique est la validation du chemin de certificat et les magasins de certificats de confiance.

Les autorités de certification racine, intermédiaires et pont chaîne de confiance. Cependant, ce n'est pas parce que quelque chose s'appelle une autorité de certification que c'est une autorité de certification.

Les fabricants de matériel et de logiciels ont beaucoup de flexibilité dans la sélection des certificats de AC qu'ils préinstallent.

Par exemple, en 2015, Lenovo aurait préinstallé une autorité de certification auto-signée afin d'intercepter les communications et les annonces d'entrée dans les sites Web (c'est-à-dire, l'homme au milieu).

S'il existait[36] une liste de certificats d'AC approuvés et non approuvés dans une blockchain publique, distribuée et inviolable, elle fournirait validation du chemin de certificat plus sécurisée.

7. Applications décentralisée

Ils fournissent un ensemble de cas d'utilisation dans lesquels les PKI sont utilisées, mais dans lequel la liaison de clés publiques avec des identités est indésirable. De telles situations se présentent particulièrement où il est nécessaire que les actions des entités ne puissent être suivis par leur utilisation de clés publiques.

7.1. Informatique omniprésente et IoT. Un utilisateur Des interactions avec un système informatique peuvent se produire via plusieurs périphériques tels que desordinateurs portables et des ordinateurs portables. les smartphones et les

périphériques IoT tels que les dispositifs portables. Les actions [37]et l'emplacement d'un utilisateur peuvent être tracés si liés sur plusieurs appareils. La confidentialité est requise l'identité et la clé publique de l'utilisateur ne peuvent pas être lié entre les appareils.

7.2. Réseaux de véhicules. Une PKI est requise pour sécuriser communications entre véhicules, mais son utilisation doit ne permet pas le suivi à distance des actions d'un véhicule.

L'identité correspondant à une clé publique doit être ne pas être divulgués publiquement, ou des clés liées lors de la mise à jour.

7.3. Forums et réseaux anonymes. Les réseaux nécessitant l'anonymat des utilisateurs ont besoin d'une PKI quels utilisateurs peuvent vérifier l'appartenance au réseau, mais ne doit divulguer aucune information supplémentaire concernant leur identité ou reliant leurs actions séparées. [30]

Dans ce cas, les clés publiques d'une entité doivent être fréquemment mises à jour et les mises à jour ne doivent pas être reliées. L'identité ne doit pas être liée à la clé publique.

7.4. Carte à puce. Les cartes à puce ont plusieurs usages - authentifier les paiements et prouver les informations d'identification ou identité. Une seule carte à puce peut être utilisée dans plusieurs [37]endroits et à des fins multiples, donc son utilisation ne devrait pas être décelable par un usage répété de la même clé publique, ou par des mises à jour pouvant être liées .

8. Louise Axon et Michael Goldsmith[38]

Est une infrastructure PKI complète basée sur une chaîne de blocs permettant de gérer les certificats X.509. se cadre comprend plusieurs innovations. Premièrement, ils étendent le certificat standard X.509 pour qu'il soit compatible avec l'approche PKI basée sur la chaîne de blocs, grâce aux champs d'extension X.509 que nous avons utilisés pour intégrer des métadonnées de chaîne.

Deuxièmement, ils concevent et mettent en œuvre une infrastructure à clé publique basée sur une chaîne de blocs qui fournit une gestion fiable des certificats numériques.[35]

8.1Chain of trust

Les systèmes PKI classiques sont basés sur une autorité de certification. Les AC émettent une signature certificat, conforme à la norme X.509, certifiant que la clé publique appartient à une entité. Par exemple, lorsqu'un utilisateur se connecte à Twitter

via un navigateur Web, ce dernier valide d'abord le certificat revendiqué qui contient la clé publique de Twitter en vérifiant le (AC) du certificat donné.

En règle générale, les navigateurs Web sont préconfigurés pour accepter les certificats de certains connus (ACxx). Par conséquent, pour qu'un certificat soit approuvé, il doit avoir été émis par une autorité de certification racine existant dans le magasin sécurisé du navigateur ou du périphérique de l'utilisateur, ou par une (sous-autorité de certification) avec laquelle le certificat a été approuvé (Root-AC Signature). En règle générale, les produits Mozilla sont livrés avec 154 certificats racine[12].

Apple, Microsoft et Google ont également leur propre magasin de certificats racine de confiance intégrés à leurs produits. Le lien entre un certificat donné et le certificatracine est connu comme une chaîne de confiance. Fait important, la chaîne de confiance peut inclure un nombre quelconque de certificats (sous-AC) entre une certificat et le certificat (Root-CA). Cependant, le X509v3 a une extension nommée Basic Contraints et cette extension peut limiter la profondeur maximale de la chaîne de certificat valide (chaîne de confiance)[39].

La figure 3 illustre un chemin de certification d'une entité finale. certificat à (l'autorité de certification racine), où commence la chaîne de confiance. Par conséquent, si le certificat d'entité finale n'a pas été émis par un utilisateur de confiance (AC), le navigateur Web vérifiera ensuite si le certificat de l'émetteur (AC) a été émis par un agent de confiance

(AC), et ainsi de suite jusqu'à soit un agent de confiance (AC) est trouvé, soit aucun agent de confiance (AC) ne peut être trouvé dans la chaîne, le navigateur affichera généralement une erreur.La Figure 4 illustre Chain Of Trust.

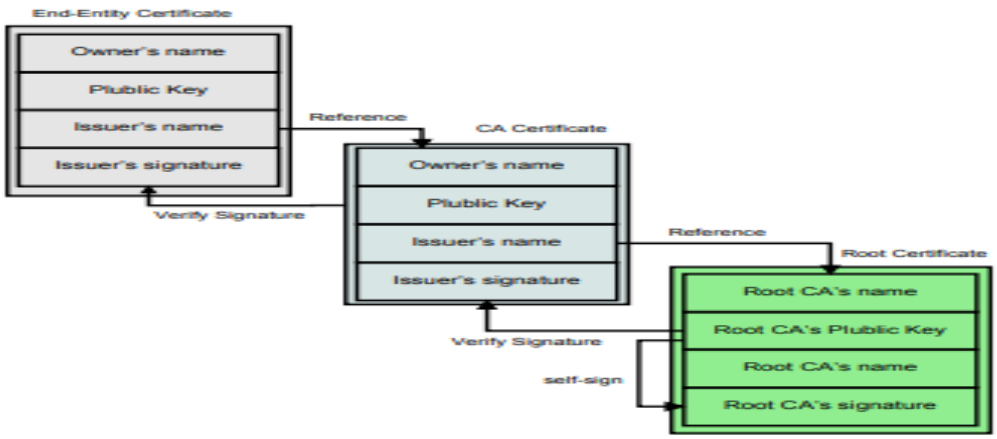

Figure 3.4 Chain Of Trust[39]

Parmi les avantages de cette approche

- niveau de sécurité très élèves
- l'isolation rapide du suspect

Lesinconvénients de cette approche

- Votre certificat SSL a-t-il été émis par une autorité de certification de confiance? Sinon, les navigateurs ne feront pas confiance à votre certificat SSL. Ce serait également un problème si vous auto-signiez votre certificat.
- Avez-vous installé vos intermédiaires correctement? Certains navigateurs essaieront de combler les lacunes de la chaîne de certificats, mais vous ne voulez pas laisser les choses au hasard.
- Votre serveur est-il configuré correctement? Le fait que vous ayez installé votre certificat SSL et les intermédiaires qui l'accompagnent ne signifie pas que vous avezcorrectement configuré votre serveur.

9. Le projet de transparence des certificats de Google

Le projet de transparence des certificats de Google corrige plusieurs failles structurelles dans le système de certificats SSL, qui est le principal système cryptographique à la base de toutes les connexions HTTPS. Ces failles affaiblissent la fiabilité et l'efficacité des connexions Internet cryptées et peuvent compromettre des mécanismes TLS / SSL essentiels, notamment la validation de domaine, le cryptage de bout en bout et les chaînes de confiance configurées par les autorités de certification. Si elles ne sont pas contrôlées, ces failles peuvent faciliter un large éventail d'attaques de sécurité, telles que l'usurpation de sites Web, l'usurpation d'identité de serveur et les attaques de type man-in-the-middle.

La transparence des certificats aide à éliminer ces failles en fournissant un cadre ouvert pour surveiller et auditer les certificats SSL presque en temps réel. Plus précisément, la transparence des certificats permet de détecter les certificats SSL émis par erreur par une autorité de certification ou acquis de manière malveillante auprès d'une autorité de certification par ailleurs irréprochable. Il permet également d'identifier les autorités de certification qui sont devenues des voleurs et qui émettent des certificats de manière malveillante.

S'agissant d'un cadre ouvert et public, n'importe qui peut créer ou accéder aux composants de base qui génèrent la transparence des certificats. Cela est

particulièrement bénéfique pour les parties prenantes de la sécurité Internet, telles que les propriétaires de domaine, les autorités de certification[40] et les fabricants de navigateurs, qui ont tout intérêt à préserver la santé et l'intégrité du système de certificats SSL.

Ils proposent de conserver des journaux publics, sur lesquels les ajouts sont uniquement, sur un nombre (par exemple supérieur a 1000) de serveurs indépendants dans le monde entier.

Chacun de ces serveurs de journalisation peut être exécuté par une autorité de certification distincte, par exemple.

Ces journaux seraient ensuite contrôlés pour détecter les certificats suspects par d'autres serveurs (gérés publiquement) et audités pour vérifier le comportement cohérent d'un logiciel d'auditeur léger pouvant être exécuté par n'importe qui.

Cela garantirait que le propriétaire d'un domaine serait en mesure de voir tous les certificats émis pour son domaine et serait ainsi en mesure de détecter tout certificat erroné, assurant ainsi la conservation de l'identité [41]Ci-dessous dans la figure 4 est présenté The Google CertificateTransparencyproject.

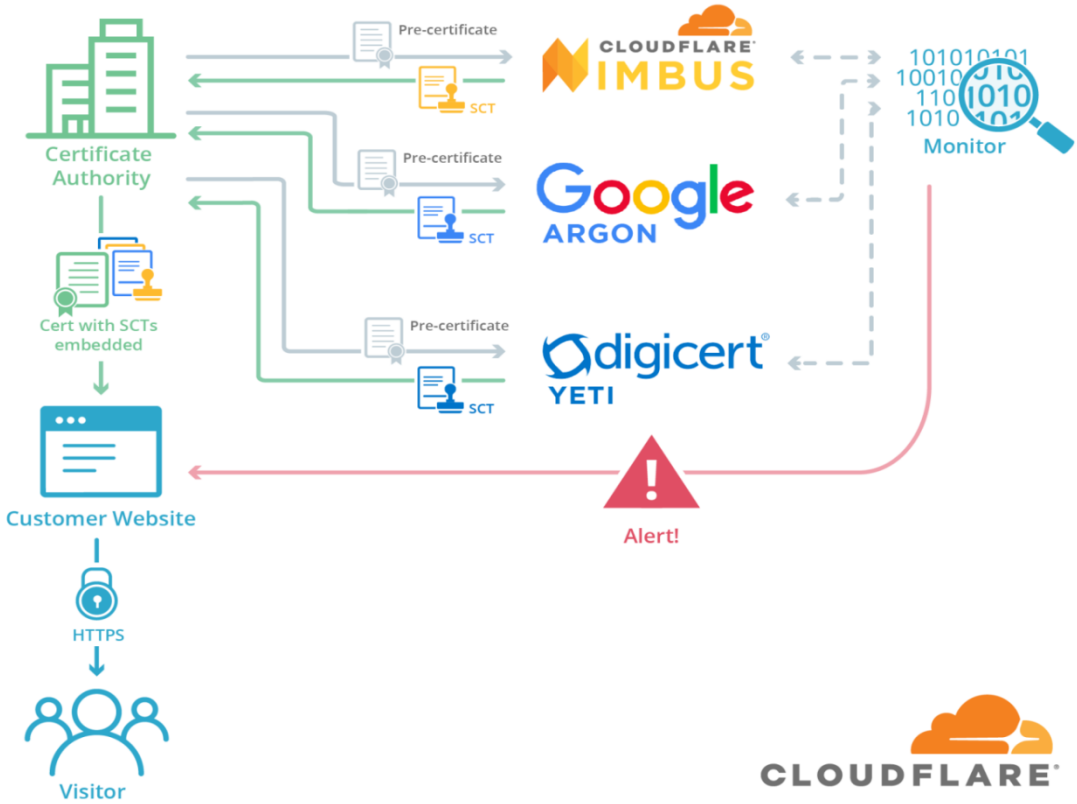

Figure 3.5 The Google Certificate Transparency project[42]

Parmi les avantages de cette approche

1-Un avantage de la transparence des certificats est qu'elle ne nécessite aucune modification importante du modèle commercial actuel d'une autorité de certification. Les autorités de certification fourniront toujours des certificats SSL comme par le passé. Le seul changement est qu'ils devront d'abord envoyer les certificats à quelques serveurs de journalisation et obtenir un horodatage, qu'ils incluent avec le certificat.
2-La transparence des certificats offre aux autorités de certification la possibilité de fournir plusieurs nouveaux services à leurs clients. Par exemple, une autorité de certification peut proposer des services de surveillance des certificats aux opérateurs de serveurs ou aux propriétaires de domaine, ou des services d'audit de certificats aux clients TLS.
3-flexible et extensible
et l'inconvénient de cet approche
1-niveau de sécurité faible

10. PGP web of trust

Un autre approche pour déterminer la validité des clés publiques, en particulier pour les utilisateurs de PGP. Les utilisateurs qui publient de nouvelles clés publiques ont une connaissance, avec une paire de clés publique / privée, signée sur la nouvelle clé.

Une fois que le signataire vérifie l'identité de la personne avec la nouvelle clé (par exemple, en la voyant en personne ou par reconnaissance vocale sur le téléphone), le signataire vérifie que la nouvelle clé est authentique.

Avant de le signer, le signataire s'assure que la clé contient la bonne empreinte digitale (code réel). Après la signature, la clé signée est publiée sur les serveurs de clés. Toute personne qui fait confiance au signataire pour suivre les procédures d'identification appropriées peut décider de faire confiance à toutes les clés signées par cette personne. Pour étendre le réseau de confiance, les utilisateurs doivent décider de faire confiance à toutes les personnes dont les clés ont été signées par d'autres personnes en qui elles ont confiance (leurs clés sont signées par des personnes de confiance). Ce système contraste avec les crypto systèmes à clé publique formels, car il n'existe pas de pouvoir de signature central ou hiérarchique(la blockchain).

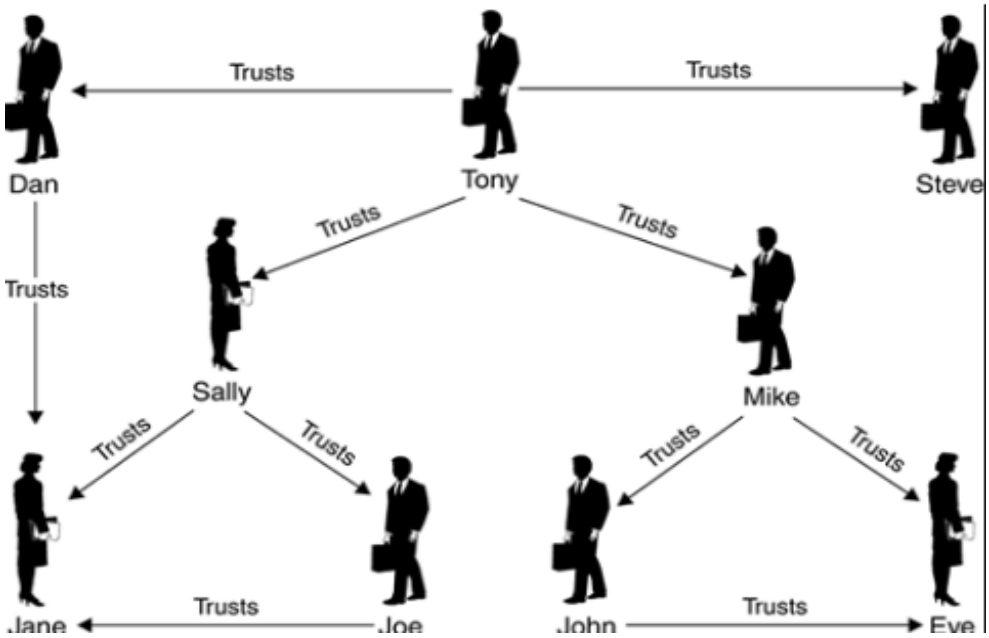

Figure 3.6 PGP web of trust [17]

parmi les avantages de cette approche la confiance entre les utilisateurs
l'inconvénient de cette approche est dans le cas d'utilisateur distant

10.Conclusion

Cette technologie est encore jeune, complexe et reste limitée à certaines communautés ou à certains secteurs. Elle devra lever plusieurs contraintes avant d'envisager un déploiement industriel (techniques, organisationnelles, juridiques ou encore éthiques). Pour autant, on se rend bien compte que la Blockchain a une portée globale, qu'elle est capable de faire fonctionner des écosystèmes privés ou publics de manière quasi autonome, uniquement sur la base d'algorithmes informatiques. Potentiellement, elle peut ainsi remettre en cause le rôle de certains agents de confiance qui sont à la base du fonctionnement de nos sociétés actuelles. Le processus d'appropriation de cette technologie est d'ores et déjà enclenché. Si son potentiel de désintermédiation a pu inquiéter dans un premier temps, l'ensemble des acteurs a désormais saisi l'opportunité de simplification et de digitalisation des traitements : réduction des coûts et possibilité de créer de nouveaux services à valeur ajoutée. En plus nous avons vu la différence entre le PKI Conventionnel et Pki Base sur la Blockchain et la meilleur choix.

CHAPITRE 4

1. Introduction

Dans le chapitre 4 on parler sur l'environnement matériel et logiciel. Aussi nous Avon présenté les fonctions et les bibliothèques utilisé pour construire une x.509 certificat et valider se certificat.

2. Environnement logiciel

Plateforme utilisé est Windows 7 professionnel pack1 .le langage de développement choisit est java.On a utilisé l'environnement NetBeans IDE 8.2 pour simplifiait le travail a fin de développer notre application . L'environnement NetBeans adopte l'IDE (Integrated Développent Environment) java gratuitement. L'IDE est un logiciel open source développé par SUN Microsystems utilisé pour exécuter, compilé. Un IDE est dédié à un seul langage de programmation. Le choix se fait pour les raison suivante :

- Les logiciels écrits dans ce langage sont très facilement portables sur plusieurs
- systèmes d'exploitation.
- NetBeans IDE est un outil gratuit et flexible.
- Nous souhaitions, à travers ce projet, améliorer notre connaissance du langage.

2.1.Environnement java

Le langage Java est un langage de programmation informatique orienté objet créé par James Gosling et Patrick Naughton, employés de Sun Microsystems, avec le soutien de Bill Joy (cofondateur de Sun Microsystems en 1982), présenté officiellement le 23 mai 1995 au SunWorld. La société Sun a été ensuite rachetée en 2009 par la société Oracle qui détient et maintient désormais Java. La particularité et l'objectif central de Java est que les logiciels écrits dans ce langage doivent être très facilement portables sur plusieurs systèmes d'exploitation tels que UNIX, Windows, Mac OS ou GNU/Linux, avec peu ou pas de modifications. Pour cela, divers plateformes et frameworks associés visent à guider, sinon garantir, cette portabilité des applications développées en Java [43].

2.2.NetBeans IDE

NetBeans est un environnement de développement intégré (EDI), placé en open source par Sun en juin 2000 sous licence CDDL (Common Development and Distribution License) et GPLv2. En plus de Java, NetBeans permet la prise en charge

native de divers langages tels le C, le C++, le JavaScript, le XML, le Groovy, le PHP et le HTML, ou d'autres (dont Python et Ruby) par l'ajout de greffons. Il offre toutes lesfacilités d'un IDE moderne (éditeur en couleurs, projets multi-langage, refactoring, éditeur graphique d'interfaces et de pages Web). Compilé en Java, NetBeans est disponible sous Windows ,Linux, Solaris (sur x86 et SPARC), Mac OS X ou sous une version indépendante des systèmes d'exploitation (requérant une machine virtuelle Java). Un environnement Java Development Kit JDKest requis pour les développements en Java.

NetBeans constitue par ailleurs une plate forme qui permet le développement d'applications spécifiques (bibliothèque Swing (Java)). L'IDE NetBeans s'appuie sur cette plate forme [43].

2.3.Bouncy Castle

On a utilisé plusieurs bibliothèques pour intégrer la sécurité et la cryptographie pour la génération de x.509 certificat comme :

1-java.security

2-java.util

3-asn

4-org.bouncycastle

5-x.509

Bouncy Castle est une bibliothèque de cryptographie libre et open-source. Elle s'apparente à la librairie C openssl qui est conform[44]e aux différents standards en vigueur.

3. Environnement matériel

Pour développer l'application, nous avons utilisé comme environnement matériel un ordinateurs Dell qui possède comme caractéristiques :

- Un processeur Intel Pentium® Core (TM) i5, 1.80 GHz.
- Une mémoire vive de 8Go.
- Un disque dur 500 Go.
- Un écran 15.6 pouces.

4.Les fonctions utilisées

4.1. SHA

L'acronyme SHA, pour Secure Hash Algorithme, désigne une fonction de hachage cryptographique conçue par l'Agence Nationale de Sécurité américaine. Il en existe plusieurs versions.

Parmi les plus connues, on peut citer le SHA-2, le SHA-256 ou encore le SHA-512. Tous définissent des algorithmes de hachage utilisés par des autorités administratives pour la signature de certificats. Tous génèrent des condensates uniques.

4.2MD5

Le Message Digest 5 (MD5) et un algorithme de hachage le plus utilisés au monde à l'heure actuelle en matière d'empreinte numérique et de cryptographie. Leur rôle est multiple, il permet par exemple de vérifier l'intégrité de fichiers ou messages, la vérification de mot de passe ou encore l'identification de fichiers ou données.

Le MD5 a été créé en 1991 par le cryptologue Ronald Rivest, qui est également connu pour être l'un des inventeurs de l'outil de cryptographie à clé publique RSA. Il permet d'obtenir des condensats ou « hash » de 128 bits.

Les algorithmes MD5 et SHA sont utilisés dans les antivirus, les pare-feu « Firewall », les signatures électroniques ou encore dans tous les systèmes de contrôle d'intégrité.

Ces fonctions de hachage ne permettent pas de retrouver les données originales : le hachage ne fonctionne en effet que dans un sens.

5. Approches implémentées

Au début on a crée un certificat sur les critères de la norme x.509 pour ce travail on a besoin des fonctions de la bibliothèque bouncy castle comme MD5 et SHA.

pour la génération de certificats on a utilisé les sept champs nécessaire serial number, subject, issuer, key, version, algorithme id pour la signature numérique (SHA) et le deuxième algorithme pour l'hachage (MD5) , et la dernier champ la validité pour ce champ on a utilisé la fonction prédéfinie Date() pour obtenir la date actuelle et faire l'addition avec le délai .

A la fin de cette étape on a appelé la fonction file.write() pour créer le certificat. Le temps de création est : 5s.

pour la validation on a crée une autre class (Validate) cette class obtenir les informations haches de certificat a partir de la fonction readfileasstring() après on a

utilisé la fonction substring() pour la division et on a connu l'hachage de clé et les autres champs.

Après la division on a recherché si ces hachages existés ou non et faire la soustraction pour la validité de date ne pas expiré.

Pour la Blockchain on a besoin de créer trois classes :

- La première class pour les blocs (block), les fonctions plus utilisées dans cette class sont get() et set() ,cette class contient des constructeurs de la class transaction et contient les hachages des blocs précédents .
- La deuxième class(Transaction) contient les sommes, l'émetteur, l'expéditeur, chaque attribut avec ces fonctions et ces rôles.
- La troisième class si la class principal pour la combinaison des autres classes (main).

L'objectif de ce travail c'est la liaison entre ces classes et ajouter des nouveaux champs sur le certificat conventionnelle pour spécifier la blockchain comme ID, le nom de blockchain, l'algorithme de hachage utiliser par la blockchain, et les informations de certificat enregistrer dans la blockchain, La Figure 1 illustre le stockage de certificat dans la blockchain.

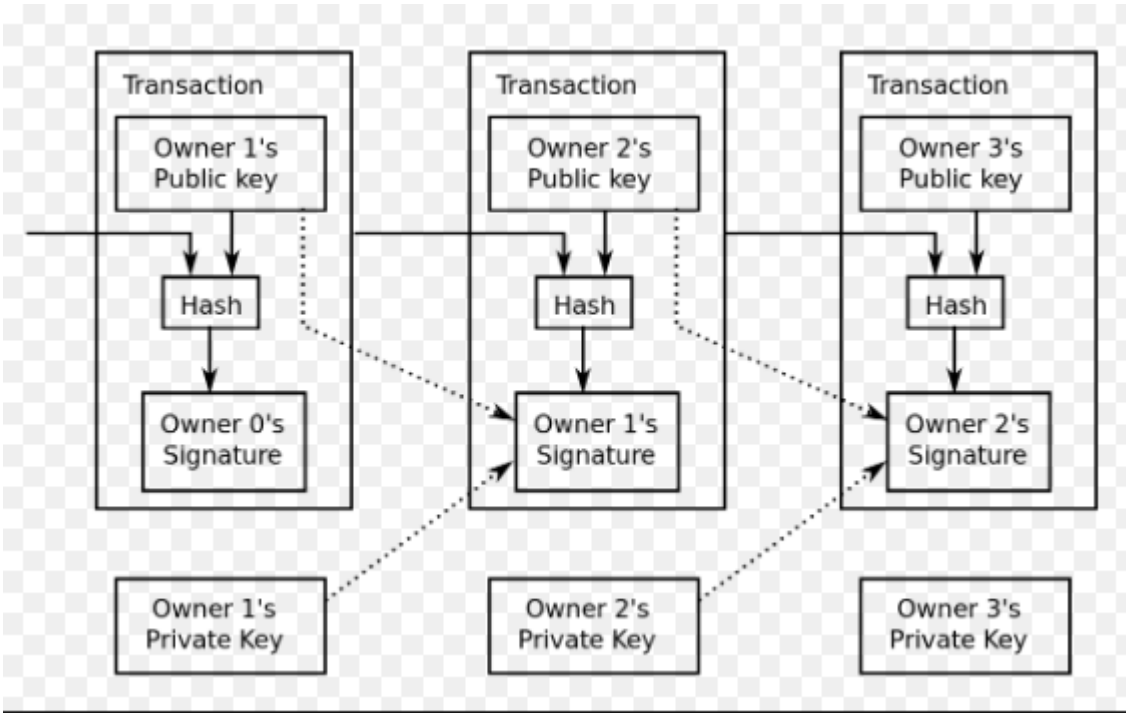

Figure 4.1 Le stockage de certificat dans la blockchain[40]

6. Résultats expérimentaux

La Figure 1 illustre le x.509 certificat développé.

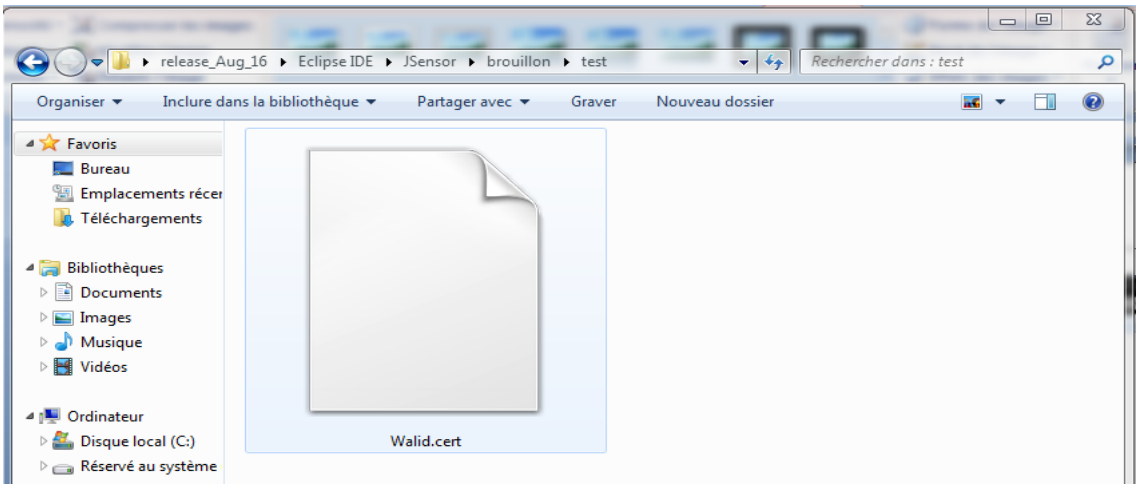

Figure 4.2certificatx.509

```
63
64      Date since = new Date();
65      Date until = new Date(since.getTime() + validDays * 864000001);
66
        CertificateValidity interval = new CertificateValidity(since, until);
68      BigInteger sn = new BigInteger(64, new SecureRandom());
69
        info.set(X509CertInfo.VALIDITY, interval);
        info.set(X509CertInfo.SERIAL_NUMBER, new CertificateSerialNumber(sn));
        info.set(X509CertInfo.SUBJECT, distinguishedName);
        info.set(X509CertInfo.ISSUER, distinguishedName);
        info.set(X509CertInfo.KEY, new CertificateX509Key(kp.getPublic()));
        info.set(X509CertInfo.VERSION, new CertificateVersion(CertificateVersion.V3));
76
        AlgorithmId algo = new AlgorithmId(AlgorithmId.md5WithRSAEncryption_oid);
        info.set(X509CertInfo.ALGORITHM_ID, new CertificateAlgorithmId(algo));
79
80
        X509CertImpl cert = new X509CertImpl(info);
82      cert.sign(privkey, "SHA1withRSA");
```

Figure 4.3 les éléments de certificat x.509

Le certificat obtenue contient :

- une période de validité
- numéro de série
- version
- nom d'autorité de certification
- algorithme de signature

7. Certificat de PKI basée sur la blockchain

Le nouveau a ce certificat est que la partie extension qui spécifier la blockchain.
La blockchain est une ensemble des blocks chaque block a ses caractéristiques (ID, Adresse....) .
Quand le certificat entre a la blockchain il faut spécifie le nom et l'algorithme de hachage utilise par cette dernière.

Figure 4.4 Structure de certificat basèe sur la blockchain[36]

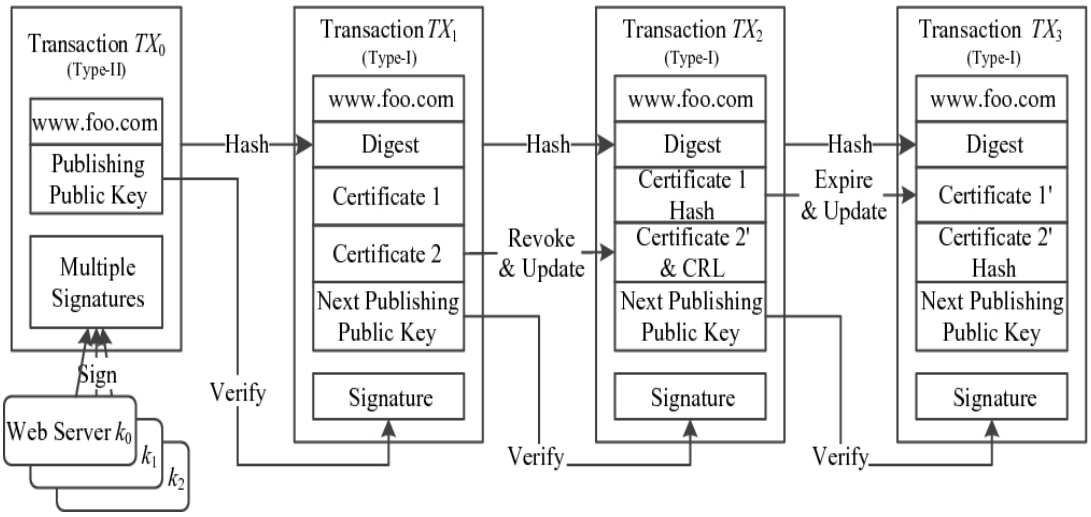

Figure 4.5 La route de certificat dans la blockchain[35]

8. Etude comparative

Dans le domaine de sécurité chaque technologie contient des vulnérabilités dans sa structure ou dans sa fonctionnement parmi ces technologies la PKI conventionnelle et la PKI Basèe sur la Blockchain, en plus chaque technologie a ces points d'efforts Ce qui les distingue des autres c'est à dire il n'existe pas une technologie parfaite C'est ce qui a conduit au lien PKI et la blockchain.

La PKI Basèe sur la Blockchain sécurisé Plus que la PKI conventionnelle par ce qu' elle utilise le point d'effort de la blockchain dans le stockage des certificats et de CRL par contre la PKI conventionnelle stocke ses éléments dans l'annuaire LDAP ce dernier moins sécurisé que la blockchain .

La PKI conventionnelle accéde au l'annuaire LDAP tout simplement pour vérifier le CRL et les certificats par contre la PKI Basèe sur la Blockchain nécessite à accéder à la blockchain et cette étape nécessite de résoudre des équations mathématiques, des liens entre les blocks qui considérées la base de sécurité de la blockchain c'est ce qui le rend lent par rapport à la PKI conventionnelle.

La PKI Base sur la Blockchain élimine la centralisation qui a été utilisée par la PKI conventionnelle et remplacée par le consensus c'est à dire plusieurs éléments connaissent qu'est ce qu'il y'a mais dans la PKI conventionnelle elle est la seule à apprendre qu'est ce qu'il y'a.

Le niveau de sécurité de la PKI Basèe sur la Blockchain permet de faire une vérification très complexe sur les objets et isole le suspect rapidement. Si le pirate accéde au premier bloc il ne peut pas au deuxième.

L'utilisation de PKI Base sur la Blockchain nécessite des grands moyens et couteuse ce qui la rend indisponible pour tout le monde contraire au le PKI conventionnelle.

L'utilisation de la blockchain dans la PKI réduit le risque d'attaque man in the middle, et ajoute plusieurs domaines pour l'utilisation de PKI ceci est bénéfique pour les autorités de certification.

Le problème de PKI conventionnelle est dans les algorithmes qui imposent des clés de taille élevée (au moins 1024 bits).

Une autre différence entre la PKI conventionnelle et la PKI Basèe sur la Blockchain dans la structure de certificat de chaque technologie, dans le certificat de PKI Base sur la Blockchain il ya une extension n'existe pas dans le certificat de PKI

	Sécurité	Rapidité	Flexibilité	Transparence	Isolation de suspect	Moins Chère
PKI Conventionnel	-	+	-	-	-	+
Pki Base sur la Blockchain	+	-	+	+	+	-

conventionnelle cette extension contient des informations de la blockchain comme ID, algorithme de hachage, nom de blockchain....

Ce qui empêche le travail de pirate.

Table4.1 Etude comparative

9. Discussion

A partir de cette étude et ce résultat et la nature décentralisée de la PKI Basée sur la Blockchain et la nature centralisé de la PKI conventionnelle on conclue les points d'effort et les points faibles de chaque approche.

Les solutions PKI basées sur blockchain fournissent des propriétés de sécurité souhaitables. Toutefois, comme ils relient publiquement des entités à des clés publiques, ils ne conviennent pas aux applications dans lesquelles un niveau de confidentialité est requis. Dans les applications PKI telles que l'Internet des objets, les réseaux ad-hoc et les cartes à puce, il est important d'empêcher le traçage des entités et de leurs actions. Nous nous intéressons donc à la protection de la vie privée dans les PKI basées sur les blockchains.

Si on parle sur le coté performance on trouve deux points liés a la performance, la rapidité et la sécurité, la PKI Basée sur la Blockchain mieux que la PKI conventionnelle au coté sécurité, la PKI conventionnel mieux que la PKI Base sur la Blockchain au coté rapidité.

Alors le meilleur choix c'est la PKI Base sur la Blockchain malgré elle inclue des points faibles telles que le manque de rapidité , disponible pour tout le monde mais capable de s'améliorer dans le future.

10. Conclusion

Dans le chapitre 4 nous avons présenté le programme, On a commencé par présenter l'environnement matériel et logiciel ensuite présenté les fonctions et les bibliothèques nécessaires utilisé. en fin on a présenté le certificat obtenu.

Comme on a fait une comparaison entre la PKI Conventionnel et la PKI Basée sur la Blockchain et obtenu un résultat est que la PKI Basée sur la Blockchain mieux que la PKI Conventionnelle.

CONCLUSION GENERALE

Le travail exposé dans ce mémoire s'intéresse à l'étude d'une problématique de la relation et les points d'efforts d'ajouter par la blockchain à la PKI. Dans le début on a présenté la blockchain en général les types, comment ajouter des nouveaux blocs a la blockchain sa structure les différentes relations et les actions entre les blocs, les algorithmes utilisés.

Après avoir présenté la PKI en général ces composants, comment fonctionner et spécifier une partie pour étudier x.509 certificat ces éléments, la création et la validation et la révocation de cet type de certificat.

La construction d'une infrastructure à clé publique sur la chaîne de blocs est une alternative viable aux approches classiques AC et WoT et offre des propriétés de sécurité souhaitables.

La blockchain fonctionne de manière décentralisée et est un enregistrement fiable des transactions, ce qui en fait une solution naturelle à de nombreux problèmes liés à la PKI classique: points de défaillance uniques et transparence - toutes les parties concernées ont la possibilité de vérifier l'enregistrement de la transaction - en particulier grâce à la méthode de la blockchain.

Les propositions de pki existantes basées sur des chaînes de blocs sont conçues comme des enregistrements transparents des transactions et ne permettent pas de conserver des niveaux de confidentialité.

La PKI doit faire l'objet d'une sensibilisation à la vie privée dans les applications actuelles et émergentes; en particulier, les réseaux mobiles et véhiculaires et l'informatique omniprésente nécessitent des PKI dans lesquelles des entités peuvent rester membres de réseau anonymes ou pseudonymes.

Cette proposition et cette analyse montrent que la PKI respectueuse de la vie privée peut s'appuyer sur la blockchain et que des propriétés souhaitables sont absentes de la pki classique - contrôle décentralisé de l'accès à l'information.

On a discuté sur deux approches existantes et on a donné les avantages et les inconvénients de chaque approche.

A la fin on a faire une comparaison entre la PKI conventionnelle et la PKI basé sur la blockchain et connaitre les points d'efforts et les points de faible de chaque technologie et les applications utiliser ces technologies et on a trouvé que le meilleur choix si la PKI basée sur

malgré que la blockchain inclut des inconvénients mais très sécurisé et transparent, malgré tout la PKI une valeur constante et solide dans le monde de la sécurité.

REFERENCES

[1] Cryptolia, https://www.cryptolia.fr/ consulté le : 15/02/2019

[2] R.Teuscher, R.Pensec, Y.Fasla, and T.Kuselj, Blockchain La nouvelle révolution technologique ?, Juin 2018,1-2.

[3] w. Stornetta, La première blockchain de l'histoire date de 1995, *LE MONDE*, 2018.

[4] F.Valèrian, *La Réalités Industrielles*. PARIS: Printcorp , 2017.

[5] Blockchainfrance, https://blockchainfrance.net ,consulté le : 16/02/2019.

[6] hal-univ, consulté le : https://hal-univ-lyon3.archives-ouvertes.fr/hal-01796727/document , 16/02/2019.

[7] Blokchain use cases, https://www.lafabriquedunet.fr/blog/definition-blockchain/, consulté le : 16/02/2019.

https://www.lafabriquedunet.fr/blog/definition-blockchain/, consulté le : 17/02/2019.

[8] Cryptoast ,cryptoast.fr/blockchain-avantages-inconvenients/, consulté le : 18/02/2019.

[9] DÉCLARATION DE RESPECT DE LA VIE PRIVÉE , fr.express.live/blockchain-les-avantages-et-les-inconvenients-de-cette-technologie/, consulté le : 18/02/2019.

https://fr.express.live/blockchain-les-avantages-et-les-inconvenients-de-cette-technologie/ , consulté le : 19/02/2019.

[10] G. Ferréol, PRINCIPES CLES D'UNE APPLICATION BLOCKCHAIN,2016.

[11] Certeuropehttps://www.certeurope.fr/blog/quest-ce-quune-pki-ou-infrastructure-a-cles-publiques/, consulté le : 19/02/2019.

[12] Mozilla included ca certificate list, https://wiki.mozilla.org/CA/Included_Certificates, consulté le : 20/02/2019.

[13] Securiteinfo,https://www.securiteinfo.com/cryptographie/pki.shtml, consulté le : 20/02/2019.

[14] LeMaGiT, https://www.lemagit.fr/definition/Certificat-numerique, consulté le : 24/02/2019.

[15] N.Chikouche, Sécurité informatique, polycopié de cours, 2018.

[16] (2019) securiteinfo. [Online]. https://www.securiteinfo.com/cryptographie/pki.shtml

[17] wikipedia. [Online]. www.wikipedia.com

[18] J. Buchmann, E.Karatsiolis, and A.Wiesmaier, *Introduction to public key infrastructures*, Springer Science & Business Media, 2013.

[19] Certification Request Syntax Specification,https://www.rfceditor.org/info/rfc2986, consulté le : 29/02/2019.

[20] rfc2459, https://tools.ietf.org/html/rfc2459#page-21, consulté le : 02/03/2019.

[21] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, https://www.rfc-editor.org/, consulté le : 09/03/2019.

[22] X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP , https://www.rfc-editor.org/info/, consulté le : 11/03/2019.

[23] Supinfo,https://labo-microsoft.supinfo.com/articles/pki-windows-server-2003/, consulté le : 12/03/2019.

[24] Cryptosec, http://www.cryptosec.org/?Certificats-X509-v3, consulté le : 16/03/2019.

[25] Introduction à la sécurité informatique https://moodle.utc.fr/pluginfile.php/16777/mod_resource/content/0/SupportIntroSecu/co/CoursSecurite_20.html, consulté le : 18/03/2019.

[26] H.Kalodner, An empirical study of namecoin and lessons for decentralized namespace design, In Workshop on the Economics (WEIS)," 2015.

[27] Hari Lakshman, *The internet blockchain*., 2016.

[28] S.Nakamoto, Bitcoin: A peer to-peer electronic cash system, 1-9,2008.

[29] D.Velicanu, and S.Yakoubov, Certcoin: A namecoin based decentralized authentication system, 2014.

[30] Louise Axon and Michael Goldsmith, PB-PKI: a Privacy-Aware Blockchain-Based PKI, 18,2017,1-5.

[31] Askfrance,https://askfrance.me/q/quelle-est-la-racine-de-merkle-25235184666, consulté le : 14/04/2019.

[32] BNP PARIBAS,http://blogchaincafe.com/merkle-roots-et-merkle-trees-expliques, consulté le : 16/04/2019.

[33] C.Ellison et B.Schneier, *Ten risks of pki*, 2000, pp. 1-7.

[34] Google certificate transparency project,http://www.certificate-transparency.org/, consulté le : 15/05/2019.

[35] Alexander Yakubov, A Blockchain-Based PKI Management Framework,6,2016,2-5.

[36] TELEGRID_3-Ways-Blockchain-Can-Improve-PKI, TELEGRID.com ,consulté le : 24/05/2019.

[37] Louise Axon and Michael Goldsmith, PB-PKI: a Privacy-Aware Blockchain-Based PKI, 8,2017,3-7.

[38] Louise Axon and Michael Goldsmith, PB-PKI: a Privacy-Aware Blockchain-Based PKI, 8,2017,3-7.

[39] D. Cooper, Internet x. 509 public key infrastructure certificate and certificate revocation list , 2008.

[40] Google,https://www.certificate-transparency.org/, consulté le : 20/06/2019.

[41] Conner Fromknecht, A Decentralized Public Key Infrastructure with Identity Retention, 2014.

[42] Certificate Transparency,http://www.certificate-transparency.org/what-is-ct, consulté le : 29/06/2019.

[43]Javas ,http://www.javas.com, consulté le : 03/07/2019.

Résumé :

Le travail de ce mémoire concerne l'étude des technologies blockchain et PKI, l'objectif principal de ce travail est de faire une comparaison entre le PKI conventionnelle et la PKI basée sur la technologie Blockchain. De plus, on présente la relation entre la PKI et la blockchain.

Le nouveau concept présenté par la PKI basée sur la blockchain est de l'utilisation du consensus et l'élimination de la centralisation qui a été utilisé par le PKI conventionnelle. Elle est très efficace mais il est très cher et lourd.

La relation entre la blockchain et la PKI si que chaque partie cherche à améliorer l'autre, la PKI crée et gère les certificats et la blockchain utilise sa point d'effort de sécurité pour stocker les certificats.

ملخص:

الهدف من هذه المذكرة هو دراسة تقنية البلوكشيين و البنية التحتية للمفاتيح العامة , والهدف الرئيسي هو المقارنة بين البنية التحتية للمفاتيح العامة التقليدية و البنية التحتية للمفاتيح العامة المبنية على أساس البلوكشيين. بالإضافة إلى معرفة العلاقة بين البنية التحتية للمفاتيح العامة و البلوكشيين.

الشيء الجديد الذي قدمته البنية التحتية للمفاتيح العامة المبنية على أساس البلوكشيين هي استخدام الإجماع والقضاء على المركزية التي تم استخدامها من قبل البنية التحتية للمفاتيح العامة التقليدية, وهو ما يعتبر مصدر فاعليتها لكنه يعتبر غالي جدا وبطيء.

العلاقة بين البلوكشيين و البنية التحتية للمفاتيح العامة هو أن كل طرف يحاول تحسين الآخر, فالبنية التحتية للمفاتيح العامة تعمل على إنشاء وإدارة الشهادات أما البلوكشيين فتستخدم نقطة قوتها في الأمن لتخزين الشهادات.

Abstract :

The work of this thesis concerns the study of blockchain and PKI technologies, the main objective is working if to make a comparison between the conventional PKI and PKI based on the blockchain we know more about the relationship between the PKI and the blockchain.

The new concept presented by the PKI based on the blockchain if the use of the consensus and the elimination of the centralization that was used by the conventional PKI is it the efficiency of the PKI based on the blockchain but it is very expensive and heavy.

The relation between the blockchain and the PKI if each part tries to improve the other, the PKI to create and manage the certificates and the blockchain to use its point of security effort to store the certificates.