الجمهورية الجزائرية الديمقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التعليم العالي والبحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة أبي بكر بلقايد– تلمسان –

Université Aboubakr Belkaïd– Tlemcen –

Faculté de TECHNOLOGIE

MEMOIRE

Présenté pour l'obtention du **diplôme** de **MASTER**

En : Télécommunications

Spécialité : Réseaux et Télécommunications

Par : **SIDI AISSA Ikram** et **KEDDAR Souria**

Sujet

Proposition d'un système à base de blockchain pour la gestion des opérations sur les véhicules au niveau national

Soutenu publiquement, le**28 / 06 / 2018**, devant le jury composé de :

Mme F.BENMANSOUR	MCB Univ. Tlemcen	Président
Mr. B. KADRI	MCA Univ. Tlemcen	Encadrant
Mr A. ABDELMALEK	MCB Univ. Tlemcen	Examinateur

Remerciement

Au terme de ce modeste travail,

Tout d'abord, louange à notre seigneur « Allah » qui nous a guidé sur le droit chemin tout le long de cette expérience, nous a donné le courage et la volonté pour terminer ce travail et nous a inspiré les bons pas et les justes reflexes. Sans sa miséricorde, ce travail n'aurait pu aboutir.

Par la suite, nous voudrions exprimer nos profondes gratitudes à notre encadreur monsieur Kadri Benamar et pour sa générosité en nous transmettant ses connaissances et ses précieux conseils ainsi que son temps qu'il nous a dispensé, et sa disponibilité dont il a fait preuve ; nous avouons que toutes ces conditions nous ont énormément facilité la tâche.

Nos vifs remerciements aux membres du jury d'avoir accepté d'examiner et d'évaluer notre travail. Un grand merci à tous les professeurs de Télécommunication qui ont participé à notre progrès pendant ces 5 ans.

Enfin Nous tenons à remercier chaleureusement nos parents qui grâces à eux nous sommes arrivées là, à nos frères et sœurs qui avec leurs encouragements nous ont donné la volonté de travailler plus encore, et à nos amis qui étaient toujours présents à nos côtés dans les bons moments pour se réjouir avec nous et pour nous soulager dans les mauvais moments.

Dédicace

Je dédie ce modeste travail

A l'homme de ma vie, mon exemple éternel, mon soutien moral et source de joie et de bonheur, celui qui s'est toujours sacrifié pour me voir réussir, que dieu te garde dans son vaste paradis, à toi mon père.

A la lumière de mes jours, la source de mes efforts, la flamme de mon cœur, ma vie et mon bonheur ; maman que j'adore.

Aux personnes dont j'ai bien aimé la présence dans ce jour,

A mon frère : Aymen

A mes très chères sœurs : Asmaa *et* Meriem

A ma grand-mère, mes grands-pères, mes tentes, mes oncles, mes cousins et mes cousines et à toute ma famille

A mon Binôme Souria *et à tous mes amies qui n'ont jamais cessé de m'encourager qui étaient toujours à mes côtés, et qui m'ont accompagné durant mon chemin d'études. Ou de m'aider :* Imen ; Akila ; Ilyés *et à ma sœur de cœur, toi* Iman *; ,,,,,,,,, ; tous mes amis de la promo à qui je souhaite bonne chance dans leur vie professionnelle.*

Et en fin Je le dédie à tous ce qui m'a donné leur moindre coup de pouce pour réussir ce travail.

Ikram

Dédicaces

Je dédie ce modeste travail :

A mes très chers parents, pour leurs assistances, conseils, patience, soutien et sacrifices.

A mon grand-père, Qu'Allah Lui accorde une saine et longue vie.

A mon très cher frère MOHAMMED EL-Amine, et mes chères sœurs : FATIMA, SAMIHA, YOUSSRA et ma cousine ACHWAK.

A tous ceux que j'aime et qui m'aiment, mes tantes et mes oncles et ma famille.

Je dédie également ce travail à ma grande famille « KEDDAR » et la famille « MOUSBAH ».

A toutes mes amies de l'université de TLEMCEN

A tous ceux qui sont proches de mon cœur et qui m'encouragent à donner le meilleur en moi.

Souria

Résumé

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

Les différents avantages que pourrait apporter la technologie Blockchain au secteur public, permettras la protection des données critiques, de pouvoir s'assurer de la propriété de biens, ou encore de créer un réseau puissant entre les différents services publics et surtout le stockage des données Ceci est fondamental pour plusieurs contextes au secteur publique.

Dans ce travail on s'intéressait à l'utilisation du Blockchain pour la gestion des opérations sur les véhicule (vente / achat et enregistrement). La proposition donne solution au différent problème liée au domaine du véhicule fraude du vol on se bassons sur des transactions similaire à la transaction du bitcoin.

Mots clés : Blockchain, cryptomonnaie, bitcoin, transaction, carte grise biométrique.

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.

With the various benefits that Blockchain technology could bring to the public sector, it is believed that it could help protect critical data, ensure ownership of assets, or create a powerful network between different public services. And especially the storage of data this is fundamental for several contexts in the public sector.

In this work we will use the blockchain technology for running the operation related to the vehicles domain such as sale, bay and registration. The proposed blockchain gives solution to different problem related to the vehicle market such as theft, fraud ……. etc.

Keywords: Blockchain, cryptocurrency, bitcoin, transaction, biometric gray card.

Table des matières

Table des illustres

Liste des Tableaux

Introduction Générale

Introduction générale

La gestion et l'utilisation des données administratives peuvent être compliquées, même pour les gouvernements avancés. Les secteurs publics critiques tels que le service du certificat d'immatriculation des véhicules (système de gestion de carte grise) a tendance à construire leur propre base de données et de protocoles de gestion de l'information,

Le processus d'immatriculation des véhicules a toujours été fastidieux. C'est un processus de prise de temps où plusieurs parties sont impliquées et qui présente également un risque de manipulation d'informations non autorisés, de duplication de données et d'erreurs diverses.

Dans un tel scénario, l'information critique peut devenir très vulnérable aux fraudes et aux falsifications de données ou même devenir non-traçable. Plusieurs vagues technologiques ont structuré les développements et Internet révolutionne les échanges entre les individus en permettant la création et la publication d'informations portées par des terminaux toujours plus variés et nombreux.

La décentralisation des bases de données sous-jacentes à une blockchain pourrait simplifier la gestion des informations fiables, ce qui permettrait aux administrateurs et même les utilisateurs d'accéder plus facilement aux données critiques du secteur tout en préservant la sécurité de ces informations. Une blockchain est un registre numérique codé stocké sur plusieurs ordinateurs dans un réseau public ou privé.

Pour ce faire, nous étudions les crypto-systèmes existants et la nouvelle technologie blockchain.

Dans ce contexte et dans le cadre de notre projet de fin d'étude, on va organiser ce manuscrit de la façon suivant :

Dans le chapitre 1 on va donner une définition sur la cryptographie qui définisse qu'est-ce-que la cryptologie, la cryptographie et la cryptanalyse et déférente définitions sur déférente concept de base, du chiffrement a paire de clés et ces algorithmes présente chacun d'eux des points positives et d'autre négatives.

Le chapitre 2 introduit le concept du Blockchain, ces caractéristiques, son fonctionnement, l'architecture, après ça on va donner une vision sur la notion fondamentale de la transaction blockchain et sa preuve de travail.

Dans le chapitre 3 nous essayant d'expérimenter et de tirer parti du potentiel de Blockchain sur différentes applications. Pour comprendre comment Blockchain peut être utilisé dans autre chose qu'une transaction monétaire.

Introduction générale

Le chapitre4 nous étudions et nous proposant une solution basée sur les blockchains pour organiser et gérer le domaine des véhicules au niveau national, la solution sera entièrement distribuée et basé sur l'utilisation des certificats numériques gérées par une autorité nationale. La solution proposé traite la majorité des aspects du service de gestion de carte grise au niveau national et propose une solution pour les opérations existant dans ce service telles que là vent/achat, la registration des véhicules…etc.

Chapitre 01

Cryptographie

I. Introduction

De tout temps, les codes ont existé. Ils ont d'abord servi à retranscrire des idées, à écrire un langage. L'homme a perçu le besoin de cacher, de dissimuler des informations personnelles ou confidentielles. La cryptographie est une science très ancienne. Des recherches indiquent qu'un scribe égyptien a employé des hiéroglyphes non conformes à la langue pour écrire un message.

De ce temps-là et au long de l'histoire, la cryptographie a été utilisée exclusivement à des fins militaires.

Cela bien avant l'ère informatique. Mais avec ces nouveaux moyens de communication est arrivée la nécessité de protéger le contenu de certains messages des inévitables curieux.

Aujourd'hui, les réseaux informatiques exigent une phase de cryptographie comme mécanisme fondamental afin d'assurer la confidentialité de l'information numérique. Dans ce chapitre nous pressentons les notions de base de la cryptographie.

II. Généralité sur la cryptographie

II.1. Définition de la cryptographie

La cryptographie est l'**art de chiffrer**, coder les messages est devenue 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. [1]

II.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.**

- **La confidentialité** : consiste à rendre l'information intelligible à d'autres personnes que les acteurs de la transaction.

- **L'intégrité** : vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication.
- **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.
- **Le non répudiation :** de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction. [2]

III. Chiffrement symétrique

III.1 Définition

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

Cette clé possède plusieurs appellations :

- Clé secrète
- Clé partagée

On parle de chiffrement conventionnel puisque c'est le premier chiffrement par clé à avoir été découvert et utilisé. [3]

III.2. Principe de fonctionnement

Le chiffrement symétrique se déroule sur les étapes suivantes :

- Génération de la clé secrète par Alice.
- Envoi de cette clé secrète à Bob, de manière sécurisée.
- Chiffrement du message par Alice, avec la clé secrète.
- Envoi de ce message chiffré à Bob.
- Réception du message chiffré par Bob.
- Déchiffrement du message avec la clé secrète reçue auparavant. [4]

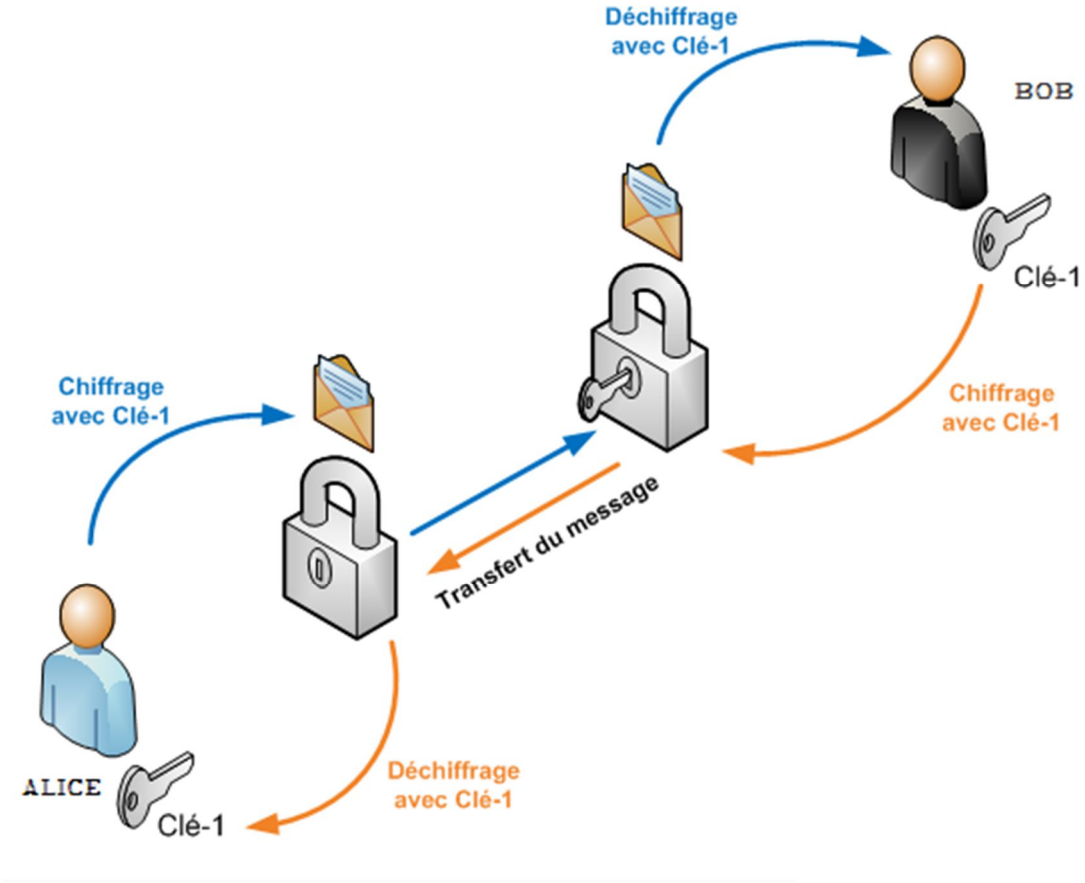

Figure 1- chiffrement symétrique

Il en est de même dans le sens inverse c'est-à-dire de Bob vers Alice.

IV. Cryptographie Asymétrique

IV.1. Définition

La cryptographie symétrique consiste à chiffrer puis déchiffrer un message en utilisant la même clé et le même algorithme.

La distribution des clés a été le point faible des systèmes de cryptographie symétrique, d'où la proposition des algorithmes à clés publiques (algorithmes asymétriques) La cryptographie asymétrique (à clés publiques) exige que chacun des correspondants possède une clé publiée dans un annuaire utilisée par tout le monde pour chiffrer des messages destinés à un individu particulier, et l'autre privée que cet individu est seul à détenir et qui lui permet de déchiffrer les messages qu'il reçoit. [5]

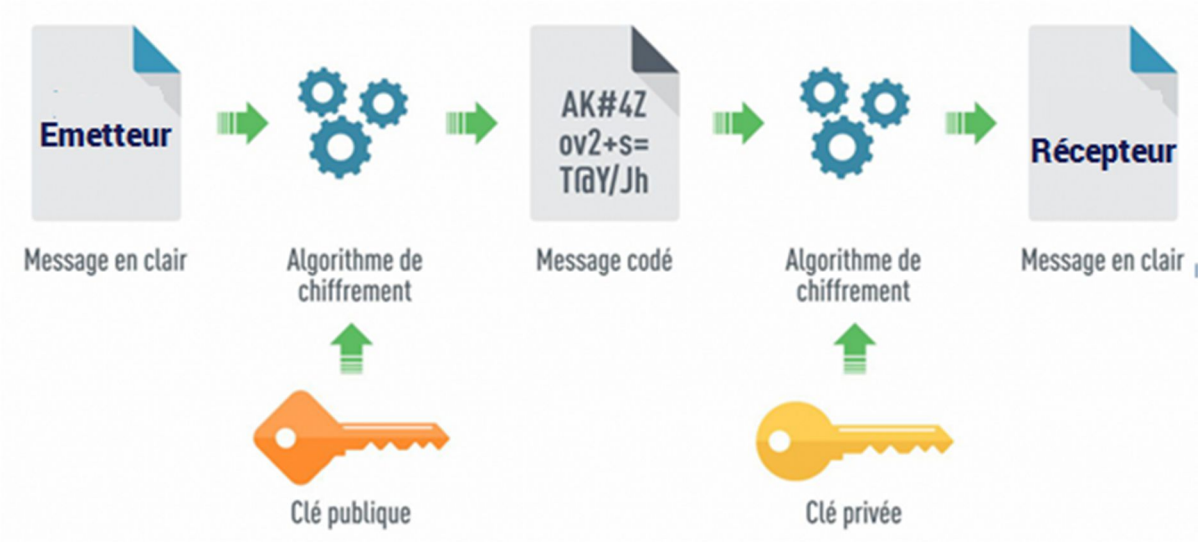

Figure 2 – Génération des clés.

IV.2. Principe du de fonctionnement

Le principe de chiffrement asymétrique (appelé aussi chiffrement à clés publiques) est apparu en 1976, avec la publication d'un ouvrage sur la cryptographie par Whitfield Diffie et Martin Hellman.

Dans un cryptosystème asymétrique (ou cryptosystème à clés publiques) les utilisateurs choisissent une clé aléatoire qu'ils sont seuls à connaître (il s'agit de la clé privée). A partir de cette clé, ils déduisent chacun automatiquement un algorithme (il s'agit de la clé publique). Donc les clés existent par paires (le terme de bi-clés est généralement employé). Les utilisateurs s'échangent cette clé publique au travers d'un canal non sécurisé.

Et voilà comment cela fonctionne :

- Un utilisateur écrit un message, et souhaite l'envoyer à un destinataire en s'assurant qu'aucun intermédiaire ne puisse le lire.
- Cet utilisateur comme le destinataire possèdent tous deux une paire de clés, et chacun connait la clé publique de l'autre.
- Afin de chiffrer un message pour le destinataire, l'utilisateur va alors utiliser la clé publique du destinataire.
- Cette clé active un algorithme, et le message écrit est alors transformé en texte incompréhensible, qui peut alors être envoyé au destinataire.

Du côté du destinataire maintenant :

- Lorsqu'il reçoit le message chiffré, le destinataire devra utiliser sa propre clé privée, celle que lui seul détient, afin d'activer l'algorithme pour le déchiffrer.
- Ainsi, même si quelqu'un intercepte le message en chemin, il ne pourra pas le déchiffrer, puisqu'il ne dispose pas de la clé privée du destinataire !

Voici le schéma équivalent :

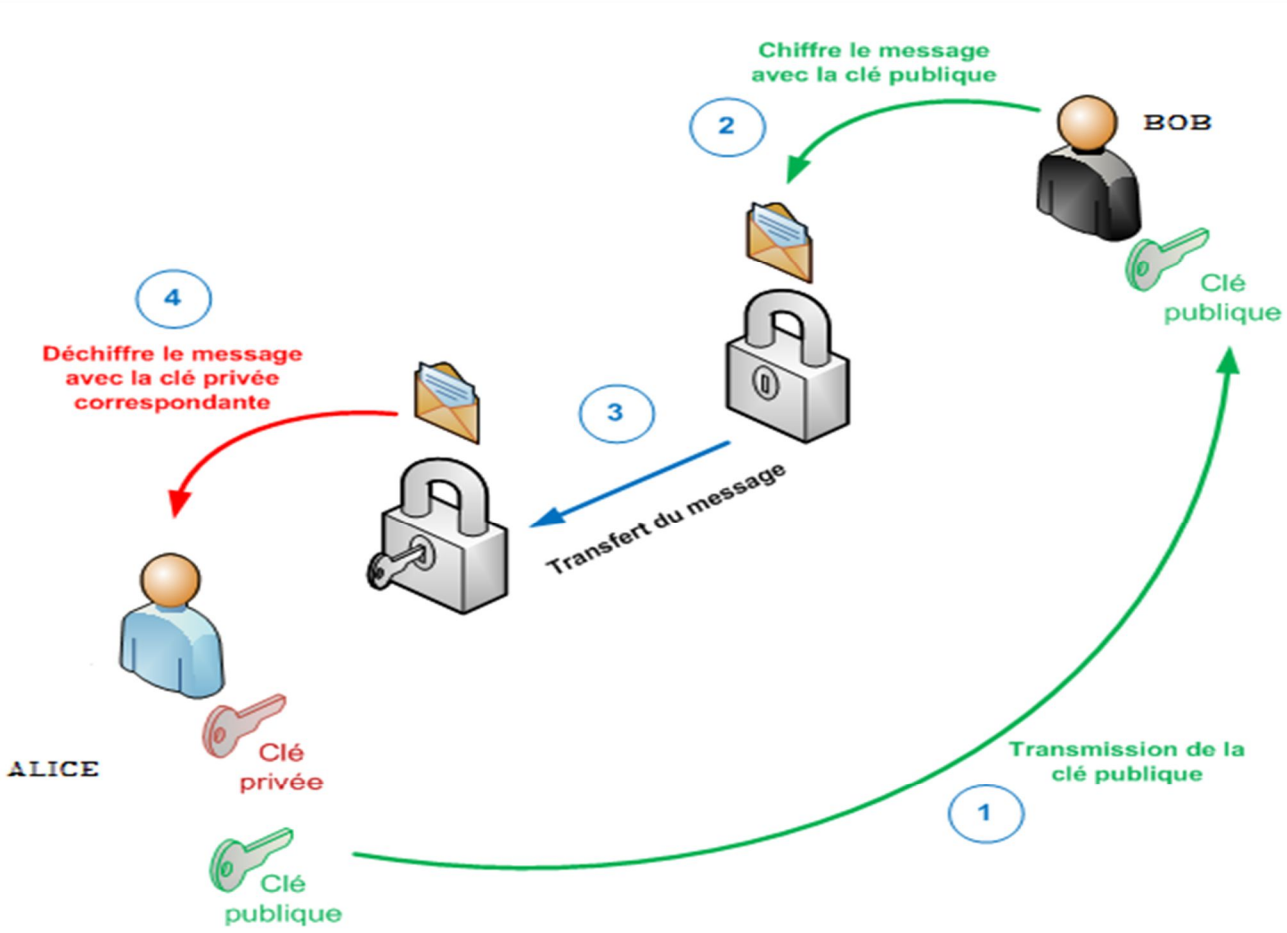

Figure 3- chiffrement asymétrique.

V. Le chiffrement RSA

En 1976, Diffie et Hellman suggérèrent la possibilité d'assurer la confidentialité sans recourir à un secret partagé, au moyen d'une clé connue de tous. Cette idée a profondément transformé la cryptographie. Le système de chiffrement à clé publique RSA, proposé en 1977

par Rivest, Shamir et Alemany, est maintenant couramment utilisé par les systèmes de chiffrement, par exemple par PGP, généralement en complément d'un chiffrement à clé secrète à usage unique. Le développement du commerce électronique et l'irruption de l'Internet dans la vie privée ont entraîné une large diffusion des outils cryptographiques, longtemps réservés à des usages militaires. L'exponentielle modulaire intervient dans les algorithmes de la cryptographie à clé publique, car elle est considérablement plus facile à calculer que son inverse, le logarithme modulaire.

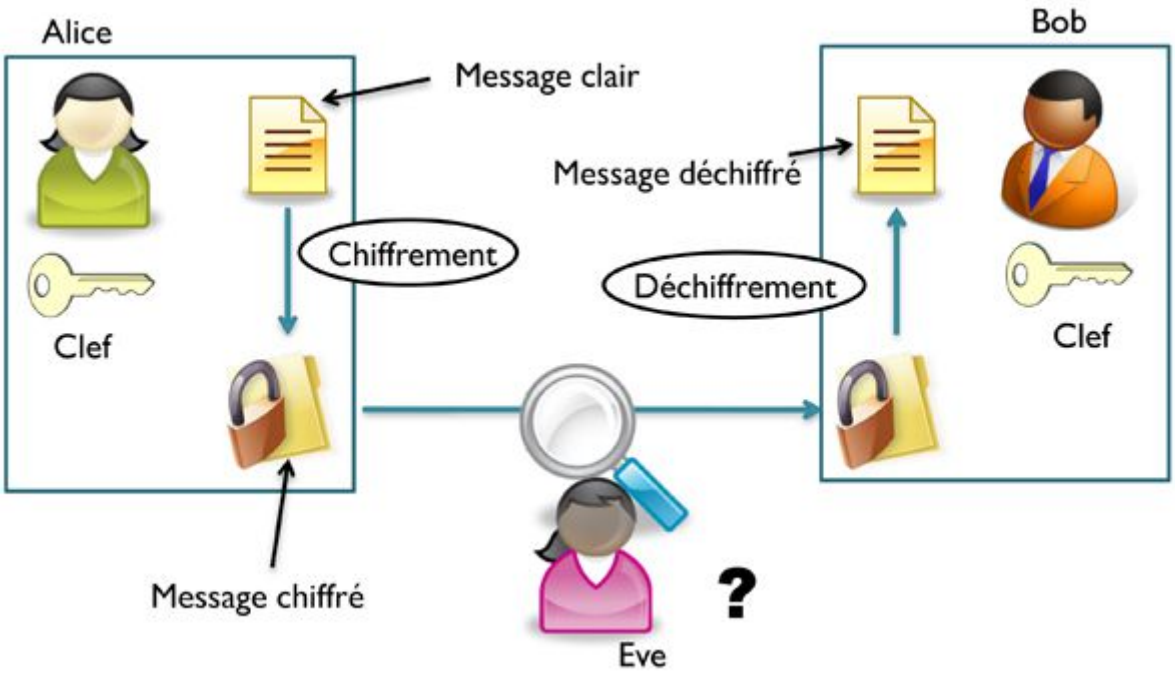

Figure 4- chiffrement RSA

Pour construire ses clés, chaque utilisateur de RSA

- choisit deux grands nombres premiers **p** et **q** ;
- Calcule **n=p. q** ;
- choisit un entier **e<n** qui est premier avec **(p-1)(q-1)** ;
- calcule l'inverse d de e modulo **(p-1)(q-1)** ;
- publie sa clé publique, qui est formée des deux entiers **e** et **n** ;
- conserve sa clé privée **d** ;
- détruit les entiers **p** et **q** qui ne doivent pas être divulgués.

Les fonctions de chiffrage et de déchiffrage sont respectivement :

$$C(m) = m^e mo\ d_n \quad \text{..... (3)}$$

$$C(m) = m^d mo\ d_n \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \textbf{(4)}$$

- ✓ Les fonctions et paramètres d'un utilisateur **A** sont notésC_A , D_A,n_A, e_A, d_A.
- ✓ La fonction de chiffrage C_A est connue de tous, tandis que la fonction de déchiffrage D_An'est connue que de **A**.

Soient **A** et **B** deux utilisateurs de RSA. Quand A veut communiquer confidentiellement un entier **m** (0<m<n) à **B**, il calcule C_B**(m)** à l'aide de la clé publique de **B**, qu'il envoie à **B** ; à la réception d'un message chiffré **c**.

B calculeD_B**(c)** à l'aide de sa clé privée. Il s'agit bien d'un déchiffrage car :

$$D_B\big(C_B(m)\big) = C_B(m)^{d_B} \textbf{mo}\ dn_B = m^{e_B\, d_B}\ \textbf{mo}\ d_n = m \ldots\ldots\ldots\ldots\ldots\ldots \textbf{(6)}$$

Grâce au théorème d'Euler qui assure que :

$$m^{\emptyset(n)} = \textbf{1mo d}\, n \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \textbf{(5)}$$

La sécurité de ce schéma provient de la difficulté à factoriser de grands entiers. En effet, déterminer **d** à partir de **e** demande la connaissance de **(p-1) (q-1)** ; or la publication de **n=p. q** n'est en aucune façon une aide pour calculer **(p-1) (q-1)**, qui ne peut être obtenu qu'à partir de **p** et **q**. D'autre part, on ne sait pas calculer efficacement des racines e-ièmes, ce qui permettrait d'avoir le texte clair m à partir du texte chiffré C**(m)**. Contrairement à la plupart des autres problèmes, pour lesquels on cherche des algorithmes efficaces, le chiffrement n'est utile que si le problème de déchiffrement est difficile, c'est-à-dire que si tous les algorithmes que l'on peut proposer sont extrêmement inefficaces.

La méthode RSA est également employée pour l'authentification des données.

Si **A** veut communiquer un entier **m (0<m<n)** à **B** et garantir à **B** qu'il est l'auteur de ce message, il joint à m sa signature **s=** C_A**(h(m)) …… (7)** grâce à sa clé privée et à une fonction de hachage **h** publique (cela est détaillé dans la partie suivante).

Recevant **m** et **s** de la part de **A**, **B** calcule à la fois C_A**(s)** grâce à la clé publique de **A** et ; normalement, $C_A(s) = C_A(D_A(h(m))) = h(m)$ **……. (8)** par le même théorème d'Euler ; donc si **B** obtient le même nombre par deux calculs, le message est authentifié ; sinon, c'est que **A** n'en est pas l'auteur, ou bien que **m** a été altéré au cours de la transmission. La sécurité de ce schéma d'authentification repose sur la difficulté, étant donné **h**, à trouver **m** tel que **h(m)=h.** [3]

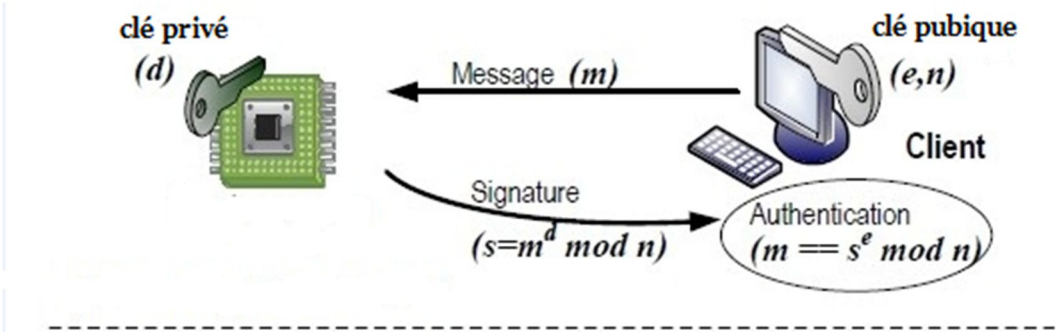

Figure 5 - Authentification par signature électronique.

VI. Fonction de Hachage

VI.1. Définition

Les fonctions de hachages sont des fonctions à sens uniques « sans collision », générant une sortie de taille fixe (appelée condensat ou empreinte), caractéristique 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. [6]

Une fonction de hachage cryptographique idéale possède les quatre propriétés suivantes :

- ✓ La valeur de hachage d'un message se calcule « très rapidement » ;
- ✓ Il est par définition, impossible, pour une valeur de hachage donnée, de construire un message ayant cette valeur de hachage ;
- ✓ Il est par définition, impossible de modifier un message sans changer sa valeur de hachage ;
- ✓ Il est par définition, impossible de trouver deux messages différents ayant la même valeur de hachage. [5]

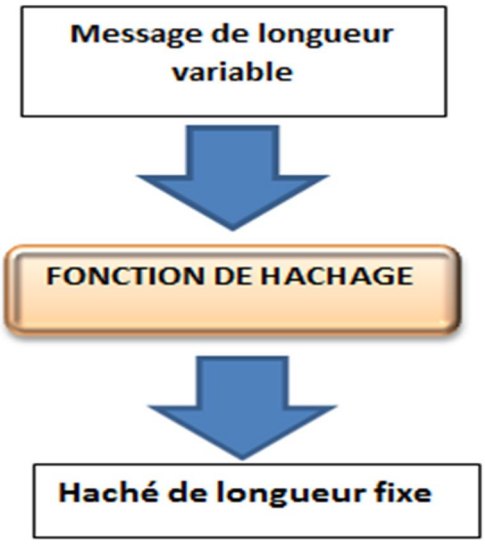

Figure 6- principe de hachage.

La fonction de hachage est dite aussi une fonction de contraction, digest, empreinte digital, "hash code"...

En général, t>n si bien que cette fonction est surjective et l'on parle alors de collision entre des entrées $\boldsymbol{x}$ et$\boldsymbol{x'}$.

$$\begin{cases} \boldsymbol{x} \neq \boldsymbol{x'} \\ \boldsymbol{H(x)} = \boldsymbol{H(x')} \end{cases} \text{ ..... (9)}$$

Si $\boldsymbol{y}$est tel que $\boldsymbol{y} = \boldsymbol{H(x)}$..... **(10)**,

Alors$\boldsymbol{x}$ est appelé la préimage de $\boldsymbol{y}$.

VI.2. Propriété de base d'une fonction de hachage

Les propriétés de base d'une fonction de hachage sont la compression et la facilité de calcul. Elle peut également bénéficier des additionnelles suivantes

- ✓ résistance à la préimage : étant donnéy, il est calcul aléatoirement difficile de trouver un x tel que $y = H(x)$.
- ✓ résistance à la seconde préimage : étant donné x , il est calcul aléatoirement difficile de trouver $\boldsymbol{x'} \neq \boldsymbol{x}$ tel que$\boldsymbol{H(x)} = \boldsymbol{H(x')}$.

- ✓ résistance à la collision : il est calcul aléatoirement difficile de trouver x et x' tels que $(x) = H(x')$.

Une fonction est dite « sans collision » ou « injective » lorsqu'il est réputé très difficile de trouver deux sources différentes conduisant à un même résultat.

- ✓ **F** à collision faible donc il est difficile de créer un message m significatif tel que **f(m) = K**
- ✓ **F** à collision forte donc il est difficile de trouver **m** et **m'** significatifs tels que **f(m) = f(m').** [7]

VI.3. Utilisations en cryptographie

Les fonctions de hachage sont utilisées par des nombreux systèmes cryptographiques, à la fois en cryptographie symétrique et en cryptographie asymétrique. Elles en ont hérité le surnom de "couteau suisse" de la cryptographie.

Les fonctions de hachage permettent entre-autres, grâce au calcul du condensat d'un document et la comparaison de celui-ci avec sa valeur initiale, de :

- Contrôler l'intégrité d'un document.
- Comparer un mot de passe entré par un utilisateur à un mot de passe stocké dans une base de données.
- Publier l'empreinte d'un logiciel : pour comparer l'empreinte fournie par l'éditeur et l'empreinte qu'il obtient sur le fichier téléchargé.
- Vérifier l'intégrité d'un message de son point d'envoi jusqu'au destinataire.

VI.4. Classification fonctionnelle

A. Une fonction de hachage sans clef

C'est une fonction de hachage à sens unique qui peut être calculée sans connaissance d'un secret (par n'importe qui) -. Exemple type : MD4, MD5, SHA etc...

Elle est aussi appelée modification détection code (MDC). On peut s'en servir pour s'assurer de l'intégrité d'un message.).

B. Une fonction de hachage avec clef

C'est une fonction de hachage à sens unique qui ne peut être calculée que par une entité détentrice de la clé. Nombreux exemples de fonctions de hachage à sens unique avec clé déduites de méthodes de cryptographie.

Elle est aussi appelée message authentiquassions code (MAC). Elle a un paramètre additionnel (la clef) qui permet de vérifier l'intégrité et la provenance du message en même temps. [7]

VI.5. MD5

MD5 est une fonction de hachage inventée par Ronald Rivest en 1991. Une fonction de hachage permet de calculer une empreinte de toute donnée numérique (allant d'une simple chaîne de caractères à un fichier de plusieurs giga octets). L'empreinte générée est d'une longueur de 128octets (soit 32 caractères). MD5 est sensée être irréversible, c'est-à-dire qu'il est impossible de retrouver la séquence originelle d'après l'empreinte produite. Cette dernière est aussi unique ; une chaîne de caractère ne possède qu'une seule empreinte MD5.

L'utilitaire md5sum permet de calculer ce qu'on appelle l'empreinte d'un fichier. En anglais, finger-print, message-digest ou encore checksum est une valeur de 128 bits correspondant à une somme de contrôle calculée à partir de l'archive. Cette signature est unique pour chaque fichier et il est pour le moment non-craqué

Un checksum MD5 n'a pas pour but de garantir la provenance d'un fichier ou d'un groupe de fichiers. Son intérêt est de permettre la vérification de l'intégrité des données récupérées. En effet, nul n'est à l'abri d'une perturbation ou d'un problème réseau ayant pour conséquence la corruption d'une archive en cours de téléchargement.

En gros, en comparant le MD5 du fichier que vous venez de récupérer au MD5 que le site de téléchargement vous donne, vous pouvez être sûr que le site et vous ayez le même fichier.

On peut donc assurer que le fichier est bien "entier" ou qu'il n'a pas été modifié par un tiers dans un but mal intentionné [Rc5]

VI.6. SHA

SHA-0 est créé par la NSA en 1993. Suite à de premières rapides découvertes de vulnérabilités dans cette fonction, la NSA publie SHA-1 en 1995, très similaire mais complexifié. Les utilisations des fonctions de la famille SHA sont les mêmes que pour MD5.

Comme toute solution cryptographique, le SHA se doit d'évoluer en même temps que les capacités de calcul de nos ordinateurs et éviter de devenir vulnérable.

Il existe donc plusieurs versions de SHA : SHA0 (obsolète puisque totalement vulnérable), SHA1 (actuellement le plus utilisé), SHA2 (qui nous intéresse) et enfin le tout dernier SHA3 né en 2012.

Pour installer un certificat SHA256 sur un client (authentification forte par certificat), il faut donc s'assurer que le client (navigateurs, webservices, ...) et les serveurs sont compatibles, même si le serveur continue à utiliser un certificat signé en SHA1 / MD5.

Pour installer un certificat SHA256 sur le serveur, alors tous les clients qui se connectent (navigateurs, clients mails, webservices, ...) et le serveur doivent être compatibles avec l'algorithme de hachage SHA256.

Pour utiliser un certificat SHA256 pour la signature d'emails ou de documents seuls les outils de lecture du mail ou du document doivent être compatibles. [Rc5]

VII. Signature numérique

VII.1. Définition

Comme la signature manuscrite, la signature électronique est un terme générique qui indique tout simplement un mécanisme permettant de lier un document à un signataire. Dans les deux cas, les signatures peuvent être vérifiées publiquement. Donc elle permet de garantir l'intégrité d'un document électronique une fois signé 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, notamment en utilisant le format RSA. [2]

VII.2. Principe de signature

1. Lorsque on clique "signer", une empreinte numérique unique se crée (appelée un hachage) grâce à un algorithme mathématique. Ce hachage est spécifique à ce document, 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.

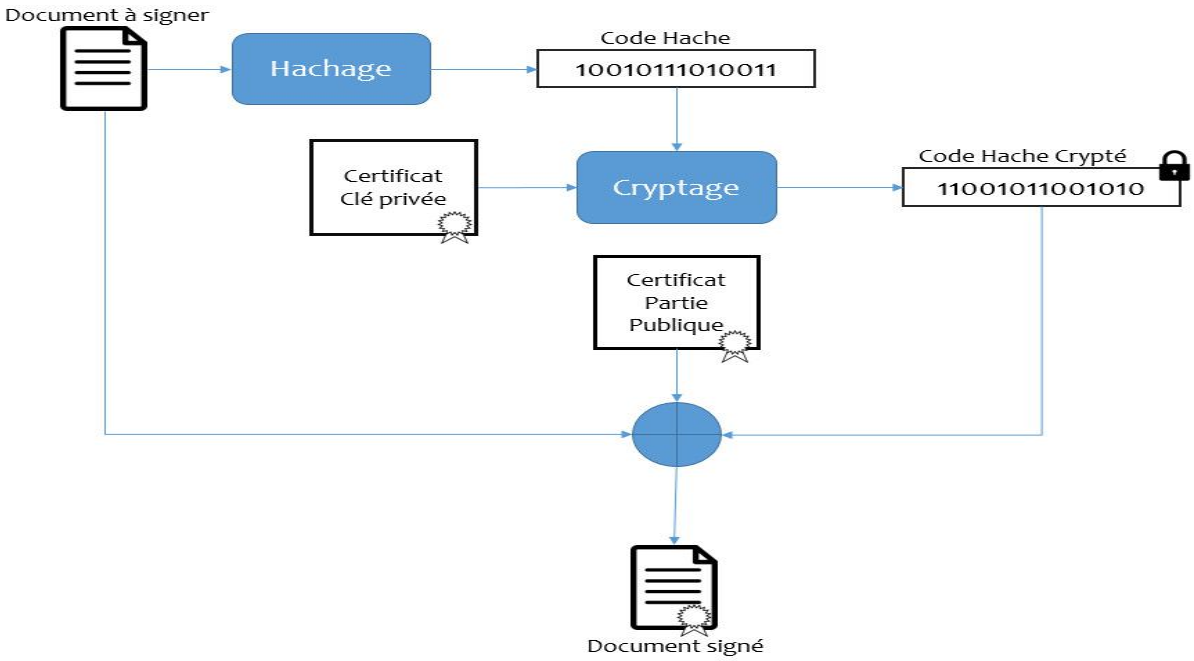

Figure 7 - signature numérique.

VII.3 Vérification de la signature

1. Lorsque 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.

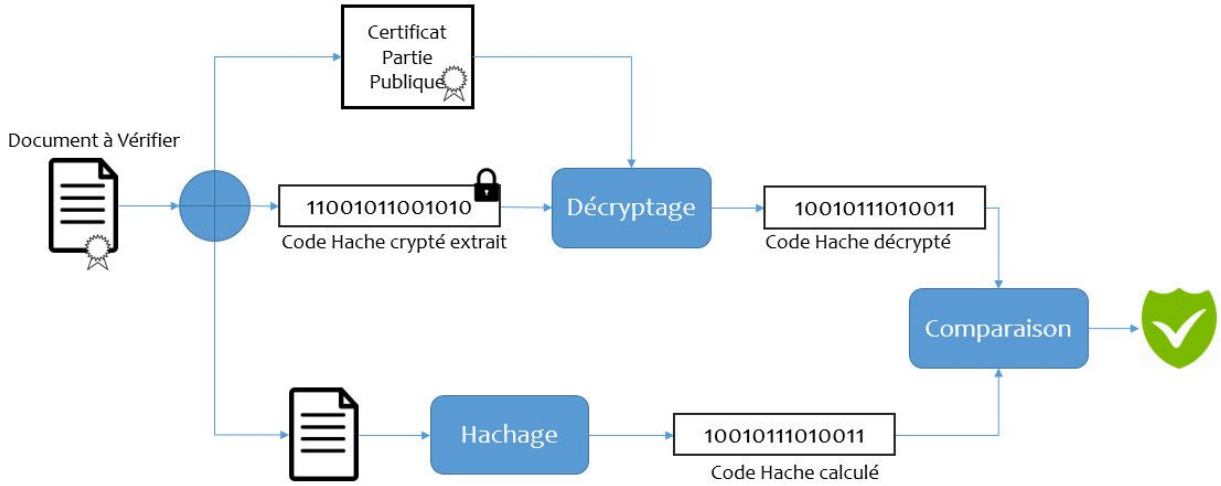

Figure 8 - vérification de la signature.

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.

VIII. Certificat numérique

VIII.1. Problem de Man in the middle

Jusque-là, nous avions toujours supposé que la clé publique est distribuée d'une manière sécurisée. Si cette hypothèse n'est pas vérifiée, un schéma asymétrique peut subir une attaque de type "Man in the Middle". Une telle attaque est illustrée dans le scénario ci-après.

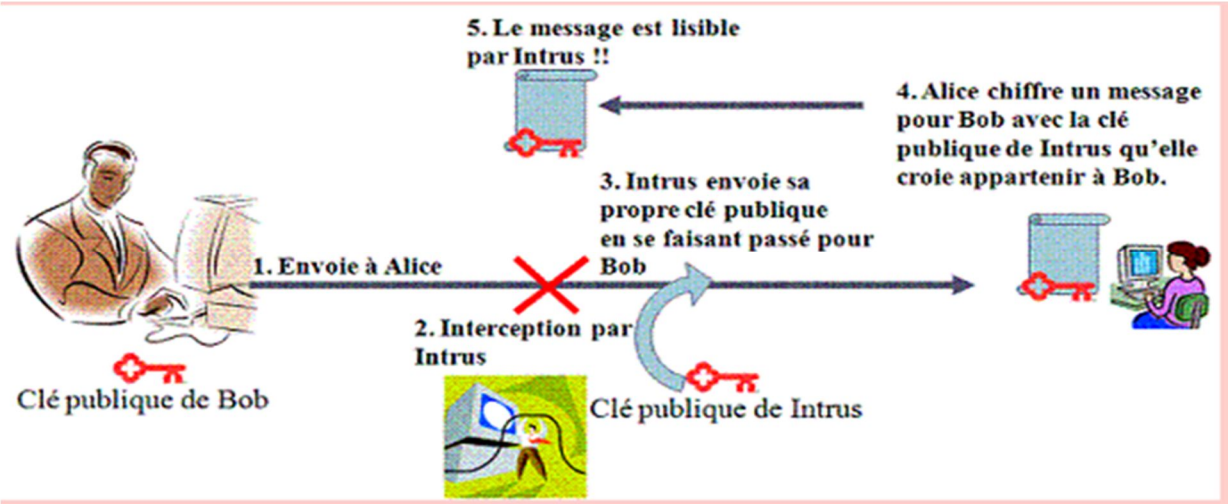

Figure 9 - Man in the middle.

VIII.2. Certificat numérique

La solution au problème dit "man in the middle" est l'usage d'un certificat numérique qui assure la liaison entre l'identité et la clé publique correspondante dans un document numérique signé par une tierce partie de confiance dite autorité de certification. C'est dans ce contexte que la NIST (National Institute of Stantards and Technology) s'est vu imposer en 1994 la tâche d'étudier et de définir un standard afin de gérer l'authentification dans un environnement international. [5]

Pour obtenir un certificat numérique, le client doit effectuer une requête auprès d'un organisme reconnu. Il transmet avec sa requête sa clef publique. L'organisme construit un certificat incorporant la clef publique du client, il signe le certificat à l'aide de sa clef privée. L'autorité de certification publiera le certificat signé comportant la clef publique et l'identité précise du propriétaire, quiconque consultera ce certificat aura l'assurance dans l'authenticité de la clef publique contenue dans celui-ci car il a confiance dans l'autorité de certification qui a délivré ce certificat.

VIII.3 Structure d'un certificat X.509

- Version
- Numéro de série
- Algorithme de signature du certificat
- Signataire du certificat
- Validité (dates limite)
- Pas avant

- Pas après
- Détenteur du certificat
- Informations sur la clé publique
- Algorithme de la clé publique
- Clé publique
- Identifiant unique du signataire (Facultatif)
- Identifiant unique du détenteur du certificat (Facultatif)
- Extensions (Facultatif)
- Liste des extensions...

IX. PKI (Infrastructure à clés publiques)

IX.1. Définition

PKI (Public Key Infrastructure) : est un système de gestion des clefs publiques qui permet de gérer des listes 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 que lors d'échanges d'information avec l'extérieur. [3]

IX.2. Fonctionnalités d'une PKI

IX. 2.1. Création d'une paire de clés et demande de certificat

Anne crée une paire clé publique/clé privée avec un algorithme tel que RSA. Elle crée ensuite une demande de certification (un certificat qui n'est pas encore signé). Le certificat contient des informations sur son identité, ainsi que la clé publique de Anne.

IX.2.2. Signature du certificat

Anne envoie son certificat à une autorité d'enregistrement (RA pour Registration Authority). Cette autorité approuve ou désapprouve la certification. Si elle est approuvée, le certificat est envoyé à l'autorité de certification (CA). Le résultat — le certificat signé — est retourné à Alice et stockée sur le serveur de la CA.

Anne peut alors annoncer que sa clé publique est certifiée.

IX.2.3. Chaîne de certification

Bernard, qui veut communiquer avec Anne, lui demande son certificat. Afin de vérifier le certificat, Bernard recherche la clé publique de l'autorité qui a signé le certificat de Anne. Si la

clé et le certificat sont chez la même autorité, la recherche est terminée. Sinon, Bernard demande à l'autorité de certification de contacter l'autre autorité pour obtenir sa clé publique. Pour chaque autorité de certification interrogée par Bernard, il doit disposer de la clé publique de l'autorité précédente. Si une chaîne peut être trouvée, aboutissant à l'autre autorité de certification, la recherche est terminée.

IX.2.4. 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 partir 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.

IX.3. La gestion des clefs

La gestion des clefs 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 clefs plutôt que de casser un algorithme. Et le moment le plus propice pour espérer se procurer les clefs est sans conteste le moment où l'échange des clefs a lieu. C'est pourquoi, l'échange des clefs 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 clefs doivent être générées de manière aléatoirement.
- **Distribution :** La distribution est l'action de déplacer une clef de cryptage. Un exemple de distribution est la clef de session.
- **Stockage :** La clef doit être protégée et doit garder à tout prix son intégrité et sa confidentialité.
- **Suppression :** La suppression de clefs intervient quand la clef à atteint sa fin de validité ou lorsqu'un doute subsiste sur sa confidentialité. La suppression signifie la destruction des toutes les copies de la clef symétrique ou de la clef publique.

- **Archivage :** L'archivage des clefs permet de conserver une copie des clefs même si elles ne sont plus utilisées, une clef archivée ne peut pas être remise en service dans un environnement d'application.
- **Recouvrement :** Le recouvrement des clefs est une procédure délicate qui permet de retrouver la clef privée d'un client. Par exemple lorsqu'un utilisateur a perdu sa clef privée. Ce principe permet aussi le recouvrement des données chiffrées par cette clef. [5]

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

IX.4. Infrastructure de gestion de privilèges (PMI)

Beaucoup de systèmes se contentent de vérifier l'identité de l'interlocuteur au moyen de certificats et cela est suffisant.

Cependant, de plus en plus de systèmes ont besoin d'une gestion plus fine du contrôle d'accès : rule-based, role-based ou rank-based. Pour prendre des décisions, ces systèmes ont besoin d'informations complémentaires qui ne sont pas véhiculées par le certificat. Les certificats d'attributs (AC pour Attribut Certifiâtes) ont été créés à cette fin.

Ces sont des structures des données signées qui permettent d'ajouter des références vers un ou plusieurs certificats spécifiques lorsque le sujet dispose de différentes identités sur le même certificat. De plus, un AC peut être créé de telle manière qu'il ne puisse être utilisé que par un destinataire spécifique.

Les utilisateurs de PMI doivent être assurés non seulement que la clé publique est bien celle de l'interlocuteur (gestion normale des certificats), mais ils doivent aussi être sûr que leur interlocuteur à le droit de posséder tel ou tel attribut. [3]

IX.5. L'approche de PKIX

PKIX utilise les termes de PKI et de PMI. Les deux peuvent paraître similaires, mais il existe une différence essentielle : une PKI gère des certificats sur des clés publiques, tandis qu'une PMI gère des certificats sur des attributs.

Une bonne métaphore est le cas d'une personne possédant un passeport et un visa : le premier concerne son identité tandis que le second lui accorde des droits. [20]

IX.6. Acteur 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 a 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 disponible aux utilisateurs. [Rc3]

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

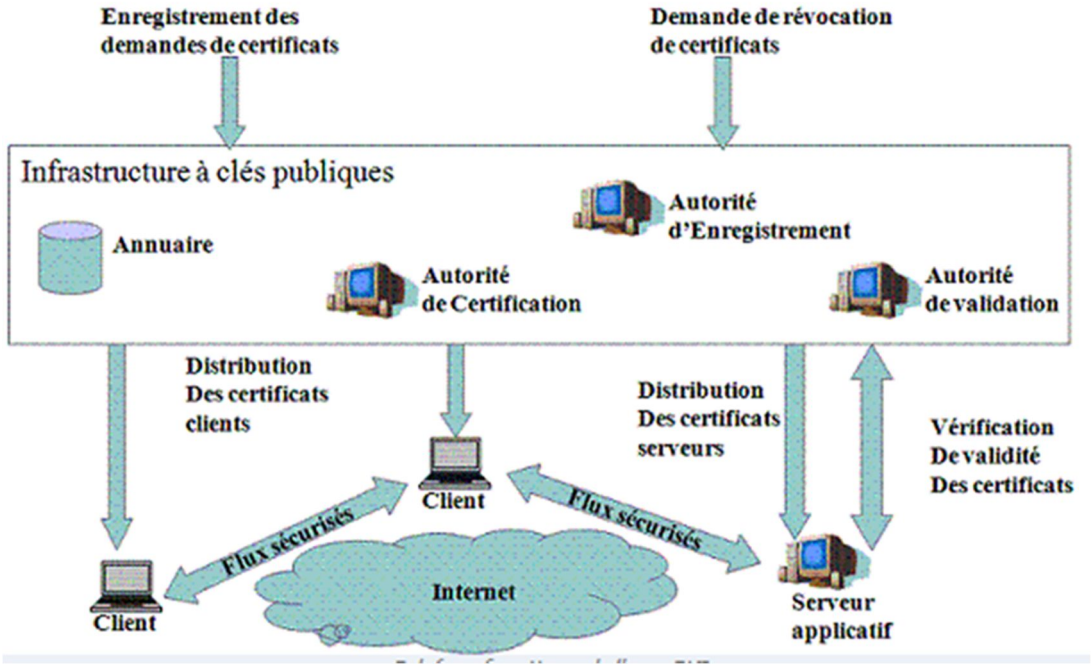

Figure 10-composantes PKI

X. Conclusion

Ce chapitre a présenté une introduction aux cryptosystème qui est basé sur plusieurs méthodes de chiffrements. Aujourd'hui, les algorithmes de chiffrement sont universellement répondus.

Le but traditionnel de la cryptographie est d'élaborer des méthodes permettant d'échanger des données de manière sécurisée. C'est pour ça la cryptographie moderne s'attaque en fait plus généralement aux problèmes de sécurité des communications.

Les systèmes de cryptographie Symétrique et Asymétrique permettent donc de s'assurer à la fois de certain nombre de sécurité de base : Confidentialité, Intégrité et Authentification des données transmises, ainsi que l'authentification des tiers et la Non répudiation. Toutefois la mise en œuvre des algorithmes de cryptage, de signature et de vérification allonge considérablement la longueur du message signé. On contourne alors cette difficulté à l'aide 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

Chapitre 2

Blockchain

I. Introduction

La protection des données sur internet a toujours été un sujet qui a affolé la toile : il ne se passe pas une journée sans que les médias nous parlent de piratage de coordonnées bancaires ou de géant du e-commerce qui se font hacker. C'est pourquoi les chercheurs se concentrent aujourd'hui sur les technologies de cryptage et de sécurisation des données comme la blockchain.

II. 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. Envoyer 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 l'utilisation d'une signature numérique. Pour assurer la confiance dans le grand livre, les participants du réseau ont exécuté des algorithmes compliqués pour vérifier ces signatures numériques et ajouter des transactions à la chaîne de blocs. [21]

Les prochaines années pour le bitcoin ont été tumultueuses, y compris l'effondrement de l'échange de bitcoin de premier plan, Mt. Gox, et une réputation de plus en plus aigrie comme la monnaie alimentant le bazar de drogue en ligne souterrain Silk Road.

Mais beaucoup d'entreprises ont vu une opportunité dans la technologie sous-jacente - la blockchain - qui a rendu possible l'existence de bitcoin.

III. Définition

Une blockchain, ou chaîne des blocs, est une technologie de stockage et de transmission d'informations sans organe de contrôle. Techniquement, il s'agit d'une base de données distribuée dont les informations envoyées par les utilisateurs et les liens internes à la base sont vérifiés et groupés à intervalles de temps réguliers en blocs, l'ensemble étant sécurisé par cryptographie, et formant ainsi une chaîne. Par extension, une chaîne de blocs est une base de données distribuée qui gère une liste d'enregistrements protégés contre la falsification ou la

modification par les nœuds de stockage. Une blockchain est donc un registre distribué et sécurisé de toutes les transactions effectuées depuis le démarrage du système réparti.

Une analogie avec l'Internet (TCP/IP) peut être dressée, car il s'agit dans les deux cas de protocoles informatiques sous-jacents à une infrastructure décentralisée. Internet transfère des paquets de données d'un point A à un point B, alors que la blockchain permet à la « confiance » de s'établir entre des agents distincts du système [22]

Voici le principe général d'une blockchain :

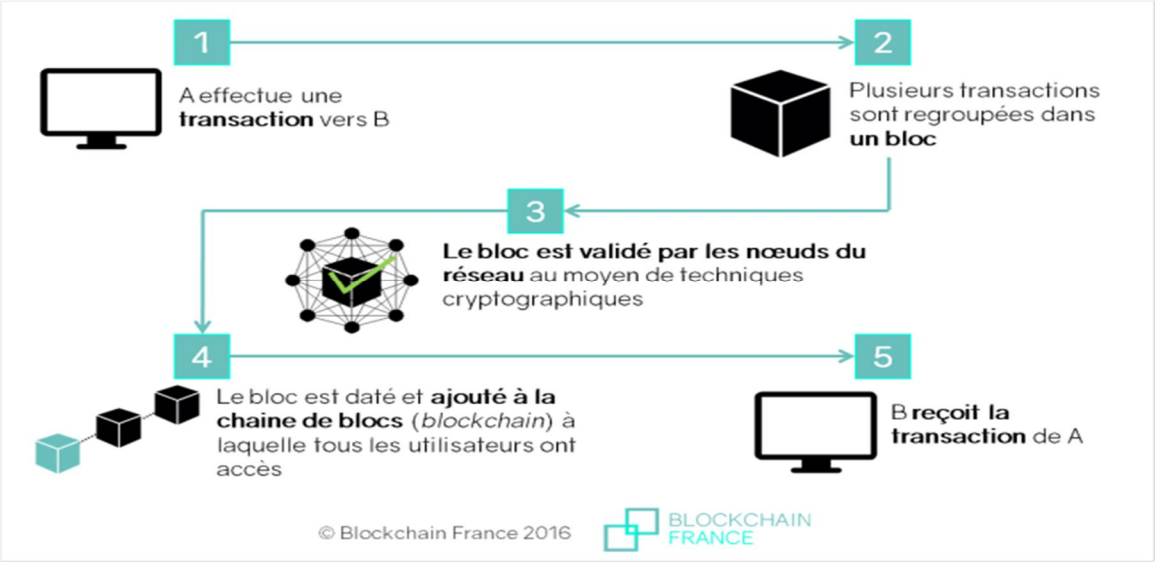

Figure 11- Application blockchain

Une blockchain présente plusieurs intérêts majeurs :

- **Elle est transparente :** bien que les échanges demeurent anonymes, n'importe qui peut les consulter.
- **Elle est sécurisée :** les transactions sont infalsifiables et sécurisées par des protocoles basés sur la cryptographie asymétrique.
- **Elle est 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.

IV. Fonctionnement

La transparence de ce système repose sur le fait que tous les échanges effectués entre les utilisateurs depuis la création de la chaîne y sont inscrits.

Ils y sont enregistrés sous forme de "blocs de transactions" qui, mis bout à bout, forment une "chaîne"... D'où le nom de "chaîne de blocs" ou blockchain en anglais !

Les transactions effectuées entre les utilisateurs du réseau sont regroupées en blocs. Chaque bloc est validé par les nœuds du réseau ou "mineurs", quand il y a une preuve de travail (qui consiste, dans le cas du bitcoin, en la résolution de problèmes algorithmiques).

Les "mineurs" chargés de vérifier la validité des transactions bloc par bloc sont des particuliers, qui sont rémunérés pour mettre à disposition la puissance de calcul de leurs processeurs. [22]

Les problèmes mathématiques que ces ordinateurs doivent résoudre sont si complexes que les mineurs se sont regroupés et que de gigantesques fermes d'ordinateurs ont été créées.

Le fonctionnement d'une transaction peut schématiquement être décrit en 5 étapes :

1. A effectue une transaction vers B.
2. Plusieurs transactions sont regroupées dans un bloc.
3. Le bloc est validé par les nœuds du réseau au moyen de techniques cryptographiques.
4. Quand le bloc est validé, il est daté et ajouté à la chaîne de blocs à laquelle tous les utilisateurs ont accès.
5. B reçoit la transaction de A.

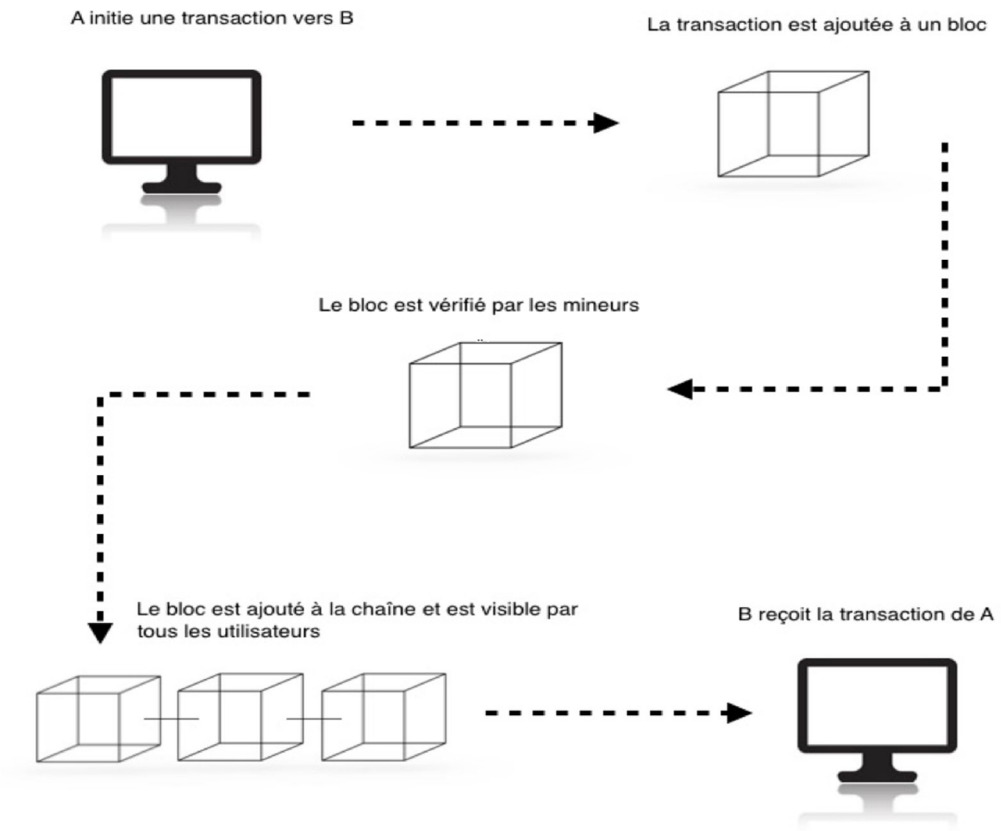

Figure 12-Echange de transaction

V. Le système blockchain

Pour faire partie d'un système blockchain, les entités participantes installent et exécutent chacune un logiciel qui connecte leur ordinateur ou leur serveur à d'autres participants du réseau. En exécutant ce logiciel, les participants agissent comme des validateurs individuels, appelés nœuds de réseau.

Lorsqu'un nœud se connecte au réseau pour la première fois, il télécharge une copie complète de la base de données blockchain sur son ordinateur ou son serveur

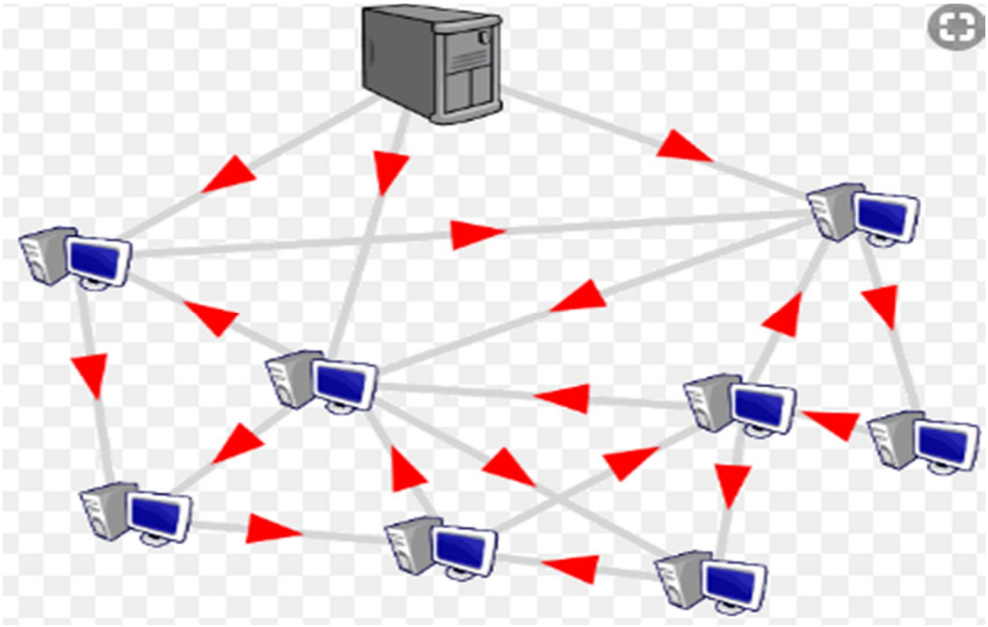

Figure 13-Base de données blockchain.

Le réseau de nœuds gère la base de données, également appelée blockchain. Les nœuds sont des points d'entrée pour de nouvelles données, ainsi que la validation et la propagation de nouvelles données qui ont été soumises à la blockchain.

Figure 14 -le réseau des nœuds.

Mais dans un système distribué sans source de vérité en or, comment le réseau parvient-il à un consensus ou se met-il d'accord sur les données à écrire sur la blockchain ? Comment résoudre une situation où des personnes équivalentes peuvent dire des choses confuses, mais il n'y a pas de chef à arbitrer ? La réponse - en utilisant des protocoles. Dans un système de blockchain, il y aura un protocole, c'est-à-dire des règles pré-convenues pour la validité technique et commerciale des données à écrire, et une règle pour déterminer comment un consensus est atteint

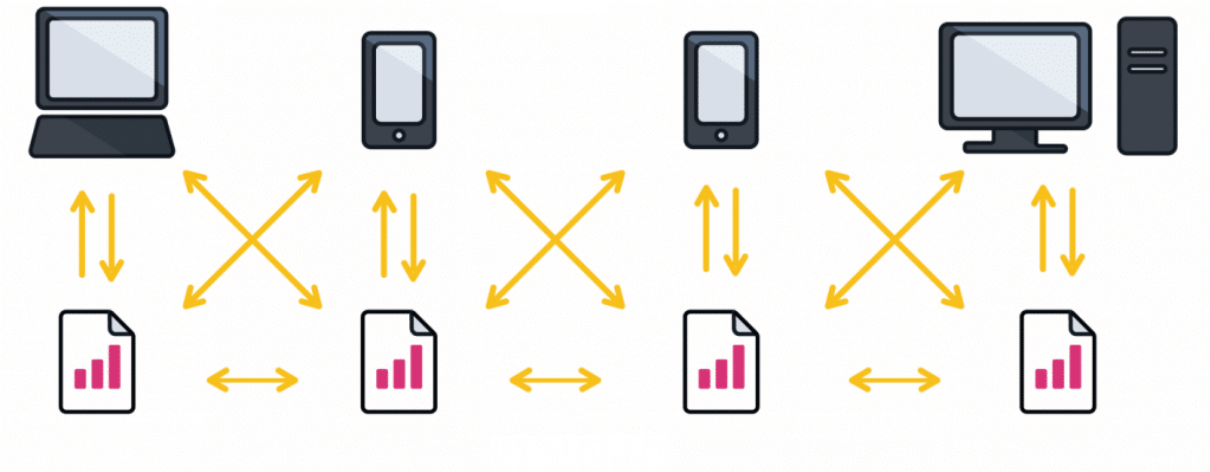

Figure 15- le réseau des nœuds.

Un bloc est créé en regroupant des transactions similaires. Ces blocs sont ajoutés dans l'ordre chronologique, d'une manière qui ressemble à une chaîne, d'où le nom blockchain. Les nœuds stockent ensuite ces nouveaux blocs sur la base de données blockchain locale sur leur ordinateur ou serveur [9]

VI. Type de blockchain

Il existe 3 types de Blockchain

- **Les blockchains publiques :** Ouvertes et accessibles à tous, tout le monde peut y effectuer ou vérifier des transactions.
- **Les blockchains privées :** Ces dernières sont exécutées sur un réseau privé et les nœuds (utilisateurs) du réseau doivent avoir une autorisation pour y accéder. Elles sont principalement utilisées pour expérimenter la technologie. On peut également retrouver des blockchains privées au sein d'entreprises pour faire communiquer différents systèmes

d'information. De nombreux tutoriels existent pour les développeurs, afin de mettre en place leur propre blockchain privée et appréhender la technologie.

- **Les consortiums :** Il s'agit d'une blockchain hybride : certains nœuds peuvent être rendus publiques, tandis que d'autres restent privés pour les actions sensibles. C'est donc une blockchain avec des accès gérés par une partie des acteurs, qui convient aux contextes réglementés comme les banques ou assureurs. [8]

VII. Composition d'une blockchain

Comme indiqué précédemment, une blockchain est une chaîne de blocs contenant 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.
- ✓ Un hash servant à identifier le bloc.
- ✓ Le hash du bloc précédent.
- ✓ Un timestamp.
- ✓ Un ensemble de transactions.

Le premier bloc d'une blockchain est appelé le "Genesis Block". [21]

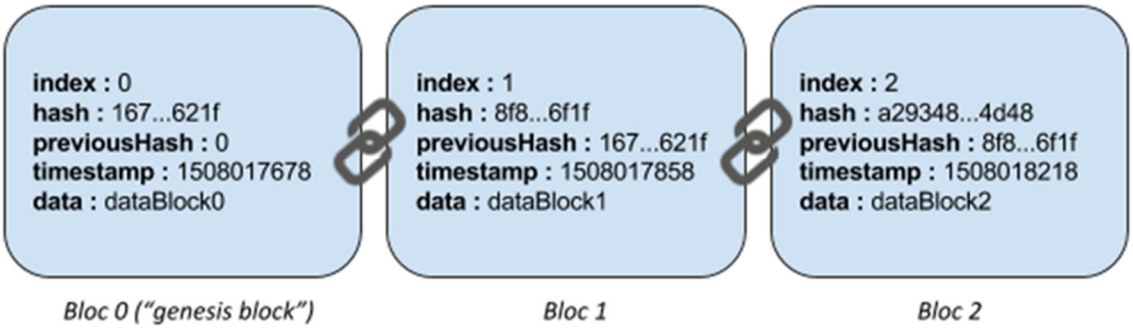

Figure 16- composante de bloc

VIII. 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.

IX. Transactions

IX.1. Sérialisation

Une 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.

Nous appelons "sérialisation" 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. [Rc-10]

IX.2. 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 deux fois, pour des raisons historiques, et pour augmenter la sécurité.

IX.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.

IX.4. 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. [21]

X. Structure d'une transaction

X.1. Les atouts

Une transaction enregistre les transferts de blockchain entre participants. Nous appelons "actif" un montant dans le cas de crypto-monnaie ou une information quelconque qui a été assigné à un utilisateur. Un atout matérialise :

- L'information quand il n'a pas encore été dépensé,
- Transaction vient d'être créée, et est transféré en tant que message,

- Une entrée de grand livre, lorsqu'une transaction a été enregistrée dans un bloc de la blockchain.

X.2. Tableaux d'entrée et de sortie

La transaction se compose de deux tables, la table d'entrée, qui répertorie les actifs dépensés par un ou plusieurs utilisateurs et la table des sorties, qui répertorie les nouveaux actifs affectés à un ou plusieurs bénéficiaires. Lorsqu'un bénéficiaire souhaite utiliser un actif en tant que payeur, une nouvelle transaction est créée et cet actif apparaît dans la nouvelle table d'entrée. Chaque entrée de table d'entrée référence un actif d'une entrée de table de sortie d'une transaction précédente. Cette référence est constituée de l'identifiant de la transaction qui l'a affecté et d'un numéro d'entrée dans la table de sortie.

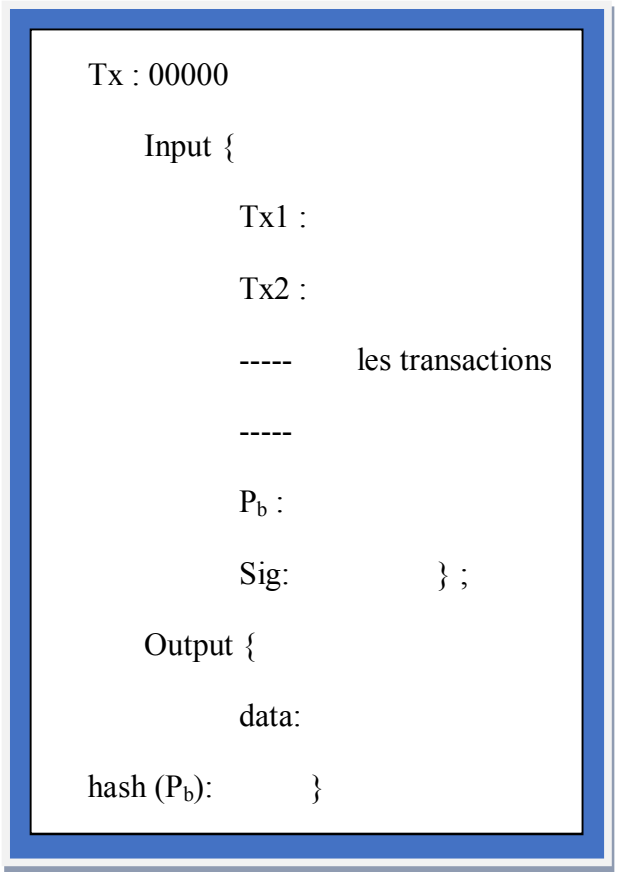

Figure 17- Transaction blockchain

- Tx : c'est la version de bloc

- Txx : transaction s (on peut avoir plusieurs transactions dans 1 seul bloc).
- Pb : la clé publique
- Sig : signature du l'émetteur.
- Data : les informations envoyées.
- Hash(P) : le haché de clé publique du destinataire.

La clé publique est verrouillée avec un double hachage et codée en alphanumérique pour faciliter la communication par le bénéficiaire à l'émetteur.

Pour recevoir une transaction, le bénéficiaire génère une clé privée, une clé publique est calculée et transformée en une adresse, qui sera communiquée à l'émetteur r, pour ajouter des entrées de sortie de la nouvelle transaction.

Pour effectuer un échange, l'émetteur crée une nouvelle transaction, pour affecter des data à l'adresse du bénéficiaire, et pour collecter des actifs non dépensés pour cette dépense. Pour chaque actif collecté, une entrée de la table d'entrée sera créée. Cette entrée fait référence à un actif non dépensé par l'identifiant d'une transaction précédente et le numéro d'entrée dans la table de sortie de cette transaction précédente.

Le diagramme ci-dessous montre la structure d'une transaction et les verrous définis avec les clés privées de l'utilisateur dans le cas d'une transaction bitcoin :

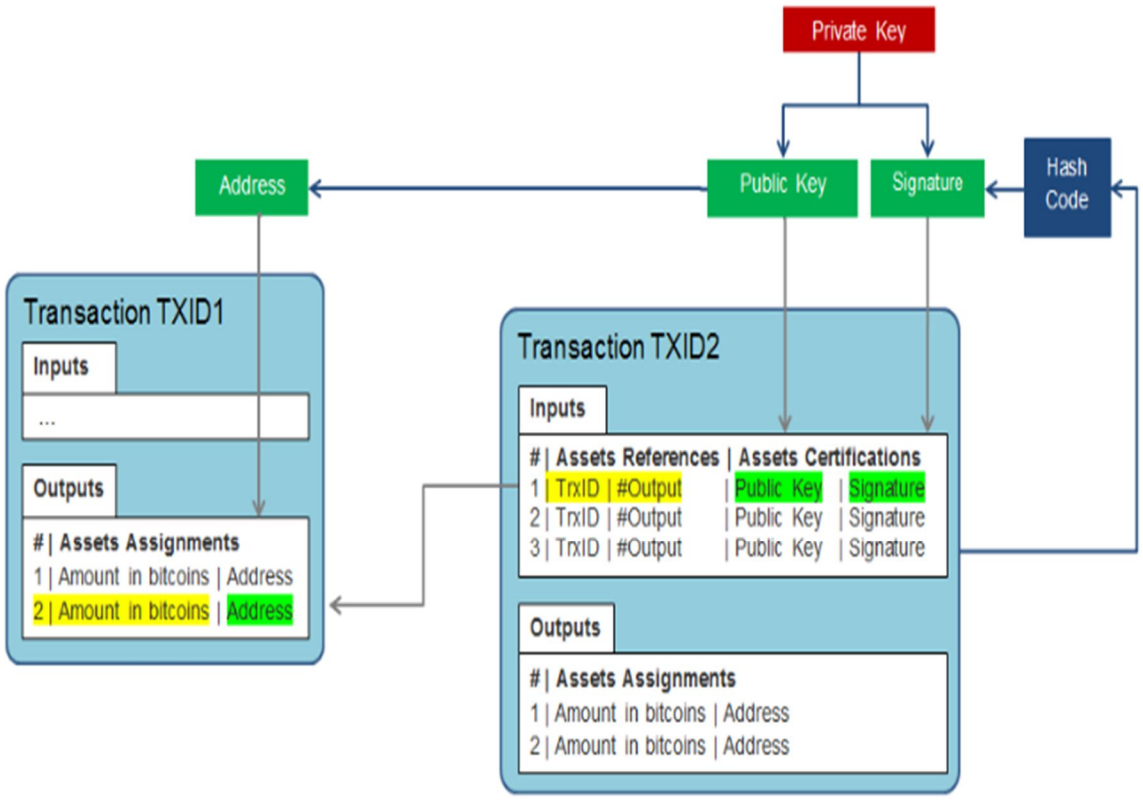

Figure 18- Transaction bitcoin

Ensuite, deux données de certification sont ajoutées :

- **La clé publique** :

  - Il déverrouille l'actif non dépensé de la transaction précédente, car la clé publique doit correspondre à l'adresse,

  - Cela permet de vérifier la signature pour dépenser cet actif. Si la signature a été créée avec une autre paire de clés publique / privée, les agents réseau invalideront la transaction

- **La signature** : elle joue deux rôles :

  - Il atteste que l'utilisateur possédant la clé privée a confirmé cette dépense (principe de non-répudiation). En effet, la signature ne peut être calculée qu'avec la clé privée, mais peut être vérifiée avec la clé publique.

  - Il verrouille la dépense pour cette transaction (principe d'intégrité).

Ainsi, seul le propriétaire de la clé privée sera capable de générer l'adresse pour une nouvelle assignation, et sera capable de fournir l'information qui permet la dépense. Les transactions sont chaînées ensemble car elles définissent l'identifiant des transactions précédentes, permettant de tracer l'origine d'un actif à la transaction initiale.

L'algorithme de signature cryptographique permet à chaque agent du réseau qui diffuse cette transaction ou l'enregistre dans un bloc, de vérifier la cohérence de l'adresse, de la clé publique et de la signature ; sans avoir accès à la clé privée.

X.3. Transaction initiale

Un seul type de transaction déroge à cette représentation, il s'agit des transactions initiales, appelées "transactions de base". Ces transactions créent seulement des sorties pour créer la blockchain.

X.4. Scripts

Les clés publiques et les signatures sont en fait stockées sous forme de fragments de scripts qui seront exécutés par des agents pour effectuer la vérification d'une transaction. Ce script n'est pas du logiciel, mais inséré dans les transactions. L'exécution de ces scripts entraînera les vérifications décrites ci-dessus.

Ces scripts permettent à l'utilisateur de définir d'autres méthodes de paiement telles que la signature multiple pour autoriser la dépense d'un actif.

X.5 Vérification de la transaction

La vérification d'une transaction est le résultat d'une exécution de script. Ce script est divisé en deux parties :

Le premier est situé dans l'entrée de la table de saisie de la nouvelle transaction, il contient la signature numérique et la clé publique prouvant que le payeur possède l'actif affecté dans la table de sortie d'une transaction précédente.

Le second est situé dans l'entrée de la table de sortie de la transaction précédente, il implémente un algorithme pour vérifier l'information de l'actif de sortie.

XI. Preuve de travail

Lorsqu'un nœud reçoit une nouvelle transaction, il la place dans ce qu'on appelle « l'ensemble des transactions non confirmées ». Cet ensemble est propre à chaque nœud, et peut

différer d'un nœud à l'autre, du fait du temps de propagation des transactions sur le réseau. C'est une sorte de liste d'attente pour transactions, qui en sortent une fois qu'elles sont incluses dans un bloc.

N'importe quel nœud peut collecter un certain nombre de transactions dans sa liste, vérifier leur validité et former un bloc. Cependant, le bloc n'est pas valide tant que la « preuve de travail » (de l'anglais Proof of Work ou PoW) associée au bloc n'est pas valide. Cela permet entre autres au réseau de ne pas avoir à choisir entre des milliers de blocs possibles mais de s'accorder sur un seul candidat (i.e. sur un set de transactions valides). [11]

XI.1. Vérification d'une transaction

Il faut bien faire la différence entre set de transactions valide et bloc valide. Un set de transactions est valide si l'ensemble de ses transactions est valide (un set de transactions constitue le contenu d'un bloc). Un bloc est quant à lui valide si son set de transactions est valide ET si la preuve de travail associée à ce bloc est valide (+ 2 autres conditions, cf. algorithme de validation de bloc plus bas). La preuve de travail n'est pas une preuve de validité du set de transactions, mais une preuve que le mineur a résolu le problème mathématique de non-dépassement de seuil correspondant au bloc (expliqué ci-après).

Une fois que les transactions non confirmées sont validées et incluses dans le bloc en préparation, le nœud calcule l'en-tête du bloc. Cet en-tête contient 6 éléments : la version du bloc (définit son type et les règles qu'il suit), l'empreinte (que nous appellerons hash) du bloc précédent, la racine de l'arbre de transactions (plus de précisions plus bas), la date, la difficulté et un nonce.

XI.2. Vérification d'en-tête du bloc

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.

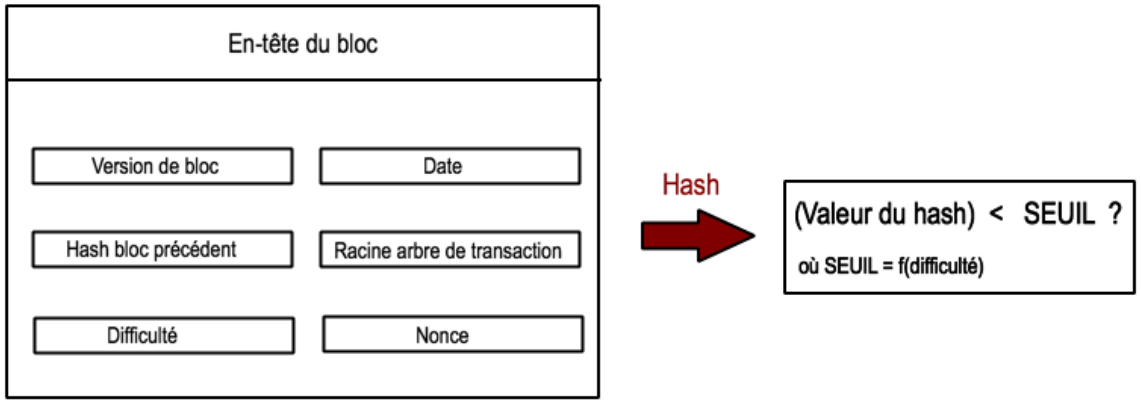

Figure 19 - Vérification de la validité de l'en-tête du bloc.

En paradigme, la preuve de travail peut être exprimée comme suit :

Tant que (valeur du hash) ≥ seuil :

1. Calculer le hash de l'en-tête du bloc
2. Si (valeur du hash) < seuil, retourner le hash

Sinon, incrémenter le nonce de 1 (=ajouter 1 au nonce)

Pour un nœud seul, il faudrait en moyenne plusieurs années pour trouver un bloc valide. À l'échelle du réseau, la difficulté est établie de telle sorte qu'il faut en moyenne 10 minutes pour qu'un noud trouve un bloc valide. Le noud « gagnant » ajoute son bloc à la chaîne, on dit qu'il a « miné le bloc ». Il reçoit en compensation une somme fixe déterminée par le réseau ainsi que les éventuels frais de transaction.

La preuve de travail a une autre implication d'importance : plus un mineur possède une capacité de calcul élevée, plus la probabilité qu'il trouve le prochain bloc est élevé. C'est pourquoi on a vu se former des « pool », ou coopératives, de mineurs qui mettent en commun leur capacité de calcul afin de régulariser leurs revenus.

La puissance de calcul d'un mineur par rapport à l'ensemble du réseau permet d'estimer ses chances de gagner seul la course au nonce qui produira le hash valide. En pratique, elles sont extrêmement faibles. En revanche, dans une coopérative, la mise en commun de la

puissance de calcul permet de trouver des nonces valides plus régulièrement et d'assurer de fait des revenus plus stables aux mineurs qui y participent.

À noter également : plus il y a d'ordinateurs dans le réseau, plus le temps moyen pour trouver un bloc est faible. Pour conserver un temps moyen de bloc à 10 minutes, le réseau ajuste la difficulté tous les 2016 blocs. Le pourquoi de ces 10 minutes sera discuté dans un prochain article.

XI.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 et inférieure à 2h après,

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 set de transactions dans l'ensemble des transactions non vérifiées et recommence la preuve de travail pour ce set. [12]

XI.4. 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'.

XI.5. 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 de facto. [12]

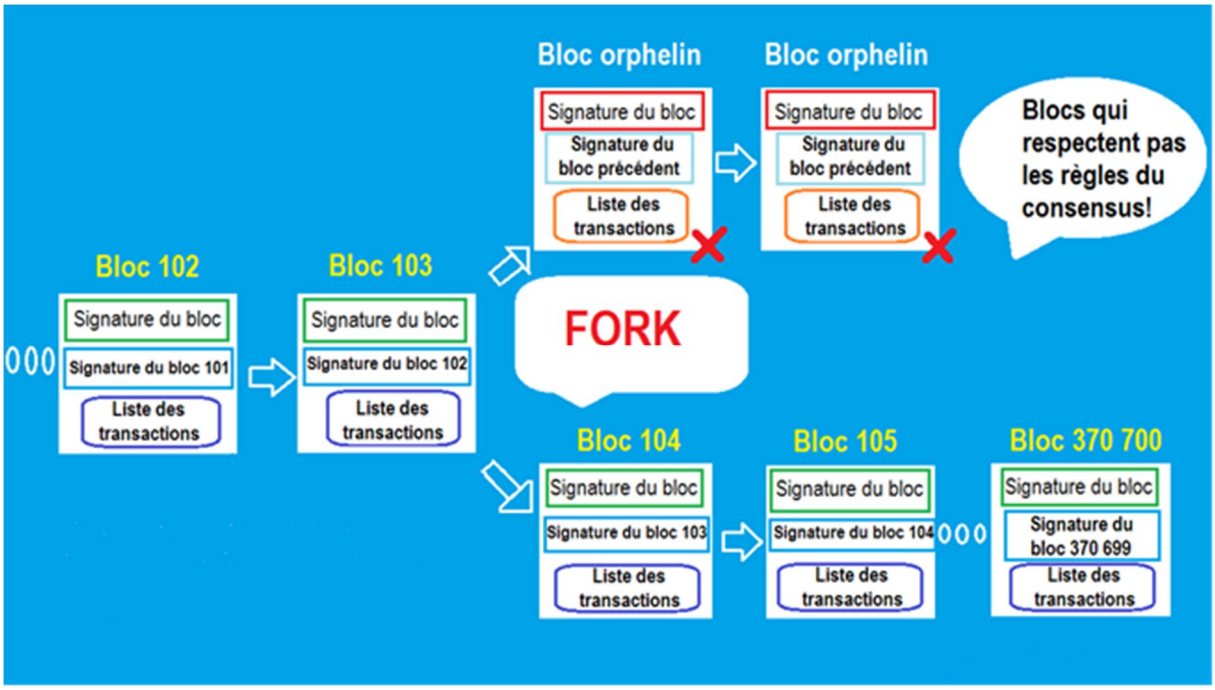

Figure 20- la fourche de blockchain

XI.6. Fraude à double dépense

XI.6.1 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.

XI.6.2 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. [23]

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.

XII. Le réseau

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 sur 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 la 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 réalise qu'il en a

manqué un. [13]

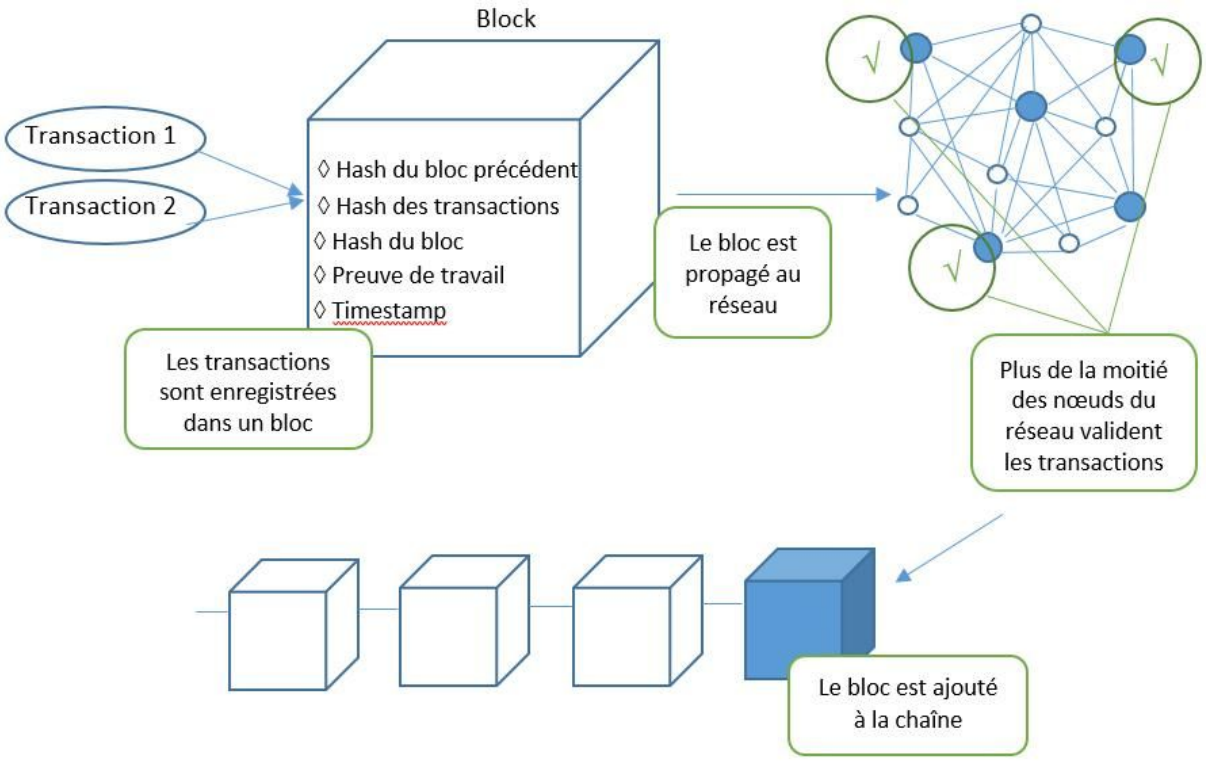

Figure 21- réseau blockchain

XIII. Confidentialité

Les identités des personnes réalisant les transactions sont gardées secrètes, malgré une diffusion publique des transactions elles-mêmes. [14]

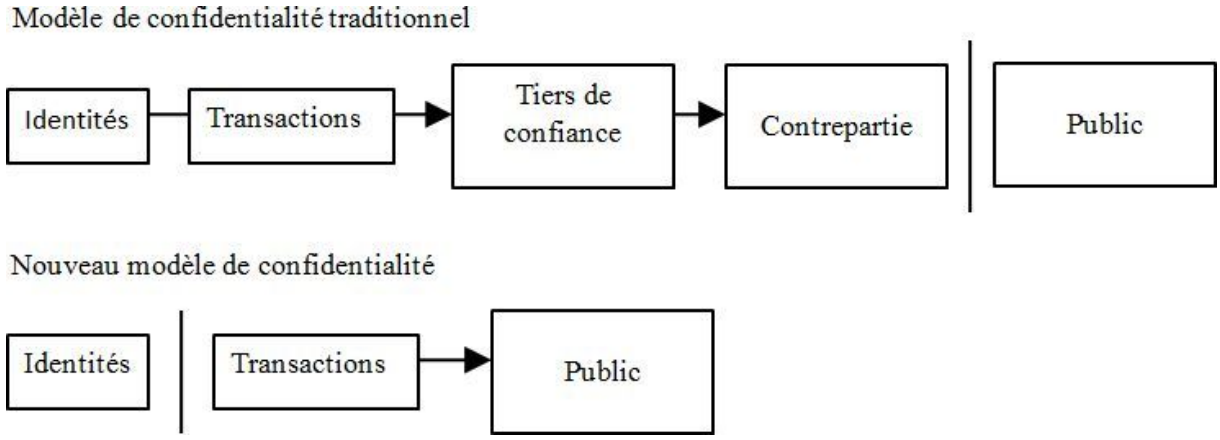

Figure 22- Confidentialité de blockchain.

XIV. CONCLUSION

Dans ce document, 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 distribué, assurant une sécurisation des 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 3

Application Blockchain

I. Introduction

La blockchain peut sembler abstraite sans exemples concrets. Nous avons choisi de présenter un certain nombre de cas d'usage destinés à illustrer le potentiel de cette technologie complexe et à montrer l'étendue de ses possibilités. Ces cas d'usage sont loin d'être exhaustifs, d'autant que la plupart des applications restent encore à construire. Ils suffisent néanmoins à comprendre l'étendue des possibilités offertes par la technologie.

II. Partie I : Crypto-monnaie

II.1. Définition

Crypto-monnaie (Les monnaies virtuel) : permettent de transférer de l'argent sans avoir besoin de support physique et, généralement, sans faire appel à un intermédiaire. Elles doivent avoir au moins les mêmes propriétés de sécurité que les monnaies réelles : permettre les échanges, empêcher la duplication ou encore garantir l'anonymat des transactions. Récemment, plusieurs monnaies virtuelles cryptographiques ont vu le jour, telles que Bitcoin, Peercoin, Primecoin ou Litecoin. Aujourd'hui, ce sont des monnaies alternatives, car elles n'ont de cours légal dans aucun pays, même si elles sont pour l'instant largement tolérées.

La technologie à la base du fonctionnement des crypto-monnaies à le potentiel de transformer un large éventail de transactions, au-delà des paiements traditionnels. Les services financiers pourraient utiliser la technologie blockchain partout où se trouvent des enregistrements digitaux des transactions et pour tout type de transaction nécessitant la vérification d'un tiers de confiance. [23]

II.2.Historique

L'énigmatique Satoshi Nakamoto explique dans son article de 2008 comment mettre en place, grâce à un réseau pair à pair – c'est-à-dire sans nœud central jouant un rôle de chef d'orchestre – et à la cryptographie mathématique moderne, une monnaie autonome et décentralisée, à l'opposé de toutes les monnaies existantes et de tous les systèmes de paiement, en ligne ou non. Le 3 janvier 2009, les programmes nécessaires au lancement de ce qu'on appelle maintenant une crypto-monnaie sont prêts et les premiers bitcoins sont émis. Après des débuts confidentiels où seuls quelques cryptologues avertis s'y intéressent, elle commence à prospérer et son cours, totalement dérisoire en 2009, prend alors son envol lui donnant une réalité concrète.

II.3. Porte-monnaie virtuel

Posséder des Bitcoins, c'est connaître une suite de chiffres et de lettres qui constituent un compte. Une personne peut bien sûr posséder plusieurs comptes. Chaque compte comporte le montant en Bitcoins de l'argent qu'il contient, une clef publique qu'on peut laisser circuler (c'est le numéro de compte), et une clef privée qui doit absolument rester secrète car qui conque en dispose peut dépenser l'argent du compte.

Voici des numéros de compte :

1FxkfJQLJTXpW6QmxGT6oF43ZH959ns8Cq13cia2KGVASavNmRs4niK5RSRfwkB 1uLAu 1A6dpTWvoLWmTgwezLmyQti8oDUcLtjTKX

Voici aussi un exemple de clef secrète

E9 87 3D 79 C6 D8 7D C0 FB 6A 57 78 63 33 89 F4 45 32 13 30 3D A6 1F 20 BD 67 FC 23 3A A3 32 62

Tout support est bon pour conserver la suite de symboles définissent compte d'un utilisateur, y compris un papier, une clef USB ou une mémoire. On gérer un compte à l'aide d'un logiciel appelé « wallet » ou « porte-monnaie ». On peut aussi confier la gestion des comptes à un site internet de confiance. [15]

II.4. Bitcoin

II.4.1. Définition

Bitcoin : unité d'information binaire et coin « pièce de monnaie »), est d'une part une monnaie virtuelle de type monnaie cryptographique et d'autre part un système de paiement pair-à-pair, présenté par une personne sous le pseudonyme de Satoshi Nakamoto, qui annonce son système en 2008 et publie le code source en 2009.

Le Bitcoin reste toujours la crypto-monnaie la plus connue du grand public et la plus médiatisée parmi les différentes monnaies virtuelles et les applications blockchain existantes. Il possèderait un million de bitcoins, valeur de plus de 500 millions US$ [21]

II.4.2. Caractéristiques de la monnaie Bitcoin

- Une monnaie « déflationaire » : 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. [21]

II.4.3. 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 I transferts de fonds (transactions)
- Un moyen d'éviter la double utilisation d'un bitcoin Un registre de transactions horodaté.

II.4.4. Outils technologiques nécessaires

1. Réseau pair-à-pair (P2P).
2. Signature électronique.
3. Hachage cryptographique.
4. Horodatage.
5. Mécanisme de preuve de travail.

II.4.5. Transaction Bitcoin

- ✓ Les participants sont identifiés par des pseudonymes.
- ✓ Un bitcoin est défini par une séquence de transactions signées numériquement, qui débute avec la création du bitcoin.
- ✓ Celui qui possède le bitcoin le transfert à un autre usager en signant électroniquement le transfert.
- ✓ Celui qui reçoit le bitcoin peut vérifier sa validité en regardant l'historique de possession du bitcoin.
- ✓ Transaction est irréversible. [12]

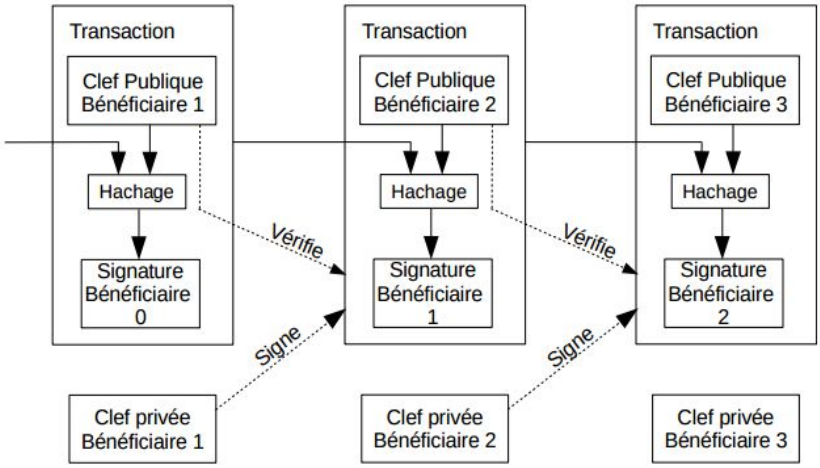

Figure 23-Chaîne de transactions.

II.4.6. Composition d'une transaction

1. Débiter certains comptes pour créditer d'autres comptes.
2. Une transaction est composée d'un certain nombre d'entrées (inputs) et d'un certain nombre de sorties (outputs).
3. Un input est une référence à un output d'une transaction antérieure.
4. Un output comporte un montant et la clé publique de l'adresse créditée. [10]

Les transactions peuvent affecter simultanément plusieurs bitcoins Inputs et outputs multiples. Les bitcoins peuvent ainsi être partagés ou combinés.

Une transaction peut provenir d'un seul input ou de la combinaison de plusieurs sources, et résulter en un ou deux outputs un pour le paiement et un pour le I « change » retourné au payeur. Il peut aussi y avoir des frais de transactions.

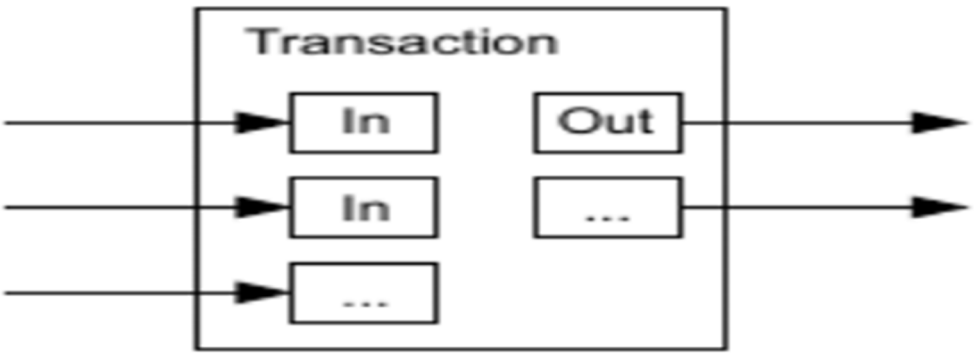

Figure 24- composition d'une transaction

II.4.7. 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, dans l'ordre : script d'output puis script d'input.
2. La transaction n'est validée que si le résultat est « vrai » pour tous les inputs.

II.5. Ethériuem

II.5.1. Définition

Ethereum : est un protocole d'échanges décentralisés permettant la création par les utilisateurs de contrats intelligents grâce à un langage Turing-complet. Ces contrats intelligents « smart contracts » sont basés sur un protocole informatique permettant de vérifier ou de mettre en application un contrat mutuel, ils sont déployés et consultables publiquement dans la blockchain. [23]

Ethereum, c'est donc la décentralisation d'applications. Ces applications fonctionnent sur le réseau Ethereum, qui est constitué de plusieurs milliers d'ordinateurs qui communiquent en permanence. Ils partagent une même base de données, la blockchain. Cette base de données peut être comparée à un grand registre, qui serait rempli ligne par ligne par les participants au réseau, ou un tableau Excel sur lequel on ne pourrait qu'entrer une nouvelle ligne, sans pouvoir modifier les autres.

II.5.2. Création

L'idée d'Ethereum a été avancée fin 2013 par Vitalik Buterin, un informaticien russo-canadien de 19 ans à l'époque. La plateforme, lancée le 30 juillet 2015, connaît un boom de popularité depuis mars 2017, devenant aujourd'hui le deuxième plus gros crypto monnaie en circulation. La partie monétaire au sens strict d'Ethereum est pour le moment largement inspirée du bitcoin ; mais ce qui rend cette plateforme aussi intéressante, c'est la porte qu'elle ouvre pour le concept de contrat intelligent, en anglais « smart contract ». [23]

II.6. Smart Contractes

II.6.1. Définition

Les contrats intelligents sont des contrats à exécution automatique, les termes de l'accord entre l'acheteur et le vendeur étant directement écrits dans des lignes de code. Le code et les accords qu'il contient existent sur un réseau décentralisé de chaînes de blocs décentralisées. Les contrats intelligents permettent d'effectuer des transactions et des accords de confiance entre des parties disparates et anonymes, sans avoir besoin d'une autorité centrale, d'un système juridique ou d'un mécanisme d'exécution externe. Ils rendent les transactions traçables, transparentes et irréversibles

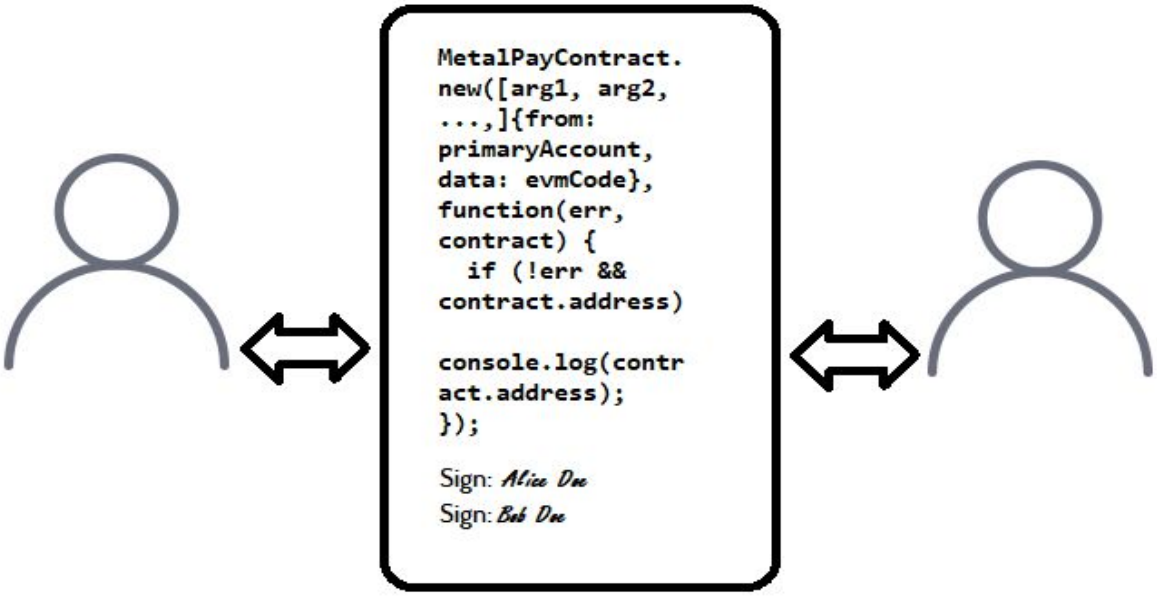

Figure 25- contrat intelligente

Les contrats intelligents réduisent radicalement les coûts de transaction. Le code auto-exécutable - que ce soit au niveau du protocole ou au niveau de l'application - normalise les règles de transaction, réduisant ainsi les coûts de transaction de :

- Parvenir à un accord,
- Formalisation,
- Mise en vigueur. [13]

II.6.2. Caractéristiques d'un contrat intelligent

Les contrats intelligents sont capables de suivre la performance en temps réel et peuvent apporter des économies considérables. La conformité et le contrôle ont lieu à la volée. Pour obtenir des informations externes, un contrat intelligent nécessite des informations oracles, qui alimentent le contrat intelligent avec des informations externes.

Les contrats intelligents sont :

- Auto-vérification,
- Auto-exécutable,
- Inviolable,

Les contrats intelligents peuvent :

- Transformer les obligations légales en processus automatisés.
- Garantir un plus grand degré de sécurité.
- Réduire la dépendance envers les intermédiaires de confiance.
- Réduction des coûts de transaction.

Au lieu d'exiger qu'une seule autorité centrale dise « oui » ou « non », ces contrats sont autogérés. Cela rend non seulement l'ensemble du processus plus efficace, mais aussi plus équitable et objectif.

Les smart contrats sont des programmes autonomes qui, une fois démarrés, exécutent fonctionnement comme toute instruction conditionnelle de type "if - then" ("Si" condition vérifiée "Alors" conséquence s'exécute), et présentent trois principaux apports : une vitesse accrue, une meilleure efficacité, et une certitude que le contrat sera exécuté comme convenu. Ces programmes sont capables de surmonter les problèmes d'aléa moral, et de réduire les coûts de vérification, d'exécution, d'arbitrage et de fraude. L'avantage de mettre en place des smarts-contracts dans une blockchain réside dans la garantie que les termes du contrat ne pourront pas être modifiés. Un smart-contract qui ne serait pas dans la blockchain serait un programme dont les termes pourraient être changés en cours d'exécution [10].

Figure 26- Principe de smart contract

III. PARTIE II : L'Internet of Things et la Blockchain

En effet, au même titre que la monnaie virtuelle, les besoins sont forts aussi bien en termes de sécurisation des données, d'historique associé à un objet connecté et d'interopérabilité. Son organisation décentralisée et sans intermédiaire pourrait aussi permettre à un objet de communiquer avec un autre objet pouvant conduire à certaines prises de décisions autonomes par celui-ci. En amont, les propriétés du code délimiteront les barrières et capacités des objets à prendre les décisions. Le schéma, ci-dessous, montre le possible changement de paradigme à terme concernant la communication inter-objet associant IoT et Blockchain.

Figure 27- internet des Object.

En termes de sécurisation des données, l'enjeu est fort au vue des données sensibles et critiques qui pourraient transiter dans des solutions de Smart Cities ou encore de santé connectée. La blockchain, qui sécurise déjà les transactions Bitcoin, pourrait ajouter une couche de sécurité en ajoutant une 'chaine' associée à l'identité de l'objet connecté. Ainsi, cette "chaine d'identification" permettra aux objets d'interagir entre eux sans avoir à

communiquer via une tierce partie (type plateforme cloud) limitant, en conséquence, les sorties d'information ou les attaques potentielles venant de l'extérieur. [16]

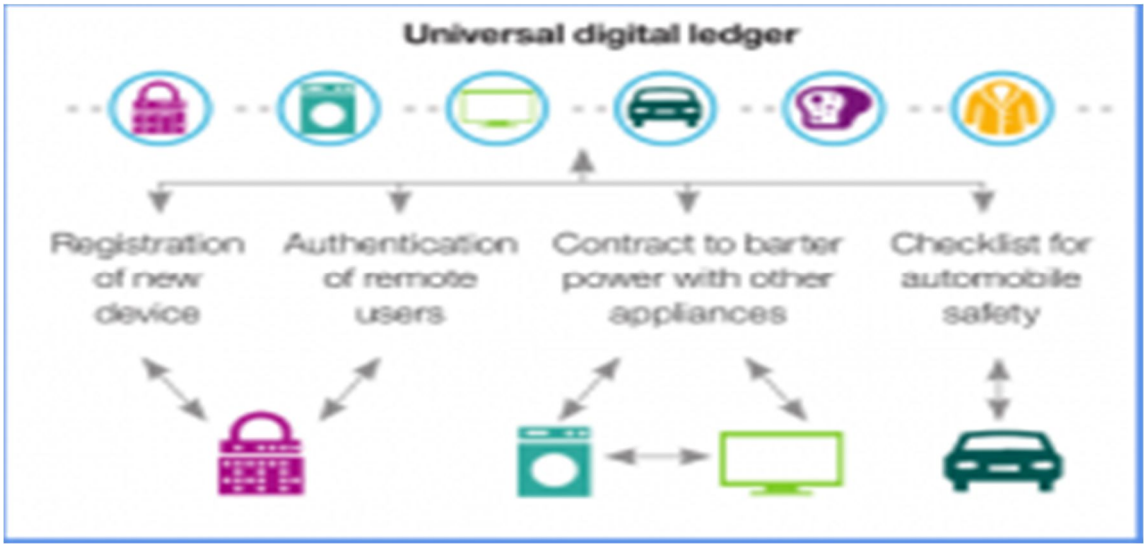

Figure 28- Sécuriser les échanges entre objets pour limiter les risques de hacking.

III.1 Architecture IoT basée sur un bloc

Nous considérons un environnement de maison intelligente typique où un utilisateur, Alice a équipé sa maison avec un certain nombre d'appareils IoT, y compris un thermostat intelligent, des ampoules intelligentes, une caméra IP et plusieurs autres capteurs.

L'architecture proposée représentée sur la figure 28 comprend trois niveaux, à savoir la maison intelligente (ou plus généralement le réseau local), le réseau de superposition et le stockage en Cloud.

Nous considérons les cas d'utilisation de stockage de données et d'accès : Alice devrait être en mesure d'accéder aux données de sa maison intelligente, par exemple, la température actuelle dans sa chambre, à distance. De plus, les dispositifs intelligents devraient être capables de stocker des données sur des stockages devant être utilisés par un tiers (par exemple, le fournisseur de thermostat intelligent) pour bénéficier de certains services.

Avant de discuter des détails de l'architecture proposée, nous présentons brièvement les niveaux de réseau :

Smart Home : La maison intelligente est composée des trois parties suivantes :

- ✓ **Dispositifs** : Tous les dispositifs intelligents situés dans la maison.

✓ **Local BC :** Un BC sécurisé et privé qui est extrait et stocké par un (ou plusieurs) périphérique capable de ressources, qui est toujours en ligne. Un exemple pourrait être un hub intelligent ou ordinateur à la maison.

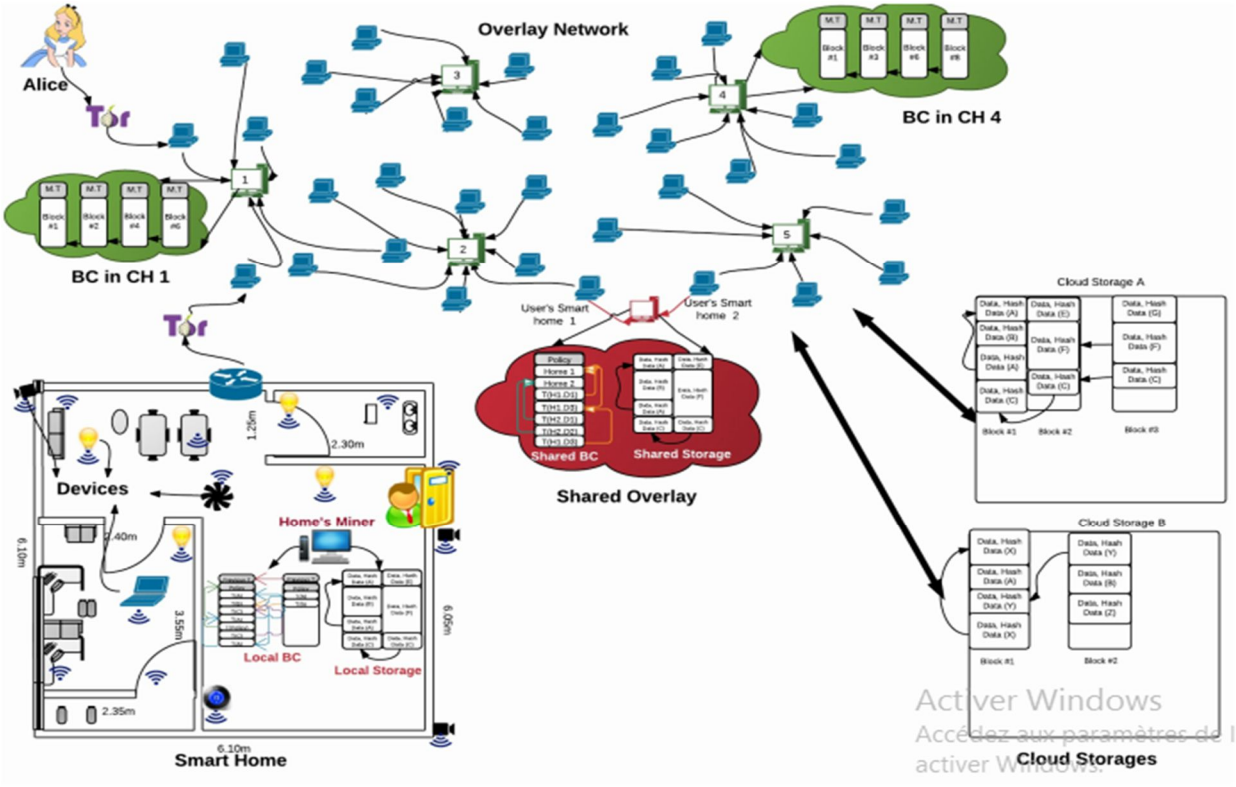

Figure 29 - Représente l'architecture d'une maison intelligente.

✓ **Stockage local** : Dans chaque maison, il peut y avoir un stockage local facultatif pour le stockage des données comme indiqué dans la maison intelligente de la Fig.1. Cela pourrait être un lecteur de sauvegarde local. En plus de ces parties, le mineur de chaque maison a une liste de PK utilisées pour donner aux autres la permission d'accéder aux données de la maison. [17]

III.2. Blockchain Recommandations pour IoT à exploiter

Quatre recommandations importantes pour l'IoT comprennent :

III.2.1. Bâtiment de la confiance

IoT Blockchain permet aux appareils d'effectuer des transactions et les communications en tant que parties de confiance. Alors que le périphérique A peut ne connais pas le dispositif B, et peut ne pas le croire, l'enregistrement permanent des échanges et des informations

dispositifs stockés sur la chaîne de blocs confirme et permettent le vital faire confiance aux organisations, aux individus et aux dispositifs pour coopérer.

III.2.2. Réduction des coûts

Il est important que les périphériques Edge IoT réduisent le traitement frais généraux et éliminer le « intermédiaire » (passerelles IoT) de la procédure. Communication, échange de données et les informations sur le dispositif sont effectuées sur une base d'égal à égal, en supprimant tout protocole, matériel ou frais généraux de communication.

III.2.3. Accélérer les échanges de données

Amélioration des échanges de données en tant que « intermédiaire » (passerelle IoT ou tout dispositif de filtrage intermédiaire) est expulsé du processus. Contrats à base de dispositifs peer-to-peer et grands livres (Blockchain) diminuer le temps nécessaire pour compléter l'appareil échange d'informations et temps de traitement.

III.2.4. Sécurité à l'échelle pour IoT

Les technologies décentralisées sont très prometteuses pour un système qui doit gérer le stockage et la récupération des informations des millions et des milliards, d'appareils connectés. Ces futurs les systèmes doivent fournir une faible latence, un débit élevé, interrogation, autorisations et contrôle décentralisé.

L'adoption de la Blockchain dans l'espace IoT peut changer la façon dont IoT les périphériques échangent des données dans un environnement fiable, mécanisation et encodage des transactions, tout en sauvegardant échanges de données et assurer la sécurité de tous les appareils impliqués

IV. Patrie III : Identité Digital et La Blockchain

ID-Blockchain fournit des services de sécurité pour la gestion de l'Identité (ID) numérique dans le respect de la vie privée basés sur les technologies dites blockchain dont Bitcoin est l'exemple le plus connu. Cette approche disruptive doit permettre d'augmenter le niveau de sécurité et de respect de la vie privée, de contrôle par l'utilisateur et de transparence dans l'usage et d'améliorer la productivité tout en diminuant les couts et les niveaux de risque potentiel.

IV.1. Identificateurs décentralisés (DID)

IV.1.1. Motivations pour les DID

Le besoin croissant d'identificateurs décentralisés a créé deux exigences spécifiques pour un nouveau type d'URL qui s'adapte à l'architecture Web et présente quelques exigences supplémentaires que les URL plus traditionnelles, telles que les URL basées sur HTTP, ne possèdent pas :

Le nouveau type d'URL NE DEVRAIT PAS demandé à une autorité centralisée d'enregistrer, de résoudre, de mettre à jour ou de révoquer l'identificateur. L'écrasante majorité des URI aujourd'hui sont basés sur des noms DNS ou des adresses IP qui dépendent des autorités centralisées pour l'enregistrement et le contrôle final. Les DID peuvent être créés et gérés sans une telle autorité.

URL dont la propriété et les métadonnées associées, y compris les clés publiques, peuvent être vérifiées cryptographiquement. L'authentification via DID et DID Documents utilise la même cryptographie à clé publique / privée que les ledgers distribués.

IV.1.2. Identificateurs décentralisés (DID)

Le concept d'identifiant décentralisé unique au monde n'est pas nouveau ; Les identificateurs universels uniques (UUID) ont été développés dans les années 1980 et sont devenus par la suite une caractéristique standard de l'environnement informatique distribué de l'Open Software Foundation. Les UUID atteignent l'unicité globale sans un service de registre centralisé en utilisant un algorithme qui génère des valeurs de 128 bits avec une entropie suffisante pour que le risque de collision soit infinitésimalement petit. UUID sont formellement spécifié dans

Un DID est similaire à un UUID sauf : (a) comme une URL, il peut être résolu ou déréférencé en une ressource standard décrivant l'entité (un document DID - voir la section4. Documents DID), et (b) contrairement à une URL, le document DID contient généralement du matériel cryptographique qui permet l'authentification d'une entité associée au DID

Le premier défi consiste à rendre ces identifiants globalement uniques, globalement résolvables et reconnaissables.

La spécification des identificateurs décentralisés, développée sous les auspices du World Wide Web Consortium (W3C), constitue la base de la solution. [18]

IV.1.3. Les principes de conception de l'architecture DID

Décentralisation : devrait élimine l'exigence d'autorités centralisées ou de points de défaillance uniques dans la gestion des identifiants, y compris l'enregistrement des identificateurs uniques au niveau mondial, des clés de vérification publiques, des points de terminaison de service et d'autres métadonnées.

- **Auto-Souveraineté :** donne aux entités, tant humaines que non humaines, le pouvoir de posséder et de contrôler directement leurs identifiants numériques sans devoir recourir à des autorités externes.
- **Intimité:** permettre aux entités de contrôler la confidentialité de leurs informations, y compris la divulgation minimale, sélective et progressive des attributs ou d'autres données.
- **Sécurité** : permettre aux parties utilisatrices de disposer d'une sécurité suffisante pour dépendre des documents DID pour leur niveau d'assurance requis.
- **Basé sur des preuves :** permettre à une entité de fournir des preuves cryptographiques d'authentification et de preuve des droits d'autorisation.
- **Découvrabilité :** permettre aux entités de découvrir des DID pour que d'autres entités en apprennent davantage sur ces entités ou interagissent avec elles.
- **Interopérabilité :** utilise des normes interopérables afin que l'infrastructure DID puisse utiliser les outils et bibliothèques logicielles existants conçus pour l'interopérabilité.
- **Portabilité** : être indépendante du système et du réseau et permettre aux entités d'utiliser leurs identifiants numériques avec tout système prenant en charge les DID et les méthodes DID.
- **Simplicité** : Pour atteindre ces objectifs de conception, l'architecture DID devrait être (pour paraphraser Albert Einstein) « aussi simple que possible mais pas plus simple ».
- **Extensibilité** : permettre l'extensibilité à condition qu'elle n'entrave pas grandement l'interopérabilité, la portabilité ou la simplicité. [19]

IV.1.4. Gestion d'identité décentralisée

Gestion d'identité basée sur des identifiants décentralisés. La gestion décentralisée des identités étend l'autorité de création des identifiants au-delà des racines traditionnelles de confiance requises par les services d'annuaire X.500, le système de noms de domaine et la plupart des systèmes d'identification nationaux. [24]

IV.2. Identification Digital et la blockchain ID

IV.2.1. Contexte de technologie

Permet aux individus de créer des ancrages numériques pour leurs identités numériques qui sont totalement uniques au monde, un identifiant décentralisé, ou DID. Ces identifiants uniques peuvent être stockés dans des ledgers partagés (blockchains).

Une identité auto-souveraine est une identité numérique portable à vie pour toute personne, organisation ou chose qui ne dépend pas d'une autorité centralisée et ne peut jamais être retirée.

Les identificateurs décentralisés (DID) sont globalement réservables, identifiants uniques cryptographiquement vérifiables ne nécessitant aucune autorité d'enregistrement centralisée.

Notation, qui enregistre des informations simples sur le DID particulier. Logiciel tiers est ensuite utilisé pour soutenir les individus avec la gestion de la vaste gamme de DID qui sont connecté à leur identité numérique. Dans ce système, il n'y a pas d'identifiants persistants qui lient toute l'activité ensemble. Chaque relation avec chaque partie crée de nouveaux DID pour le spécifique interaction et l'utilise pour prendre en charge une interaction Peer-2-Peer cryptée. [25]

Ceci est une image simplifiée de la pile d'identité décentralisée

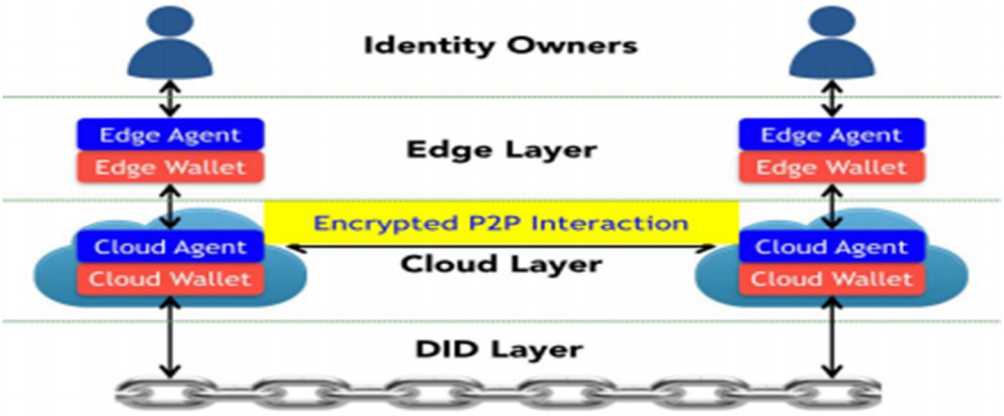

Figure 30- identité décentralisé

Dans ce diagramme, chaque individu et chaque organisation a son propre "agent de cloud". Plusieurs sociétés offrent des services d'agent de cloud. Ce sont des comptes de stockage liés pour aider les individus à gérer leur identité et leurs données. Les individus auront plusieurs DID, un pour chaque relation jumelée, qui doit être géré par des fournisseurs tiers. Les

particuliers peuvent autoriser un fournisseur tiers à gérer leur dossier de numéro DID dans l'agent de cloud et y accéder via un portefeuille Edge (application au téléphone).

IV.2.2. Revendications vérifiées

Cette Identité digital fournit des conteneurs pour que les individus puissent centrer les données numériques qu'ils possèdent et contrôlent. Cependant, les identifiants par eux-mêmes, sans aucun contexte, ne sont pas particulièrement utiles.

L'architecture des réclamations vérifiables permet aux particuliers de recueillir des réclamations à propos d'eux-mêmes de diverses parties qui pourraient être qualifiées ou faire autorité pour émettre de telles réclamations.

Une université est qualifiée pour conférer des réclamations aux étudiants qui ont rempli les conditions d'un diplôme. Les gouvernements délivrent des certificats de naissance aux parents qui enregistrent les naissances de leurs enfants. Une grande partie de la gestion de ces réclamations est faite avec du papier. Ce n'est pas sûr et pas évolutif dans le domaine numérique

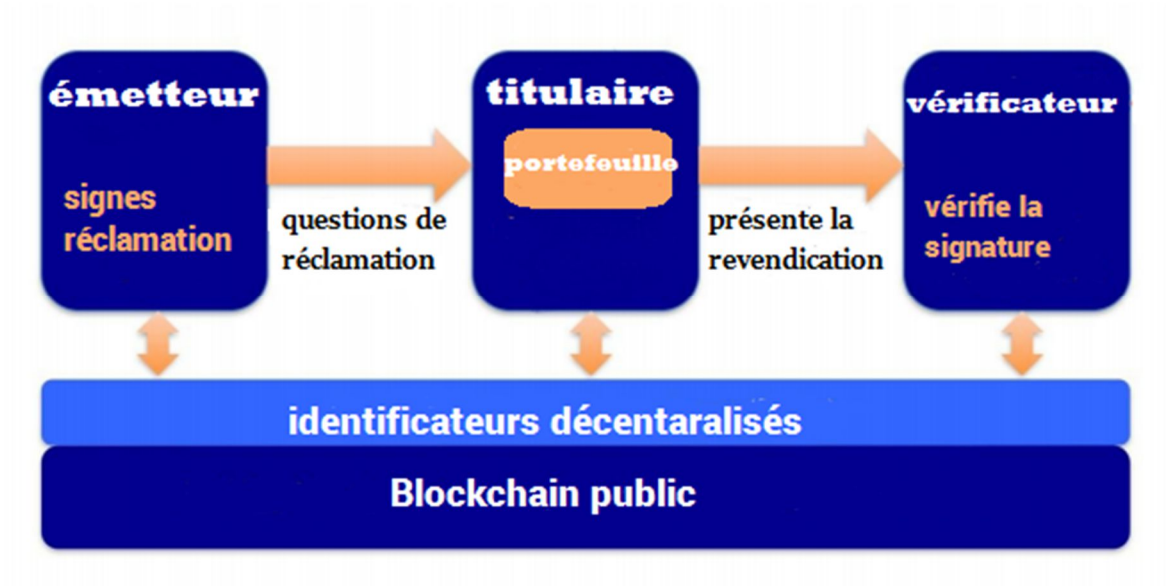

Figure 31- concept d'identité

Une fois qu'un individu a reçu une réclamation, comme une demande d'accès numérique, il est libre de la présenter à qui il veut. La partie à laquelle ils présentent la réclamation, le vérificateur comme un notaire, peut vérifier la véracité de la réclamation avec le reçu enregistré dans la blockchain sur la base d'un accès autorisé sans exiger tous les PII d'un citoyen en utilisant une méthode appelée preuves zéro connaissance.

Le W3C est en train de mettre au point des normes ouvertes pour permettre la création d'un écosystème numérique de réclamations vérifié. [26]

IV.2.3. Utilisation de contrats intelligents pour gérer la clé publique

De plus il y a une méthode pour décentraliser la maintenance des clés publiques par le propriétaire de l'identité à l'aide de contrats blockchain et smart. Le but d'avoir un contrat de mandataire en tant qu'identificateur principal est qu'il permet à l'utilisateur de remplacer sa clé privée tout en maintenant un identificateur persistant (uPort). Si l'identificateur uPort de l'utilisateur était à la place la clé publique correspondant à sa clé privée, il perdrait le contrôle de son identifiant s'il perdait le périphérique sur lequel la clé privée est conservée.

Ainsi, avoir un ID persistant qui peut avoir une clé publique remplaçable et un ensemble de clés privées rend la possession de l'identité plus facile et plus sûre. [27]

IV.2.4. DPKI pour récupérer des clés privées

Les données d'identité décentralisées nécessitent un stockage cloud sécurisé pouvant être récupéré en cas de perte de données. Les données comprennent des certificats, des attributs de profil, etc. qui nécessiteraient un chiffrement.

Le chiffrement lui-même peut être symétrique et la clé doit être sauvegardée pour la récupération. Tout stockage centralisé de telles clés rendrait l'ensemble du système vulnérable et irait à l'encontre de l'objectif initial de la décentralisation. Le problème a été correctement identifié et résolu par les membres de reboot-the-web-of-trust en utilisant un schéma de récupération basé sur le groupe.

Les problèmes de sécurité et de facilité d'utilisation de DNS et de PKIX peuvent être résolus par l'utilisation de magasins de données à valeur-clé décentralisée, tels que des chaînes de blocs, pour créer une spécification pour une infrastructure à clé publique décentralisée (dPKI). En décrivant les propriétés de dPKI, il fonctionne même sur les périphériques mobiles à ressources limitées et il est capable de préserver l'intégrité des identifiants en protégeant les organisations et les indivis de la perte ou de la compromission de la clé privée

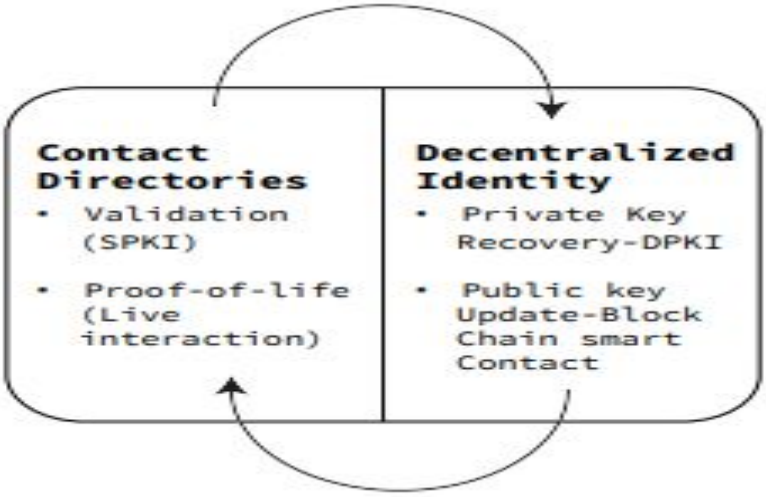

Figure 32- structure dPKI

IV.2.5. SPKI pour signer des données d'identité pour valider l'identité

Les identités numériques doivent être certifiées par d'autres agences ou un consensus social pour devenir plus fiables. SPKI propose un modèle décentralisé pour émettre de tels certificats et autorisations dans le cadre d'annuaire. SPKI offre une opportunité spéciale pour renforcer l'empreinte sociale Il rend les identités dans les répertoires de contact dignes de confiance par des tiers. Une personne peut être certifiée à travers plusieurs répertoires et le graphe social des numéros mobiles dans une architecture décentralisée similaire à un Web-of-trust. Une identité unique est générée à l'aide de SPKI sans nom et liée à un MSISDN actif avec un identificateur global unique. Ces certificats peuvent être facilement découverts à l'aide de répertoires ou de MSISDN.

Les répertoires peuvent être vérifiés par le biais de la vérification du courrier électronique ou, mieux encore, être signés à l'aide d'un certificat validé par un domaine. [Wb-8]

V. Conclusion

Nous avons vu ce que cette innovation technologique induit, en termes de changements potentiels, dans différents secteurs d'activités différents, et nous avons essayé d'en retirer les éléments clés qui font de la blockchain une invention disruptive. 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 d'avantage d'expérience et d'initiatives afin de la rendre viable dans le monde de l'entreprise.

Les initiatives blockchains sont très nombreuses et dispersés. Comme pour la plupart d'autres technologies informatiques, 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 4

Blockchain pour véhicule

I. Introduction

Comme nous l'avons vu dans les chapitres précédents, la technologie blockchain consiste une évolution informatique dans le domaine de la sécurité et la disputation des données. Vu que cette technologie donne un support robuste et sécurisé pour partager une base de données à travers l'internet ou bien au sein d'une communauté limité sur internet (états, constructeur de véhicule, des communes, association …).

Actuellement, la crypto-monnaie consiste l'application la plus connue qui à efficacement exploité la maniérer dont une blockchain garantie l'authentification la non-répudiation et la confidentialité des données sans avoir recours à des tiers de confiance tel que les banques ou bien les états. Cependant la crypto-monnaie n'est qu'un début d'utilisation de cette technologie dans des domaines plus vaste et plus sensible tel que les ID [19] distribuer, IOT [16].

Dans ce chapitre on va proposer l'exploitation de la blockchain pour organiser la vente/achat des véhicules, voire même la possibilité de remplacer le système administratif de registration, vent/achat… des véhicules existants.

II. Présentation du projet

II.1. Problématique

Le système administratif algérien gère d'enregistrement là vente/achat des véhicule (DRAG) d'une façon traditionnelle en gardant en permanence une archive de toutes les opérations effectuer au niveau national, ce qui donne aux fraudeurs et voleurs de véhicule la possibilité de modifier cette archive en vue d'insérer de nouveaux véhicules volés. Malgré la dernière tentative du gouvernement remplacer l'archive par une base de données centralisé, cependant le fait que l'agent administrative épar payé aux niveaux national détient le privilège d'insérer et modifier dans données, ce que garde toujours la possibilité de fraude.

Notre objective sera donc de mettre fin à ces fraudes par la bais d'une blockchain.

II.2 Objectif

L'objectif dans ce projet est de créer un système de gestion carte grise à base de la technologie Blockchain, qui est sans doute le moyen le plus efficace, sécurisé et le plus transparent, pour gérer l'achat, vente, et l'enregistrement des véhicules.

Il pourrait 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 opérations sur les véhicules au niveau national.

La blockchain va garder trace de toutes les opérations sur chaque véhicule à l'instar de la blockchain gérant et la transaction du crypto-monnaie ce qui va permettre aux citoyens d'être à l'aber des fraudes et corruption car il est le seul qui détient le privilège sur son véhicule à l'aide de sa clé privé.

III. Structure administrative algérien

III.1. Le service DRAG

Direction de la réglementation et des affaires générales est le service responsable de gestion de l'enregistrement des véhicules au niveau national est le DRAG, qui se trouve dans chaque commune au niveau national. Ce service détient une base de données ou bien une archive pour gérer les vents/achats des véhicules, ce service délivre pour chaque véhicule un certificat nommé la carte grise. Ce document gère l'authenticité des véhicules imprimé sur papier dont on a aussi la possibilité de fraude ce qui nous a donné l'idée de remplacé cette structure administrative (DRAG) par une blockchain.

III.2. Carte grise biométrique algérienne

Nous détaillons dans cette section les cartes grises biométriques existantes et mises en place ainsi que les caractéristiques utiles à notre étude.

La carte électronique d'immatriculation des véhicules (carte grise) est mise en circulation par le ministère de l'intérieur et des collectivités locales au début de l'année 2017,

La nouvelle carte grise intégrera les fonctionnalités associées au contrôle et la vérification qui s'effectueront de manière automatique. Elle implémente des fonctionnalités liées au contrôle du véhicule et aux assurances et essentiellement à la nationalisation de la consommation de carburant et ce, en étant associé à un système d'information dédié à cet effet.

Figure 33-certificat d'immatriculation de véhicule.

Cette carte est bien évidemment gérée par un système d'information connecté à une base de données qui permettra d'effectuer des analyses. Ce même système est en réalité une sorte de bases de données classiques basé sur les schémas informatiques traditionnels de la mise à disposition et du partage sécurisés d'information, la validation d'une écriture ou tout type de modification est fournie par la base elle-même et non pas par la majorité des acteurs (propriétaire des voitures) de base de données centralisé et cela risque d'être falsifier ou trafiquer par les employés des services concernés.

D'autre part, l'échange de données à caractère sensible nécessite l'intervention de tiers de confiance, d'intermédiaires.

III.3. Règles de gestion de chaque véhicule

La carte grise électronique intègre une puce porteuse un certificat électronique port toutes les informations du véhicule, parmi ces informations on note :

- ✓ un numéro d'immatriculation qui est unique ;
- ✓ un numéro d'ordre du véhicule qui est unique ;
- ✓ un numéro de châssis qui est unique ;
- ✓ une marque ;
- ✓ une année de fabrication ;
- ✓ une date d'achat ;
- ✓ un coût à l'achat.

Dans notre étude nous nous intéressant sur le numéro de série. Généralement dite « numéro de châssis ».

III.4. Le numéro d'identification du véhicule :

V.I.N, N.I.V, parfois appelé numéro de série ou numéro de châssis mais son appellation officielle est Numéro d'Identification du Véhicule (N.I.V ou Vehicle Identification Number, V.I.N, en angle numéro d'identification du véhicule (VIN) pour les voitures telles que l'ADN. Ce numéro d'identification du véhicule est un moyen de différencier votre voiture de millions de voitures similaires dans le monde entier.

Les composantes du numéro d'identification du véhicule :

Figure 34- Numéro d'identification du véhicule

Il est composé de 17 caractères (lettres et chiffres), il ne peut contenir les lettres I (i), O (o), or Q (q) afin d'éviter la confusion avec les chiffres 0 et 1.

- **VIN :** Véhicule Identification Number (Numéro d'identification du véhicule)
- **WMI :** World Manufactured Identificroutier. Identification du constructeur à l'échelle mondiale)
- **VDS :** Véhicule Description Section ; Caractéristiques générales du véhicule (type mines)
- **VIS :** Véhicule Identification Section ; Identification du véhicule (numéro de série).
- Voici un exemple du code VIN chez Renault

W.M.I. (3 caract.) identification mondiale du constructeur			**V.D.S.** (6 caractères) description du véhicule					**V.I.S.** (8 caractères) identification du véhicule	
zone	pays	marque	type de carrosserie	code projet	indice de motorisation	constante véhicule		année	n° de série
V	F	1	S	B	0R	O	F	2	3000596
			société 5 p.	Clio II	diesel		Flins	2002	

Figure 35-VIN chez Renault

IV. Blockchain pour véhicule

IV.1. Structure générale

L'objectif étant de définir une nouvelle structure administrative du service DRAG algérien utilisant la technologie en vue de remplacer l'ancienne structure.

Auparavant, il était possible que chaque employé ayant le privilège nécessaire dans le service DRAG de modifier les informations de n'importe quel véhicule ce qui ouvre une très grande porte pour le fraude et la corruption. Par exemple un employé corrompu peut créer des fichiers ou des enregistrements dans la base de données pour des véhicules volés au niveau national ou international. Mais avec l'utilisation d'une blockchain destiné à sauvegarder toutes les données et les opérations sur les véhicule, ces cas de fraude devient impossible, vue que la blockchain sera publier sur internet et chaque citoyen pourra obtenir une copie à jour de la blockchain.

Figure 36 –Blockchain pour véhicule.

Dans ce nouveau système on propose de se débarrasser des anciennes bases de données de la carte grise et le remplacer avec un système blockchain (réseau de carte grise). Ce réseau est distribué sur toute une chaine administrative (le gouvernement, les constructeurs, les particulier). Elle est le symbole d'une modernisation radicale du service public et plus largement du pays.

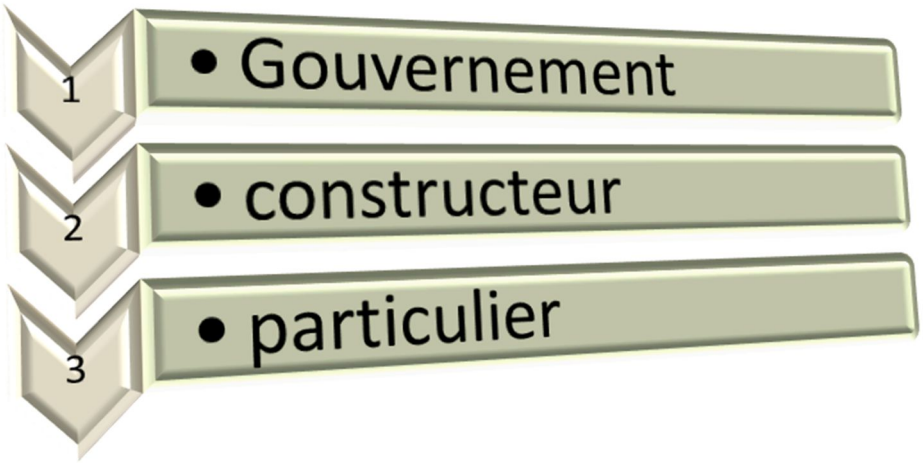

Figure 37 -les acteurs du système

IV.2. Architecture générale du système

Afin de pouvoir gérer toutes les opérations sur les véhicules de tout sort en propose d'enregistrer notre système sous forme de deux catégories de blockchain national ou plusieurs blockchains international proposé à chaque constructeur de véhicule.

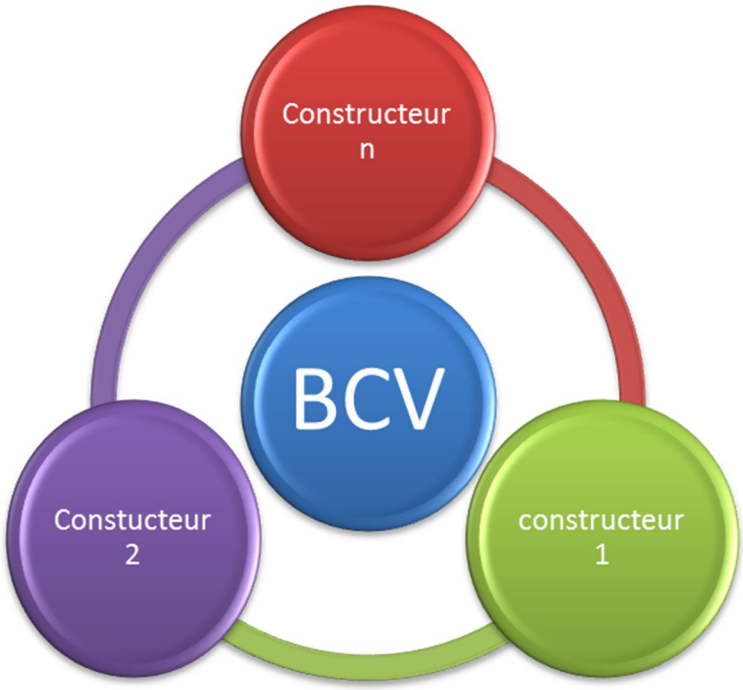

Figure 38-Architecture du la blockchain des véhicule

IV.2.1. Blockchain National

Cette Blockchain est destinée à enregistrer tous les véhicules existant sur le territoire national. On pourra aussi utiliser une blockchain pour chaque catégorie de véhicule (touristique, lord, transport, …), cette blockchain sera aussi destinée à enregistrer les opérations effectuer sur chaque véhicule.

IV.2.2. Blockchain Constructeur

Cette blockchain est propre à chaque constructeur, elle sauvegarde les VIN de chaque véhicule produit par ce constructeur.

Cette blockchain aura un identificateur unique qui sera mentionné dans les opérations effectué sur les véhicules produit par son constructeur. Ce dernier aura donc une paire de clé (clé publique et clé privée) largement diffusé sur internet à l'instant du reste de la blockchain existant cette blockchain est publier sur internet et télécharger par importe quel particulier ce qui élimine la possibilité de fraude.

Figure 39- blockchain constructeur

IV.3. Structure de bloc

Comme nous l'avons dit dans la séquence précédente le système composé de deux types de blockchain national et blockchain constructeur (Bcc).

IV.3.1. Structure blockchain constructeur (Bcc)

Bcc est destiné à publier sous forme d'une base de données. Les VIN de chaque véhicule produit par un constructeur (Nissan, Renault, …) après la production de chaque véhicule un VIN est gravé sur le châssis des véhicules. La même opération sera donc appliquée dans le monde virtuel et qui consiste à ajouter dans le bloc, une transaction signée par la clé privée des constructeurs.

Cette blockchain à un identifiant unique et chaque transaction dans cette blockchain à elle aussi un identifiant Tx unique qui va être mentionné dans les opérations effectuer sur le véhicule pour tout le VIN montre dans la transaction.

IV.3.2 Structure de la transaction

Chaque transaction est composée de :

- **Tx :** l'identifiant de transaction.
- **VIN :** ce champ contient le N° de châssis de véhicule produit par ce constructeur.
- **Date :** c'est la date de production de véhicule.
- **Sig :** permet la vérification du l'authenticité de la transaction et contient :
  - La clé publique.
  - Le haché de la totalité de transaction crypté par la clé privée du constructeur.

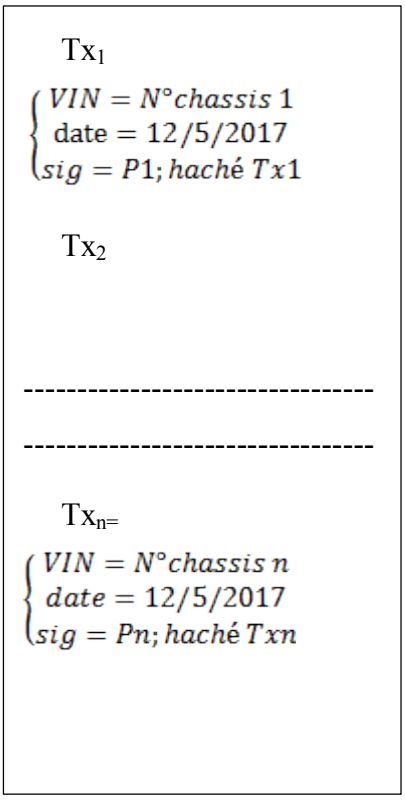

Figure 40 - Transaction du constructeur

IV.4. Blockchain nationale

La blockchain nationale est destinée à enregistrer les différentes opérations effectuées sur les véhicules au niveau national (vente / achat, enregistrement).

Cette blockchain va implémenter les opérations réelles d'une blockchain .il va être composé de plusieurs bloc générer à des intervalles réguliers et contenant des transactions générées par différente catégorie d'utilisateur (particulier, commun, douane…exact).

IV.4.1 Structure de transaction

Il existe plusieurs types de transaction vue qu'il existe d'ancien véhicule qui doivent être enregistré, des nouvelles voitures vient d'être importé de l'étrange, aussi que des voiture vendu ou acheté par des particuliers.

A. Enregistrent des anciens véhicules

Ces transactions sont contenues dans des blocs initiaux (bloc de genèse) et qui contient le VIN de chaque véhicule existant aux niveau national ces transaction sont signé par une clé déterminée par le ministère de l'intérieur.

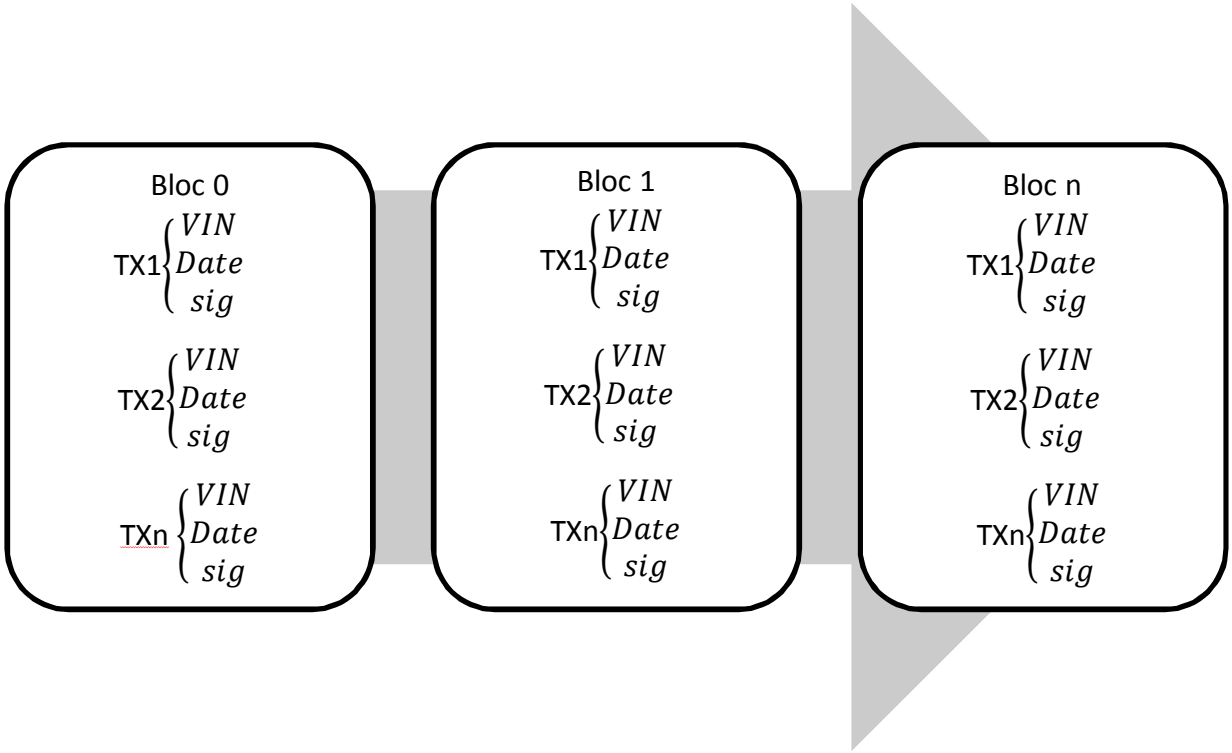

Figure 41- composante du bloc

- **Tx** : l'identifiant de transaction.
- **VIN** : ce champ contient le N° de châssis de véhicule produit par ce constructeur.
- **Date** : c'est la date de production de véhicule.
- **Sig** : permet la vérification du l'authenticité de la transaction et contient :
  - La clé publique.
  - Le haché de la totalité de transaction crypté par la clé privée du constructeur.

B. Enregistrement de nouveau véhicule

Ces transactions sont généralement signées par l'automobile responsable de l'importation ou bien la mise en circulation des véhicules. Au niveau national, la douane est responsable de cette opération.

❖ **Transaction**

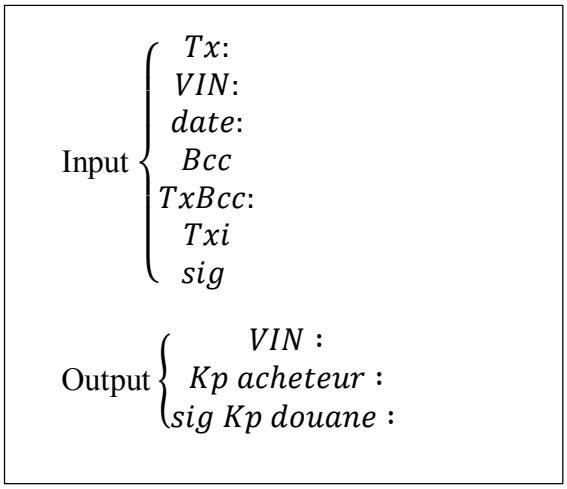

Figure 42-transaction d'un nouveau véhicule

- **Tx :** l'identifiant de transaction.
- **VIN :** ce champ contient le N° de châssis de véhicule produit par ce constructeur.
- **Date :** c'est la date de production de véhicule.
- **Sig :** permet la vérification du l'authenticité de la transaction et contient **:**
  - La clé publique.
  - Le haché de la totalité de transaction crypté par la clé privée du constructeur.
- **Bcc :** ce champ contient l'identifiant du bloc qui a produit le véhicule courant. Ce Bcc est disponible sur internet ou sur un support de stockage local pour pouvoir vérifier l'authenticité de véhicule.
- **Tx_{Bcc} :** Ce champ contient l'identifiant de la transaction contenant le **VIN** numéro de constructeur.
- **Txi :** Ce champ contient l'identifiant de la transaction contenant. Utilisé dans la blockchain constructrice ayant l'identifiant Bcc = 0.

Tableau 1- exemple des codes WMI

Code VMI	Constructeur	Code VMI	Constructeur
VN1	Opel France	**VWV**	Volkswagen Espagne
VNV	Nissan France	**VSX**	Opel Espagne
VNK	Toyota France	**VS6**	Ford Espagne,

C. Transaction (vent / achat)

Cette transaction est exécutée par des particuliers seul à une opération d'échange de main de voiture.

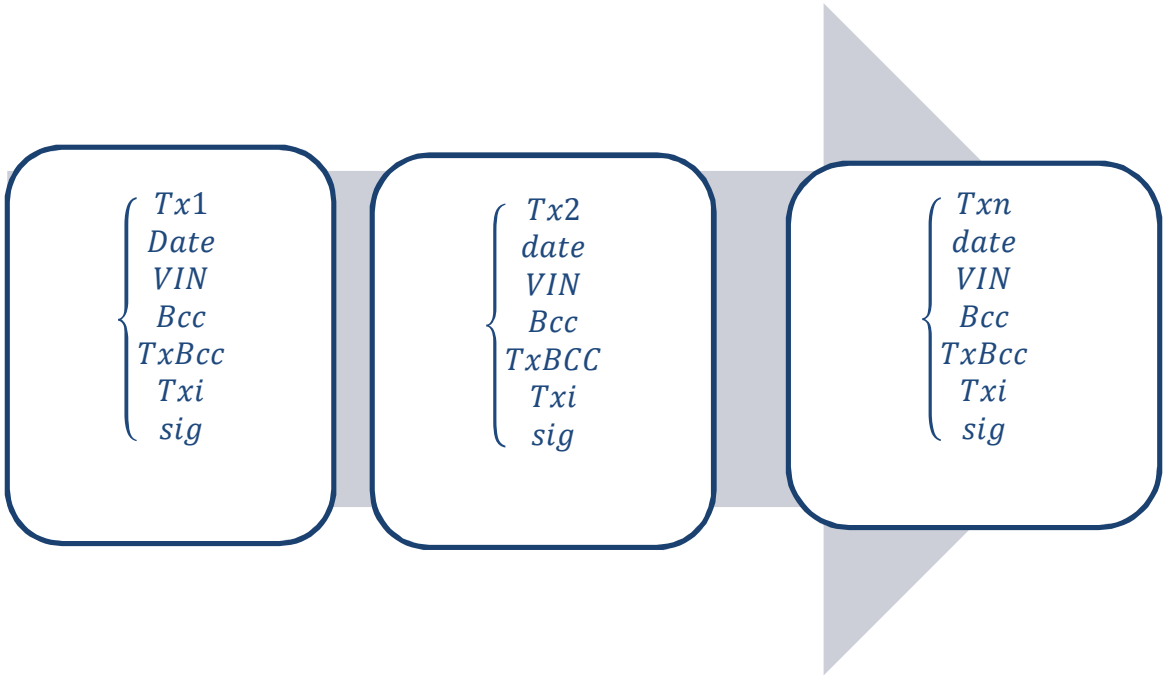

Figure 43- Composante du bloc de vente

Avec **Txi** est l'identifiant de la transaction du véhicule.

Cette transaction est composée d'une input et output

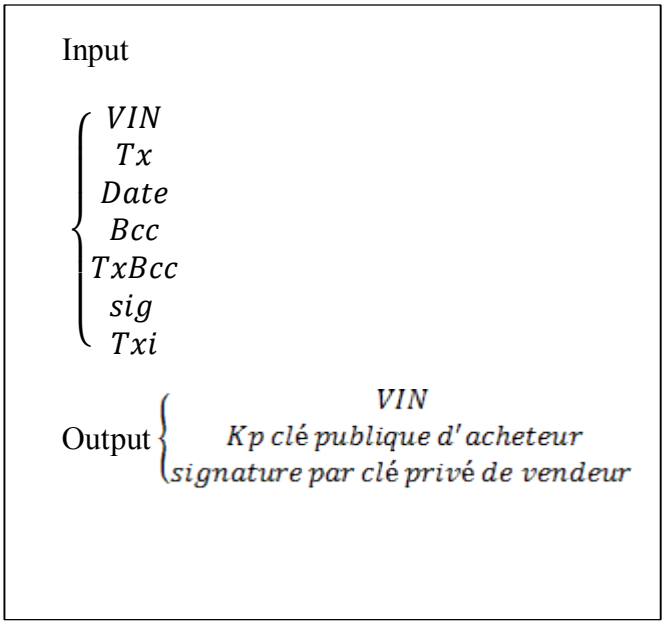

Figure 44- composante de la transaction de vente

Chaque transaction est composée de :

- **Tx :** l'identifiant de transaction.
- **VIN :** ce champ contient le N° de châssis de véhicule produit par ce constructeur
- **TxBcc :** Ce champ contient l'identifiant de la transaction contenant dans cette opération le TxBcc =0
- **Bcc :** ce champ contient l'identifiant du bloc qui a produit le véhicule courant. Ce Bcc est disponible sur internet ou sur un support de stockage local pour pouvoir vérifier l'authenticité de véhicule. Avec Bcc =0
- **Date :** c'est la date de production du véhicule.
- **Sig :** permet la vérification du l'authenticité de la transaction et contient :
  - La clé publique du constructeur.
  - Le haché de la totalité de transaction crypté par la clé privée du constructeur.
- **Kp :** clé publique de l'acheteur
- **Txi :** Ce champ contient l'identifiant de la transaction contenant

Le diagramme ci-dessous montre et résume les procédures au sein du réseau blockchain :

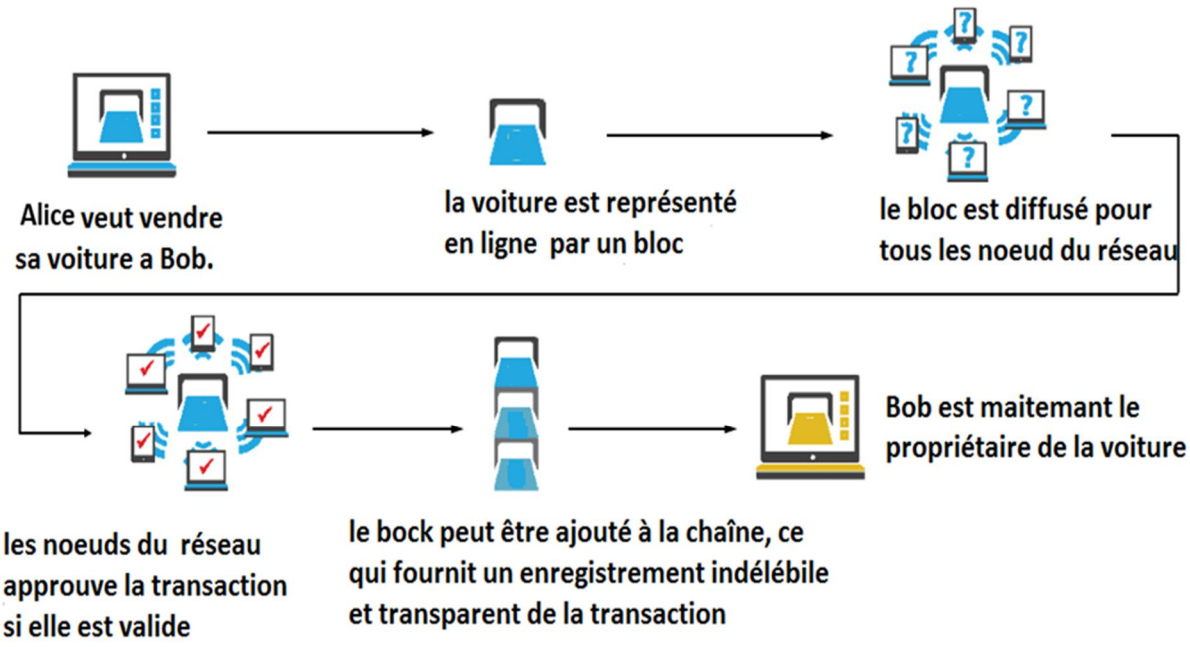

Figure 45- scénario de vente/achat dans la blockchain

V. Gestion de pair de clé

Pour pouvoir vendre ou acheter un véhicule sur une blockchain l'utilisateur doit avoir une paire de clés (privés / publique). Cependant l'utilisateur d'une thèse technique au niveau national se voit difficile car les blockchains et les paires de clés existant on ne met aucune relation entre la clé publique et l'identité réel d'utilisateur.

C'est pour ça on propose de crée une autorité de certificat national.

VI. Proposition de certificat Algérien (CA)

Cette autorité joue le rôle de tiers de confiance : vérifie l'identité d'utilisateur et garantir que la clé publique utilisé dans le système blockchain appartient au même utilisateur concerné

Ce certificat est fourni par le gouvernement pour chaque propriétaire et contient essentiellement une clé publique. Cette dernière est considérée comme le moyen d'authentification le plus sûr pour éviter la fraude à l'identité et protéger de manière efficace tous les données personnelles des propriétaires.

L'utilisateur demande au service de délivrance de CG, une demande de certificat accompagne de documents nécessaires. Lorsque l'autorité d'enregistrement reçoit la demande de l'utilisateur,

il vérifie l'identité de l'utilisateur et valide sa demande s'il est apte à recevoir un certificat. Par la suite, il passe cette demande à l'autorité de certification qui va appliquer les procédures.

Une fois que ces procédures sont faites, L'autorité de certification va signer un certificat contenant la clef publique de l'utilisateur. Par la suite, le certificat et la clef publique de l'utilisateur seront insérés dans une carte à puce. De plus, le certificat sera ajouté dans l'annuaire étant été signé par l'autorité de certification. La carte sera remise à l'utilisateur.

- **La solution initiale :** la carte à puce contient la clé publique et la clé privée d'utilisateur chiffré avec un mot de passe. Cette méthode est vulnérable au piratage et au piratage.
- **Deuxième solution :** l'enregistrement de la clé privé dans un document sous forme un code QR.

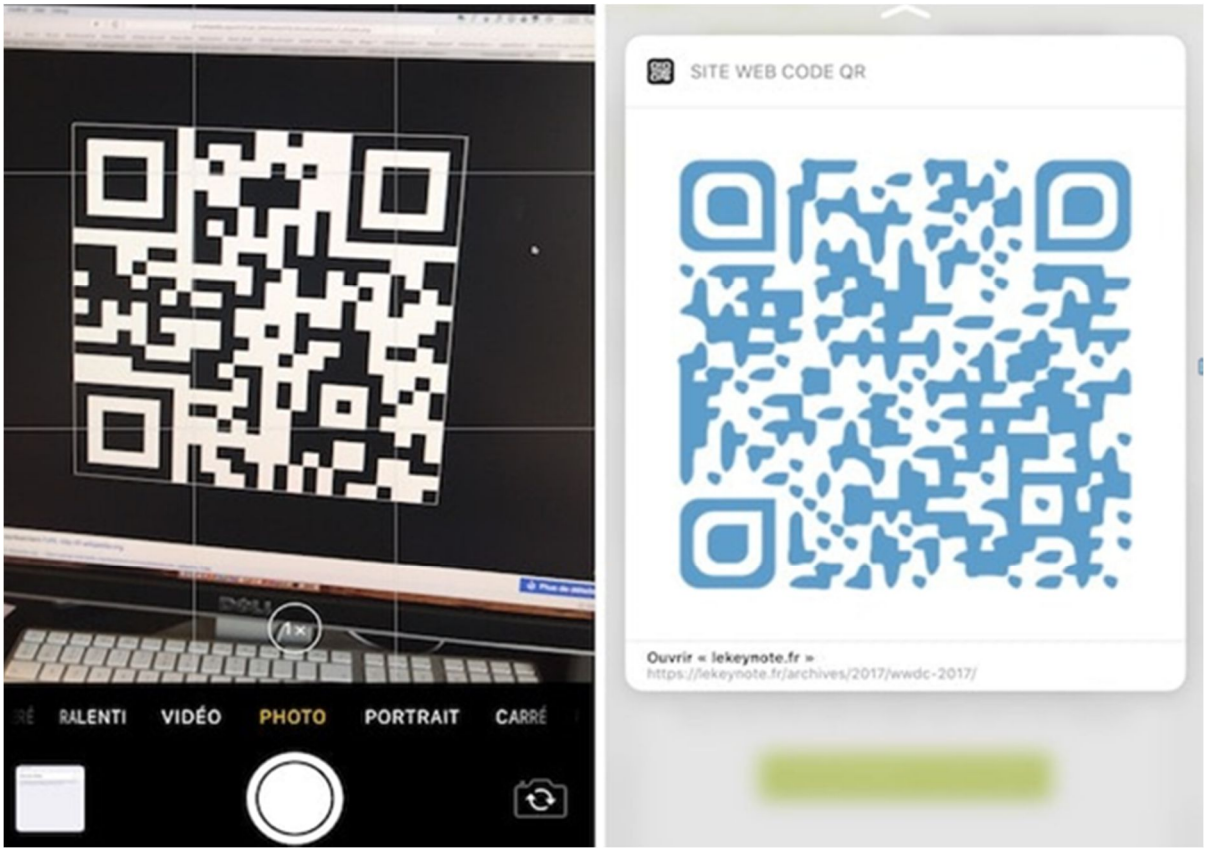

Figure 46- clé privé en code QR

VII. Structure de certificat

Ce certificat est divisé sur deux parties :

- **La partie 1 :** contient l'information de l'utilisateur (son nom et prénom, son pseudo ou son N° de dossier…) et sa clé publique.
- **La partie 2 :** contient la signature qui est le haché d'ensemble des informations avec sa clé publique (partie 1) et puis signé par une clé privée.

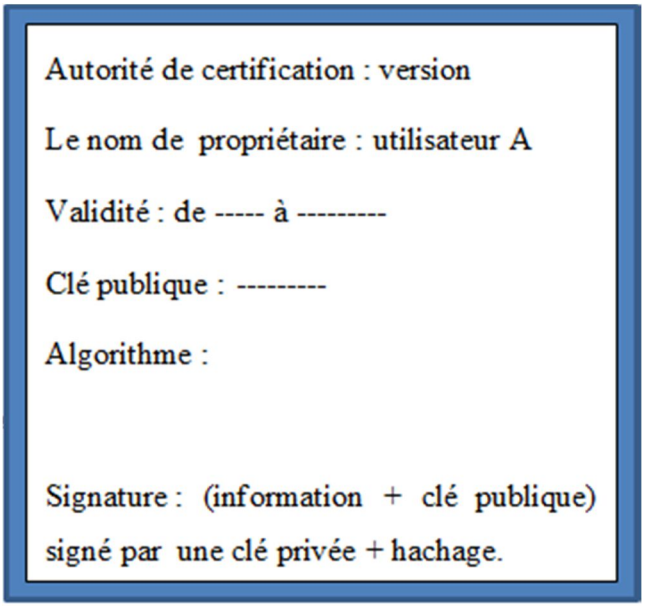

Figure 47- Certificat x509

VIII. Fonctionnement du système

VIII.1. La vente du véhicule

Pour vendre un véhicule les deux utilisations doivent se rapprocher d'une administrative local ou bien direct sur Internet en présentent la clé publique de l'acheteur et la clé privée du vendeur qui se trouve généralement sur une carte à puce.

Figure 48 - vente de véhicule

VIII.2. Vérification

Pour que les services de sécurité peuvent vérifier la propriété d'un véhicule ils doivent être équipé par un lecteur de carte à puce (on cas ou la clé publique) connecté à l'internet pour pouvoir vérifier l'existence de ce véhicule et sa relation avec la clé privée dans la blockchain.

IX. Conclusion

Ce présent chapitre a été consacré aux différents outils ayant contribués à l'aboutissement de ce 1projet. Ensuite on a détaillé du système proposé et son fonctionnement (architecture, les transactions, …etc.) a été mise en évidence. Enfin nous avons conclu par le service qui permettre de contrôler différentes entités du système de gestion de carte grise.

Conclusion générale

Conclusion Générale

On utilise la blockchain pour créer la confiance sur deux dimensions : l'origine de l'information et son inaltérabilité (son intégrité dans le temps).

Il est utile de comprendre les blockchains dans le contexte de bitcoin, mais surtout ne pas supposer que tous les écosystèmes blockchain ont besoin de mécanismes bitcoin tels que preuve de travail, règle de chaîne la plus longue. D'un autre côté, des registres distribués privés et des blockchains peuvent être déployés pour résoudre d'autres problèmes. Comme toujours, il existe des avantages et des inconvénients pour chaque solution, et on doit les considérer individuellement pour chaque cas d'utilisation.

L'intégration d'une blockchain dans IoT permettrait à l'utilisateur de mieux protéger sa vie privée en contrôlant l'accès à ses data qui sont les seuls à pouvoir accéder à la chaîne informatique sur laquelle les objets connectés communiquent.

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.

À l'heure où émerge la technologie blockchain, celle-ci peut apparaître comme une opportunité de restaurer une horizontalité entre utilisateurs du réseau, en faisant simultanément des prestataires et des utilisateurs de services tant numériques que réels, dans une approche pair-à-pair : l'action publique a tout à gagner à se saisir de cette possibilité pour assurer le maintien des registres d'opérations ou de propriété au service du contrôle, dans des domaines aussi distincts que le système de gestion de carte grise . Cette évolution permettra non seulement une meilleure fluidité des échanges, mais également un contrôle plus aisé des opérations, conduisant à un fonctionnement efficient au marché des véhicules. Cette évolution supposera toutefois une évolution substantielle de la relation contrôleur/contrôlé, en plaçant les contrôlés en capacité d'assurer une partie du contrôle de la correction des saisies dans la chaîne

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

Bibliographie

Bibliographie

[1] Mammeri Ilham, GuerricheNor El Houda<< Cryptographie homomorphe pour les réseaux « Vehicular Cloud Computing »>>, thèse de Master en Réseaux Mobiles et Services de Télécommunications, Université Abou bakrBelkaïd – Tlemcen – Faculté de TECHNOLOGIE

[2] BOUCHAMA Meryem <<Exploitation des transformées paramétriques dans le cryptage des image fixes. >>, Thèse magister communication, Université Ferhat Abbas de Sétif 1 ,28/10/2012.

[3] TouradjEbrahimi, Franck Leprévost, Bertrand Warusfel, le livre de << Cryptographie et sécurité des systèmes et réseaux>>, Editeur 'Hermès – Lavoisier', Informatique et systèmes d'information, 07/02/2006, UTF-8 / MARC-8

[4] Renaud Dumont<< Cryptographie et Sécurité informatique >>, cours 2009-2010, Université de Liège -Faculté des Sciences Appliquées.

[5] A. Abdelmalek, Cours cryptographie moderne 2017/2018, Master Réseau de Télécommunication université de Tlemcen.

[6] Thomas Fuhr<<Conception, preuves et analyse de fonctions de hachage cryptographiques >>, THÈSE de DOCTORAT, Informatique et Réseaux, ParisTech, 3 octobre 2011

[7] Laurent Fousse, Cours Cryptographie, <<Fonctions de hachage>>, 10/11/2008.

[8] « la révolution Blockchain » Algorithmes ou institutions, à qui donnerez-vous votre confiance ? » PHILIPPE RODRIGUEZ, 2017, ISBN : 978-2-10-076360-3

[9] « Comprendre la blockchain » Richard Caetano Stratumn, CEO Livre Blanc sous licence Creative Commons '' uchange.'' 2017

[10] : l'article de Satoshi Nakamoto Bitcoin « Système de Monnaie Electronique en Pair-à-Pair. » - publié le 1er novembre 2008 dans la liste de diffusion "The Cryptography Mailing List".

[11] « Les Blockchains » 'De la théorie à la pratique, de l'idée à l'implémentation 'Billal CHOULI - Frédéric GOUJON - Yves-Michel LEPORCHER -janvier 2017 - ISBN : 978-2-409-00536-7

[12] GODEBARGE Ferréol « Principes clés d'une application blockchain » ROSSAT Romain EM Lyon Business School -15/12/2016

Bibliographie

[13] « blockchain une opportunité pour les consommateurs d'énergie » version anglais

[14] une série des annales des mines « Blockchains et smart contracts : des technologies de la confiance ? » Publié l'Août 2017 dans ‘’RÉALITÉS INDUSTRIELLESS ‘‘série trimestrielle ‘’

[15] Bitcoin Éléments de compréhension technique Jean-Luc Parouty Institut de Biologie Structurale (IBS)

[16] K. Christidis, M. Devetsiokiotis "Blockchains and Smart Contracts for the IoT" IEEE ACCESS. 10, 2016, Department of Electrical and Computer Engineering, North Carolina State University, Raleigh,

[17] Das, Manik Lal, "Privacy and Security Challenges in Internet of Things," Distributed Computing and Internet Technology., pp. 33-48, 2015.

[18] “SelfKey “ SelfKey Foundation 11 septembre 2017

[19] Le registre des méthodes d'identificateur décentralisé. Manu Sporny ; Drummond Reed. Groupe de la communauté de vérification numérique. CG-DRAFT. URL: https://w3c-ccg.github.io/did-method-registry/

[20] Mustapha Benjada << PKI (Public Key Infrastructure)>> article au journal on ligne La sécurité informatique - La sécurité des informations, www.securiteinfo.com.

[21] bitcoin site official www.bitcoin.org.fr

[22] blockchain France « Qu'est-ce que la blockchain» https://blockchainfrance.net.

[23] www.ethereum-france..

[24] Groupe communautaire W3C. « Identificateurs décentralisés (DID) » v0.7. Récupérée de Github. (2017, 30 novembre)

[25] Team Tokens24, « Identité décentralisée (DID) : Tout ce que vous devez savoir », April 27, 2018.

[26] Shaan Ray « Blockchains et identité numérique » ‘’ Towards Data Science ‘’10 mars 2018

[27] Tema Jendela Gambar Arpil crass « identité distribuer » 22 Mai 2018

Glossaire

A

AC : Attribut Certificat.

B

Bcc: Blockchain constructer

C

CA: Certificate Authority.

CG : carte grise. (Certificat de propriété de véhicule)

CRL : Contribution sur les Revenus Locatifs.

D

DID : Identificateurs Digital Décentralisés.

DNS : Domain Name System.

DRAG : Direction de la réglementation et des affaires générales

E

ECDSA : Elliptic Curve Digital Signature Algorithm.

EDGE: Enhanced Data rates for GSM Evolution.

H

Http: HyperText Transfer Protocol.

I

ID: Identity Digital.

IOT: Internet of Thing.

IP : Internet Protocol.

M

MAC : Message Authentiquassions Code.

MD5 : Message Digest 5.

MDC : Modification Détection Code.

MSISDN: Mobile Station International Subscriber Directory Number.

N

NIST: National Institute of Standards and Technology.

NSA: National Security Agency

P

P2P: Peer-TO-Peer.

PGP: Pretty Good Privacy.

PKI: Public Key Infrastructure.

PMI: Project Management Institute.

POW: Proof of Work.

Q

QR : Code-barres 2D

R

RA: Registration Authority.

S

SHA: Secure Hash Algorithm.

T

TC : Transmission Control Protocol.

U

URL: Uniform Resource Locater.

UUID : Universel Unique Identifier.

V

VIN : Vehicle Identification Number.

VPN: Virtual Privat Network.

W

WMI: World Manufactured Identificroutier.

Résumé

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

Les différents avantages que pourrait apporter la technologie Blockchain au secteur public, permettras la protection des données critiques, de pouvoir s'assurer de la propriété de biens, ou encore de créer un réseau puissant entre les différents services publics et surtout le stockage des données Ceci est fondamental pour plusieurs contextes au secteur publique.

Dans ce travail on s'intéressait à l'utilisation du Blockchain pour la gestion des opérations sur les véhicule (vente / achat et enregistrement). La proposition donne solution au différent problème liée au domaine du véhicule fraude du vol on se bassons sur des transactions similaire à la transaction du bitcoin.

Mots clés :

Blockchain, Cryptographie, Cryptomonnaie, Bitcoin, transaction, Carte grise biométrique.

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.

With the various benefits that Blockchain technology could bring to the public sector, it is believed that it could help protect critical data, ensure ownership of assets, or create a powerful network between different public services. And especially the storage of data this is fundamental for several contexts in the public sector.

In this work we will use the blockchain technology for running the operation related to the vehicles domain such as sale, bay and registration. The proposed blockchain gives solution to different problem related to the vehicle market such as theft, fraud ……. etc.

Keywords:

Blockchain, Cryptography, Cryptocurrency, Bitcoin, Transaction, Gray card.