République Algérienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la recherche scientifique
Université Larbi Tébessi - Tébessa
Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie
Département : Mathématiques et Informatique

Mémoire de fin d'étude
Pour l'obtention du diplôme de MASTER
Domaine : Mathématiques et Informatique
Filière : Informatique
Option : Systèmes d'information

Thème

Contribution basée Blockchain pour la planification urbaine

Présenté Par :

Touati-Hamad Zaineb

Devant le jury :

Dr.Derdour Makhlouf	*MCA*	*Univérsité Larbi Tébessa*	*Président*
Dr.Haouam Med Yassine	*MCB*	*Univérsité Larbi Tébessa*	*Examinateur*
Pr.Laouar Med Ridda	*Prof*	*Univérsité Larbi Tébessa*	*Encadreur*

Date de soutenance : 06/2019

Remerciement

Je voudrais tout d'abord exprimer mes plus profonds remerciements à mon encadreur Pr.LAOUAR MED RIDDA pour son accord d'être mon directeur de mémoire et de sa disponibilité et son aide pendant toute la préparation de ce travail.

Je tiens aussi à remercier tous les membres de jury : Dr.Dardour Makhlouf et Dr.Haouam Med Yassine, pour leur disponibilité et acceptation d'examiner et de rapporter mon travail.

Je remercie ainsi Dr. Bendhib Issam le chef de spécialité Système d'information et Dr. Bourogaa-tria Salima pour ses conseils et son encouragement ainsi que tous les enseignements de département Mathématique et informatique.

Je remercie tous mes collègues de l'université de Tébessa, pour leurs encouragements et précieuses orientations pendant toute la période de l'élaboration de ce travail.

Je ne saurais oublier de remercier ma mère ainsi que mes sœurs pour leur soutien moral, leurs encouragements et leur patience durant les étapes de réalisation de ce travail.

Enfin, Que tous ceux qui directement ou indirectement m'ont apporté leur aide, trouvent ici l'expression de mes sincères remerciements.

Dédicace

A ma mère, ma pow algorithme... !

الملخص

تعد إمكانات التخطيط الحضري لحل المشكلات البيئية وإدارة النفايات مهمة لأن الإغراق غير القانوني للنفايات الصلبة هو أحد الأحداث المتعلقة بأنشطة معالجة النفايات بشكل غير قانوني. عملية إدارة النفايات سيئة للغاية، خاصة عندما يتعلق الأمر بتأكيد الوجهة الصحيحة لتسليم النفايات. في هذا العمل، نقترح اتباع نهج قائم على سلسلة البلوكتشين لتتبع النفايات لتمكين الإبلاغ عن بيانات النفايات في نظام واحد. سلسلة الكتل هي تقنية أثبتت نفسها بالفعل في القطاع المالي. إنه يسجل المعاملات بأمان في دفتر الأستاذ الكبير والمختوم زمنياً باستخدام الخوارزمية إثبات العمل، ويسمح لنا بصياغة عقود ذكية على شبكة الإيثريوم. إن تطبيق هذه التكنولوجيا على قطاع النفايات سيمكن من تسجيل موثوقة وشفافة وآمنة لجميع حركات النفايات، وبالتالي تمكين تتبع النفايات من المصدر إلى المعالجة والتخلص منها. سيتمكن المستخدمون من استيراد وتصدير البيانات من خلال واجهة مستخدم تقدم مستويات مختلفة من الوظائف والوصول. كما سيتم تحديد الجرائم غير القانونية المهدرة والتصرف فيها.

الكلمات المفتاحية: التخطيط الحضري، سلسلة الكتل، إدارة تتبع النفايات، العقد الذكي، الإيثريوم، خوارزمية إثبات العمل

ABSTRACT

The potential of urban planning to solve environmental problems and manage waste is important because the illegal dumping of solid waste is one of the events related to illegal waste treatment activities. The waste management process is very poor, especially when it comes to confirming the correct destination for the delivery of waste. In this work, we are proposing a chain-based approach to waste tracking to enable waste data reporting in a single system. The block chain is a technology that has already proven itself in the financial sector. It securely records transactions in a large, time-stamped ledger using the PoW algorithm, and allows us to write smart contracts on the ethereum network. The application of this technology to the waste sector will enable reliable, transparent and secure recording of all waste movements, thus enabling waste to be traced from source to treatment and disposal. Users will be able to import and export data through a user interface offering different levels of functionality and access. It will also identify and act on illegal wasteful crimes.

Key words: Urban planning Blockchain, waste-tracking management, Smart contract, Ethereum, PoW.

RÉSUMÉ

Le potentiel des planifications urbaines pour résoudre les problèmes environnementaux et gérer les déchets est important, car le déversement illégal de déchets solides est l'un des événements liés aux activités de traitement illégal des déchets. Le processus de gestion des déchets est très médiocre, notamment lorsqu'il s'agit de confirmer la destination correcte pour la livraison des déchets. Dans ce travaille, nous proposons une approche du suivi des déchets basée sur la chaine des blocs afin de permettre la création de rapports sur les données de déchets dans un système unique. La chaine des blocs est une technologie qui a déjà fait ses preuves dans le secteur financier. Elle enregistre les transactions de manière sécurisée dans un grand livre distribué basé sur un horodatage à l'aide de l'algorithme de PoW, et elle nous permet de rédiger des contrats intelligents sur le réseau etherium. L'application de cette technologie au secteur des déchets permettra un enregistrement fiable, transparent et sécurisé de tous les mouvements de déchets, permettant ainsi le suivi des déchets depuis leur source jusqu'à leur traitement et leur élimination. Les utilisateurs pourront importer et exporter des données via une interface utilisateur offrant différents niveaux de fonctionnalité et d'accès. Il identifiera et agira également sur les crimes illégaux liés au gaspillage.

Mots clés : Planification urbaine, La chaine des blocs, gestion de suivi des déchets, Smart contract, Ethereum, PoW.

Table des matières

Liste des abréviations

Dapp	Application decentralize
Ddos	Distributed Denial of service attack
EVM	Ethereum Virtual Machine
HDPE	Polyéthylène Haute densité
LDPE	Polyéthylène Base densité
MD	Message Digest
PET	Polyéthylène téréphtalate
POC	Proof Of Concept
POW	Proof Of Work
POS	Proof Of Stake
PP	Polyéthylène très facile à colorer
PS	Polymère styrénique
PVC	Polyéthylène de vinyle
QR	Code Quick Response
RPC	Remote Procedure Call
SHA	Secure Hash Algorithm

LISTE DES FIGURES

LISTE DES TABLEAUX

INTRODUCTION GÉNÉRALE

Les déchets ont toujours été générés par les activités humaines. Les déchets n'étaient pas un gros problème car la population était relativement jeune et nomade. Cependant, il est devenu un grave problème d'urbanisation et de croissance de troubles importants. Une mauvaise gestion des déchets a contaminé l'eau, le sol et l'atmosphère et a eu un impact majeur sur la santé publique. L'absence de contrôle, une législation inadéquate et les effets négatifs sur l'environnement et la santé humaine dus à de nombreux incidents de pollution graves et à la publicité ont suscité des préoccupations. Ces pratiques de gestion des déchets ont obligé de nombreux gouvernements nationaux et fédéraux à mettre en place de nouveaux cadres réglementaires pour traiter les processus de gestion des déchets dangereux et non durables. La gestion des déchets comprend des activités comprenant : a) la collecte, le transfert, le traitement et l'élimination des déchets, b) la surveillance, le suivi et la réglementation de la production, de la collecte, du transport, du traitement et de l'élimination des déchets. Dans cette étude, nous avons évalué l'applicabilité de la technologie blockchain à la gestion des déchets.

L'immatriculation des véhicules a toujours été fastidieuse. Il s'agit d'un processus multipartis prenant beaucoup de temps, qui risque également d'altérer des informations non autorisées, de répéter des données et de commettre diverses erreurs.

Dans un tel scénario, des informations importantes peuvent être exposées à la fraude, à la falsification de données ou même ne plus être suivies. Plusieurs vagues technologiques ont organisé les développements et révolutionné les échanges entre individus en permettant la création et la diffusion d'informations transmises par des stations toujours plus diverses et pluralistes.

La décentralisation des bases de données blockchain peut simplifier la gestion d'informations fiables, en permettant aux administrateurs et même aux utilisateurs d'accéder plus facilement aux données importantes du secteur tout en préservant la sécurité de ces informations. Blockchain est un enregistrement numérique crypté stocké sur plusieurs ordinateurs d'un réseau public ou privé et qui constitue un outil de contrôle pour la chaîne logistique.

Pour ce faire, nous abordons la question de recherche suivante ***: Comment les organismes municipaux peuvent-ils utiliser la technologie de la blockchain pour traiter des données transactionnelles sur la gestion des déchets ?***

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

Une introduction générale,

Le premier chapitre est consacré au contexte d'étude il est divisé en deux parties, dans la première en parle le contexte urbain nous essayons de définir le plus précisément possible. Qu'est-ce qu'un projet urbain, Le développement durable, la gestion urbaine, l'urbanisme, les problèmes liés au contexte urbain et la seconde partie précise la gestion de déchet ainsi que la problématique a à traiter dans cette thèse.

Dans ***le deuxième chapitre*** nous mettons l'accent sur la technologie utilisée. Il est divise en deux parties, dans la première partie nous présentons la cryptographie derrière la technologie blockchain nous donnons quelques notions de base liées à la cryptographie ; des concepts importants pour la suite du mémoire. La deuxième partie introduit le concept du Blockchain, ces caractéristiques, son fonctionnement, l'architecture, et nous terminons ce chapitre avec les diffèrent application de la technologie blockchain.

L'état de l'Aat est présenté dans ***le troisième chapitre***, dans laquelle nous présentons une synthèse sur les différentes technologies utilisées dans les systèmes de suivi de déchets.

Le quatrième chapitre, comporte en première partie notre contribution, dans laquelle nous détaillons notre architecture basée sur la technologie blockchain ainsi que dans la deuxième partie nous présenterons notre cas d'étude et les outils fournis pour l'implémentation de notre contribution proposée suivi par les résultats obtenus et quelques discussions autour de ces derniers.

Enfin, Nous conclurons ce manuscrit en présentant quelques perspectives ouvertes par notre travail.

CHAPITRE 1

LE CONTEXTE DU PROJET URBAIN & PROBLEMATIQUE

Les milieux urbains constituent une dimension fondamentale dans le monde et la conception de ces milieux devient une tâche très difficile à cause des besoins très divers auxquels l'aménagement des surfaces doit répondre tels que : l'agriculture, la protection de l'environnement, la vie sociale, les activités économiques et financières, etc.... En effet, cet aménagement est assuré par la discipline nommée : la planification urbaine. La planification urbaine est l'ensemble des outils et des moyens permettant la mise en œuvre des politiques sectorielles et la rationalisation de la gestion urbaine à travers la définition d'objectifs, de principes de développement et de projets d'aménagement. La planification urbaine constitue, donc une composante importante et un élément moteur dans le processus de développement des villes. Dans ce chapitre, nous allons présenter un aperçu sur le contexte de la planification urbaine en mettant l'accent sur ses différents aspects, objectifs, missions et principes fondamentaux afin de présenté notre problématique.

Partie I : Le contexte du projet urbain

1.1 Principes de la planification urbaine

L'expression "planification urbaine" a été définie et abordée selon différentes sources, parmi lesquelles nous citons :

- Le dictionnaire d'urbanisme (Merlin and Choay, 1988) définit la planification urbaine comme étant un « ensemble d'études, de démarches, voire de procédures juridiques ou financières, qui permettent aux collectivités publiques de connaître l'évolution des milieux urbains, de définir des hypothèses d'aménagement concernant à la fois l'ampleur, la nature et la localisation des développements urbains et des espaces à protéger, puis d'intervenir dans la mise en œuvre des options retenues ».

- D'après (Laborde, 1994) la planification urbaine est : « les plans, les institutions, les pratiques et les techniques qui cherchent à organiser la ville. La planification part de la demande sociale et non de la quête d'une quelconque ville idéale. Elle est apparue comme moyen d'empêcher l'anarchie urbanistique, de réaliser l'harmonie entre les besoins en logements, en emplois, en services, en circuits de distribution et en infrastructures de circulation. Elle traduit le passage de l'urbanisme d'autrefois à l'aménagement de l'espace de la ville de demain ».

- Finalement, selon Nigel Taylor (Ineichen, 2007) « la planification urbaine n'est pas, au sens strict, une science (pas même une science sociale). C'est plutôt une forme d'action sociale, mue par certaines valeurs morales, politiques et esthétiques dans le but de donner forme à l'environnement physique. C'est pour cette raison que ce type d'action sociale peut se retrouver sous de multiples formes». La planification urbaine n'est pas donc un acte en soi mais l'outil qui permettra la mise en œuvre du développement et l'expression d'un projet de société.

La planification urbaine couvre un ensemble de secteurs physiques et sociologiques, nous citons la démographie, l'emploi, l'habitat, l'utilisation des sols, les services publics, le budget, l'environnement, le transport… etc. La figure 1.1 illustre l'interaction entre ces différents secteurs.

Robert Laurini (Laurini, 2014) a mentionné que ces activités de planification ont les quatre qualités suivantes en commun :

1. **La planification est orientée vers l'avenir :** Les décisions prises dans le processus de planification sont généralement faites pour affecter une condition future dans l'environnement.

2. **La planification est politique :** Chaque décision de planification publique a lieu dans un

contexte politique. Il est important de réaliser que la majorité des activités de planification impliquent l'utilisation ou la réglementation des terrains sous une certaine forme.

3. **La planification concerne la définition et l'évaluation des solutions alternatives pour résoudre les problèmes :** Cela est profondément ancré dans les théories de la planification rationnelle qui sous-tendent la pratique de la planification actuelle.

4. **La planification a une responsabilité particulière pour représenter les besoins des minorités :** les personnes handicapées, pauvres et les groupes sous-représentés. Les planificateurs doivent prêter une attention particulière aux besoins de ces groupes dans le cadre de leur code professionnel de déontologie.

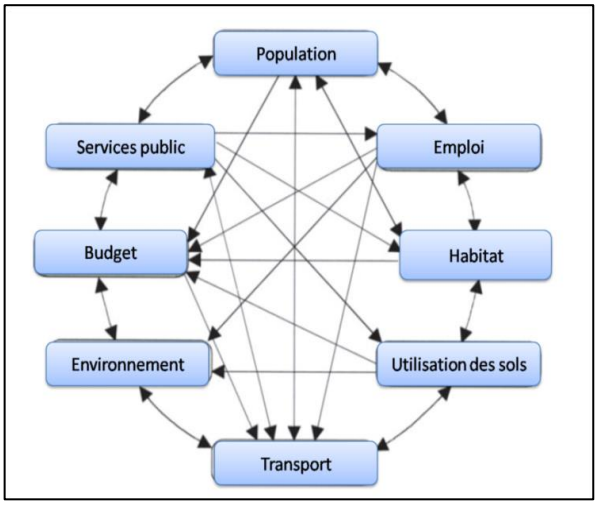

FIGURE 1.1 Quelques composantes du système urbain (Laurini, 2014)

1.2 Les objectifs de la planification urbaine

La réalisation des objectifs de la planification urbaine est essentiellement une tâche politique. Les objectifs de la planification territoriale urbaine sont résumés comme suit (Guder, 2003):

- La planification urbaine doit coordonner les différentes fonctions du sol.
- La planification urbaine doit coordonner les affectations, arbitrer les conflits d'utilisation, etc.
- La planification urbaine doit s'inscrire dans les perspectives du développement durable à savoir la durabilité, principe de prévention voire de précaution, le développement socio-économique équilibré des régions, l'amélioration de la qualité de la vie et la protection de l'environnement.
- En effet, la planification territoriale urbaine ne permet pas uniquement de légaliser les zones à bâtir, mais elle propose aussi une approche globale d'urbanisation, de transport, d'environnement, de nature, d'économie…

1.3 La planification urbaine en Algérie

L'Algérie est classée deuxième pays le plus grand géographiquement en Afrique. Toutefois elle occupe peu son l'espace. Afin d'atteindre cette situation, l'Algérie a tracé une nouvelle vision de la planification urbaine visant plusieurs buts (MATE, 2004) :

- Assurer un développement harmonieux et durable de l'ensemble du territoire national
- Compenser les handicaps naturels et géographiques des régions et des territoires.
- Protéger les territoires contre les risques liés aux aléas naturels et technologiques.
- Promouvoir les potentialités et les avantages comparatifs de chaque espace.
- Organiser la croissance des villes et favoriser le développement qualitatif des agglomérations.

1.4.1. Les instruments de la planification urbaine

La politique de la planification urbaine en Algérie est menée au moyen d'un ensemble de schémas et de plans d'aménagement situés à différents niveaux d'échelles, dont on peut citer :

Schéma	**Description**
SNAT : le Schéma National d'Aménagement du Territoire	Il exprime la vision prospective de l'occupation du territoire national en liaison avec la stratégie du développement économique, social et culturel. (CFU, 2001)
SRAT : le Schéma Régional d'Aménagement du Territoire	Un instrument d'appui qui assure avec une plus grande précision la définition des choix et des actions d'aménagement du territoire à l'échelle régionale. (MATE, 2004)
PDAU : le Plan Directeur d'Aménagement et d'Urbanisme	Un instrument de planification spatiale et de gestion urbaine.(CFU, 2001) Il fixe les orientations fondamentales de l'aménagement de la commune ou des communes qu'il couvre tout en tenant compte des schémas d'aménagement et des plans de développement.
POS : Plan d'Occupation des Sols	Fixe de manière détaillée les droits d'usage des sols et de construction. Il est établi progressivement pour couvrir le territoire défini par le PDAU.

Tableau 1.1 Les instruments de la planification urbaine

1.4.2. Evolution de planification urbaine

La planification urbaine s'imposée avec l'essor des villes, la croissance démographique mais aussi la rente pétrolière. En Algérie, la préoccupation de la ville et ses implications sur l'environnement ne s'est manifestée que tardivement avec le 2ème plan quadriennal de

développement (1947-1977). C'est dans le contexte de la libéralisation de l'économie algérienne des années 90, que l'État se donne de nouveaux objectifs dans le cadre de l'aménagement du territoire. Ainsi, les instruments de la planification urbaine ont évolué dans des contextes de développement économique différents. (RAHMOUN, 2013).

1.4.3. Le développement durable

Le terme développement durable a été véritablement défini pour la première fois en 1987 dans le rapport Bruntland (Vaillancourt, 1998): « le développement durable doit assurer la croissance économique, l'amélioration de l'environnement et la préservation des ressources naturelles. Il doit permettre de répondre aux besoins actuels, sans compromettre les possibilités pour les générations futures de répondre à leurs propres besoins.»

Ainsi, le développement durable peut être considéré comme étant un développement qui prend en compte les besoins des générations présentes sans compromettre la satisfaction des besoins des générations futures. Il repose sur les trois piliers (Destais, 2011) : le pilier écologique, le pilier social et le pilier économique et se réaliserait à leurs intersections ; un compromis doit alors se faire entre les dimensions écologiques, sociales et économiques .

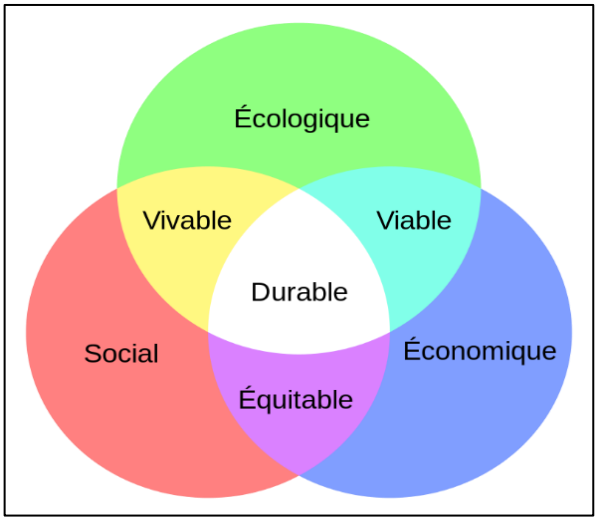

FIGURE 1.2 Quelques composantes du système urbain (Laurini, 2014)

En Algérie, la prise en charge de l'environnement sous ses différents aspects a été pendant fort longtemps méprisé : la pollution de l'air, la désertification, les changements climatiques, la remontée des eaux dans le Sud, l'appauvrissement de la diversité biologique, etc. Le souci, de mieux prendre en charge le secteur de l'environnement se fait sentir de manière plus sérieuse, plus pressante et plus éminente ces dernières années (Kaouther, 2007).

En effet, la création du ministère de l'aménagement du territoire et de l'environnement est venue pour engager parallèlement à la politique nationale de l'aménagement du territoire une stratégie nationale de l'environnement permettant d'assurer les principes de développement durable

1.4 Les principes fondamentaux de la planification urbaine

La planification urbaine s'appuie sur trois grands principes (voir figure 1.3) (MATE, 2004) :

1. La coordination

Une des principales missions de la planification territoriale urbaine, elle consiste à coordonner les différentes demandes formulées en matière d'affectation des sols compte tenu de ses propres objectifs et des exigences des politiques sectorielles.

2. La coopération

La coopération une action collective par laquelle des sujets contribuent à un même résultat. En ce sens, les processus optant pour un mode de fonctionnement coopératif attendent en retour une minimisation des risques et une réduction de l'incertitude.

3. La participation

La participation est un moyen indispensable pour la validation d'un projet en planification urbaine. Elle permet l'intégration des différents acteurs (individus ou groupes) pour aider le décideur à établir un choix et améliorer les procédures décisionnelles.

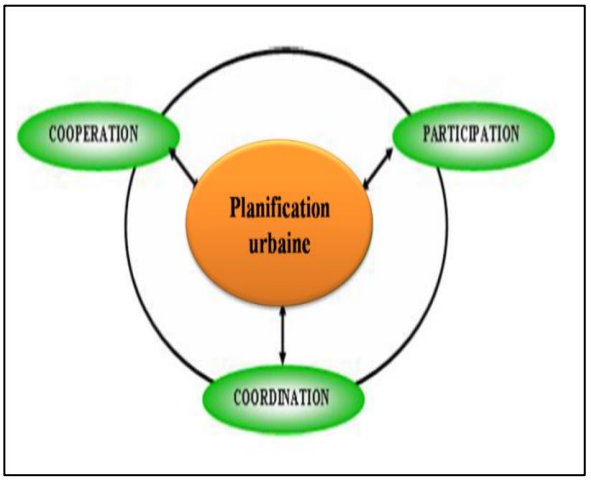

FIGURE 1.3 Principes de la planification urbaine (MATE, 2004)

1.5 L'évaluation dans le cadre de la planification urbaine

1.5.1 Notion du projet urbain

La notion de « projet urbain » apparaît dans les années 1970 comme une réponse à de nombreux bouleversements (Tomas, 1998). Selon (Masboungi and De Gravelaine, 2002), le projet

urbain « organise un territoire afin d'en améliorer l'usage, la qualité, le fonctionnement, la dynamique économique et culturelle et les relations sociales. Il doit assurer à tous l'accessibilité à l'espace public, à l'habitat, aux équipements, aux transports ; se préoccuper de la qualité des espaces publics, de l'architecture, des paysages, de l'environnement naturel, de la mise en valeur du patrimoine ; servir les enjeux du développement durable, avec une utilisation économe de l'espace tout en garantissant le fonctionnement des infrastructures, ainsi que des réseaux de transports et de distribution.»

1.5.1.1 Types de projets urbains

Il existe trois types de projets urbains :

- **Le projet urbain politique :** regroupe les projets dits « de territoire », « de ville, « de développement » ; il couvre tout le territoire communal ou intercommunal (Arab, 2004).
- **Le projet urbain opérationnel :** est considéré comme des opérations urbaines d'une certaine ampleur, durant au moins une dizaine d'années, généralement multifonctionnelles, associant des acteurs privés (Ascher, 1995).
- **Le projet urbain architectural :** est réservé à l'approche du « design urbain », en lien avec sa réhabilitation faite par les architectes-urbanistes. Il est centré sur un bâtiment, ou un ensemble de bâtiments.

1.5.1.2 Acteurs du projet urbain

Il existe plusieurs groupes qui ont un rôle important pour l'avancement du projet urbain (Dind and Da Cunha 2011):

1) **Les acteurs concernés :** qui ont un rôle dans la marche du projet urbain. On distingue :
   - **Les décideurs :** Il s'agit des élus concernés, ainsi que des chefs de service des administrations ayant un pouvoir décisionnel sur le projet urbain. Leur rôle est de donner une orientation au projet urbain, et de mettre à disposition les ressources nécessaires.
   - **Les opérationnels :** Ce sont les acteurs en charge de la gestion concrète du projet : le chef de projet, les collaborateurs des administrations impliquées dans la structure opérationnelle. Leur rôle est de mener le projet urbain, en réalisant les objectifs fixés par les décideurs.
2) **Les acteurs intéressés :** qui s'impliquent plus ou moins ponctuellement sur un aspect ou un autre du projet urbain. On distingue :
   - **Les mandataires :** sont des professionnels qui ont une mission sur un aspect ou l'autre du projet urbain : consultants stratégiques, architectes, sociologues et animateurs des démarches participatives.

- **Les associations :** ce sont des interlocuteurs clés pour la gestion des projets. Non seulement elles amènent de précieuses connaissances sur le contexte local, mais elles proposent le plus souvent un regard pointu et complémentaire sur des thématiques particulières.

3) **Les acteurs touchés :** sont ceux que le projet urbain affecte directement. On distingue :

- **Les propriétaires :** il peut s'agir de simples propriétaires privés souhaitant valoriser leur parcelle, ou de propriétaires institutionnels tels que les caisses de pension et les assurances.
- **Les habitants :** les habitants ne constituent pas un groupe d'acteurs homogène. Ils se distinguent par leur attitude, par leur niveau de participation, par les enjeux qu'ils défendent (privés, collectifs, sociaux, environnementaux,..).

Il est important de noter qu'il existe entre les différents acteurs des relations. D'après (Laurini, 2014) ces relations peuvent être :

- **En coopération** : les acteurs travaillent ensemble pour résoudre les mêmes types de problèmes, partagent les mêmes plans d'action, et ils mettent en commun leurs ressources.
- **En conflit :** les acteurs ont des intérêts divergents dans la résolution du problème ; peut-être un conflit d'objectifs ou de signification ; le plus fréquent est celui des objectifs.
- **En négociation :** les acteurs ils acceptent partiellement ou temporairement de partager certaines ressources pour résoudre un problème.

1.5.1.3 Principales étapes du projet urbain

Le déroulement d'un projet urbain s'articule autour d'un processus d'étapes séquentielles et complémentaires (Laouar, 2005) (Figure 1.4) :

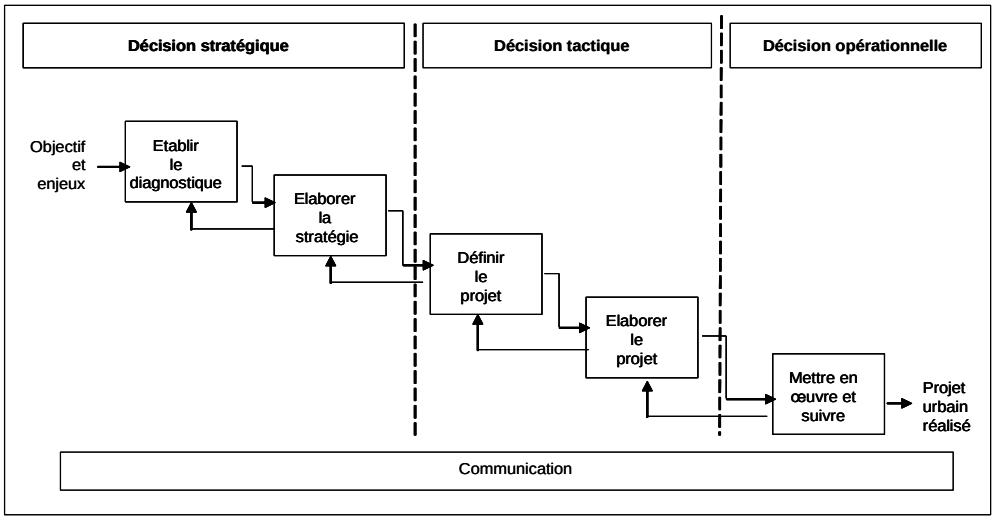

FIGURE 1.4 Processus de conduite d'un projet urbain (Laouar, 2005)

- **Etablir le diagnostic :** pour préciser les réflexions menées en matière d'urbanisme, la consultation des différents acteurs et les études et les données existantes. Il est nécessaire pour définir le contexte, la problématique et le périmètre d'intervention.

- **Elaborer la stratégie :** c'est l'étape la plus difficile à franchir et la plus sensible politiquement. En effet elle oblige les responsables politiques à s'avancer, à se positionner vis-à-vis d'un avenir par définition incertain.

- **Etablir le projet :** c'est l'étape la plus classique, elle consiste à mettre en forme (textes, documents graphiques, …) la stratégie définie à l'étape précédente en termes de grandes politiques d'aménagement et de développement économique, social, environnemental, …

- **Elaborer le projet :** à la suite du diagnostic, les objectifs et les grandes lignes du projet urbain se formalisent dans le cadre d'un plan de référence. Ce document est constitué de plans synthétiques qui traduisent les grandes options de développement du projet urbain.

- **Mettre en œuvre et suivre** : dès la conception du cahier des charges. Celle-ci va de la collecte des données jusqu'à la définition précise et concrète des différents secteurs étudiés et leur programmation dans le temps.

- **Communication du projet :** cette étape est essentielle, mais souvent négligée. Elle sert à communiquer le projet aux entreprises, institutions, associations et habitants ; autrement dit à tous les acteurs du projet urbain.

1.6 L'environnement durable

A l'heure actuelle, la qualité environnementale reste à un bas niveau, la situation est très sévère et inquiétante due à une pollution de l'air, de l'eau, du bruit et des ordures. Le problème environnemental est devenu l'un des goulots d'étranglement du développement économique et social des villes :

1) **La pollution de l'eau en milieu urbain :** 50% des eaux souterraines en milieu urbain sont polluées, et 86% des eaux de cours en ville ne sont pas de la qualité tolérable.

2) **La pollution atmosphérique :** la pluie acide tombe sur la plupart des régions urbaine ; presque toutes les villes algériennes sont frappées à la fois par les entreprises pollueuses et l'utilisation des ressources pollueuses ; la présence des particules fines est plus que tolérable.

3) **Les déchets sont catastrophiques :** deux tiers de villes sont entourées par les ordures de la vie quotidienne, entassées en banlieue sans avoir été traitées et qui sont devenues une deuxième source de pollution.

4) **Les nuisances acoustiques :** les résultats de la supervision sur la plupart des villes montrent que plus de deux tiers de la population citadine vivent dans un environnement plus ou moins bruyant.

5) **Le bruit** : La circulation trop intense en milieu urbain à cause de grande nombre de voiture et la circulation intense.

La principale cause de ces problèmes est l'homme qui ne cesse de s'accroître chaque année et qui laisse de plus en plus son empreinte sur l'environnement pour satisfaire ses besoins et pour améliorer sa condition de vie. Comme mentionné dans le coran :

ظَهَرَ الْفَسَادُ فِي الْبَرِّ وَالْبَحْرِ بِمَا كَسَبَتْ أَيْدِي النَّاسِ لِيُذِيقَهُم بَعْضَ الَّذِي عَمِلُوا لَعَلَّهُمْ يَرْجِعُونَ

(سورة الروم الآية 41)

1.7 Les stratégies pour développer l'environnement urbain

1) **Inciter toute la société à l'aménagement de l'environnement :** mettre en place un mécanisme de motivation incitant le public à participer à la protection environnementale ; mettre pleinement en jeu le rôle actif des organisations non-gouvernementales ; participer à la coopération internationale et chercher les meilleures approches à l'aménagement de l'environnement à l'échelle du monde.

2) **Optimaliser l'utilisation circulaire des ressources :** faire payer pour la protection de l'environnement ; attribuer des subventions environnementales ; les échanges du marché.

3) **Appliquer un aménagement selon les lois :** renforcer la direction verticale ; prémunir les travaux d'aménagement contre les interférences locales ; normaliser les actes d'application de la loi ; mettre en application la poursuite de responsabilité ; renforcer la supervision administrative ; mettre en œuvre la vérification verte.

4) **Eviter un cycle vicieux de la pauvreté et des problèmes environnementaux :** réduire la pauvreté par la répartition des recettes, la sécurité sociale et la régulation fiscale ; mettre en place un mécanisme de développement environnemental équitable, avantageux réciproquement et à responsabilité partagée par une coordination entre la ville et la campagne et une coordination régionale.

Tous les points ci-dessus sont indirectement contenus dans le processus de gestion des déchets. Ce processus est introduit dans la partie suivante.

1.8 Economie circulaire

Concept apparu dans les années 1970, l'économie circulaire est un système économique d'échange et de production qui, à tous les stades du cycle de vie des produits, vise à augmenter l'efficacité de l'utilisation des ressources et à diminuer l'impact sur l'environnement tout en développant le bien-être des individus. (Zhijun and Nailing, 2007)

L'économie circulaire s'oppose à l'économie dite linéaire. Selon le Ministère du Développement Durable "L'économie circulaire propose en effet de transformer les déchets en matière première réutilisée pour la conception des produits ou pour d'autres utilisations. En d'autres termes, ne plus créer de résidus que les systèmes industriel et naturel ne puissent absorber. La boucle est bouclée. Cela représente bien entendu un gain de compétitivité énorme pour les industries qui ont une maîtrise de leur flux de matières premières."

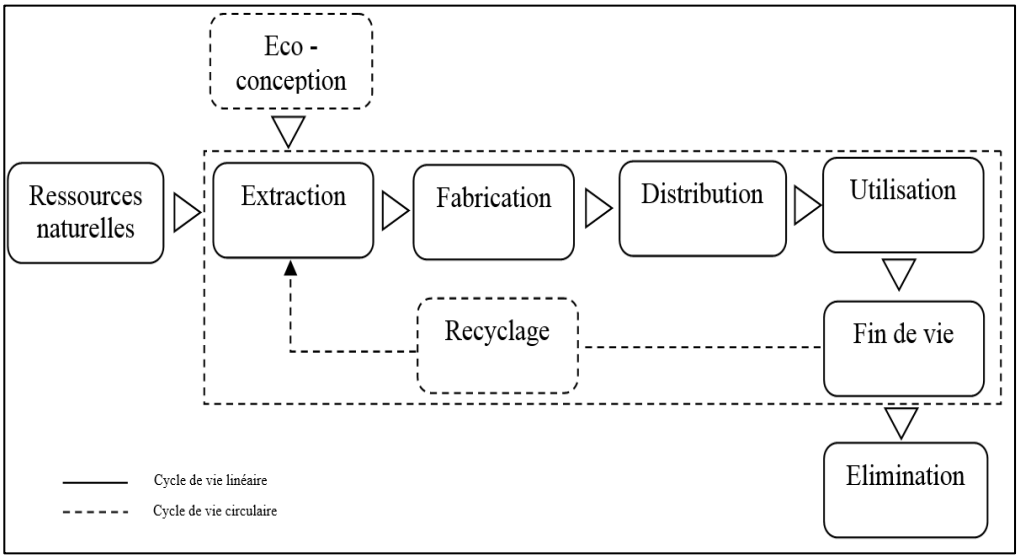

FIGURE 1.5 Comparaison des cycles de vie linéaire et circulaire

Partie II : La gestion des déchets urbain

1.9 Définition de déchets

Dans le langage courant, le terme déchets désigne ordure, immondice, ou tout autre résidu rejeté parce qu'il n'est plus consommable ou utilisable et donc n'a plus de valeur.

La Loi $N^{\circ}01-19$ du $12/12/2001$ (article 03) relative à la gestion, au contrôle et à l'élimination des déchets arrête (officiellement) les définitions des différents types de déchets comme suit : " Tout résidu d'un processus de production, de transformation ou d'utilisation et plus généralement toute substance, ou produit et tout bien meuble dont le propriétaire ou le détenteur se défait, projette de se défaire, ou dont il a l'obligation de se défaire ou de l'éliminer. "

1.10 Nomenclature des déchets

Tous les déchets sont identifiés par un code à six chiffres comprenant :

- sa catégorie d'origine (1^{er}et $2^{éme}$ chiffres),
- son regroupement intermédiaire (et $3^{éme}$ et $4^{éme}$ chiffres),
- sa désignation (et $5^{éme}$ et $6^{éme}$echiffres).

Un astérisque (*) est ajouté pour distinguer les déchets dangereux.

1.11 Origine de la production des déchets

La production des déchets est inéluctable pour les raisons suivantes :

- **Biologiques :** tout cycle de vie produit des métabolites ;
- **Économiques** : les produits en une durée de vie limitée ;
- **Technologiques :** tout procédé industriel conduit à la production de déchet ;
- **Écologiques :** les activités de la dépollution (eau, air) génèrent inévitablement d'autres Déchets qui nécessiteront une gestion spécifique ;
- **Accidentelles :** l'inévitable dysfonctionnement des systèmes de production et de consommation sont eux aussi à l'origine de déchets.
- **Chimiques :** toute réaction chimique est réagie par le principe de la conservation de la matière et dès que veut obtenir un produit à partir de deux autres on en produira un quatrième ;

1.12 Les Caractéristiques des déchets

On caractérise les déchets par quatre paramètres essentiels suivants :

- **La densité :** La connaissance de la densité est d'une grande importance pour le choix des moyennes décollectes et de stockage.
- **Le degré d'humidité** : Les ordures renferment une suffisante quantité d'eau variant en fonction des saisons et le milieu environnemental
- **Le pouvoir calorifique :** Le pouvoir calorifique est défini comme la quantité de chaleur dégagée par la combustion de l'unité de poids en ordures brutes.
- **Le rapport des teneurs en carbone et azote :** Le rapport C/N a été choisi comme critère de qualité des produits obtenus par le compostage des déchets.

1.13 Classification des déchets

Déchets organiques. Ce sont les déchets issus de déchets organiques (Kawai and Huong, 2017). Ils sont générés principalement dans des résidences, des restaurants et des établissements commerciaux travaillant avec des produits alimentaires. Ils doivent être séparés des autres types de déchets car ils sont principalement destinés aux décharges municipales.

Déchets recyclables. Ce sont tous les déchets qui peuvent être utilisés dans le processus de transformation en d'autres éléments ou dans la fabrication de matières premières (Seyring et al., 2016). Elle est générée dans les résidences, les entreprises et les industries et doit être séparée de manière à ce que les équipes de collecte sélective se rassemblent puis se chargent de la transformation finale dans les coopératives et les entreprises de recyclage.

Déchets industriels. Ce sont les résidus, principalement solides, provenant du processus de production dans les industries. Il est généralement composé de restes de matières premières destinées au recyclage ou à la réutilisation dans le processus industriel (Zobel, 2015).

Déchets hospitaliers. Ce sont les déchets produits dans les hôpitaux et les cliniques médicales qui peuvent présenter une contamination et transmettre des maladies aux personnes qui entrent en contact avec eux (Ali et al., 2017). Il doit être traité conformément aux normes établies, avec tous les soins possibles. Ce type de déchets est destiné aux entreprises spécialisées dans le traitement de tels déchets, où ils sont généralement incinérés.

Déchets commerciaux. C'est celui produit par les établissements commerciaux, tels que les magasins de vêtements, les jouets et les appareils ménagers. Ces déchets sont presque entièrement destinés au recyclage (Bacot et al., 2002).

Déchets verts. C'est le matériau qui résulte principalement de l'élagage des arbres, des branches, des troncs, des écorces et des feuilles qui tombent dans les rues. Parce qu'il s'agit de matière organique, il pourrait être utilisé pour le compostage et la production d'engrais organique (Krzywoszynska, 2012).

Déchets électroniques. Il s'agit des déchets générés par la mise au rebut de produits électroniques grand public qui ne fonctionnent plus ou sont devenus obsolètes (Babu et al., 2007). Pour l'élimination, il existe des lieux appropriés, tels que des sociétés et des coopératives actives dans le domaine du recyclage. Ils envoient ces déchets de manière à ne pas nuire à l'environnement.

Déchets nucléaires. C'est celui qui est généré principalement par les centrales nucléaires. Il s'agit d'un déchet extrêmement dangereux, car il s'agit d'un élément radioactif et doit être traité conformément à des normes de sécurité strictes (Gan and Yang, 2017).

1.14 La gestion des déchets

1.14.1 Gestion des déchets

Consiste en toute opération relative à la collecte, au tri, au transport, au stockage, à la valorisation et à l'élimination des déchets, y compris le contrôle de ces opérations. À partir de cette définition, plusieurs opérations se distinguent dans le mode de gestion des déchets existant en Algérie

1.14.2 La gestion de collecte des déchets

1) **Collecte des déchets :** Le ramassage et/ou le regroupement des déchets en vue de leur transfert vers un lieu de traitement.

2) **Les différents modes de récupération :**

- **Le tri à la source :** La collecte séparative nécessite au préalable un tri des ordures, soit à la source soit dans un centre de tri.
- **La collecte par apport volontaire :** Elle consiste à mettre à disposition de la population des lieux de réception, convenablement choisis (en centre-ville ou en périphérie) de façon à permettre une desserte satisfaisante de la population,
- **La collecte séparative :** Elle consiste à rassembler les produits valorisables, en particulier les emballages, dans un ou plusieurs bacs conteneurs, les collectes séparatives peuvent être réalisées en porte à porte ou en apport volontaire.

1.14.3 Le traitement des déchets

« La définie le traitement des déchets comme toute mesure pratique permettant d'assurer que les déchets sont valorisés, stockés et éliminés d'une manière garantissant la protection de la santé publique et/ou de l'environnement contre les effets nuisibles que peuvent avoir ces déchets ».La loi 01-19 du 12 décembre 2001 .

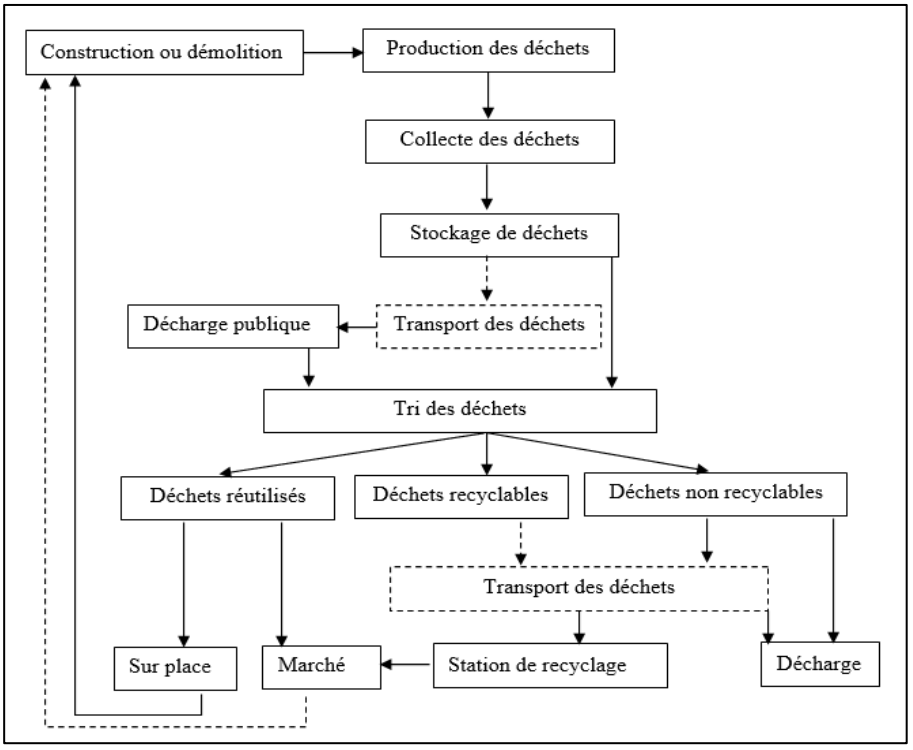

FIGURE 1.6 Diagramme de gestion de déchets (Abdelhamid, 2014)

1) La valorisation de matière :

- **Le réemploi :** Consiste à utiliser une nouvelle fois un produit ou objet usagé, pour un usage analogue à celui de sa première utilisation ou pour une autre utilité, sans qu'il y ait de traitements intermédiaires.

  Exemple : la consignation des bouteilles qui sont à nouveau remplies après leur nettoyage.

- **La réutilisation :** Consiste à utiliser de nouveau un déchet, pour usage différent de son premier emploi.

  Exemple : l'utilisation de pneus usagers pour protéger la coque des bateaux.

- **Le recyclage :** Le recyclage désigne la réintroduction d'un matériau contenu dans un déchet dans le cycle production, en remplacement total ou partiel d'une matière neuve.

  Exemple : utiliser les bouteilles cassées et les refondre pour en faire des bouteilles neuves.

La chaîne du recyclage :

i. **Collecte de déchets** : Les opérations de recyclage des déchets commencent par la collecte des déchets. Les déchets collectés pour le recyclage ne sont pas destinés ni à l'enfouissement ni à l'incinération mais à la transformation. La collecte s'organise en conséquence. La collecte sélective est la forme la plus répandue pour les déchets à recycler.

ii. **Transformation** : Une fois triés, les déchets sont pris en charge par les usines de transformation. Ils sont intégrés dans la chaîne de transformation qui leur est spécifique, sous forme de déchets et en sortent sous forme de matière prête à l'emploi.

iii. **Commercialisation et consommation** : Les produits finis issues du recyclage sont utilisés pour la fabrication de produits neufs qui seront à leur tour proposés aux consommateurs et consommés. Pour être en fin de vie, à nouveau jetés, récupérés et recyclés. (Sabrina, 2006)

2) La valorisation organique par le compostage ou la méthanisation :

- Le compostage : C'est un procédé biologique aérobie de dégradation et de valorisation de matière organique en un produit stabilisé et hygiénisé disposant des caractéristiques d'un terreau enrichi en composés humiques.

- Bio-méthanisation : L'opération de méthanisation consiste à transformer des matières organiques en conditions anaérobies (sans oxygène), produisant à la fois un gaz combustible, appelé biogaz (mélange de gaz carbonique et méthane), et un amendement organique.

3) La valorisation énergétique :

Consiste à utiliser une source d'énergie résultant de l'incinération ou de la thermolyse, ces modes de traitement des déchets sont tout à fait applicables dans un système industriel appliquant les principes de l'écologie industrielle puisqu'ils permettent de récupérer l'énergie de la combustion.

- L'enfouissement : Le dernier mode de traitement des déchets est l'enfouissement, méthode la moins écologique de toute puisque le déchet n'est ni réutilisé, ni valorisé, ce mode de gestion s'applique essentiellement aux déchets ultime dont aucune solution, à l'heure actuelle n'été trouvée. (Vorburger, 2006)

1.15 Les déchets solides urbains

1.15.1 Définition

Déchets solides urbains Le dictionnaire de l'Environnement définit un déchet solide comme un déchet qui n'est pas à l'état liquide. (Rushbrook et Pugh 1999) ont précisé que le terme déchet

solide peut se référer au déchet municipal qui contient sept catégories : résidentiel (ménager ou déchets domestiques), commercial, institutionnel, déchets de nettoyage des voies publiques, déchets de construction et de démolition, déchets hospitaliers, déchets industriels.

1.15.2 Type de déchets solides

Selon leur origine, les déchets solides peuvent être de types différents, tels que (Alam and Ahmade, 2013)

- industrielle
- institutionnel
- Déchets résidentiels.
- Services municipaux
- Construction et démolition

1.15.3 Caractéristiques des déchets solides

- **Corrosif :** il s'agit de déchets contenant des acides ou des bases capables de corroder des conteneurs pour l'esprit, p. Ex. réservoirs
- **Allumable :** ce sont des déchets qui peuvent provoquer des incendies dans certaines conditions, par exemple. huiles usagées et solvants
- **Réactifs :** de nature instable, ils provoquent des explosions, des vapeurs toxiques lorsqu'ils sont chauffés.
- **Toxicité :** déchets nocifs ou mortels ingérés ou absorbés (Alam and Ahmade, 2013)

1.15.4 Impacts des déchets solides sur l'environnement et la santé

1.15.4.1 Impacts sur la santé humaine

a) Pathologies liées à des conditions environnementales favorables et maladies spécifiques de la manipulation des déchets (agents de nettoiement, chiffonniers…)

- Tétanos.
- Conjonctivites épidémiques.
- Proéminence de la tuberculose.
- Intoxications aux produits dangereux.
- Effets multiples des substances radioactives.
- Maladies de contact de la peau et des muqueuses.

b) Impacts sanitaires des décharges non contrôlées (Figure 1.7)

- Multiplication des maladies infectieuses et parasitaires .
- Multiplication des rongeurs qui sont à l'origine de la peste.
- Prolifération des chiens errants (la rage)
- Prolifération des vecteurs nuisibles (mouches, moustiques,…).

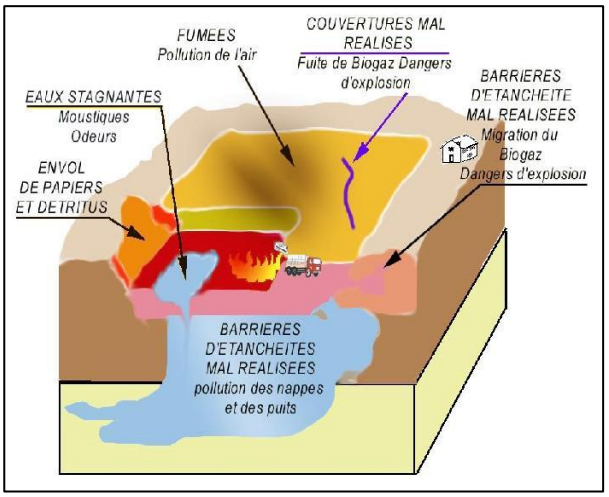

FIGURE 1.7 Impacts d'une décharge incontrôlée sur l'environnement (Tahar, 2017)

Les déchets solides ont un impact environnemental sévère qui se manifeste par la (Figure 1.8) :

- Altération de la qualité de l'air (gaz, fumées et poussières) ;
- Altération des sols et des paysages par des polluants chimiques ;
- Pollution des ressources en eau par les infiltrats et les eaux usées.

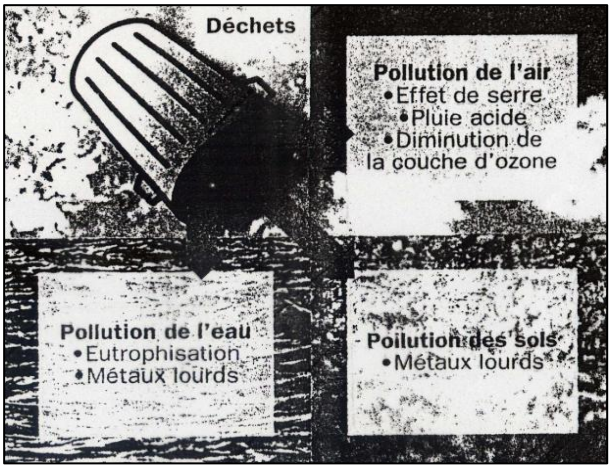

FIGURE 1.8 Types de pollution générée par les déchets solides (Navarro, 2003)

1.15.5 Les Obstacles empêchant la chaîne de recyclage des déchets solides

- Manque d'incitations ;
- Infrastructure médiocre ;
- Absence de technologie ;
- Informations inadéquates ;
- Manque de sensibilisation ;
- Dominance du secteur non organisé ;
- Problèmes de financement et de durabilité ;
- les passagers clandestins (produits orphelins) ;
- Manque de coordination entre les différentes autorités.
- Capacité limitée des agences gouvernementales ;
- Les recycleurs doivent supporter tous les coûts du processus de recyclage ;

1.16 Les crimes de déchets

La gestion des déchets s'effectue de manière responsable et légale, et l'élément criminel est toujours tenté de rechercher un bénéfice financier en enfreignant la loi.

Malheureusement, la criminalité liée au gaspillage est un très gros problème. Elle cause d'importants problèmes d'environnement et de santé et peut porter préjudice aux communautés locales, ainsi qu'à l'épuisement de l'économie internationale, à des sommes importantes chaque année en frais de nettoyage et à la perte de recettes fiscales.

Les criminels se livrent souvent à des activités illicites en matière de déchets - de la collecte des déchets aux décharges illégales, en passant par la combustion des déchets pour les éliminer. Leur motivation est de gagner de l'argent. Ils reçoivent généralement le taux de transfert légal pour la collecte, le transport, puis l'élimination illégale de déchets et la réalisation de bénéfices. S'ils ne sont pas manipulés correctement, les déchets peuvent causer une grave pollution de l'environnement - air, terre et eau - et cela peut être nocif pour la santé. L'activité de déchets criminels a également un impact économique sur les entreprises légitimes impliquées dans l'élimination des déchets. Ces entreprises sont incapables de rivaliser efficacement dans le secteur des déchets car elles sont minées par les criminels.

1.17 La problématique

Les déchets sont constitués d'une multitude de composants, dont certains contiennent des substances toxiques qui ont un impact négatif sur la santé humaine et l'environnement, si elles ne sont pas manipulées correctement. Ces dangers résultent souvent de procédés de recyclage et d'élimination incorrects. Les éléments dangereux présents dans les déchets solides comprennent les métaux ferreux et non ferreux, les plastiques, le verre, les circuits imprimés, le caoutchouc, les retardateurs de flamme et d'autres articles. La présence de ces éléments incite le secteur informel à suivre des méthodes d'extraction non scientifiques comme la combustion, les bains acides, ou bien traitent leurs déchets en les exportant illégalement vers des pays en développement, qui sert de plaque tournante au recyclage inapproprié. Les ouvriers non éduqués et non qualifiés impliqués dans la ségrégation et le démantèlement des déchets risquent également leur santé en raison des mauvaises pratiques suivies au cours de ce processus.

En raison de la négligence des bons systèmes de suivi la chaine des déchets, de nombreux problèmes ont été créés talque :

- le crime des déchets
- Fraude et manipulation
- Mauvaise ou perte d'informations
- Processus manuels
- Manque de connaissances sur la technologie
- Manque de contrôle

La gestion des déchets désigne le processus d'élimination des déchets dans le respect de l'environnement. La première étape consiste à collecter les déchets auprès des consommateurs, puis à les trier et les désassemblés. Les pièces démontées subissent plusieurs cycles de déchiquetage et de séparation. Ils sont soit recyclés pour être réutilisés comme neufs, soit éliminés en toute sécurité après un traitement approprié des composants dangereux.

Pour assurer le bon fonctionnement de ce processus, nous suggérons que l'introduction de la technologie de l'information soit nécessaire pour faciliter les efforts de gestion des déchets.

1.18 Notre objective :

Cette étude a pour objectif de comprendre comment les déchets sont générés, manipulés et éliminés afin de «progresser vers une économie plus circulaire où les déchets sont valorisés en tant que ressources et réutilisés». Prendre des mesures pour lutter contre la criminalité liée au gaspillage et repérer les possibilités pour les entreprises de gérer leurs déchets de manière plus durable, un suivi intelligent aidera à maximiser la valeur des déchets en tant que ressource et à minimiser les dommages causés à l'environnement, en stimulant une économie plus circulaire.

Nous proposons une solution intelligente de suivi des déchets basée sur la nouvelle technologie "blockchain", un nouveau système de suivi destiné à unifier les nombreux systèmes utilisés par les entreprises pour consigner leurs données en un seul.

Ce système de suivi des déchets est basé sur une approche blockchain, qui a déjà prouvé son efficacité dans le secteur financier, qui enregistre de manière sécurisée les transactions dans un grand livre distribué, horodaté et offre une solution simple, flexible et très évolutive pour suivre les mouvements de déchets, et qui offre aussi un haute niveau de traçage de la supply chain. L'application de cette technologie au secteur des déchets permettra un enregistrement fiable et sécurisé de tous les mouvements de déchets, ce qui permettra de suivre les déchets depuis leur source jusqu'à leur traitement final. Les utilisateurs pourront importer et exporter des données via une interface utilisateur avec différents niveaux de fonctionnalité et d'accès. Il veillera également à ce que les producteurs et les gestionnaires de déchets se conforment aux réglementations en matière de déchets et aidera les régulateurs à identifier et à lutter contre les infractions illicites en matière de déchets

1.19 Conclusion

Le domaine de la planification territoriale urbaine est un domaine très riche et vaste. Il inclut de nombreuses et différentes problématiques telles que La protection de l'environnement. L'informatisation de ces problèmes apparait une tâche très intéressante à cause de nombreux obstacles qui empêchent l'élimination appropriée des déchets. Dans le cadre d'une vision intégrée du développement durable, il convient d'appliquer les technologies les plus récentes afin de réduire ces obstacles et d'appliquer le principe de l'économie économique, l'application des principes de responsabilité et la maîtrise de la bonne gestion des déchets de manière transparente et crédible.

De ce fait, le développement d'une application en planification urbaine pour résoudre la problématique d'évaluation des projets urbains nécessitera l'intégration de différentes disciplines, à savoir la sécurité, décentralisation et la distribution des donnes.

Le chapitre suivant introduit la technologie de Blockchain et la cryptographie derrière cette technologie ainsi que les smart contracte utilisés pour faire des systèmes distribue.

ABDELHAMID, M. S. 2014. Assessment of different construction and demolition waste management approaches. *HBRC Journal,* 10**,** 317-326.
ALAM, P. & AHMADE, K. 2013. *Impact of Solid Waste on Health and The Environment*.
ALI, M., WANG, W., CHAUDHRY, N. & GENG, Y. 2017. Hospital waste management in developing countries: A mini review. *Waste Management & Research,* 35**,** 581-592.
ARAB, N. 2004. *L'activité de projet dans l'aménagement urbain: processus d'élaboration et modes de pilotage Les cas de la ligne B du tramway strasbourgeois et d'Odysseum à Montpellier.* Ecole des Ponts ParisTech.
ASCHER, F. 1995. *Métapolis: ou l'avenir dês villes*, Odile Jacob.
BABU, B. R., PARANDE, A. K. & BASHA, C. A. 2007. Electrical and electronic waste: a global environmental problem. *Waste Management & Research,* 25**,** 307-318.
BACOT, H., MCCOY, B. & PLAGMAN-GALVIN, J. 2002. Municipal commercial recycling: Barriers to success. *The American Review of Public Administration,* 32**,** 145-165.
CFU 2001. Code du Foncier et de l'Urbanisation (CFU), Complication de textes juridiques législatifs et réglementaires de la république algérienne. *Berti Editions*.
DESTAIS, G. Les théorisations économiques du développement durable. Proposition de décryptage critique. Le développement durable: débats et controverses, 2011.
DIND , J.-P. & DA CUNHA , A. 2011. La gestion de projets urbains, Projets d'aménagement concertés dans des secteurs déjà bâtis : exemples en Suisse Romande, Mémento à l'usage des responsables de projet. *Université de Lausanne* Suisse.
GAN, L. & YANG, S. 2017. Legal context of high level radioactive waste disposal in China and its further improvement. *Energy & Environment,* 28**,** 484-498.
GUDER, U. 2003. L'amenagement du territoire et la politique regionale en Allemagne. *Notre Europe, Octobre*.
INEICHEN, J. 2007. Copropolis. Recherche-Action au sein de la communauté Chico Mendes, Recife, Nord-Est du Brésil.
KAOUTHER, L. 2007. *Expérimentation des Algorithmes Génétiques Multiobjectifs dans un Processus Décisionnel Multicritère en Aménagement du Territoire.* Université d'Oran1-Ahmed Ben Bella.
KAWAI, K. & HUONG, L. T. M. 2017. Key parameters for behaviour related to source separation of household organic waste: A case study in Hanoi, Vietnam. *Waste Management & Research,* 35**,** 246-252.
KRZYWOSZYNSKA, A. 2012. 'Waste? You mean by-products!'From bio-waste management to agro-ecology in Italian winemaking and beyond. *The Sociological Review,* 60**,** 47-65.
LABORDE, P. 1994. les espaces urbains dans le monde. *professeur à l'université Michel-de-Montaigne de Bordeaux-III,* éditions NATHAN**,** 83.
LAOUAR, M. R. 2005. *Contribution pour l'aide à l'évaluation de projets de déplacements urbains.* Valenciennes.
LAURINI, R. 2014. *Information systems for urban planning: a hypermedia cooperative approach*, CRC Press.
MASBOUNGI, A. & DE GRAVELAINE, F. 2002. Projets urbains en France/French urban strategies. *Editions du Moniteur, Paris*.
MATE 2004. Ministère de l'Aménagement du Territoire et de l'Environnement (MATE), Aménagement de l'Algérie 2020, Alger, Algérie.
MERLIN, P. & CHOAY, F. 1988. *de l'article/du chapitre Dictionnaire de l'urbanisme et de l'aménagement*, distributeur Presses Universitaires de France.
NAVARRO, A. 2003. *Approche systémique des déchets*, Ed. Techniques Ingénieur.
RAHMOUN, N. 2013. *La planification urbaine à travers les PDAU-POS et la problématique de la croissance et de l'interaction villes/villages en Algérie. Référence empirique à la willaya de Tizi-Ouzou.* Université de Tizi Ouzou-Mouloud Mammeri.
SABRINA, S. 2006. Comportement des bétons à base de granulats recyclés. *Génie civil*.
SEYRING, N., DOLLHOFER, M., WEIßENBACHER, J., BAKAS, I. & MCKINNON, D. 2016.

Assessment of collection schemes for packaging and other recyclable waste in European Union-28 Member States and capital cities. *Waste Management & Research,* 34**,** 947-956.
TAHAR, B. 2017. Les bases de traitement des déchets solides.
TOMAS, F. 1998. Vers une nouvelle culture de l'aménagement des villes. *Projet urbain. Ménager les gens, aménager la ville, Wavre: Mardaga***,** 15-34.
VAILLANCOURT, J. 1998. Evolution conceptuelle et historique du développement durable. *RNCREQ (Regroupement National des Conseils Régionaux de l'Environnement du Québec), Rapport de recherche, mai*.
VORBURGER, J. 2006. *Écologie industrielle & valorisation des déchets.* Université Laval.
ZHIJUN, F. & NAILING, Y. 2007. Putting a circular economy into practice in China. *Sustainability Science,* 2**,** 95-101.
ZOBEL, T. 2015. ISO 14001 adoption and industrial waste generation: The case of Swedish manufacturing firms. *Waste Management & Research,* 33**,** 107-113.

CHAPITRE 2

LA CRYPTOGRAPHIE & LA TECHNOLOGIE BLOCKCHAIN

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.

La réputation de Chain de blocs grandit de jour en jour et attire de plus en plus d'attention à l'échelle mondiale. Certaines personnes comparent blockchain au début d'Internet dans les années 1970 et certains l'appellent la révolution du web 2.0, et il est parlé par de nombreuses personnes dans différentes disciplines : économistes, programmeurs et autres.

Dans ce chapitre nous allons introduire les principes et les concepts de base de la technologie block Chain. Dans une première partie, nous allons définir la cryptographie. La deuxième section présente la technologie blockchain leur architecture et leur mécanisme et enfin les applications de la technologie aux déférentes échelles.

Partie I : La technologie derrière la blockchain

2.1 La cryptologie

Est la science qui englobe la cryptographie et la cryptanalyse. C'est l'étude des principes, méthodes et techniques mathématiques reliées aux aspects de sécurité de l'information.Lotfi (2017)

2.1.1 La cryptographie

La cryptographie est l'art de chiffrer, coder les messages est l'étude des méthodes donnant la possibilité d'envoyer des données de manière confidentielle sur un support non sécurisé.

2.1.2 La cryptanalyse

Opposée à la cryptographie, elle a pour but de retrouver le texte clair à partir de textes chiffrés en déterminant les failles des algorithmes utilisés.

2.2 Type de la cryptographie

2.2.1 Chiffrement symétrique

Dans un chiffrement symétrique (chiffrement à clef secrète), deux utilisateurs voulant communiquer vont tout d'abord convenir d'une clef K à utiliser qu'ils gareront secrète.

Lorsque l'un d'entre eux souhaite communiquer le message M il lui appliquera la fonction de chiffrement $E(\,)$ en utilisant la clef K pour produire le chiffré $C = E(M, K)$. En envoyant le chiffré C sur le réseau l'utilisateur sait que s'il est intercepté par un tiers ce dernier ne pourra pas en comprendre le sens, seul son interlocuteur connaissant K pourra effectuer la transformation inverse et obtenir $M = D(C, K)$, où $D(\,)$ est la fonction de déchiffrement inverse de $E(\,)$.

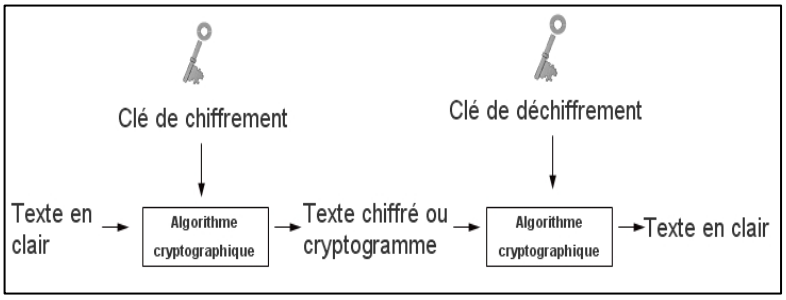

FIGURE 2.1 Chiffrement symétrique (Lotfi, 2017)

2.2.2 Chiffrement asymétrique

Dans un chiffrement asymétrique (chiffrement à clef publique), chaque utilisateur génère une paire de clefs, l'une appelée clef secrète qu'il est le seul à connaître, l'autre appelée clef publique qu'il diffuse sur un annuaire et qui peut servir aux autres pour le contacter.

Lorsqu'un utilisateur veut envoyer un message M il va aller chercher la clef publique du destinataire $K_{pub,dest}$ et l'utilise pour créer un chiffré $C = E(M, K_{pub,dest})$ Contrairement au chiffrement symétrique, il sera alors lui-même dans l'incapacité d'effectuer la transformation inverse ne possédant pas la clef privée de son interlocuteur. L'interlocuteur sera le seul à pouvoir récupérer le message originel $M = D(C, K_{priv,dest})$, grâce à sa clef privée $K_{priv,dest}$.

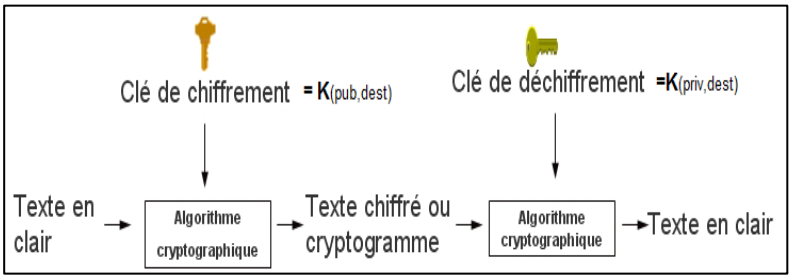

FIGURE 2.2 Chiffrement asymétrique (Lotfi, 2017)

2.3 Objectif de la cryptographie

Globalement, la cryptographie permet de résoudre cinq problèmes différents :

1. **La confidentialité :** Consiste à rendre l'information inintelligible à d'autres personnes que les acteurs de la transaction.
2. **Le contrôle d'accès :** permet de limite l'accès aux donnes, serveur ou personnes autorisées
3. **L'authentification :** Consiste à assurer l'identité d'un utilisateur.
4. **L'Intégrité :** Vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication
5. **La non-répudiation** : De l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction.

2.4 Méthodes de Chiffrement

2.4.1 Chiffrement par clé publique

i. RSA

Proposé en 1977 par (Rivest - Shamir - Adleman) ce système est basé sur le calcul exponentiel. Sa sécurité repose sur la fonction unidirectionnelle suivante : le calcul du produit de 2 nombres

premiers est aisé. La factorisation d'un nombre en ses deux facteurs premiers est beaucoup plus complexe. (Vidakovic et al., 2013)Ce crypto système utilise deux clés *d* et *e*, interchangeables. Le chiffrement C, et le déchiffrement D se fait selon :

- $C = M^e mod\ (n)$
- $M = C^d\ mod\ (n)$

ii. Courbe elliptique

Il s'agit d'un concept proposé en 1985 par deux chercheurs Miller et Klobitz, de façon totalement indépendante. Ce type de cryptographie basé sur le modèle asymétrique, permet aussi bien de chiffrer que de signer. On utilise souvent l'abréviation ECC, pour Elliptic Curve Cryptography. Parmi les schémas cryptographiques les plus connus, on retrouve l'algorithme ECDSA. (Lopez and Dahab, 2000)

- **Principe Général :**

Une courbe elliptique est un objet très simple mais qui a des propriétés tout à fait surprenantes. Elles ont la forme suivante :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Pour leur usage en cryptographie, a_1, a_2 et a_3 doivent être égaux à 0. Comme les cryptographes ont l'habitude de renommer $a_4 = a$ et $a_6 = b$, on obtient :

$$y^2 = x^3 + ax + b$$

Deux opérations mathématiques sont possibles sur les courbes elliptiques :

L'addition de points : quand on a deux points P et R sur une courbe elliptique EC, alors on peut calculer leur addition $Q = P + R$, et le résultat Q appartient aussi à EC.

La multiplication de points : quand on a un point P sur une courbe elliptique EC, alors on peut additionner K fois ce même point, ce qui résulte en la multiplication de points $Q = p * k$, et le résultat Q appartient aussi à EC.

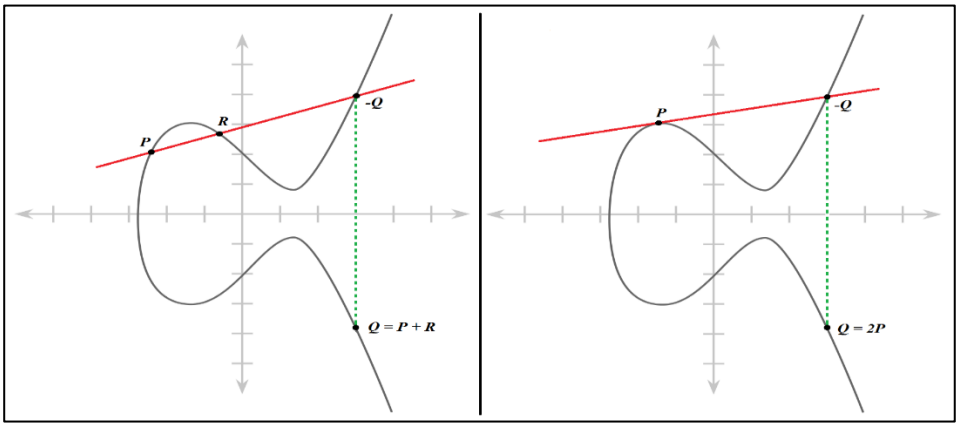

FIGURE 2.3 Adition de deux points P et Q ; Multiplication avec K=2 (Lopez and Dahab, 2000)

Pour définir l'addition $Q = P + R$, il faut tracer une droite reliant P et R. Cette droite (en rouge sur la figure 2.3) coupe la courbe elliptique en un troisième point appelé $-Q$. Le symétrique de ce point par rapport à l'axe des abscisses (obtenu en suivant la droite pointillée verte sur la figure 2.3) est le résultat Q de cette addition.

- **ECDSA** :

Soit le message m à signer, G un élément d'une courbe elliptique d'ordre n avec n un nombre premier plus grand que 2^{160}. La courbe est également définie par deux éléments a et b qui sont des éléments d'un champ de Galois de cardinalité q.

Préparation des clés

- Choisir un entier s entre 1 et $n - 1$.
- Calculer $Q = sG$ en utilisant l'élément de la courbe elliptique.
- La clé publique est Q et la clé privée est s.

Signature

- Choisir de manière aléatoire un nombre k entre 1 et $n - 1$.
- Calculer $(i, j) = kG$.
- Calculer : $x = integer(i) mod\ n$
- Calculer : $y = \frac{H(m)+sx}{k} mod\ n$; où H(m) est le résultat d'un hachage avec SHA-1 sur m
- Si *x* ou *y* sont nulles, recommencer
- La signature est la paire (*x*, *y*).

Vérification

- Contrôler que x et y sont bien entre 1 et *n*-1
- Vérifier que $x = integer(i)\ mod\ n$ sachant que $(i, j) = \frac{H(m)}{y}\ mod\ n)\ G\ \left(\frac{x}{y}\ mod\ n\right) Q$.
- Vérifier que *Q* est différent de (0,0) et que Q appartient bien à la courbe elliptique
- Vérifier que nQ donne (0,0)
- Portail de la cryptologie

2.5 Les fonctions de hachage cryptographiques

2.5.1 Définition

Formellement, une fonction de hachage est une fonction de l'ensemble des suites binaires (de longueur quelconque, non bornée) vers les suites de longueur n : $F : \{0,1\}^* \rightarrow \{0,1\}^n$

Se comporte comme une fonction choisie aléatoirement parmi toutes les fonctions de $\{0,1\}^*$ vers $\{0,1\}^n$. (BELFEDHAL, 2016) Les fonctions de hachage sont caractérisé par :

1. **Ce sont des fonctions unidirectionnelles :** A partir de $H(M)$ il est impossible de retrouver M.
2. **Ce sont des fonctions sans collisions :** A partir de $H(M)$ et M il est impossible de trouver $M' \neq M$ tel que $H(M') = H(M)$.

2.5.2 La famille MD-SHA

Les fonctions de hachage de la famille MD-SHA (Messages Digest – Standard Hash Algorithm), ont été pendant de longues années les normes en matière de fonctions de hachage cryptographiques, mais la plus part de ces fonctions ont été **cryptanalysées.**

Le principal avantage des fonctions de hachage MD-SHA est leur rapidité dans une implémentation logicielle. Dans ce qui suit nous allons présenter les principales fonctions de cette famille.

2.5.3 Conception de SHA-256

Le SHA-256 a une taille de message d'entrée inférieure à 2^{64}bits. La taille du bloc est de 512 bits et sa taille de mot est de 32 bits. La sortie est un résumé de 256 bits.

La fonction de compression traite un bloc de message de 512 bits et une valeur de hachage intermédiaire de 256 bits.

L'algorithme fonctionne comme suit :

- **Prétraitement :**

1. Remplissage du message, qui est utilisé pour rendre la longueur d'un bloc à 512 bits si elle est inférieure à la taille de bloc requise de 512 bits.
2. Analyser le message en blocs de message garantissant que le message et son remplissage sont divisés en blocs égaux de 512 bits.
3. Définissez la valeur de hachage initiale, qui correspond aux huit mots de 32 bits obtenus en prenant les 32 premiers bits des parties fractionnaires des racines carrées des huit premiers nombres premiers. Ces valeurs initiales sont choisies au hasard afin d'initialiser le processus et donnent la certitude qu'aucune porte dérobée n'existe dans l'algorithme.

- **Calcul du hachage :**

1. Chaque bloc de message est traité dans une séquence et nécessite 64 tours pour calculer la sortie de hachage complète. Chaque tour utilise des constantes légèrement différentes pour s'assurer qu'il n'y a pas deux tours identiques.
2. Tout d'abord, la planification des messages est préparée.
3. Ensuite, huit variables de travail sont initialisées.
4. Ensuite, la valeur de hachage intermédiaire est calculée.
5. Enfin, le message est traité et le hachage de sortie est généré :

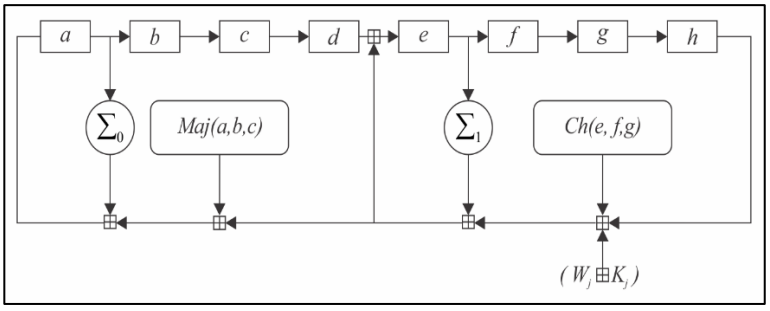

FIGURE 2.4 Algorithme de SHA-256 (Gilbert and Handschuh, 2003)

Où a, b, c, d, e, f, g et h sont les registres. Maj et Ch sont appliqués bit à bit $\sum_0 et \sum_1$ eteffectue une rotation bit à bit. Les constantes rondes sont Wj et Kj, auxquelles on ajoute mod 2^{32}. (Gilbert and Handschuh, 2003)

2.5.4 Conception de SHA-3 (Keccak)

La structure de SHA-3 est très différente des SHA-1 et SHA-2 habituels. L'idée clé derrière SHA-3 est basée sur des permutations sans clé, par opposition aux constructions d'autres fonctions de hachage habituelles qui utilisaient des permutations à clé.

Le diagramme suivant montre le modèle éponge et compression qui est à la base de SHA3 ou de Keccak. Par analogie avec l'éponge, les données sont absorbées dans l'éponge après l'application du rembourrage ; elles sont ensuite transformées en un sous-ensemble d'état de permutation à l'aide de XOR, puis la sortie est extraite de la fonction éponge qui représente l'état transformé. Rate correspond à la taille de bloc d'entrée d'une fonction éponge, tandis que la capacité détermine le niveau de sécurité générique : (Bertoni et al., 2013)

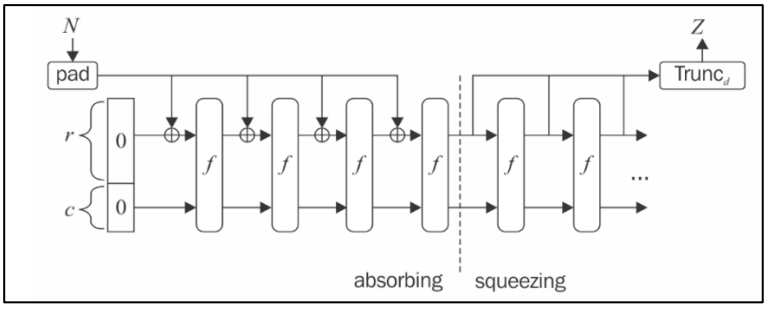

FIGURE 2.5 Algorithme de SHA-3 (Bertoni et al., 2013)

2.5.5 La famille RIPEMD

RIPEMD est l'acronyme de Race Integrity Primitives Evaluation Message Digest. Il est basé sur les idées de conception utilisées pour construire MD4.

2.5.6 Conception de RIPEMD-160

La proposition initiale se renforce suite à l'analyse pour devenir RIPEMD 160 quelque peu similaire à MD5 / SHA

-Utilise 2 lignes parallèles de 5 tours de 16 étapes

-Crée une valeur de hachage de 160 bits

Il est plus lent, mais probablement plus sûr, que SHA

- Étape 1 : ajoutez des bits de remplissage de manière à ce que sa longueur soit de 448 mod 512
- Étape 2 : ajouter une valeur de longueur de 64 bits au message. Si la longueur d'origine est supérieure à 2^{64}, la longueur est modulo 2^{64}
- Étape 3 : initialisez la mémoire tampon de 5 mots (160 bits) (32 bit pour chaque mot) (A, B, C, D, E) sur (67452301, efcdab89, 98badcfe, 10325476, c3d2e1f0)
- Étape 4 : Traitement du message en blocs de 512 bits (16 mots) Un module avec 10 tours de traitement de 16 étapes chacun. Les 10 tours sont disposés en 2 lignes parallèles de 5 tours chaque entrée - bloc 512 bits Yq, 160 bits valeur de tampon CVq (ABCDE ou A'B'C'D'E ') Sortie - Variable de chaînage 160 bits CVq + 1 (ABCDE mis à jour) Utilise la constante additive Kj. La sortie du dernier tour est ajoutée à l'entrée du premier tour (CVq) pour produire CVq + 1 de la manière suivante :

$$CVq+1(0) = CVq(1) + C + D'$$
$$CVq+1(1) = CVq(2) + D + E'$$
$$CVq+1(2) = CVq(3) + E + A'$$
$$CVq+1(3) = CVq(4) + A + B'$$
$$CVq+1(4) = CVq(0) + B + C'$$

- Etape 5 : la sortie de la dernière étape est le résumé de message de 160 bits (Prasadh and Sivasubramanian, 2017)

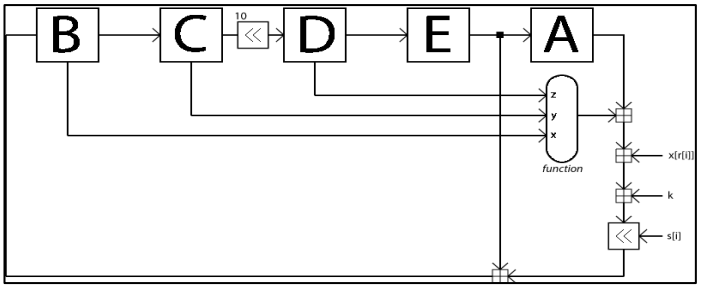

FIGURE 2.6 Algorithme de RIPEMD-160 (Prasadh and Sivasubramanian, 2017)

2.5.7 Arbre de Merkle

Le concept d'arbre Merkle (Merkle Tree) a été introduit par Ralph Merkle .C'est un arbre binaire avec des pointeurs de hachage (Narayanan et al., 2016). Les feuilles dans l'arbre contiennent les données. Le nœud parent, situé au niveau supérieur de l'arborescence, contient un hachage de ces données et est associé à un autre nœud parent. Cela continue jusqu'à la racine. De cette manière, le nœud racine est le hachage de toutes les données de l'arbre. (Voir la figure 2.7) On peut vérifier chacun des hachages de l'arbre jusqu'à la racine. Si tous les hachages sont corrects, le bloc de données est inclus dans l'arborescence. S'il y a n nœuds dans l'arborescence, la vérification d'un bloc de données prend environ le temps de log (n).

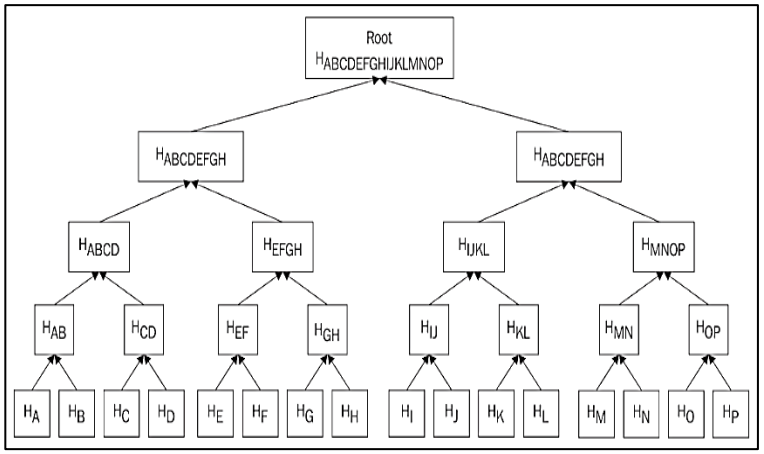

FIGURE 2.7 Arber de Merkle (Fekkes et al., 2018)

2.5.8 Signature électronique

C'est l'application la plus importante des fonctions de hachage. Ils permettent à un utilisateur de signer un message à l'aide de sa clé privée. Chacun peut vérifier la validité de cette signature grâce à la clé publique correspondante.

Des schémas de signature comme RSA permettent d'authentifier un message, mais ils demandent des calculs complexes et coûteux. En pratique**, au lieu d'appliquer un schéma de signature S directement à un long message** M, on applique la signature à un haché du message $H(M)$, La signature d'un message M est alors $S(H(M))$ (voir la Figure 2.8). Ainsi, l'opération de signature est faite sur un identifiant de petite taille et elle sera moins coûteuse.

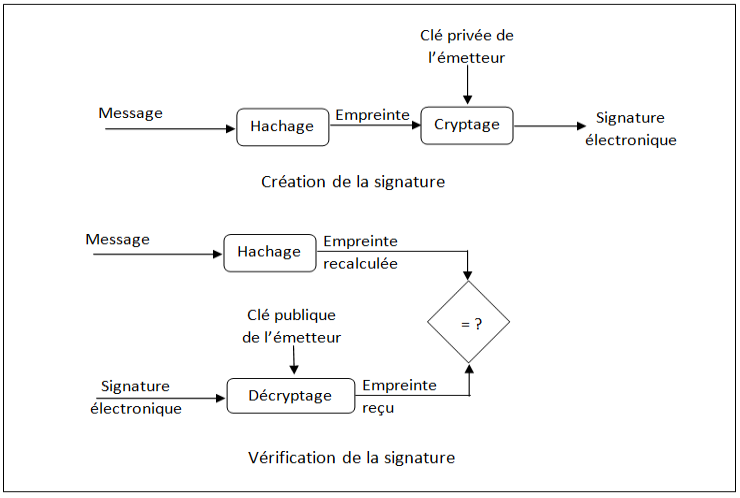

FIGURE 2.8 Schéma de signature électronique (BELFEDHAL, 2016)

L'utilisation de la cryptographie ne se limite pas dans ces applications, plusieurs fonctions de hachage peuvent utiliser dans une seule citation de sécurité, ça des pant le cas d'utilisation. La partie suivant introduit la technologie blockchain et explique la notion de cryptographie dans leur mécanisme.

Partie II : Démystifier la technologie blockchain

2.6 Historique

L'architecture derrière la technologie de la Blockchain a été décrite dès 1991 quand les chercheurs Stuart Haber et W. Scott Stornetta ont introduit une solution informatique, permettant l'horodatage des documents numériques et donc que ceux-ci ne soient jamais antidatés ou altérés.

Leur système utilisait une Blockchain sécurisée cryptographique pour stocker des documents horodatés. Par la suite, en 1992, le protocole dit « arbre de Merkle » fut introduit au fonctionnement, rendant ainsi le système plus efficace en permettant à plusieurs documents d'être rassemblés en un seul bloc. Cependant, cette technologie tomba dans l'oubli, et le brevet expire en 2004, quatre ans avant la création du Bitcoin.

En 2004, l'informaticien et activiste cryptographique Hal Finney, lance un système appelé RPoW « Reusable Proof Of Work » pour résolu le problème de la double dépense en conservant une registre de la propriété des jetons. Le système fonctionnait en recevant un jeton preuve du travail non échangeable et non fongible basé sur le système HashCash, celui-ci créait en retour un jeton possédant une signature RSA qui pouvait ensuite être transféré de personne en personne.

Fin 2008, un livre blanc (white paper) introduit un système de paiement électronique décentralisé de pair à pair (peer-to-peer), appelé Bitcoin. Le white paper fut distribué par le biais d'une liste de diffusion e-mail en rapport avec la cryptographie, par une personne ou un groupe de personnes utilisant le pseudonyme de Satoshi Nakamoto.

Le réseau Bitcoin est basé sur l'algorithme de preuve de travail HashCash, mais au lieu d'utiliser une fonction informatique de confiance comme le RPoW, la protection contre la double dépense est assurée par un protocole peer-to-peer décentralisé afin de suivre et de vérifier les transactions. En bref, les Bitcoins sont "minés" en tant que récompense, en utilisant le mécanisme de preuve du travail, par des mineurs individuels et les transactions sont ensuite vérifiées et validées par les nœuds décentralisés dans le réseau.

En 2013, Vitalik Buterin, un programmeur et co-fondateur du Bitcoin Magazine déclara que le Bitcoin avait besoin d'un langage de script pour construire des applications décentralisées. N'arrivant pas à réussir à trouver un accord au sein de la communauté, Vitalik lança le développement d'une nouvelle plate-forme informatique distribuée et basée sur la Blockchain : l'Ethereum, dotée d'une fonctionnalité de script appelée « smart contracts » (des contrats intelligents en français).

2.7 Définition :

Une Blockchain est une technologie informatique « open source », de stockage et de transmission de Données numérique fondée sur des échanges P2P, d'une manière chronologique, horizontal, transparente, décentralisée, sans intermédiaire (Leloup, 2017) et sécurisée grâce aux algorithmes de consensus. Par extension, elle constitue une base de données publique qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création décentralisée fiable, inviolable et sans organe central de contrôle, et est organisée en des sous-registres connus sous le nom de "bloc".

Elle peut être assimilée à un grand livre distribue (DLT) de comptes anonymes, Comme l'écrit le mathématicien Jean-Paul Delahaye (Delahaye, 2015), il faut s'imaginer "un très grand cahier, que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut écrire, mais qui est impossible à effacer et indestructible".

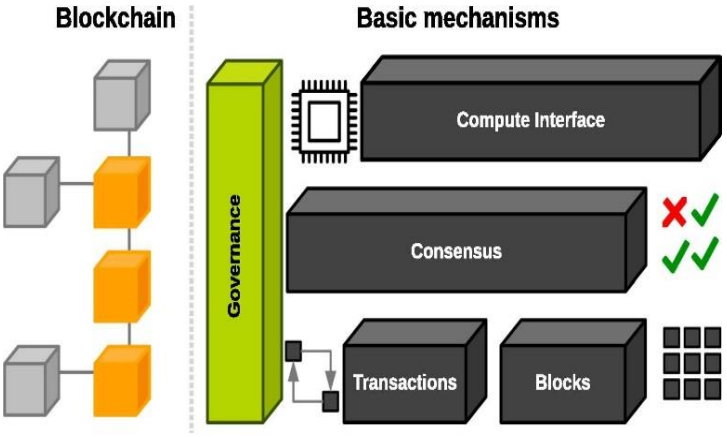

FIGURE 2.9 Un aperçu de l'architecture de blockchain (Casino et al., 2018)

2.8 Les problèmes adressés

La blockchain constitue en elle-même une innovation car elle permet la résolution de deux problèmes : le problème de la double dépense et le problème des généraux byzantins.

2.8.1 Le problème du double paiement

Ce problème survient dans tout système de paiement électronique. Le problème est le suivant : un individu avec de mauvaises intentions pourrait, avec une seule et même monnaie, payer deux bénéficiaires différents. La blockchain résout ce problème en utilisant l'horodatage : à chaque transaction sont associées une date et une heure. Ainsi, il est possible de vérifier chaque transaction étant donné que leur chronologie est publiée. (Nakamoto, 2008)

2.8.2 Le problème des généraux byzantins

Est une métaphore mathématique qui traite de la remise en cause de la fiabilité et de l'intégrité des transmissions .Le problème s'interroge sur la façon dont plusieurs ordinateurs peuvent atteindre un consensus, sans autorité centrale et à éviter les attaques.

La force de la technologie blockchain réside dans le fait qu'elle arrive grâce à ses mécanismes de consensus qui sont basés sur des concepts cryptographiques offre à tous les généraux de se mettre d'accord et confiance grâce à des messages écrits et signés entre les eux. La résolution de la preuve requiert une puissance de calcul élevée fournie par les mineurs. De cette façon, le système est capable de maintenir sa fiabilité dans le cas où des membres envoient des informations erronées.

2.9 Architecture de blockchain

La Blockchain est une séquence de blocs, qui contient une liste complète d'enregistrements de transaction comme le grand livre public classique. La figure 2.10 illustre un exemple de blockchain. Avec un hachage de bloc précédent contenu dans l'en-tête de bloc, un bloc n'a qu'un seul bloc parent. Il est à noter que les hachages des blocs oncle (enfants des ancêtres du bloc) seraient également stockés dans une chaîne de blocs ethereum. Le premier bloc d'une blockchain s'appelle un bloc de genèse « Genesis block » qui n'a pas de bloc parent.

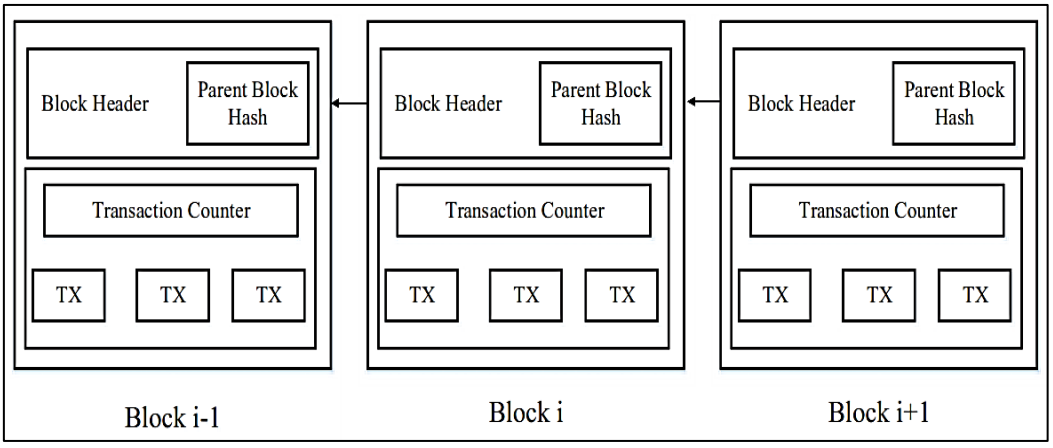

FIGURE 2.10 Structure du blokchain (Zheng et al., 2017)

2.9.1 Architecture du bloc

Les transactions effectuées dans le système blockchain sont enregistrées dans les blocs. Un bloc contient un en-tête et un corps, comme le montre la figure 2.11.

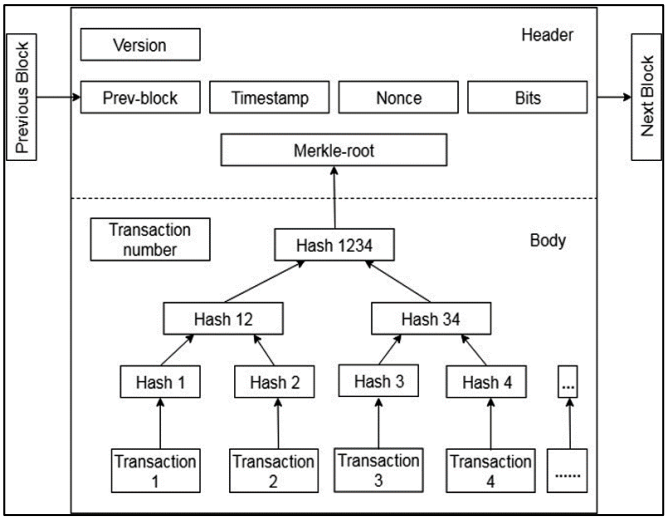

FIGURE 2.11 La structure du bloc (Wang et al., 2018) (Yuan and Wang, 2016)

L'en-tête contient les métadonnées du bloc (voir le tableau 2.1). Le corps inclut principalement les détails des transactions dans la structure de l'arbre de Merkel (tableau 2.2)

Octets	Nom	La description
80	En-tête de bloc	Inclut les champs de l'en-tête de bloc décrit dans le tableau suivant.
variable	Compteur	Le champ contient le nombre total de transactions dans le bloc.
variable	Transactions	Toutes les transactions dans le bloc.

Tableau 2.1 La stucture d'un bloc (Bashir, 2017)

Octets	Nom	La description
4	Version	Le numéro de version du bloc qui dicte les règles de validation de bloc à suivre.
32	hachage précédent	Il s'agit d'un double hachage SHA256 de l'en-tête du bloc précédent.
32	Racine de merkle	Il s'agit d'un double hachage SHA256 de l'arbre de sélection de toutes les transactions incluses dans le bloc.
4	Horodatage	c'est le moment où le mineur a commencé à hacher l'en-tête
4	Difficulté	C'est la cible de difficulté du bloc.
4	Nonce	Il s'agit d'un nombre arbitraire que les mineurs modifient à plusieurs reprises afin de produire un hachage qui remplit le seuil de difficulté.

Tableau 2.2 La structure du corps de bloc (Bashir, 2017)

2.10 Caractéristiques

Selon (Data Flair, 2018) la blockchain présente les caractéristiques clés suivantes :

1. **Décentralisation :** Il n'existe pas de tiers de confiance. Deux personnes peuvent réaliser une transaction en comptant sur le système lui-même pour confirmer l'échange. De plus, le réseau entier a accès à la base de données et aux opérations qui y sont effectuées.

2. **Transparence :** Bien que les participants intervient sous des pseudonymes, mais leur transactions sont traçable .L'historique des transactions est consultable à tout moment par toutes les membres de réseaux, rendre le système transparent.

3. **Sécurisation :** La Blockchain est conçue pour stocker les données de manière **immuable et inviolable**. La nature décentralisée de la blockchain et les algorithmes de cryptage rend trop difficile de tirer parti du système par des personnes mal intentionnées utilisateurs.

4. **Immutabilité.** Étant donné que chacune des transactions réparties sur le réseau doit être confirmée et enregistrée sous forme de blocs répartis dans tout le réseau, il est presque impossible de falsifier. De plus, chaque bloc diffusé serait validé par d'autres nœuds et les transactions seraient vérifiées. Ainsi, toute falsification pourrait être facilement détectée.

5. **Authenticité :** Chaque transfert d'objet, d'actif, de document, de propriété, de contrat est authentique étant donné que la blockchain l'enregistre dans la base de données. De plus, il est possible d'ajouter à chaque transfert l'heure, le jour, l'année et le propriétaire.

6. **Automatisé** : Les règles préétablies par les membres de la blockchain sont effectuées par des programmes informatiques. Des « contrats intelligents » seront auto-exécutants

2.11 Les catégories :

2.11.1 Blockchain publique

C'est le modèle le plus connu (*Permissionless) (historique),* est un registre ouvert accessibles à n'importe qui dans le monde, aucune permission d'autorisation ni d'être authentifiés demander pour effectuer des transactions ou pour participer au processus de consensus.

2.11.2 Blockchain privée

Il y a les blockchains totalement fermé (*permissioned*), dont l'accès d'écriture est délivré par une organisation centralisée (par exemple une banque centrale), mais où les autorisations de lecture peuvent être publiques ou privée (Leloup, 2017). D'une façon générale les nœuds du réseau sont authentifiés et autorisés selon des critères prédéfinis.

2.11.3 Blockchain de consortium

Est une combinaison hybride de blockchain publics et privés. Bien qu'elle partage le même niveau d'évolutivité et de protection de la confidentialité avec la chaîne de blocs privée, leur différence principale réside dans le fait qu'un ensemble de nœuds, nommés nœuds leaders, est sélectionné à la place d'une seule entité pour vérifier les processus de transaction. Cela permet une conception partiellement décentralisée où les nœuds leaders peuvent accorder des autorisations à d'autres utilisateurs. (Casino et al., 2018)

Propriétés	**Blockchain Public**	**Blockchain hybride**	**Blockchain prive**
détermination du consensus	Tous les mineurs	Ensemble de nœuds	Une organisation
autorisation de lecture	Publique	Public ou restreint	Public ou restreint
immutabilité	Impossible de falsifier	pourrait être altéré	Pourrait être altéré
Efficacité	Faible	Haute	Haute
centralisé	Non	Partielle	Oui
processus de consensus	Sans permission	Autorisée	Autorisée

Tableau 2.3 Classification de blockchain

2.12 Le fonctionnement

Tout d'abord, il s'agit de bien mettre en contexte les composantes les plus importantes de la blockchain :

1) Le nœud

Un nœud est un ordinateur qui est relié au réseau blockchain. Chaque nœud représente donc un utilisateur. Celui-ci conserve à tout moment une copie du registre blockchain et peut être réparti partout dans le monde.

2) Le réseau P2P

La blockchain repose sur un réseau pair-à-pair composé d'un ensemble de nœuds qui sont interconnectés entre eux. Ce réseau ne possède aucune autorité centrale et est donc entièrement décentralisé. L'entièreté de ce réseau a accès au registre blockchain.

3) Le bloc

Un bloc enregistre les transactions récentes émises par le réseau. Une fois rempli, un nouveau bloc est créé pour enregistrer les nouvelles transactions et le bloc rempli va se faire valider par le réseau.

4) Le registre blockchain

Le registre est la chaîne de blocs (qui contiennent toutes les transactions) qui est partagée à l'ensemble des utilisateurs du réseau. En d'autres mots, le registre est une base de données qui classe toutes les transactions de manière chronologique et qui est accessible par tous les membres du réseau.

Toute blockchain fonctionne nécessairement avec une monnaie ou un token (jeton) programmable. Bitcoin est un exemple de monnaie programmable.
Les transactions effectuées entre les utilisateurs du réseau sont regroupées par blocs. Chaque bloc est validé par les nœuds du réseau appelés les “mineurs”, selon des techniques qui dépendent du type de blockchain. Ces technique sont appelée les algorithmes de consensus tel que “Proof-of-Work” et “Proof-of-stake”, et consiste en la résolution de problèmes algorithmiques.

Une fois le bloc validé, il est horodaté et ajouté à la chaîne de blocs. La transaction est alors visible pour le récepteur ainsi que l’ensemble du réseau.

La figure 2.12 illustre les différentes étapes par lesquelles passe la technologie et qui permettent à un utilisateur A d'effectuer une transaction vers un utilisateur B: (Hannesse et al.)

.

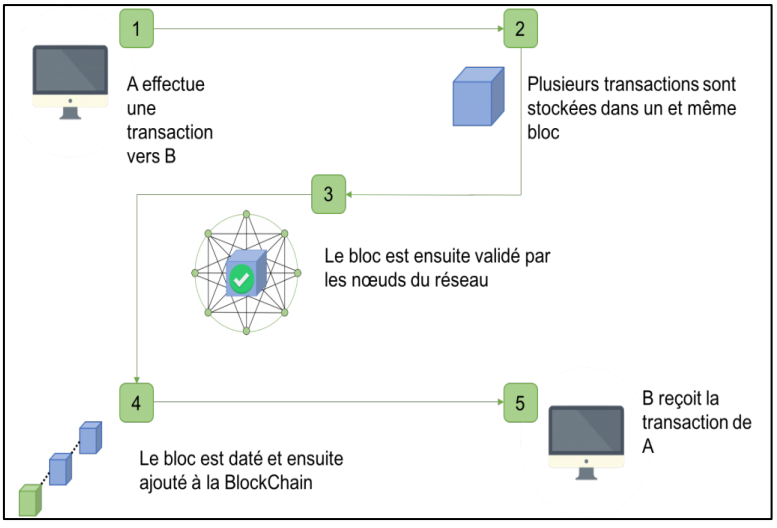

FIGURE 2.12 Fonctionnement général de la blockchain

2.13 Le hachage et algorithme de signature

L'algorithme spécifique utilisé par Bitcoin est l'algorithme ECDSA. Les signatures dans cet algorithme sont très importantes pour valider les transactions et de cette manière, seul le propriétaire des bitcoins peut envoyer ces bitcoins à une autre adresse.

- **ECDSA**

Pour générer des clés, nous avons besoin d'une courbe elliptique et d'un point de base. En tant que courbe, secp256k1 avec la forme $y^2 = x^3 + 7$ est utilisé pour avoir un niveau de sécurité de 256 bits. Avec cette norme, la courbe, le point de base G et l'ordre de G, n sont connus. Certaines clés privées (sk) et publiques (pk) peuvent maintenant être générées. La clé secrète est de 256 bits de long et la clé publique non compressé est de 512 bits et 257 bits de long compressés. La figure 2.13 résume la génération des clés public et privée.

- **Le hachage**

Dans l'algorithme, la plupart des messages sont hachés avec une fonction de hachage. De cette manière, le message peut avoir n'importe quelle longueur, mais l'entrée de l'algorithme doit être de 256 bits et ainsi, tout message peut être signé. La fonction de hachage utilisée est SHA-256 et, parfois, lorsqu'un hachage plus court est requis, RIPEMD-160 est utilisé [10]. Ceci est principalement utilisé pour créer des adresses. Dans Bitcoin, presque tout est haché deux fois, double SHA-256 ou d'abord avec SHA-256, puis avec RIPEMD-160 pour un hachage plus court.

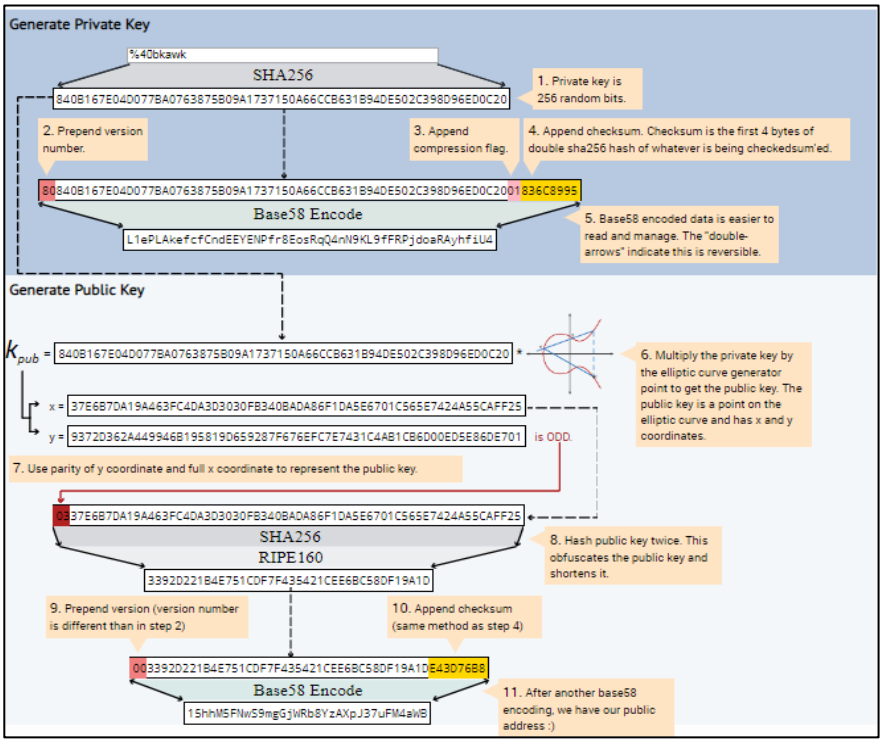

FIGURE 2.13 Génération des clés (Antonopoulos, 2017)

2.14 Les méthodes de consensus

Un consensus se définit par l'accord généralisé et unanime entre des personnes pour décider de la marche à suivre. Pour la technologie blockchain, il s'agit d'un consensus informatique où les utilisateurs se mettent d'accord sur un processus pour valider des transactions et mettre à jour la base de données.

2.14.1 La preuve de travail

Est un protocole dont le but principal est de prévenir les cyberattaques, tel qu'une attaque par déni de service distribué (DDoS).

Dans PoW, chaque nœud du réseau calcule une valeur de hachage de l'en-tête de bloc à l'aide d'un puzzle mathématique. Ce casse-tête mathématique a une caractéristique essentielle : l'asymétrie (Miraz, & Donald, 2018). L'en-tête de bloc contient un nonce et les mineurs le changeraient fréquemment pour obtenir des valeurs de hachage différentes. Le consensus n'exige que la valeur calculée soit égale ou inférieure à une certaine valeur donnée.

Lorsqu'un nœud atteint la valeur cible, le bloc est diffusé aux autres noeuds et tous les autres nœuds doivent confirmer mutuellement l'exactitude de la valeur de hachage. Si le bloc est validé, les autres mineurs ajouteront ce nouveau bloc à leur propre chaîne de blocs. Les nœuds qui calculent les valeurs de hachage sont appelés mineurs et la procédure de PoW est appelée extraction dans Bitcoin. Dans le réseau décentralisé, des blocs valides peuvent être générés simultanément lorsque plusieurs nœuds trouvent le nonce approprié presque au même moment. En conséquence, des branches peuvent être générées (Kibet, 2018)

2.14.2 Preuve d'enjeu

Preuve d'enjeu (proof of stake ou POS) désigne une méthode permettant de valider les blocs et de les inscrire dans une blockchain, contrairement au POW le POS est beaucoup moins énergivore. C'est un « minage virtuel » car il n'y a pas besoin d'acheter du matériel informatique puissant. Pour participer à un Proof-of-Stake il faut :
Posséder une certaine quantité de crypto-monnaie (tokens) pour la création et validation de nouveaux blocs investir dans l'achat de la crypto-monnaie ensuite les stocker dans le wallet officiel de la crypto-monnaie, fait donc partie de réseau.

Sur la base du dernier bloc de la blockchain, l'algorithme sélectionne aléatoirement un « validateur » qui aura le droit de créer et valider le prochain bloc. Plus cette somme est grande, plus l'utilisateur a des chances de valider le bloc. Dans ce cas-ci, le terme de minage est remplacé par celui de minting. Si le bloc n'est pas créé dans un intervalle de temps donné, une deuxième personne est sélectionnée et ainsi de suite. Une fois le bloc est valide vous gagner les récompense correspond aux frais de transactions qui sont contenues dans un bloc

2.15 Le blockhain Ethereum

Dr. Gavin Wood a introduit Ethereum en 2014, qui est une autre implémentation de la technologie blockchain qui prend en charge les contrats intelligents. La devise ou le moyen d'échange dans la blockchain Ethereum s'appelle Ether. Pour qu'une transaction soit exécutée, une certaine quantité de gaz est nécessaire. Cela évite une boucle infinie d'exécution des contrats, car ceux-ci s'arrêteront dès qu'ils seront à court de gaz. Ce gaz peut être acheté en échange d'éther. Pour être plus précis.

Le prix du gaz est flottant et régi par la loi en matière de demande et d'offre dans le réseau de chaînes à blocs Ethereum. Une transaction peut être n'importe quoi, du transfert de fonds entre comptes à l'exécution de contrats intelligents. Ainsi, si l'utilisateur X souhaite envoyer E quantité d'Ether à l'utilisateur Y, il enverra le prix du gaz par défaut à E +, le prix du gaz par défaut étant déterminé par un ensemble d'actions impliquées dans l'exécution de la transaction, telles que le cryptage SHA3. La quantité de données présentes dans la transaction

Ce coût de transaction peut être compris comme l'achat d'espace ou le prix d'inclusion pour que cette transaction soit incluse dans un bloc exploité par un mineur. Le gaz supplémentaire restant après l'exécution de la transaction est fourni au mineur par le réseau en plus de la récompense minière. Un mineur a la liberté de choisir d'inclure ou non une transaction particulière dans son bloc. Par conséquent, plus le gaz supplémentaire envoyé lors de la transaction est important, plus les chances que la transaction soit exploitée plus tôt augmentent. Ne pas envoyer suffisamment de gaz avec une transaction peut démotiver les mineurs pour inclure cette transaction dans leur bloc, entraînant ainsi une longue durée de transaction. (Mukhopadhyay, 2018)

2.15.1 Algorithmes de minage

Ethash est l'algorithme utilisé pour le minage en phase de PoW . Le mineur doit trouver un nonce inférieur à la valeur cible souhaitée (Target). Ce nonce prouve qu'un travail particulier a été accompli. L'algorithme d'Ethash repose sur un jeu de données pseudo-aléatoire, initialisé par la longueur actuelle de la blockchain. Cela s'appelle un DAG et est régénéré tous les 30 000 blocs (ou tous les 5 jours environ). En mars 2017, le groupe de disponibilité de base de données faisait environ 2 Go, et sa taille continuera de croître parallèlement à celle de la blockchain :

1. L'en-tête prétraité (dérivé du dernier bloc) et curent nonce sont combinés à l'aide d'un algorithme de type SHA3 pour créer notre mélange initial de 128 octets, appelé mélange 0 .
2. Le mélange est utilisé pour calculer quelle page de 128 octets à récupérer du DAG, représentée par le bloc Get DAG Page.
3. Le mélange est combiné à la page DAG récupérée. Ceci est fait en utilisant une fonction de mélange spécifique à Ethereum pour générer le prochain mélange, appelé Mix 1 ici.
4. Les étapes 2 et 3 sont répétées 64 fois, pour finalement aboutir au Mix 64.
5. Le mix 64 est post-traité, donnant un Mix Digest plus court sur 32 octets.

6. Mix Digest est comparé au seuil cible prédéfini de 32 octets. Si Mix Digest est inférieur ou égal au seuil cible, le nonce actuel est considéré comme ayant réussi et sera diffusé sur le réseau Ethereum. Sinon, Curent Nonce est considéré comme non valide et l'algorithme est exécuté avec un nonce différent (soit en incrémentant le nonce actuel, soit en en sélectionnant un nouveau au hasard). (Bashir, 2017)

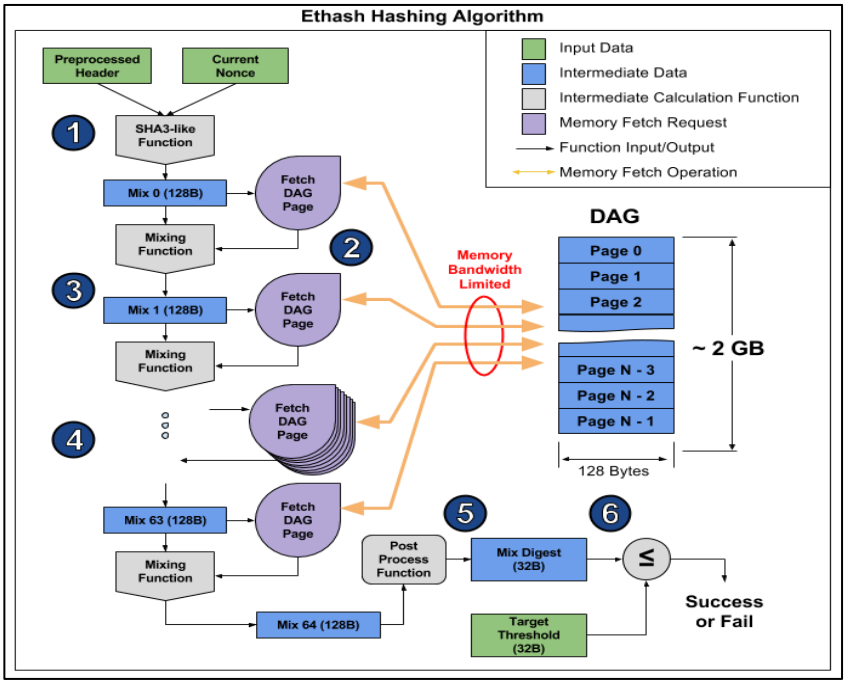

FIGURE 2.14 Fonctionnement de Ethereum

2.15.2 Etude comparative

Le tableau 2.4 résume une comparaison entre les deux protocoles du blockchain les plus utilisée :

	Bitcoin	**Ethereum**
Application	Monnaie en ligne	Monnaie en ligne et autre application diverses
Les clés	Public : 512 bits Prive : 256 bit	Public : 512 bits Prive : 256 bits Adresse : 160 bits
Hachage	SHA-256	Keccak 256 / Keccak 512
Signature size	512 bits (64 bytes)	520 bits (65 bytes)
Curve	Secp256k1	Secp256k1
Schéma se signature	ECDSA	ECDSA
Temps de block	10 minutes	12 secondes
Minage	Pow	Pow /Pos

Tableau 2.4 Comparison de Bitcoin et Ethereum

2.16 Les smart contract

Les contrats intelligents ont d'abord été théorisés par Nick Szabo en 1994, mais il était près de 20 ans avant le véritable potentiel et les avantages d'entre eux ont été vraiment appréciés.

Les contrats intelligents sont décrits par Szabo comme suit : “Un contrat intelligent est un protocole de transaction informatisé qui exécute les termes d'un contrat. Les objectifs généraux sont de satisfaire les conditions contractuelles communes, de minimiser les exceptions malveillantes et de limiter le recours à des intermédiaires de confiance. Les objectifs économiques connexes comprennent la réduction des pertes liées à la fraude, les coûts d’arbitrage et d’application, ainsi que les autres coûts de transaction. ”

2.16.1 Les caractéristiques

Les contrats intelligents sont capables de suivre la performance en temps réel et ils sont :

- ✓ Auto-vérification,
- ✓ Auto-exécutable,
- ✓ Inviolable,
- ✓ Sécurisé et imparable,

2.16.2 Le fonctionnement

Smart Contract étend les fonctionnalités de la blockchain en modélisant des scénarios réels à l'aide de langages de programmation complets de haut niveau Turing. Ethereum blockchain a son propre ensemble de langages de programmation qui peuvent être utilisés pour écrire ces contrats. Les Smart Contracts étendent les fonctionnalités de la blockchain en modélisant les concepts du monde réel dans la blockchain. Une fois déployé, le code du contrat intelligent ne peut plus être modifié.

L'exécution d'un contrat intelligent est également traitée comme une transaction. L'unité de gaz par défaut est nécessaire pour exécuter un contrat Smart. Elle est calculée en fonction du nombre d'octets contenus dans le contrat Smart. Par conséquent, plus le contrat est complexe (plus le nombre d'octets est élevé) et plus le nombre de gaz nécessaires pour exécuter le contrat est élevé. Par exécution, cela signifie que l'état de la chaîne de blocs est modifié, c'est-à-dire que des données sont ajoutées à la chaîne de blocs ou que des données en sont supprimées. Pour simplifier davantage, les opérations d'écriture dans le blockchain coûtent cher en lecture tandis que l'opération de lecture ne coûte rien. Les opérations d'écriture sont relativement plus lentes car le changement d'état de la blockchain doit être exploité comme toute autre transaction. Les opérations de lecture d’autre part sont effectuées dans la copie de l’état global ou de la base de données dans le nœud local qui reçoit l’appel de lecture, il est donc relativement plus rapide. La figure 2.15 donne un bon aperçu du schéma de Smart Contract. (Lamichhane et al., 2017)

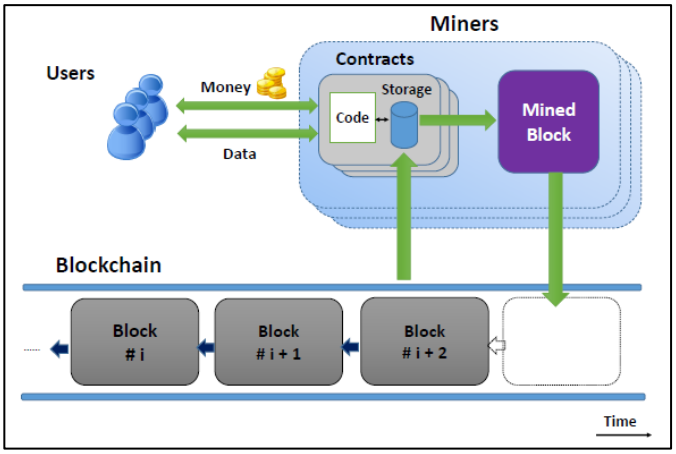

FIGURE 2.15 La structure du smart contract (Lamichhane et al., 2017)

2.17 Les réformes

La blockchain est une technologie évolutive, il est possible de modifier les règles de consensus. Ces modifications sont appelées un fork (fourche). En pratique, cela donne lieu à un soft fork ou un hard fork.

2.17.1 Fork temporelle

Dans un réseau distribué, certains systèmes du réseau seront en retard sur les informations ou auront des informations alternatives. Cela dépend de la latence du réseau entre les nœuds cela donne lieu à un confit dans le réseau. La résolution des conflits de données est un élément essentiel pour s'accorder sur l'état du réseau de chaînes de blocs. (Zheng et al., 2017)

Si deux blocs sont validés au même moment, deux chaînes parallèles se développent alors, après l'ajout de quelques blocs, seule la chaîne la plus longue subsiste

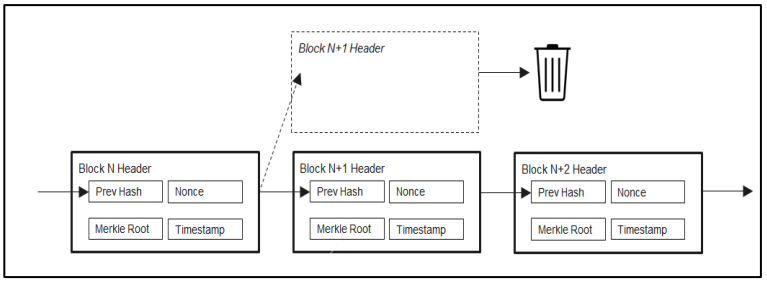

FIGURE 2.16 La fourche (Zheng et al., 2017)

2.17.2 Soft Fork

Un soft fork est une modification rétro-compatible du protocole de la blockchain. Les anciens blocs validés restent compatibles avec les nouvelles règles, plus strictes. Si la majorité des

participants du réseau adopte les modifications, la mise à jour devient effective. Les nœuds qui ne se plient pas au nouveau protocole sont exclus.

2.17.3 Hard Fork

Un hard fork est une modification majeure du protocole, dont les nouvelles règles ne sont pas compatibles avec les précédentes. Son intérêt est de pouvoir réviser n'importe quel aspect du code de la blockchain. Cependant, en l'absence de consensus entre les participants au réseau, le hard fork peut provoquer une scission entre les différents acteurs. Si une minorité de nœuds décide de ne pas suivre les nouvelles règles proposées, ils peuvent être à l'origine d'une blockchain différente dont le protocole reste incompatible avec les autres.

2.18 Attaque 51

Une attaque à 51 % est une attaque potentielle contre un réseau blockchain, par laquelle une seule entité ou organisation est capable de contrôler la majorité du taux de hachage, entraînant potentiellement une perturbation du réseau. En d'autres termes, celui qui mène une attaque 51 % disposerait de la puissance de minage suffisante pour exclure ou modifier intentionnellement l'ordre des transactions.

2.19 Blockchain vs BDD traditionnelle

Avantages de la blockchain	• Blockchain prouver l'autorité et la validité de sa propre transaction au lieu de faire appel à un administrateur central (Swan, 2015). • La Blockchain, comme tout autre bdd, doit être exécutée sur du matériel physique. Moins sensible à la corruption ou à la fraude • Les informations stockées dans une Blockchain sont transparentes pour tous les nœuds. (vérifier l'historique). ((Atzori, 2015); (Swan, 2015)). • Les données ne sont pas stockées dans un seul emplacement. Il n'y a donc pas un responsable de la sécurité. ((Ølnes, 2016); (Gervais et al., 2016)). • Le risque de défaillance du système est très faible. La robustesse de Blockchain est bien supérieure à celle d'un système de bdd traditionnel car elle est exécutée sur plusieurs systèmes et à plusieurs endroits. Si un nœud tombe en panne, les autres nœuds prendront le relais instantanément. (Ølnes et al., 2017)

Tableau 2.5 Les avantages de la blockchain

Désavantages de la blockchain	• La Blockchain est plus lente qu'un système de bdd traditionnel. Cela coûte plus cher, car il coûte plus d'énergie, de matériel et de capacité d'infrastructure(Eyal et al., 2016). • Chaque nouvelle connexion d'égal à égal, une preuve de la validité et de l'intégrité de la source doit également être fournie. Cela se fait par une signature numérique signifie alors il faudra plus de temps et de puissance de calcul (Gaetani et al., 2017). • Une transaction ne sera autorisée que si au moins 50% des nœuds la valident. Ce processus prend du temps car chaque nœud doit communiquer avec les autres nœuds. (Gaetani et al., 2017). • Blockchain doit valider et autoriser chaque transaction, mais pour chaque transaction, les calculs sont compliqués car elle chiffre toutes les informations. • Il est très difficile d'élargir la capacité d'une blockchain existante (Ølnes, 2016). Cela signifie qu'un système blockchain est moins flexible. Cela s'est avéré être un problème avec l'énorme croissance de Bitcoin, où le nombre même d'utilisateurs cause de nombreux problèmes (De Filippi and Loveluck, 2016)

Tableau 2.6 Les désavantages de la blockchain

2.20 Les domaines des applications

La plupart des applications son classe en applications financières et non financières, en revanche, Blockchain est adopté dans de nombreux domaines :

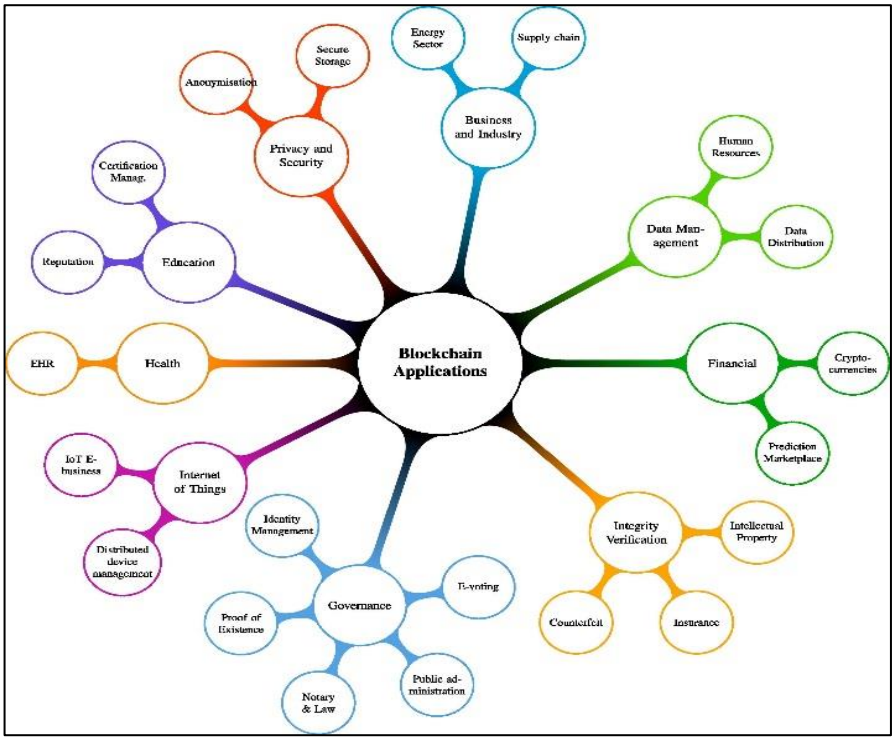

FIGURE 2.17 Les domaines d'application de la blockchain (Casino et al., 2018)

1. Applications financières : la blockchain par le secteur financier entraînera à terme des économies de coûts dans des domaines tels que les rapports financiers centraux.

2. Vérification d'intégrité : Les chaînes de caractères activées par la blockchain ont permis d'automatiser plusieurs processus dans le secteur des assurances.

3. La gouvernance : La responsabilité, l'automatisation et la sécurité offertes par Blockchain pourraient à terme entraver la corruption. Par exemple l'attestation, l'identification, les contrats de mariage, les taxes et le vote.

4. Internet des objets : L'idée principale est de fournir un échange de données sécurisé et vérifiable dans des scénarios hétérogènes tenant compte du contexte avec de nombreux dispositifs intelligents interconnectés.

5. Confidentialité et sécurité : Les organisations centralisées - publiques et privées - collectent de grandes quantités d'informations personnelles et sensibles. La Blockchain est considérée comme une occasion d'améliorer les aspects de sécurité de la donnée.

6. Gestion de la chaîne logistique : La blockchain accroître la transparence et la responsabilité dans les réseaux de supply chain, permettant ainsi des chaînes de valeur plus flexibles. Elle améliore en particulier la visibilité, l'optimisation et la demande.

7. Secteur énergétique

La blockchain peut réduire les coûts et créer de nouveaux modèles commerciaux, mieux gérer la complexité, la sécurité des données, renforcer la transparence et la confiance du système de marché de l'énergie, garantir la responsabilité tout en préservant les exigences de confidentialité, renforcer les échanges directs entre utilisateurs.

8. Éducation : La blockchain peut résoudre les problèmes de vulnérabilité, de sécurité et de confidentialité dans le cas d'environnements d'apprentissage comme la gestion des certificats éducatifs et dans le cas de l'édition savante, blockchain peut être utilisé pour mieux traiter les soumissions de manuscrits.

9. Applications diverses : Les applications de blockchain peuvent être trouvées dans le secteur humanitaire, en particulier pour lutter contre la pauvreté. Aussi pour construire des systèmes de transport intelligents dans des contextes de villes intelligentes. La blockchain devrait jouer un rôle central dans la gestion de l'environnement. Une autre application intéressante peut être trouvée dans le contexte des médias sociaux. Certaines autres applications telles que, le calcul de périphérie et la mise en place de systèmes de partage de ressources informatiques.

2.21 Conclusion

Dans chapitre, nous avons présenté la technologie 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 nouds 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.

ANTONOPOULOS, A. M. 2017. *Mastering Bitcoin: Programming the open blockchain*, " O'Reilly Media, Inc.".
ATZORI, M. 2015. Blockchain technology and decentralized governance: Is the state still necessary? *Available at SSRN 2709713*.
BASHIR, I. 2017. *Mastering blockchain*, Packt Publishing Ltd.
BELFEDHAL, A. E. 2016. *Etude et Implémentation des Fonctions de Hachage Cryptographiques Basées sur les Automates Cellulaires.*
BERTONI, G., DAEMEN, J., PEETERS, M. & VAN ASSCHE, G. Keccak. Annual international conference on the theory and applications of cryptographic techniques, 2013. Springer, 313-314.
CASINO, F., DASAKLIS, T. K. & PATSAKIS, C. 2018. A systematic literature review of blockchain-based applications: current status, classification and open issues. *Telematics and Informatics*.
DE FILIPPI, P. & LOVELUCK, B. 2016. The invisible politics of bitcoin: governance crisis of a decentralized infrastructure. *Internet Policy Review*, 5.
DELAHAYE, J.-P. 2015. Les blockchains, clefs d'un nouveau monde'. *Pour Sci***,** 80-85.
EYAL, I., GENCER, A. E., SIRER, E. G. & VAN RENESSE, R. Bitcoin-ng: A scalable blockchain protocol. 13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16), 2016. 45-59.
FEKKES, L., BATINA, L., PAPACHRISTODOULOU, L. & DE RUITER, J. 2018. Comparing Bitcoin and Ethereum. *URl: https://www. cs. ru. nl/bachelorscripties/2018/Lotte_Fekkes___ 4496426___Comparing_Bitcoin_and_Ethereum. pdf*.
GAETANI, E., ANIELLO, L., BALDONI, R., LOMBARDI, F., MARGHERI, A. & SASSONE, V. 2017. Blockchain-based database to ensure data integrity in cloud computing environments.
GERVAIS, A., KARAME, G. O., WÜST, K., GLYKANTZIS, V., RITZDORF, H. & CAPKUN, S. On the security and performance of proof of work blockchains. Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, 2016. ACM, 3-16.
GILBERT, H. & HANDSCHUH, H. Security analysis of SHA-256 and sisters. International workshop on selected areas in cryptography, 2003. Springer, 175-193.
HANNESSE, T., DE HERTAING, A. R. & DE BROQUEVILLE, O. Les banques doivent-elles craindre les blocktechs* et leur technologie blockchain?
KIBET, A. 2018. *A Synopsis of Blockchain Technology*.
LAMICHHANE, M., SADOV, O. & ZASLAVSKY, A. 2017. A smart waste management system using IoT and blockchain technology.
LELOUP, L. 2017. *Blockchain: la révolution de la confiance*, Editions Eyrolles.
LOPEZ, J. & DAHAB, R. 2000. An overview of elliptic curve cryptography.
LOTFI, I. 2017. *Cryptographie à base de courbes elliptiques.*
MUKHOPADHYAY, M. 2018. *Ethereum Smart Contract Development: Build blockchain-based decentralized applications using solidity*, Packt Publishing Ltd.
NAKAMOTO, S. 2008. Bitcoin: a peer-to-peer electronic cash system (2008).
NARAYANAN, A., BONNEAU, J., FELTEN, E., MILLER, A. & GOLDFEDER, S. 2016. Bitcoin and cryptocurrency technologies. s Princeton University Press.
ØLNES, S. Beyond bitcoin enabling smart government using blockchain technology. International Conference on Electronic Government, 2016. Springer, 253-264.
ØLNES, S., UBACHT, J. & JANSSEN, M. 2017. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. Elsevier.
PRASADH, S. & SIVASUBRAMANIAN, S. 2017. Multiple Securities for Cloud Computing Using RIPEMD-160. *Available at SSRN 3078377*.
SWAN, M. 2015. *Blockchain: Blueprint for a new economy*, " O'Reilly Media, Inc.".
VIDAKOVIC, D., PAREZANOVIC, D., NIKOLIC, O. & KALJEVIC, J. 2013. RSA Signature: Behind

the Scenes. *arXiv preprint arXiv:1304.3309*.
WANG, B., CHEN, S., YAO, L., LIU, B., XU, X. & ZHU, L. A simulation approach for studying behavior and quality of blockchain networks. International Conference on Blockchain, 2018. Springer, 18-31.
YUAN, Y. & WANG, F.-Y. Towards blockchain-based intelligent transportation systems. 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), 2016. IEEE, 2663-2668.
ZHENG, Z., XIE, S., DAI, H., CHEN, X. & WANG, H. An overview of blockchain technology: Architecture, consensus, and future trends. 2017 IEEE International Congress on Big Data (BigData Congress), 2017. IEEE, 557-564.

CHAPITRE 3

ETAT DE L'ART

Le déversement illégal de déchets solides est l'un des événements les plus importants liés aux activités de traitement illégal des déchets. Le processus de gestion des déchets est très médiocre, en particulier lorsqu'il s'agit de confirmer la destination correcte pour la livraison des déchets solides.

Dans le cas de la criminalité liée aux déchets, l'absence de registres de conservation des données numériques des déchets est fréquemment exploitée par des criminels organisés qui transfèrent ou étiquettent des sites illégaux pour éviter les taxes d'enfouissement ou les exportations illégales. L'enregistrement des mouvements de déchets est un traitement des lacunes actuelles dans les

Dans ce chapitre, nous présentons une comparaison basée sur un ensemble de critères pour l'évaluation des technologies déjà utilisées dans les processus de gestion des déchets

3.1 Les critères de l'étude critique des solutions étudiées

Afin de bien évaluer les articles et les travaux que nous allons traiter, nous avons établi une liste de critère d'évaluation, qui se compose la sécurité ou la cryptage moderne nous aide à augmenter le niveau de sécurité par rapport aux systèmes de gestion de déchets classiques , de traçabilité des transactions , transparence , décentralisation , et la responsabilité:

3.1.1 La sécurité

L'un des principaux objectifs du système de gestion des déchets est la sécurisation des donnes. Cela ne peut être réalisé que si les donnes stocker de manière immuable et inviolable, donc rend trop difficile de tirer parti du système par des personnes mal intentionnées utilisateurs.

3.1.2 La traçabilité

La traçabilité est la définition des circonstances dans lesquelles les déchets sont collectés, transportés et recyclés.

Il s'agit de mettre en application le principe de traçabilité à la filière déchet en imposant aux producteurs de déchets de collecter et de stocker toutes les informations relatives a :

- ✓ La production des déchets,
- ✓ L'expédition des déchets,
- ✓ La réception des déchets,
- ✓ L'élimination des déchets.

3.1.3 La transparence

Les transactions de tous les participants sont traçable .L'historique des transactions est consultable à tout moment par toutes les membres de réseaux. Une liste publique partagée de transactions (l'échange de données) permet chaque pair du réseau d'avoir accès à chaque transaction effectuée, rendre le système transparent.

3.1.4 La décentralisation

La suppression de tiers de confiance tell que des serveurs centraux. Les participants peuvent réaliser une transaction en comptant sur le système lui-même pour confirmer l'échange (P2P). De plus, le réseau entier a accès à la base de données et aux différentes opérations qui y sont effectuées.

3.1.5 La responsabilité

Afin d'améliorer la chaîne de gestion durable des déchets et dans un cadre moral, la responsabilité doit être appliquée.

Le concept de responsabilité concerne le droit des parties prenantes d'obtenir les informations nécessaires sur les actions des fonctionnaires dans la gestion de leurs intérêts et de leur fournir les éclaircissements nécessaires sur la manière d'utiliser leurs pouvoirs et leurs devoirs pour gérer leurs ressources.

3.2 Les technologies

Avec les progrès immédiats, les technologies de l'information et de la communication (TIC), la technologie de l'internet des objets et le cloud computing sont devenues un élément incontournable de la planification et de la conception de systèmes de gestion des déchets. Dans cette section, nous présentons un examen des technologies actuelles et de leur utilisation dans les systèmes de gestion des déchets afin de mettre en évidence les problèmes et les défis liés à l'utilisation d'un système intégré basé sur la technologie. Pour planifier, surveiller, collecter et gérer les déchets, les TIC sont divisées en quatre catégories : techniques spatiales, techniques d'identification, techniques d'acquisition de données et technologies de transfert de données.

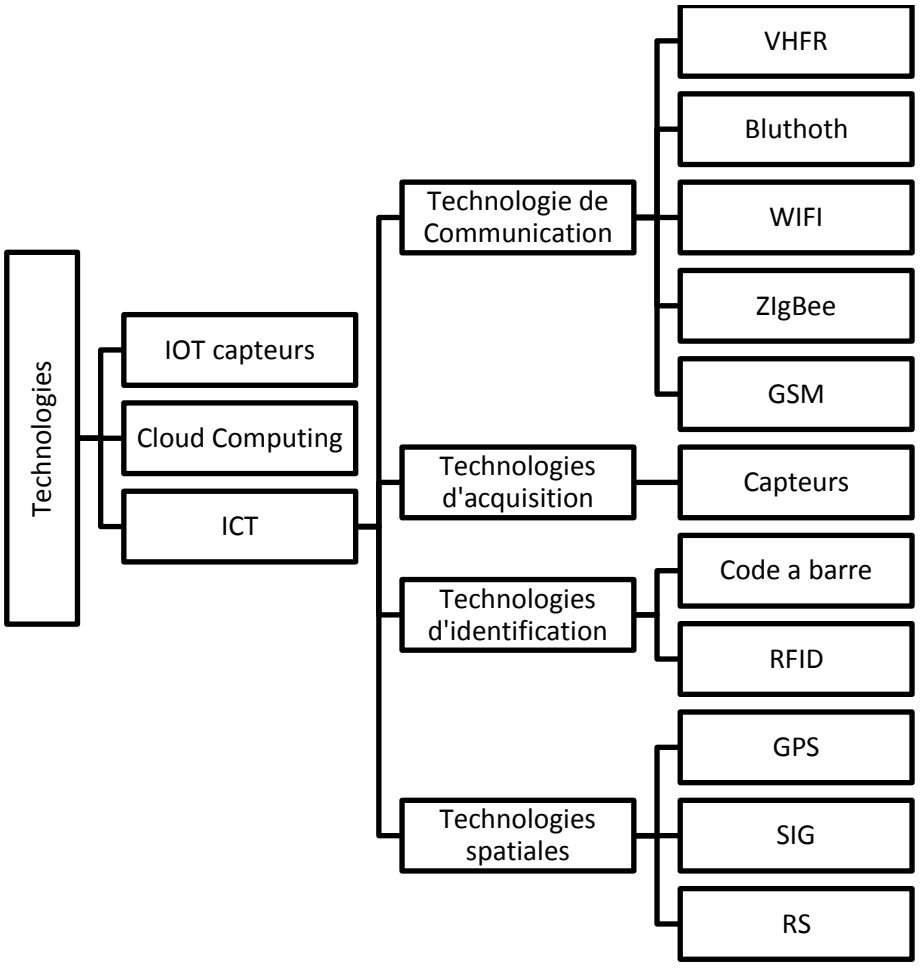

FIGURE 3.1 Les technologies de traçage du la chaine de déchets

3.2.1 Cloud computing

Est une technologie qui permet de mettre sur des serveurs localisés à distance des données de stockage ou des logiciels qui sont habituellement stockés sur l'ordinateur d'un utilisateur, voire sur des serveurs installés en réseau local au sein d'une entreprise.

Cette virtualisation des ressources permet donc à l'entreprise d'accéder à ses données sans avoir à gérer une infrastructure informatique, souvent complexe et qui représente un certain cout pour l'entreprise.

Le Cloud Computing, ou "l'informatique dans les nuages" est considéré par beaucoup, comme une évolution majeure de l'informatique et qui permet d'accéder depuis n'importe ou à vos fichiers.

- Le cloud computing est utilisé comme solution de gestion des déchets car il est caractérisé par la maintenance, la sauvegarde et la fiabilité pour améliorer l'analyse et l'efficacité, obtenez des informations exécutables à partir de données en temps réel et la simplification du contrôle des opérations quotidiennes des déchets pour lancer des affaires

3.2.2 IOT

Définition de l'Union internationale des télécommunications : « infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution »

- Pour atténuer les déchets et maintenir la propreté, il faut un «système de gestion des déchets basé sur l'intelligence». (Arunadevi, 2019) propose un système de gestion intelligente des déchets intelligents proposé par IOT qui vérifie le niveau de déchets dans les poubelles à l'aide de systèmes de capteurs. Une fois qu'il a détecté immédiatement ce système modifié pour concerner autorisé par IOT. Pour ce système, le microcontrôleur a été utilisé comme interface entre le système de capteurs et le système IOT.

3.2.3 TIC

3.2.3.1 Les technologies spatiales :

- **GPS :** Signifie "Système de positionnement global". Le GPS est un système de navigation par satellite utilisé pour déterminer la position au sol d'un objet. La technologie GPS a été

utilisée pour la première fois par l'armée américaine dans les années 1960 et a été étendue à une utilisation civile au cours des prochaines décennies. Aujourd'hui, les récepteurs GPS sont inclus dans de nombreux produits commerciaux, tels que les automobiles, les smartphones, les montres d'exercice et les dispositifs SIG.

- **SIG:** Signifie "Système d'information géographique" , l'une des technologies spatiales les plus sophistiquées, sont un système d'information informatisé capable de collecter, stocker, gérer, intégrer, manipuler, analyser et afficher des données spatiales appelées données géo spatiales ou géographiquement référencées. Généralement, ces données sont disposées dans les couches thématiques en formant des cartes numériques, là où réside la puissance des systèmes SIG. L'analyse visuelle des données permet d'identifier les modèles, les tendances et les relations qui peuvent ne pas être visibles sous forme de tableau ou d'écriture (Basaiaoclu et al., 1997)

- **RS :** pour "Remote sensing" (Télédétection) désigne l'utilisation moderne des technologies de détection aériennes pour détecter et classer des objets sur la surface de la terre à partir d'une plate-forme à distance par propagation de signal comme un rayonnement électromagnétique provenant de satellites ou d'avions (Schowengerdt, 2007).

- les systèmes basés sur les technologies spatiales fondés sur des systèmes d'information graphiques (SIG) et / ou un système de positionnement global (GPS) ou la télédétection (RS) comme technologie principale. Les opérateurs de gestion de déchet solide (GDS) adoptent ces systèmes pour surveiller l'emplacement des poubelles et des véhicules de collecte lors de la collecte (Zamorano et al., 2009)

3.2.3.2 Technologie d'identification

- **Code à barre :** est un support d'échange de données informatisé contenant une marque dichromatique lisible par machine qui code des informations pour l'étiquetage des objets à l'aide d'un agencement de symboles géométriques.

- **RFID :** pour " radio frequency identification ", ou radio-identification, est une technologie qui permet de sauvegarder et récupérer des données à distance sans assistance humaine. **(**Want, 2006**)** Sur ce que l'on appelle des puces ou tags RFID ou encore des **r**adio-étiquettes. Très utilisée dans le secteur de la sécurité, la technologie RFID a énormément d'applications.

- La technologie RFID est un outil puissant qui peut changer la façon de gérer les activités et les chaînes d'approvisionnement. Un grand avantage de cette proposition par rapport à la technologie traditionnelle des codes à barres (dans laquelle les données peuvent être lues mais non mises à jour) est qu'elle permet des opérations de lecture / écriture simultanées et sécurisées, ce qui améliore les performances opérationnelles de l'ensemble du processus. De

plus, les opérations de lecture / écriture peuvent être effectuées à distance. Par conséquent, les opérateurs humains restent aussi loin que possible du contact direct / à proximité des déchets dangereux, prévenant ainsi la contamination et réduisant les risques d'accident.

- Systèmes basés sur les technologies d'identification, dans lesquels des étiquettes d'identification par code à barres ou par radiofréquence (RFID) sont installées avec des poubelles pour permettre le suivi de l'identification afin de déterminer leur emplacement et d'acquérir le moment de la collecte (Kietzmann, 2008)

3.2.3.3 Technologie de communication

- **VHR :** La radio très haute fréquence (VHFR) est une technologie de communication désignée par l'ITU-8 dont la bande passante est comprise entre 30 et 300 MHz. Les applications courantes de VHFR sont la radiodiffusion FM, la communication de données à longue portée, la communication marine et la télédiffusion

- **ZIgbee** : La technologie ZigBee développée par ZigBee Alliance, une association de sociétés qui travaillent ensemble à l'élaboration de normes pour des réseaux sans fil fiables, économiques et à faible consommation. ZigBee s'appuie sur la norme IEEE 802.15.4 qui définit les spécifications de la couche physique (PHY) et de la sous-couche de contrôle d'accès au support (MAC) pour la connectivité sans fil à faible débit de données, qui consomme un minimum d'énergie et dont les coûts sont peu élevés

- **Bluetooth :** est une technologie de communication sans fil entre homologues qui élimine la nécessité de connexions par câble entre des périphériques tels que des téléphones portables, des assistants numériques personnels ou des ordinateurs portables. Sa norme est IEEE 802.15 et fonctionne dans les bandes ISM 2,4–2,5 GHz.

- **WIFI :** est une technologie de communication sans fil à courte portée largement utilisée dans la connexion mobile de réseaux domestiques et de petits bureaux en raison de sa flexibilité et de sa mobilité.

- **GSM :** Le système mondial de communications mobiles (GSM) est considéré comme un type de réseau 2G qui a débuté en 1982 en Europe. Il s'agit maintenant d'une norme acceptée dans le monde entier pour la technologie de communication cellulaire numérique principalement utilisée pour la transmission de la voix mobile. De plus, GSM facilite le service de transmission de données où les débits de transmission de données sont limités à 9,6 Kbps et plusieurs secondes sont nécessaires pour la configuration de la connexion.

- les technologies de communication de données qui sont normalement utilisées dans les trois types de système précédents pour faciliter la transmission des données capturées ou analysées.

3.2.3.4 Les technologies d'acquisitions de données

- **Capteur :** est un appareil qui perçoit et mesure des caractéristiques du monde réel, telles que des quantités physiques ou des propriétés chimiques, et les convertit en signaux pouvant être directement observés ou adoptés par un autre appareil

- Systèmes basés sur des technologies d'acquisition de données contenant plusieurs éléments sensoriels installés dans des poubelles telles qu'un capteur d'image, un capteur de distance, un capteur volumétrique, etc. afin d'observer son statut (Rovetta et al., 2009).

Certains systèmes intelligents ont également été étudiés sur la base de la modélisation paramétrique floue, de la programmation stochastique floue et de la programmation en nombres entiers avec contraintes aléatoires floues pour démontrer l'applicabilité, réduire les incertitudes et permettre au gestionnaire de gestion des déchets de faire des compromis entre économie, fiabilité et contrainte du système. violation sous une incertitude complexe (Xu et al., 2014). Ainsi, un système de GDS automatisé et intelligent peut réduire les coûts de gestion, le temps, les efforts et les émissions (Rada et al., 2013).

3.3 Classification

Jusqu'à présent, de nombreux systèmes ont été proposés pour résoudre les problèmes associés et optimiser l'efficacité de la gestion des déchets et de combattre le crime de déchets. Dans cette étude, les systèmes largement utilisés peuvent être classés en deux groupes, à savoir :

1- Suivi le collecte de déchets (SCD)
2- Suivi le bon endroit de déchets (SED)

3.3.1 SCD

3.3.1.1 Système 1

Dans ce travail, (Sharmin and Al-Amin, 2016) proposons un système de gestion des déchets dynamiques basé sur un service en nuage, qui utilise des données en temps réel provenant de capteurs installés dans des poubelles. Le modèle du système proposé est présenté à la figure suivant. Le processus commence par la collecte de données dans les poubelles. Chaque poubelle a un identifiant unique. Les données sont traitées puis utilisées pour trouver les itinéraires optimaux et les envoyer aux camions. Après la collecte, les déchets sont divisés en sections de déversement et de recyclage. L'ensemble du processus est géré dynamiquement et peut être mis à jour à tout moment. Leur système comprend principalement deux phases. Ils sont :

-1. Collecte et envoi de données à partir des poubelles
-2. Trouver la voie optimale pour la collecte des déchets

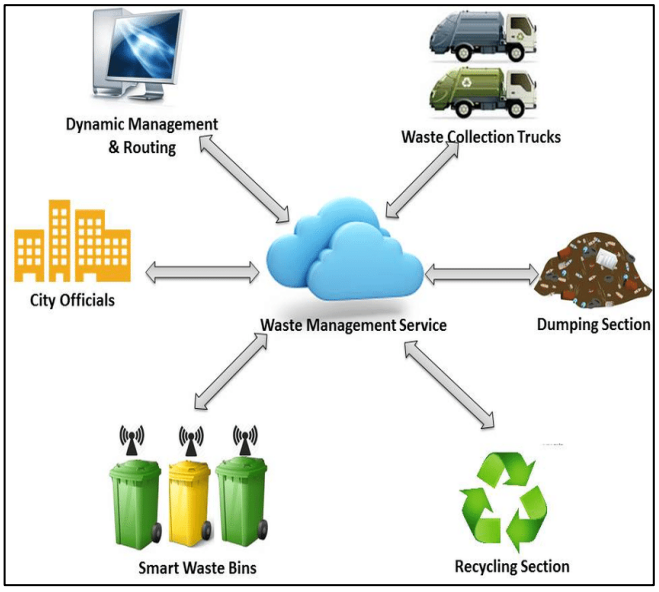

FIGURE 3.2 Le protocole de système (Sharmin and Al-Amin, 2016)

Les limites :

- L'ensemble du processus peut être surveillé de manière centralisée et fournir ainsi un service de haute qualité aux citoyens d'une ville intelligente

3.3.1.2 Système 2

Une autre étude a été réalisée par (Offenhuber et al., 2012) , Ils ont estimé que le manque de données fiables sur le comportement spatial des obstacles entravait la conception efficace de la stratégie de recyclage, où ils ont installé des capteurs GPS sur 2 000 articles mis au rebut provenant de 12 catégories de déchets différentes afin d'observer le mouvement des déchets solides municipaux. Ils ont constaté que parmi les déchets solides, les déchets ont des trajectoires plus aléatoires et voyagent beaucoup plus longtemps. Il est intéressant de noter que les distances de trajet les plus longues ont été signalées pour des produits précieux ou sans valeur, tels que les déchets électroniques et les déchets dangereux. Leur analyse a révélé que plus de 95% des déchets ciblés atteignaient leur destination finale, mais les déchets électroniques et les déchets dangereux ne suivaient pas les meilleures pratiques.

Les limites :

- Malheureusement, le suivi des déchets à l'aide de technologies de détection omniprésentes est une tâche ardue : les conditions physiques du flux de collecte des déchets sont hostiles au fonctionnement des dispositifs électroniques, et les capteurs ne peuvent pratiquement pas être récupérés une fois qu'ils entrent dans le flux de déchets.

3.3.1.3 Système 3

(Yeong et al., 2017) Proposant un système base sur NFC « Near Field Communication » avec une application Web et une application mobile permet de créer un système de suivi et de surveillance des déchets solides. Ce système a pour objectif principal d'améliorer l'efficacité du processus de collecte des déchets, de fournir le statut de poubelle en temps réel aux ménages et de fournir également une plate-forme de communication permettant aux propriétaires d'envoyer leurs commentaires sur les services fournis. Le système proposé consiste en une étiquette NFC attachée à la corbeille, à un appareil mobile compatible NFC, à une application Web et Web intégrée à NFC et à un serveur de base de données. Le périphérique mobile compatible NFC transporté par un travailleur collecte les informations de la balise NFC et les envoie à la base de données du serveur via Wifi. La base de données sera mise à jour et les propriétaires de maison pourront vérifier l'état actuel des bacs via l'application mobile et Web. Les informations sur la corbeille sont affichées sur Google Maps. Ainsi, les déchets solides de la corbeille et le calendrier des tâches de l'ouvrier sont surveillés à l'aide du système de suivi et de surveillance de la gestion des déchets basé sur la technologie NFC.

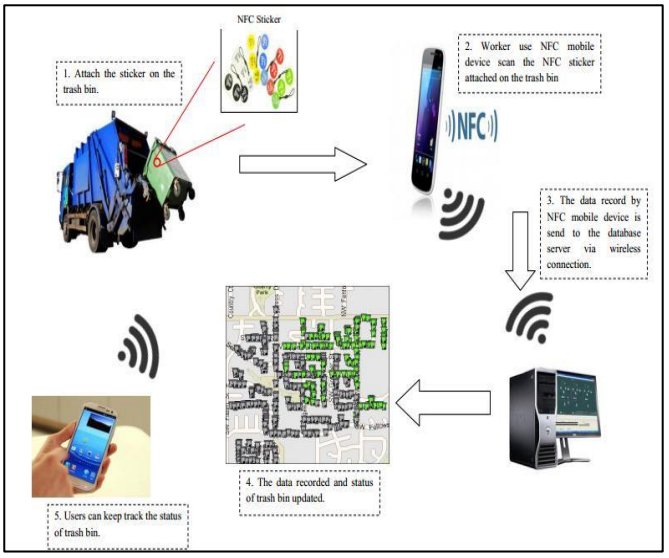

FIGURE 3.3 Le protocole base sur NFC (Yeong et al., 2017)

Les limites :

- l'hébergement de données dans un cloud computing peut l'exposer au vol ou à une mauvaise utilisation.
- Si le serveur tombe en panne, le système s'arrête. cela signifie également qu'un système de sauvegarde coûteux est requis.

3.3.2 SED

3.3.2.1 Système 4

(Namen et al., 2014) Ont proposé une nouvelle conception du système et un prototype d'application de la technologie RFID pour la gestion et le suivi des déchets dangereux afin de garantir la destination correcte pour la livraison de déchets. L'objectif de cette approche innovante, par rapport à d'autres études utilisant la même technologie dans le processus d'élimination des déchets, est de se concentrer sur le certificat attestant que les déchets dangereux seront livrés au bon endroit de destination et qu'ils ne seront pas éliminés de manière inappropriée lors du transport sur le théâtre. Avec l'utilisation d'un système d'information en nuage informatique pour intégrer toutes les données liées au processus afin de soutenir les décisions prises.

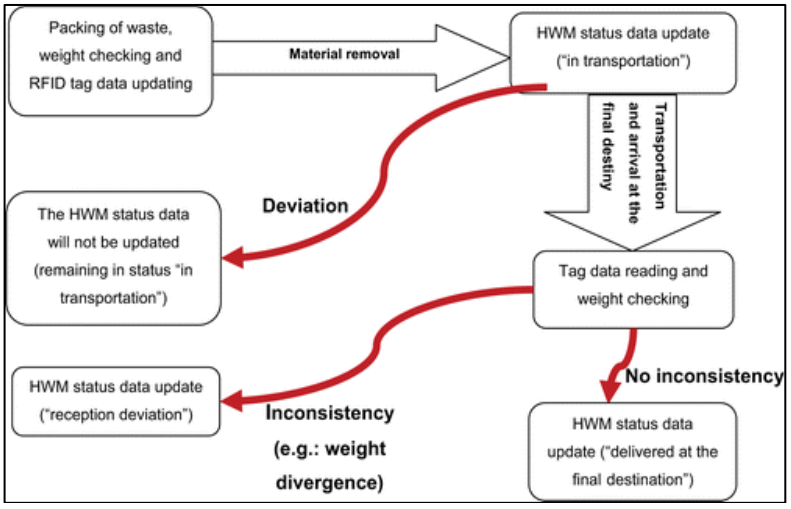

FIGURE 3.4 Processus de suivi des déchets dangereux (Namen et al., 2014)

Les limites :

- l'installation d'équipement RFID dans des endroits inappropriés et dans de mauvaises conditions atmosphériques réduit la durée de vie du service ;
- Bien que les étiquettes RFID soient beaucoup moins chères que les capteurs de localisation actifs, elles ne peuvent être détectées qu'à très courte distance.
- la réécriture des données des étiquettes peut donner lieu à une fraude dans le processus ;
- La RFID ne peut pas fonctionner correctement à proximité de métaux et de liquides .Il est nécessaire de choisir la bonne technologie RFID pour survivre à une humidité et une température extrêmes et pour surmonter les difficultés dues à la saleté, aux dommages et à la distorsion d'interférence provoquée par les métaux et les liquides ;
- l'hébergement de données dans un cloud computing peut l'exposer au vol ou à une mauvaise utilisation

3.4 Synthèse

Nous avons remarqué que certains protocoles étudiés sont plus performants que d'autres. Afin de mieux comprendre la diversité des protocoles étudiés dans ce chapitre qui traitent le problème sécurité et traçabilité d'un système de suivi de déchet, nous avons proposé une comparaison basée sur les critères cites précédemment.

Le tableau résume cette comparaison entre les travaux étudiés dans ce chapitre ; le signe (✓) signifie que le protocole assure la fonction ou résout le problème, contrairement au signe (✕).le signe (−) signifie que le problème n'a pas été étudié dans le protocole. Nous avons ajoute notre proposition, dénommée Système 5, qui sera présenté dans le chapitre suivant

Les critères	Système 1	Système 2	Système 3	Système 4	Système 5
La sécurité	✕	✕	✕	✕	✓
La traçabilité	✓	✓	✓	✓	✓
La transparence	✕	✕	✓	−	✓
La décentralisation	✕	✕	✕	✕	✓
La responsabilité	−	−	−	−	✓

Tableau 3.1 Comparaison des systèmes étudiés.

Nous avons conclu de l'analyse d'études précédentes que :

- la réalisation des critères ci-dessus nécessite la combinaison d'au moins deux technologies.
- Les études ont été axées sur le suivi de la collecte des déchets et la négligence de la partie la plus importante de la traçabilité pos-collecte afin de garantir son inclusion dans la chaîne de recyclage, en réalisant l'économie circulaire et de lutter contre la criminalité des déchets.
- Les travaux étudiés ont prouvé l'intérêt d'utiliser des techniques de suivi des déchets dans de nombreux cas pour améliorer la gestion des déchets, mais le problème réside dans le système distribué, si un nœud tombe en panne, le centre de données, par exemple, entraînera la défaillance de tout le système. Cela signifie également qu'un système de sauvegarde coûteux est requis.

3.5 Conclusion

Après l'étude de quelques solutions proposées, nous avons pu identifier deux catégories de protocoles : protocoles SCD et protocoles SED. Ainsi, nous avons pu soulever précisément les problèmes auxquels nous devons faire face pour obtenir une solution qui répond aux critères cites précédemment et qui présentera de meilleurs résultats.

Le chapitre qui suit fera l'objet de notre contribution qui est basée sur le protocole SED en utilisant une nouvelle technologie qui offre à la fois la sécurité, la traçabilité et la responsabilité de la chaine d'approvisionnement.

ARUNADEVI 2019. SMART GARBAGE MONITORING SYSTEM USING INTERNET OF THINGS. *International Research Journal of Engineering and Technology (IRJET)* 06 Issue: 03 | Mar 2019.

BASAIAOCLU, H., CELENK, E., MARIULO, M. A. & USUL, N. 1997. SELECTION OF WASTE DISPOSAL SITES USING GIS 1. *JAWRA Journal of the American Water Resources Association,* 33**,** 455-464.

KIETZMANN, J. 2008. Interactive innovation of technology for mobile work. *European Journal of Information Systems,* 17**,** 305-320.

NAMEN, A. A., DA COSTA BRASIL, F., ABRUNHOSA, J. J. G., ABRUNHOSA, G. G. S., TARRÉ, R. M. & MARQUES, F. J. G. 2014. RFID technology for hazardous waste management and tracking. *Waste Management & Research,* 32**,** 59-66.

OFFENHUBER, D., LEE, D., WOLF, M. I., PHITHAKKITNUKOON, S., BIDERMAN, A. & RATTI, C. 2012. Putting matter in place: Measuring tradeoffs in waste disposal and recycling. *Journal of the American Planning Association,* 78**,** 173-196.

RADA, E. C., RAGAZZI, M. & FEDRIZZI, P. 2013. Web-GIS oriented systems viability for municipal solid waste selective collection optimization in developed and transient economies. *Waste management,* 33**,** 785-792.

ROVETTA, A., XIUMIN, F., VICENTINI, F., MINGHUA, Z., GIUSTI, A. & QICHANG, H. 2009. Early detection and evaluation of waste through sensorized containers for a collection monitoring application. *Waste Management,* 29**,** 2939-2949.

SCHOWENGERDT, R. 2007. Remote sens: models and methods for image processing. Elsevier/Academic Press, Oxford.

SHARMIN, S. & AL-AMIN, S. T. A cloud-based dynamic waste management system for smart cities. Proceedings of the 7th Annual Symposium on Computing for Development, 2016. ACM, 20.

WANT, R. 2006. An introduction to RFID technology. *IEEE pervasive computing***,** 25-33.

XU, Y., HUANG, G. & XU, L. 2014. A fuzzy robust optimization model for waste allocation planning under uncertainty. *Environmental engineering science,* 31**,** 556-569.

YEONG, B. C., AHAMED, N. H., MALIM, H. & SINGH, M. M. NFC-based waste management tracking and monitoring system. Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing, 2017. ACM, 86.

ZAMORANO, M., MOLERO, E., GRINDLAY, A., RODRÍGUEZ, M., HURTADO, A. & CALVO, F. 2009. A planning scenario for the application of geographical information systems in municipal waste collection: A case of Churriana de la Vega (Granada, Spain). *Resources, Conservation and Recycling,* 54**,** 123-133.

CHAPITRE 4

CONTRIBUTION & IMPLIMENTATION

Comme nous l'avons vu dans les chapitres précédents, la technologie des chaînes de blocs consiste en une évolution de l'ordinateur dans le domaine de la sécurité et des conflits de données. Étant donné que cette technologie fournit un support solide et sécurisé pour la participation d'une base de données en ligne ou au sein d'une communauté en ligne limitée (États, constructeur de véhicules, municipalités, associations, etc.).

À l'heure actuelle, la crypto-monnaie est l'application la plus connue qui a efficacement exploité la manière dont l'authentification par chaîne garantit la non-répudiation et la confidentialité des données sans recourir à des tiers de confiance tels que des banques ou des banques. États. Cependant, la crypto-monnaie commence à peine à utiliser cette technique dans des zones plus vastes et plus sensibles

Dans ce chapitre, nous présentons notre contribution et les outils que nous avons utilisés pour implémenter le cas d'étude, et nous conclure avec les résultats que nous avons atteint

Partie I : La Contribution

4.1 Présentation du projet

4.1.1 Définition du problème

Chaque année, des millions de tonnes de déchets sont produites chaque année. Le problème réside dans le transport et l'élimination ultérieurs de ces déchets, qui peuvent être complexes et fragmentés.

Dans la criminalité liée aux déchets, le manque d'archivage numérique est souvent exploité dans le secteur des déchets, qui transfère les déchets vers des lieux illégaux ou est déterminé par l'erreur consistant à éviter les taxes d'enfouissement ou à les exporter illégalement. Le tableau 4.1 présente les différents problèmes :

problèmes	Description
Fraude et manipulation	Le paiement par kilogramme est effectué lors de l'élimination des déchets. Cependant, les autorités locales ne peuvent pas vérifier le nombre de kilogrammes car elles ne possèdent pas de pont-bascule. Dans le passé, certains flux de déchets générant beaucoup d'argent étaient frauduleux. Cela a été fait en partageant des informations incorrectes qui ne pouvaient pas être vérifiées au moyen d'un pont-bascule.
Mauvaise ou perte d'informations	Les lettres d'orientation et les documents physiques traitent de toutes les activités du processus en cours. Ce faisant, ces papiers sont parfois perdus. Il se trouve que les papiers volent littéralement par la fenêtre pendant le transport ou que les mauvaises lettres sont données au départ.
Manque de connaissances sur la technologie	Les connaissances et la capacité de travailler avec la technologie sont plutôt limitées. En conséquence, le système de gestion de déchets ne se concrétise pas.
Manque de contrôle	L'inspection gouvernementale périodique à la station de division des déchets prend beaucoup de temps. Les ressources étant limitées, les données ne sont pas entièrement surveillées.

Tableau 4.1 Les problèmes

4.1.2 La solution proposé

L'application de cette technologie au secteur des déchets fournira un enregistrement fiable et sûr de tous les mouvements de déchets dans le grand livre distribué et horodaté, ce qui permettra de suivre les déchets de la source au traitement final. Les utilisateurs pourront importer et exporter des données via une interface utilisateur avec différents niveaux de fonctionnalité et d'accès. Veillera également à ce que les producteurs et les gestionnaires de déchets se conforment aux réglementations

en matière de déchets et aidera les régulateurs à identifier et à lutter contre les violations illicites des déchets le tableau 4.2 présente la solution base sur la blockchain.

problème	Solution de blockchain
Fraude et manipulation	Avec la technologie blockchain, il est important que les données saisies soient correctes, car il n'est plus possible de les modifier par la suite. La séparation des déchets station ne dispose pas des solutions (automatisées) appropriées pour garantir que ces données source sont correctes. Ils sont trop dépendants d'une autre partie, qui n'est pas suffisamment confidentielle pour être utilisée comme source de données. La technologie des chaînes de blocs ne résoudra pas ce problème et, en fait, une solution doit être trouvée avant que la chaîne de chaînes ne puisse être mise en œuvre.
Mauvaise ou perte d'informations	Une fois que quelque chose est entré dans une blockchain, celle-ci est immédiatement sécurisée. Les lettres de guidage et les bons de pesée étant saisis numériquement avec une solution de blockchain, ils ne peuvent pas être perdus physiquement. Une implémentation blockchain est la bonne solution pour résoudre ce problème.
Manque de connaissances sur la technologie	La technologie Blockchain ne modifiera pas la maturité actuelle des connaissances et de l'expertise en informatique.
Manque de contrôle	Si les organisations sauvegardent les données en utilisant Blockchain et s'assurent que cela se fait de la bonne manière, il est possible d'utiliser la technologie Blockchain en tant que "facteur de confiance". Les données qu'il contient ne peut pas être modifié et s'il est entré correctement, vous pouvez garantir la fiabilité des informations. Ceci offre une solution pour les services d'inspection.

Tableau 4.2 Les solutions

4.2 Architecture proposé

4.2.1 Aperçu de la conception de l'architecture

Afin de gagner en efficacité dans la gestion de la confiance pour le réseau de gestion des déchets, nous proposons un système de suivi des déchets basé sur la blockchain.
La figure 4.1 montre l'architecture globale proposée pour le réseau de gestion des déchets. Dans le modèle proposé, le réseau est divisé en deux groupes différents - le réseau principal et le réseau de bord - en utilisant la technique de la blockchain.

- Le réseau central est constitué de nœuds de mineur dotés de ressources de calcul et de stockage élevées. Seront responsables de la création des blocs et de la vérification de la preuve de travail.
- Les nœuds de bord sont les participants dans le système de suivi de déchets. Ils disposent d'une

capacité de stockage et de calcul limitée. Ils sont cites dans le tableau 4.3 :

No	Acteurs	Description
01	Responsable de collecte	Un nœud connecté à l'ethereum blockchain, qui est responsable de emballés les déchets dans desballes, et enregistrer dans blockchain avec QR code attribuée
02	Responsable de stockage	Stockage est la place qui regroupe les déchets collectés, leur propriétaire est un nœud connecter à l'ethereum blockchain
03	Responsable de transport	Un nœud connecté à l'ethereum blockchain qui est responsable de transporter les déchets pour un traitement ultérieur
04	Responsable de traitement	Apre le traitement des déchets, le responsable de traitement est étiquète le résultat final avec le QR code

Tableau 4.3 Les nœuds de bord

Chaque nœud périphérique agit comme un serveur centralisé pour une infrastructure publique spécifique afin de fournir des services essentiels et de réaliser des localisations. La nature distribuée du modèle proposé peut améliorer la résilience de l'ensemble du système et limiter l'impact des attaques, même lorsque le nœud est compromis. En d'autres termes, si le nœud de bord est compromis, l'effet résultant doit être limité à la zone locale.

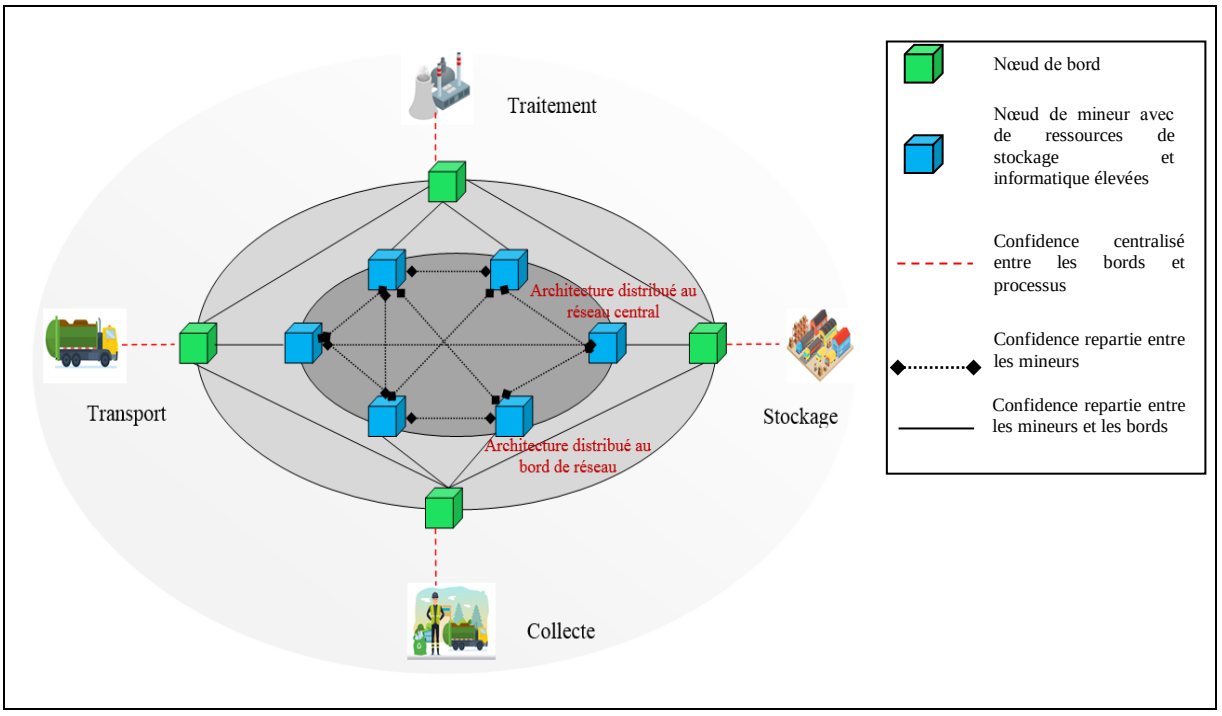

FIGURE 4.1 Architecture proposée pour le réseau de gestion des déchets

4.2.2 Workflow de modèle proposé

Dans la gestion des déchets, un grand volume de données est généré et nécessite un suivi en temps réel. Dans notre modèle proposé, les nœuds périphéries offrent un suivi en temps réel. Le nœud périphérie a une capacité de stockage et de calcul limitée. Les données collectées par ces nœuds pour suivre les déchets et obtenir des informations utiles. Une fois les données collectées, le nœud périphérie transfère les données cryptées collectées vers le réseau central. Le nœud mineur du réseau central validera et vérifiera le PoW et générera des blocs. Pour garantir l'intégrité des données stockées dans le réseau central, nous utilisons une signature numérique et stockons des hachages dans une chaîne de blocs. Ces hachages dans la blockchain sont immuables et servent de preuves pour prouver l'intégrité des données.

La figure 4.2 illustre le flux de travail de notre modèle proposé.

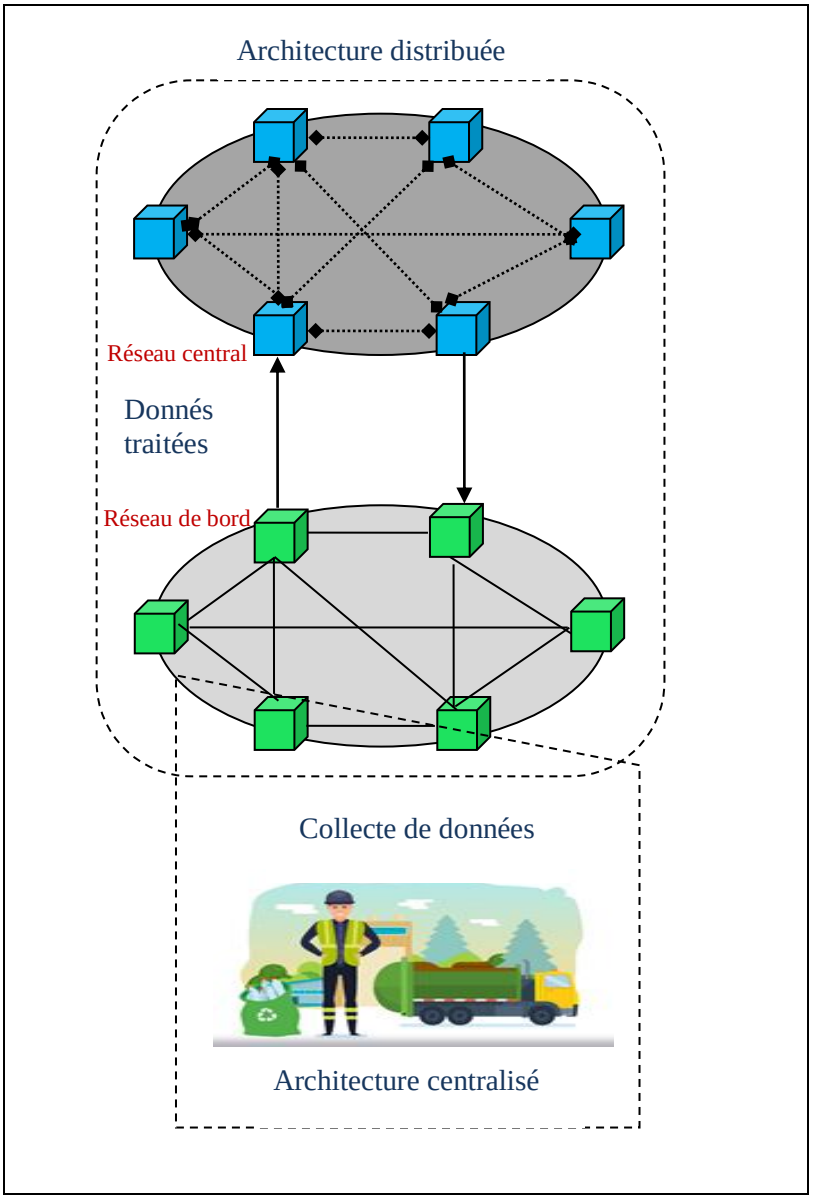

FIGURE 4.2 Architecture de workflow proposée

4.2.3 Processus de minage sur le réseau principal

Après avoir reçu une transaction sur le nœud principal du nœud périphérique, le processus d'extraction est lancé. En raison de la limitation des ressources sur le nœud périphérique, nous exécutons le processus d'extraction sur le réseau principal dans le modèle proposé. Le processus d'extraction comprend les étapes suivantes :

- **Étape 1 :** chaque fois que le noeud périphérique reçoit une nouvelle donnée (transaction) de la source de gaspillage, il envoie une demande de transaction à chaque mineur du réseau principal.
- **Étape 2 :** à la réception de la demande de transaction, le nœud mineur vérifie et vérifie si la transaction est modifiée ou non et si la transaction existe ou non dans la chaîne de blocs. Si la transaction n'est pas modifiée et qu'elle n'existe pas dans la chaîne de blocs, le nœud mineur passe à l'étape 3. Sinon, il abandonne le processus d'exploration et diffuse le rapport dans le réseau central.
- **Étape 3 :** Dans cette étape, le nœud mineur récupère l'ID de bloc précédent et lance le processus de POW. Dans le cas du bloc de genèse, l'ID de bloc précédent est zéro. Le bloc de genèse est le premier bloc de la blockchain. Dans le processus de PoW, le nœud du mineur créera un nouveau bloc en hachant de manière itérative les informations, qui comprend l'ID précédent, l'ID de bloc créé, la date et l'heure, la transaction vérifiée et la signature numérique du mineur à l'aide de l'algorithme de PoW décrit ci-dessus.
- **Étape 4 :** une fois le bloc créé, pour garantir l'intégrité des informations de tous les blocs de la chaîne de blocs, les nœuds mineurs vérifient et vérifient tous les blocs existants.
- **Étape 5 :** lors de la dernière étape, le nœud mineur envoie une chaîne de blocs mise à jour à tous les nœuds de bord.

Partie II : Implémentation

4.3 Cas d'utilisation

Dans notre cas d'étude nous avons choisi de suivi les déchets solide qui sont bien défini dans le première chapitre, et en particulier nous avons prendre comme exemple les déchets plastique.

4.3.1 Déchets plastique

Les déchets plastiques désignent tout produit plastique tel que sacs de transport, sachets ou emballages multicouches, qui ont été jetés après utilisation ou après la fin de leur durée de vie escomptée. Les matières plastiques trouvées dans nos déchets varient selon leur nature et leur utilisation. En effet, la grande majorité de la matière plastique est constituée de produits pétroliers et ils ne sont pas biodégradables.

4.3.2 Les catégories de plastique

Le tableau suivant présent les diffèrent catégorie de plastique.

Logo	Nom
	PET : Polyéthylène téréphtalate le plus largement recycle Ex : les bouteilles d'eau gazeuse
	PEHD : Polyéthylène haute densité Ex : bouteilles de lait , Bidons
	PVC : Polychlorure de vinyle, sous sa forme rigide (non plastifié). Ex boittes alimentaire
	PELD : Polyéthylène base densité . Ex sace et emballage plastique.
	PP : Polypropylène très facile à colorer. Ex sachet el film transparent
	PS : polymère styrénique. Ex pot de yaourt
	Autre comme polycarbonate. Ex cd, dvd.

Tableau 4.4 Classification de plastique

4.3.3 Fonctionnement

Nous avons base sur le cycle de vie de la bouteille P.E.T. Ce sont les déchets les plus courants mais les plus recyclables et peuvent être utilisés comme source de matière. Nous pouvons collecter une bouteille séparée de P.E.T et la recycler de plusieurs manières.

La figure suivant représente le cycle de vie de la bouteille P.E.T

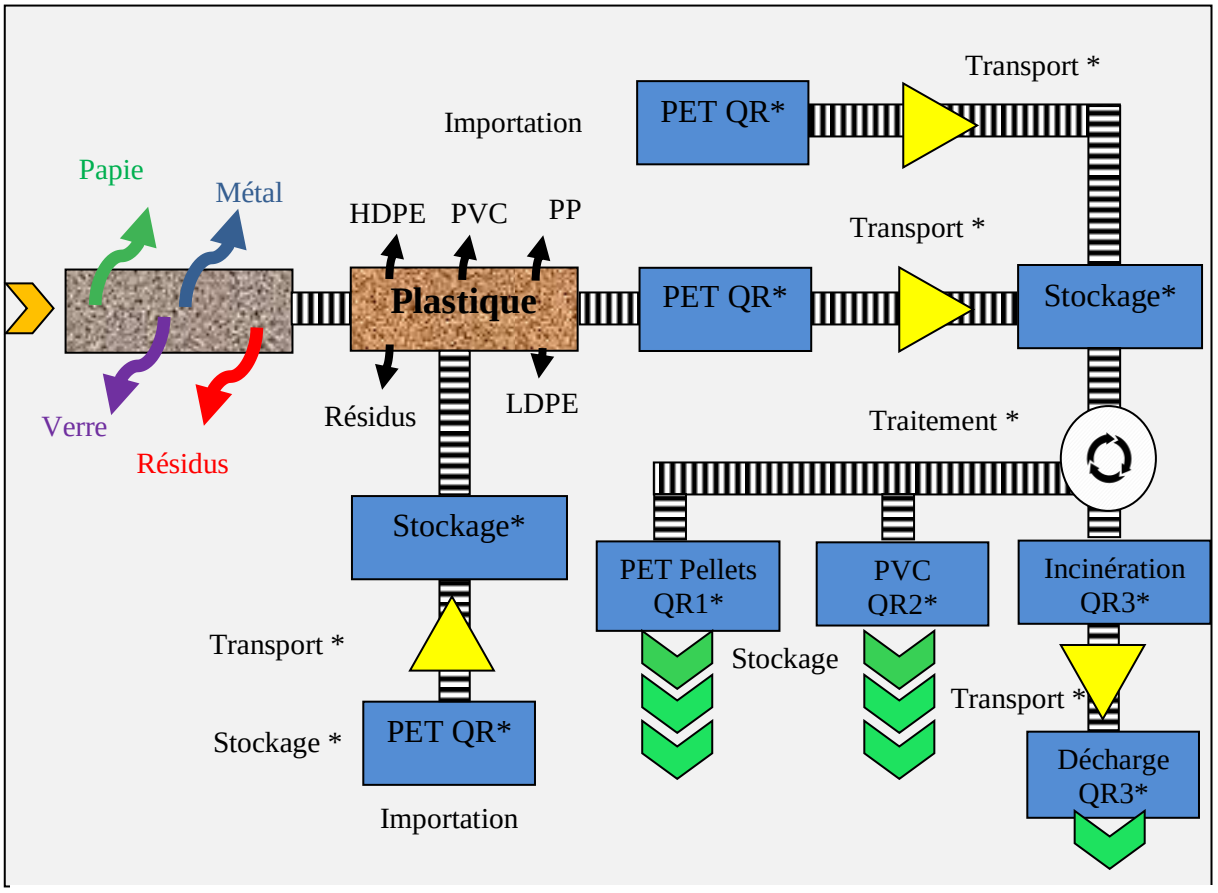

FIGURE 4.3 Fonctionnement de notre systeme

Le cycle de PET est passe par quatre étapes (separation ,transaport , stockage et traitement) ou chaque étape peut répéter plusieurs fois :

1. Collection et séparation

Les matières premières sont collectées à partir des sources de déchets, qu'elles soient générées ou des centres de collecte. Les déchets sont ensuite séparés en diverses fractions utiles : déchets organiques et autres, dangereux ou commerciaux, puis par types ; verre, métal, papier, plastique, etc.

2. Emballage

Les déchets sont ensuite emballés dans des balles, des sacs, des boîtes, etc. et sont enregistrés dans la Blockchain avec les codes QR attribués. L'enregistrement des déchets se fait via une application, simplement en saisissant les données.

3. Transports

Les déchets sont transportés par un transporteur agréé pour un traitement ultérieur. Le code QR est scanné et des informations sur cette action sont ajoutées et téléchargées sur notre dapp.

4. Stockage

Les déchets sont amenés à l'entrepôt temporaire. Pour ce faire, l'opérateur doit obtenir une licence de stockage respective. Le changement de statut est enregistré dans notre dapp.

5. Traitement des déchets

a) Usage ultérieur

Les déchets sont traités en fonction du type, de la catégorie et de la qualité. Les matériaux recyclables tels que le plastique, le verre, le papier, l'aluminium, les tissus, les pneus usés, etc. sont nettoyés et purifiés et sont transformés en une nouvelle matière première ou sous-produit pouvant être récupéré à la production, qui sont également étiquetés avec un code QR afin de relier les produits livrables. Avec son origine.

b) Incinération

Si la fraction ne peut pas être recyclée ou traitée à d'autres fins, elle est généralement incinérée et utilisée pour la production d'énergie.

c) Disposition

Les déchets qui ne peuvent être ni utilisés à des fins quelconques ni traités sont déposés en permanence dans la décharge. Cette partie des déchets ne doit pas dépasser plus de quelques pour cent de la totalité des déchets.

4.4 Implémentation

4.4.1 Application décentralisée

L'application décentralisée, également appelée dapp, est une application qui connecte directement les utilisateurs et les fournisseurs. Il fonctionne sur un réseau distribué et utilise une chaîne de blocs pour stocker ses données.

La figure 4.4 représente l'architecture décentralisée d'une Dapp.

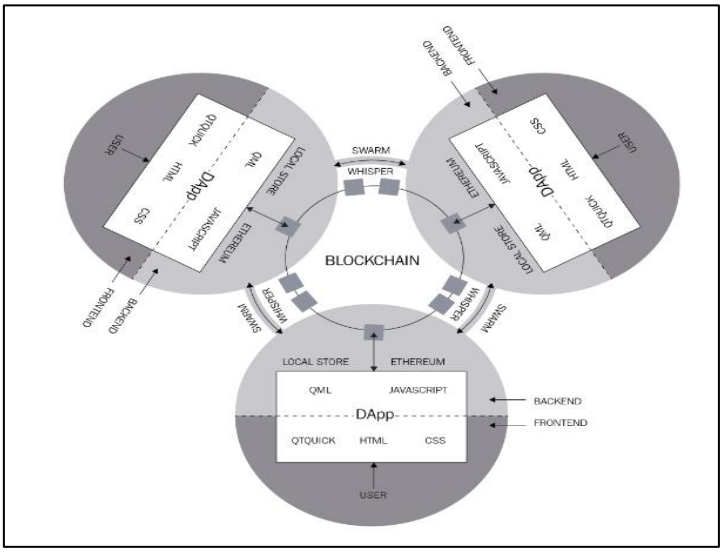

FIGURE 4.4 Architecture décentralisée (Mukhopadhyay, 2018)

4.4.2 Architecture Dapp

La figure 4.5 représente un Ethereum DApp à un niveau élevé. Si vous remarquez, chaque navigateur client communique avec sa propre instance de l'application. Il n'y a pas de serveur central auquel tous les clients se connectent. Cela signifie que toute personne souhaitant interagir avec une application décentralisée aura besoin d'une copie complète de la blockchain s'exécutant sur son ordinateur / son téléphone, etc. Cela signifie que, avant de pouvoir utiliser une application, nous devons télécharger la blockchain complète, puis commencer à utiliser l'application. Cela peut sembler ridicule au début, mais cela présente l'avantage de ne pas compter sur un seul serveur central qui pourrait disparaître demain, ou de nous faire payer des commissions par des tiers.

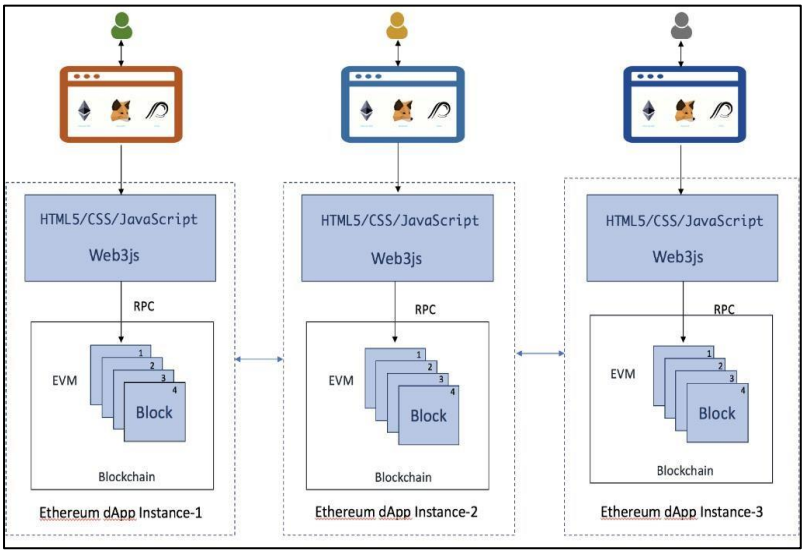

FIGURE 4.5 Architecture d'une Dapp (Mukhopadhyay, 2018)

Ethereum est livré avec une bibliothèque JavaScript très pratique appelée web3.js, qui se connecte à notre nœud blockchain à l'aide d'appels de procédure distants (RPC). Nous pouvons donc simplement inclure cette bibliothèque dans nos infrastructures JavaScript préférées, telles que ReactJS ou AngularJS, et commencer à développer notre DApp

4.4.3 Création de contrat intelligent

Les contrats intelligents contiennent les codes de programme à exécuter et sont analogues à une classe C ++, C # ou Java. Il contient :

- ✓ variables d'état
- ✓ Les fonctions
- ✓ Événements

Les contrats intelligents sont compilés en bytecodes. Ces bytecodes sont déployés en tant qu'instances de Smart Contracts dans la machine virtuelle Ethereum (EVM).

4.4.4 EVM

EVM (ou machine virtuelle Ethereum) est l'environnement d'exécution de codes octets par contrats intelligents Ethereum. Chaque nœud du réseau exécute EVM. Tous les nœuds exécutent toutes les transactions pointant sur des contrats intelligents à l'aide d'EVM, de sorte que chaque nœud effectue les mêmes calculs et stocke les mêmes valeurs. En outre, l'EVM veille à ce que les programmes n'ont pas accès à l'autre État, ce qui permet d'établir une communication sans interférence potentielle.

4.4.5 Environnement de développement

- **Environnement et technologies logicielles**

a. Ressources matérielles

• Processeur	Intel ® core ™ i3-4005U CPU @1.70GHz
• Mémoire installe (RAM) :	4.00Go
• Type de système :	système d'exploitation 32 bits

Tableau 4.5 Ressource matérielle

b. Ressources logicielles

• Système d'exploitation	Windows 7
• Editeur utilisée	Visual Studio code, Remix, Sublime

Tableau 4.6 Ressource logicielle

- **Langage utilise**

Solidity

Solidity est un langage de haut niveau orienté objet pour la mise en œuvre de contrats intelligents. Les contrats intelligents sont des programmes qui régissent le comportement des comptes au sein de l'état Ethereum. Solidity a été influencé par C ++, Python et JavaScript et est conçu pour cibler la machine virtuelle Ethereum (EVM) (Solidity, 2019)

JavaScript

JavaScript est un langage de programmation couramment utilisé dans le développement Web. Bien que JavaScript soit influencé par Java, la syntaxe est plus similaire à C.(Flanagan, 2006)

HTML

L'HTML est un langage utilisé pour créer des pages web. L'acronyme signifie, "langage de balisage d'hypertexte". ce langage permet de réaliser de l'hypertexte à base d'une structure de balisage (Duckett, 2011)

CSS

Signifie «feuille de style en cascade». utilisées pour formater la mise en page des pages Web. Ils peuvent être utilisés pour définir des styles de texte, des tailles de tableau et d'autres aspects des pages Web qui ne pouvaient auparavant être définis que dans le code HTML d'une page.(Duckett, 2011)

- **Outils utilisé**

Metamask

Le client Ethereum pour le web .Les réseaux Blockchain Ethereum sont composé d'un ensemble des nœuds. Pour qu'un utilisateur puisse interagir avec le réseau Ethereum, il doit communiquer à l'aide d'un nœud. MetaMask nous fournit justement un nœud Ethereum qui tourne directement dans le navigateur. Il va aussi exposer l'API web3 nécessaire au fonctionnement d'une DApp. Cela va donc nous permettre d'interagir avec le réseau Ethereum depuis le navigateur.

MetaMask est sous la forme d'une extension Google Chrome L'extension donne la possibilité de se connecter à différents réseaux Ethereum comme le "Main Network", des réseaux de tests comme Ropsten appelés testnets ou à un réseau local comme TestRPC.

Truffle Framework

Truffle est un framework qui facilite le développement de smart contracts Solidity. Truffle permet de compiler, tester et déployer les smart contracts. Il fournit également une couche d'abstraction JavaScript afin de faciliter l'interaction entre les smart contracts et le front-end. De plus, il est compatible avec TestRPC et web3 par défaut.

Ganache

Ganache un outil indispensable lors du développement de toute dApp. nous permet d'avoir une dizaine de comptes Ethereum avec 100 ethers chacun, ce qui permet de faire des tests facilement (Wohrer and Zdun, 2018), l'avantage aussi est de disposer des logs détaillés de tout ce qu'il se passe que la blockchain.

ReactJS

Est une bibliothèque JavaScript libre développée par Facebook depuis 2013. Le but principal de cette bibliothèque est de faciliter la création d'application web monopage, via la création de composants dépendant d'un état et générant une page (ou portion) HTML à chaque changement d'état.

Google Maps

Est un service de cartographie en ligne créé par Google. disponible sur PC, sur tablette et sur smartphone qui permet, à partir de l'échelle mondiale, de zoomer jusqu'à l'échelle d'une habitation.

MySQL

Est un serveur puissant de base de données open source intégré basé sur un système de gestion de base de données relationnelle (SGBDR) et est capable de gérer une grande base de données de connexion simultanée.

Web3Js

Dans le réseau Ethereum, chacun contient une copie de la blockchain. Lorsque vous souhaitez appeler une fonction dans un contrat intelligent, vous devez interroger l'un de ces nœuds et leur dire:

Titre du contrat intelligent La fonction à laquelle vous voulez vous connecter, et les variables que vous souhaitez transmettre à cette fonction.

Les points Etherum ne parlent qu'un langage appelé JSON-RPC, qui n'est pas lisible par les humains. Une requête apparaît pour indiquer au nœud que vous souhaitez appeler quelque chose d'un contrat

Heureusement, Web3.js masque ces mauvaises requêtes sous la surface.

Vous n'avez donc besoin que d'interagir avec une interface JavaScript confortable et facile à lire.

Node.JS

Dans la mesure où une chaîne de blocs privée ou locale est en cours d'exécution, nous devons configurer notre environnement pour développer des contrats intelligents Pour cela, nous aurons besoin du Node Package Manager ou NPM, qui inclut Node.js. (Kumar Bhosale, 2019).

4.4.6 Implémentation :

Apres avoir créé le back end les smart contracts à travers l'outil Remix en ligne, et implémenter le front end à travers les outils détaillé ci-dessous nous lançons les étapes suivant :

1) Lancer le test RPC

Après la sélection de chemin de l'application taper la commande ***testRPC*** dans le git :

```
windows 7@windows7-PC MINGW32 ~/Desktop/zaineb-Dapp
$ testrpc
EthereumJS TestRPC v6.0.3 (ganache-core: 2.0.2)

Available Accounts
==================
(0) 0x27060ca470264fdcb40c25743e6949087f50dcfe
(1) 0x155611bd1b9f27502d96b02a5e3155f18b225237
(2) 0x00ce7198a1f11dd97d26c9b0b085f1cc9f9d6fed
(3) 0x3a1e6bcdc90a3f61c59ddcbe682d5cf550cbf911
(4) 0xef2915f9eea7244b90915fd6d8a3c7599e861eb4
(5) 0xea015699c3b9b2ead5a736fb84742d1a01ff58c6
(6) 0xc19f790e02ff423ffab73f321c98f81f354dde58
(7) 0x8e78ea6f14858da4361bac43dbc41a0074f1f473
(8) 0xf84e1a0cc1a979eb183d857941d7d7e746b023c7
(9) 0x7a9cae0d04f33323361966aca912f67f5205a722

Private Keys
==================
(0) 893dff9dcab42c1dbdd4f49177aa9de0e3461f2f77ab7721c6873e8cdb03738f
(1) 28ce6e426cd1f8861014092b2b69e3d9ef211aca1f2348068eecff397b81d704
(2) 321146db2ee538cfa560694bb8e9b91d2bd494d96ae06d14b0d1e2199600dfc2
(3) 9becc86256d4e23135baff82714032c6115f11823356158d203ff89c53b1a1cc
(4) 898fce504bcfaed4e87dcda3c36c74007a7867944c832a19d1af1ca8000869e8
(5) f2dbfdcf76ac13080bf7913fc4506c9f892897541effcff8144b6f2f5eabbb52
(6) f7746f5fb1cad466d1404e45b379e20c88a63add35b9105100408050e07f6e0f
(7) 2415fd1afa8ca5252a182c78ae03d9803ac85be68ab8eed51ccd50cf6273486f
(8) 88fe404d42cd2f5dd8a8cdff28033ec8a9779f29cb85fff146f6a07215b8ecff
(9) ecbd399bb922d9143df7667bb483d0d9d6a8a575c1cc99265835642f5d5b5a50

HD Wallet
==================
Mnemonic:      mix vessel choice canyon trash liquid audit protect menu large ga
me album
Base HD Path:  m/44'/60'/0'/0/{account_index}

Listening on localhost:8545
```

FIGURE 4.6 Le test RPC

2) Compiler la smart contract

Ouvrir un autre cmd dans le même chemin d'application est lancer la commande ***truffle compile*** pour compiler la smart contract, et la commande ***truffle migrate*** pour déployer la contract.

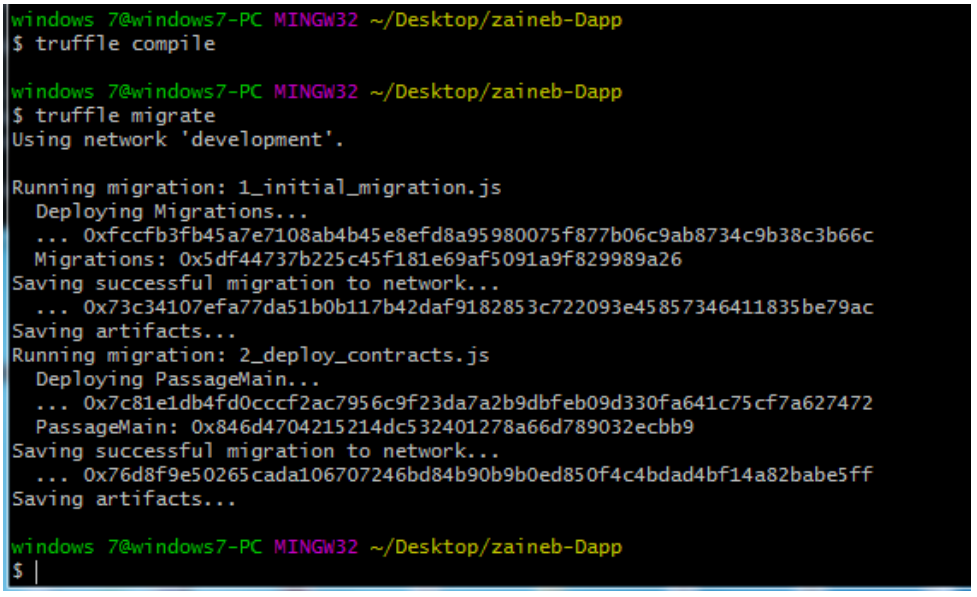

FIGURE 4.7 Compilation de contract

3) Lancer application

Une fois le smart contact est déployer ouvrier un novelle cmd est taper ***npm run start*** pour lancer l'application

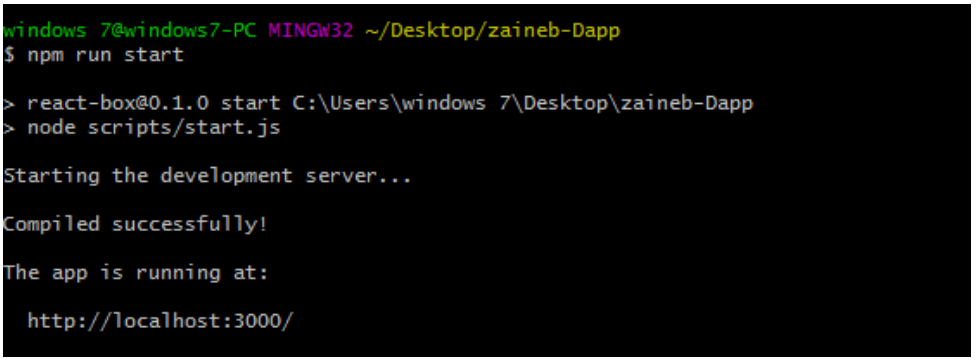

FIGURE 4.8 Lancer application

4.4.7 Les diffèrent interfaces de notre App

1) Home page

Après avoir lancé l'application, l'interface d'accueil suivant est affichée

FIGURE 4.9 Home page

2) Authentification :

Dans l'authentification nous avons choisi de travaille avec le wallet MetaMask, car elle nous offre une clé public similaire a une adresse, et une clé prive similaire a un mot de passe

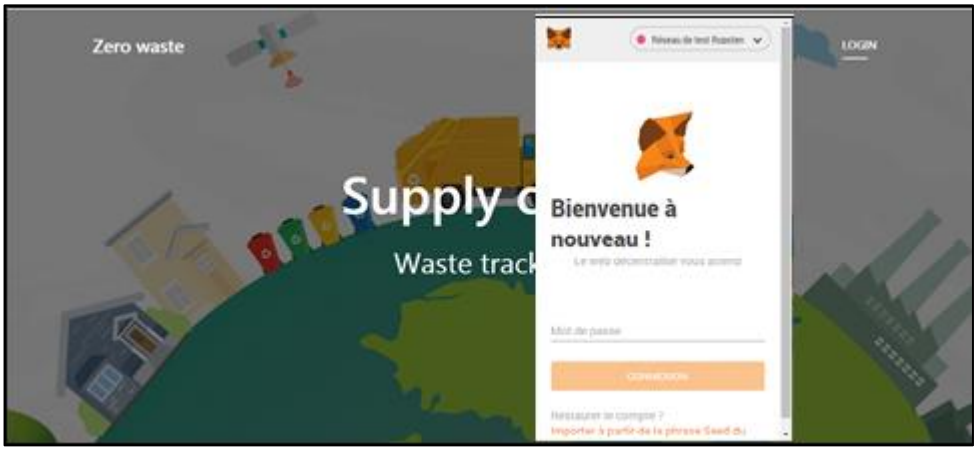

FIGURE 4.10 Page d'authentification

3) Les activités de dapp :

- **Ajouter déchets**

1. Pour ajouter un déchet cliquer sur le bouton ***create***

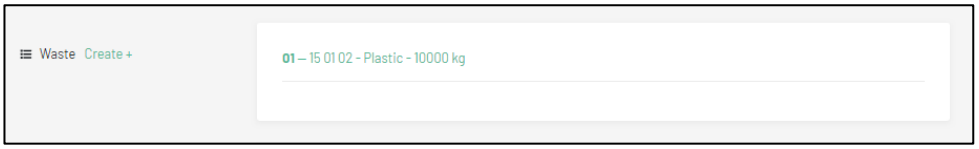

FIGURE 4.11 Interface d'ajout

2. L'interface suivant est affiché, il faut remplir le formulaire par les informations suivant :
   - Id
   - Catégorie (PET, HDPE, PVC, LDPE, PP, PS, other)
   - Classification (commercial ou non)

- Packaging (Sac, Coffin, Rinfuz, Bale)
- Type (Dangereuse ou non)
- Weight (en Kg)
- Localisation

3. Une fois vous cliquer sur ***save***, il faut payer des éthers pour que la transaction soit valider par les mineur est ajouter dans le blockchain

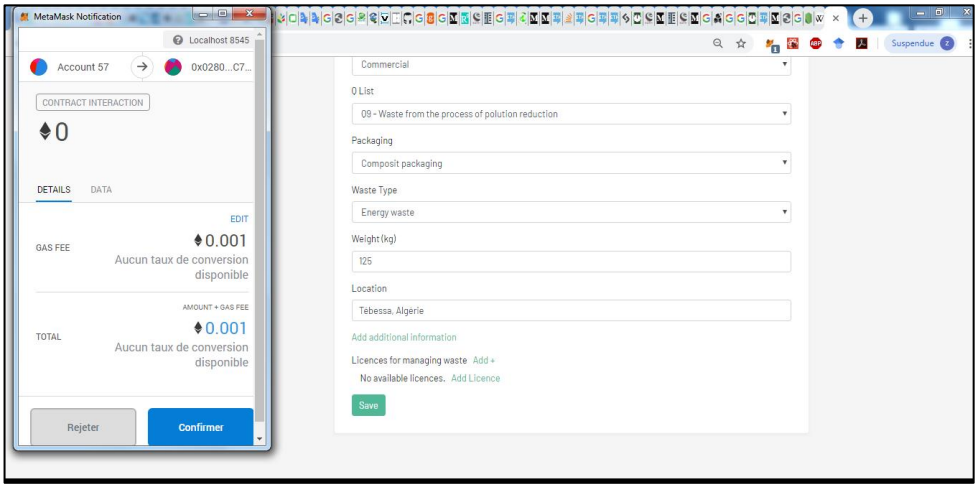

FIGURE 4.12 Formulaire d'ajout

Après la création du bloc un QR code unique est générer est le résultat afficher pour tous les nœuds.

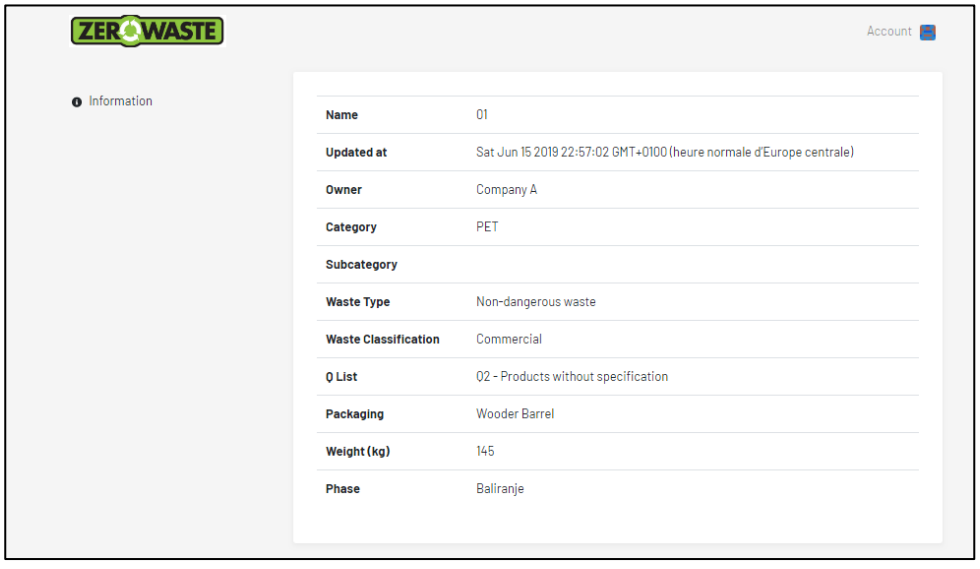

FIGURE 4.13 Résultat d'ajout

FIGURE 4.14 QR code générer

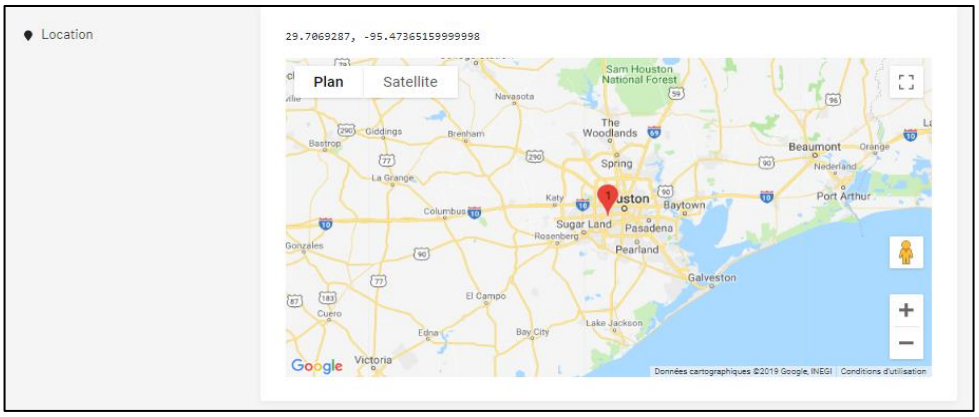

FIGURE 4.15 Affichage de localisation

- **Les actions**

Après la création de déchet les actions de (***Transport, Collecte, Storage, Traitement***) sont possibles et chaque transaction demande d'éther pour être ajuter dans un bloc et diffuser sur le réseau.

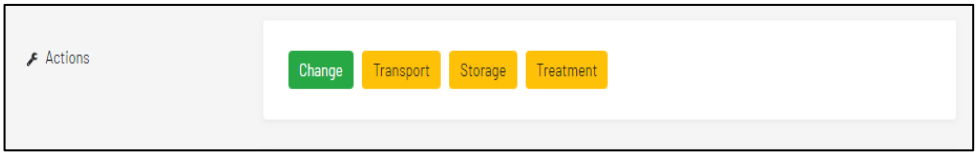

FIGURE 4.16 Les différents actions

- **Chercher un déchet**

La recherche se fait à l'aide de numéros id

FIGURE 4.17 Interface de recherche

- **Combiner déchets**

Vous prouvez combiner des déchets en un seul à travers le QR code

FIGURE 4.18 Interface de combinaison

- **Consulter l'historique de déchet**

L'historique de déchets (les blocs) est consulté à tout moment par les membres de réseaux

FIGURE 4.19 L'historique de déchets

4.5 Les résultats

Nous avons mis en place une preuve de concept (PoC) et avons eu l'idée d'appliquer la technologie blockchain à la gestion des déchets afin de prouver son utilité. Et nous avons atteint les avantages suivant :

✓ **Surveillance précise des flux de déchets :**
En téléchargeant les informations sur les flux de déchets vers l'applicatioon on obtient une base de données verrouillée et sécurisée à partir de laquelle, à tout moment et avec une fiabilité absolue, on peut identifier la source des déchets, leur composition, leur qualité, leur quantité et leur type, ainsi suivi des changements de statut et de propriété des déchets au cours de leur traitement.

✓ **Nouvelles opportunités commerciales :**
La technologie Blockchain permet la mise en œuvre complète de l'économie circulaire, en introduisant une nouvelle solution technologique, avec une efficacité accrue et en créant de nouveaux emplois.

✓ **Pas d'empreinte environnementale :**
Notre application permet une utilisation efficace des déchets, en tant que ressource matérielle précieuse, tout en réduisant l'impact sur l'environnement et en atténuant les effets négatifs du changement climatique, en offrant une vie plus saine à tous les citoyens.

✓ **Coopération transfrontalière :**
Il est possible d'avoir un trafic transfrontière transparent de déchets et de matériaux recyclés avec un registre fiable des importations et des exportations de tous types de déchets et de leurs

technologies respectives. Cela révèle des opportunités de coopération industrielle accrue.

- ✓ **Recherche & Développement :**
  Il offre la possibilité de surveiller la mise en œuvre et les ajustements de la réglementation liés à la gestion des déchets et permettant de mieux comprendre le développement de nouvelles technologies soutenant l'économie des circulaires, mais aidant également à sensibiliser le public aux avantages de l'utilisation de ce modèle économique.

- ✓ **Utilisation des déchets :**
  C'est la base pour créer un marché réglementé pour les déchets, produits et services de l'industrie du recyclage et avec des potentiels économiques exquis découlant de l'utilisation de déchets dans le cadre de l'économie circulaire.

Comme les autres applications, notre application a des limites :

- ✓ Il faut avoir un wallet d'éther pour que les donnes soit sécurisé et diffusée.
- ✓ Le temps de repense un peu plus lent que le système traditionnelle car la transaction doit diffuser sur tous le réseau pour être miner par les mineurs.

.

4.6 Conclusion

Ce présent chapitre a été consacré aux différents outils ayant contribués à l'aboutissement de ce projet. On a détaillé du système proposé et son fonctionnement (architecture, les transactions, …etc.) a été mise en évidence. Nous avons présenté aussi l'implémentation du système ainsi que les différents langage et outils utilisé. Enfin nous avons conclu par le service qui permettre de contrôler le processus de déchets.

COLLOMP, R., CHALINDAR, P., HOUSSEMAN, S., DELANOE, A., CRIDELICH, C., DANTIN, T., BÉRARD, O., MULLER, F., POITRAT, S. & SOCCOJA, G. Traçabilité et Déchets d'activités de soins à risque infectieux (DASRI): Evaluation de l'apport de la technologie RFID. Gestion et Ingénierie des SystèmEs Hospitaliers: GISEH 2010, 2010.

DUCKETT, J. 2011. *HTML & CSS: design and build websites*, Wiley Indianapolis, IN.

FLANAGAN, D. 2006. *JavaScript: the definitive guide*, " O'Reilly Media, Inc.".

KUMAR BHOSALE, K. A., JADHAV DEEPAK, AWANI SANKHE 2019. Blockchain based Secure Data Storage. *International Research Journal of Engineering and Technology (IRJET)* 06**,** 5058.

MUKHOPADHYAY, M. 2018. *Ethereum Smart Contract Development: Build blockchain-based decentralized applications using solidity*, Packt Publishing Ltd.

SOLIDITY. 2019. *Solidity v0.5.9* [Online]. Available: https://solidity.readthedocs.io/en/v0.5.9/.

WOHRER, M. & ZDUN, U. Smart contracts: security patterns in the ethereum ecosystem and solidity. 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE), 2018. IEEE, 2-8.

CONCLUTION GÉNÉRALE & PERSPECTIVES

La blockchain est utilisée pour créer la confiance dans deux dimensions : l'origine de l'information et son instabilité (intégrité dans le temps).

Il est utile de comprendre les chaînes clés dans le contexte de Bitcoin, mais surtout, ne supposez pas que tous les écosystèmes blockchain ont besoin de mécanismes tels que le travail à l'épreuve de Bitcoin, la règle de la chaîne la plus longue. D'autre part, des enregistrements distribués et des chaînes spéciales peuvent être déployés pour résoudre d'autres problèmes. Comme toujours, chaque solution présente des avantages et des inconvénients et doit être considérée individuellement pour chaque cas d'utilisation.

L'intégration de la blockchain dans l'urbanisme permettra de mieux protéger la vie privée en contrôlant l'accès à ses données.

À une époque où la technologie de blockchain évolue, elle peut être perçue comme une opportunité de restaurer des utilisateurs horizontaux sur le réseau, en créant des fournisseurs de services réels et réels et des utilisateurs de services en même temps via une approche d'égal à égal. La procédure publique a tous les avantages de profiter de cette possibilité pour s'assurer que les enregistrements des opérations ou des biens sont conservés avec le service de contrôle,

Dans les projets urbains tels que le système de gestion des déchets. Cette évolution améliorera non seulement le processus de suivi, mais facilitera également le contrôle du processus, ce qui conduira à un fonctionnement efficace ainsi aux contrôleurs d’assurer un suivi et un contrôle des responsabilités.

Enfin, bien qu’il n’existe pas encore de solution parfaite, l’adoption de technologies telles que Blockchain pour accroître la transparence de la gestion des déchets renforcera la fiabilité du processus dans son ensemble. En outre, cela réduira les tâches fastidieuses, manuelles et répétitives pour les fabricants, les clients, les autorités et toutes les autres parties prenantes, à condition que les clés de cryptage soient utilisées sous le contrôle de l'utilisateur.

En premier lieu, nous avons donné une vue globale sur les projets urbaine ainsi que notre problématique .Ensuite, nous avons présenté la cryptographie derrière la blockchain, démystifier la blockchain leur architecture, caractéristiques et domaines d’application. Par la suite, nous avons

abordé les technologies déjà utilisée pour garder la trace de déchet dans lesquelles nous avons présenté deux grandes groupes de systèmes de suivi de déchets : SCD et SED et enfin nous avons proposé une classification basée sur un ensemble de critères. Pour conclure, nous tenons à préciser que notre contribution comporte deux parties essentielles :

1. Nous avons proposé une nouvelle architecture pour suivi le déchet basée sur l'algorithme de Pow.

2. Nous avons également implémenté notre architecture à l'aide d'un ensemble des outils et sur le réseau de l'Ethereum

Comme perspective, nous envisageons de raffiner notre étude à travers les points suivants :

1. Implémenter une application mobile pour scanner et lire les QR code

2. introduire la Data-Science pour améliorer le processus de décision. Ceci va permettre de mieux estimer le temps nécessaire pour prendre une décision.

BIBLIOGRAPHIE

ABDELHAMID, M. S. 2014. Assessment of different construction and demolition waste management approaches. HBRC Journal, 10, 317-326.

ALAM, P. & AHMADE, K. 2013. Impact of Solid Waste on Health and The Environment.

ALI, M., WANG, W., CHAUDHRY, N. & GENG, Y. 2017. Hospital waste management in developing countries: A mini review. Waste Management & Research, 35, 581-592.

ARAB, N. 2004. L'activité de projet dans l'aménagement urbain: processus d'élaboration et modes de pilotage Les cas de la ligne B du tramway strasbourgeois et d'Odysseum à Montpellier. Ecole des Ponts ParisTech.

ASCHER, F. 1995. Métapolis: ou l'avenir dês villes, Odile Jacob.

BABU, B. R., PARANDE, A. K. & BASHA, C. A. 2007. Electrical and electronic waste: a global environmental problem. Waste Management & Research, 25, 307-318.

BACOT, H., MCCOY, B. & PLAGMAN-GALVIN, J. 2002. Municipal commercial recycling: Barriers to success. The American Review of Public Administration, 32, 145-165.

CFU 2001. Code du Foncier et de l'Urbanisation (CFU), Complication de textes juridiques législatifs et réglementaires de la république algérienne. Berti Editions.

DESTAIS, G. Les théorisations économiques du développement durable. Proposition de décryptage critique. Le développement durable: débats et controverses, 2011.

DIND , J.-P. & DA CUNHA , A. 2011. La gestion de projets urbains, Projets d'aménagement concertés dans des secteurs déjà bâtis : exemples en Suisse Romande, Mémento à l'usage des responsables de projet. Université de Lausanne Suisse.

GAN, L. & YANG, S. 2017. Legal context of high level radioactive waste disposal in China and its further improvement. Energy & Environment, 28, 484-498.

GUDER, U. 2003. L'amenagement du territoire et la politique regionale en Allemagne. Notre Europe, Octobre.

INEICHEN, J. 2007. Copropolis. Recherche-Action au sein de la communauté Chico Mendes, Recife, Nord-Est du Brésil.

KAOUTHER, L. 2007. Expérimentation des Algorithmes Génétiques Multiobjectifs dans un Processus Décisionnel Multicritère en Aménagement du Territoire. Université d'Oran1-Ahmed Ben Bella.

KAWAI, K. & HUONG, L. T. M. 2017. Key parameters for behaviour related to source separation of household organic waste: A case study in Hanoi, Vietnam. Waste Management & Research, 35, 246-252.

KRZYWOSZYNSKA, A. 2012. 'Waste? You mean by-products!'From bio-waste management to agro-ecology in Italian winemaking and beyond. The Sociological Review, 60, 47-65.

LABORDE, P. 1994. les espaces urbains dans le monde. professeur à l'université Michel-de-Montaigne de Bordeaux-III, éditions NATHAN, 83.

LAOUAR, M. R. 2005. Contribution pour l'aide à l'évaluation de projets de déplacements urbains. Valenciennes.

LAURINI, R. 2014. Information systems for urban planning: a hypermedia cooperative approach, CRC Press.
MASBOUNGI, A. & DE GRAVELAINE, F. 2002. Projets urbains en France/French urban strategies. Editions du Moniteur, Paris.
MATE 2004. Ministère de l'Aménagement du Territoire et de l'Environnement (MATE), Aménagement de l'Algérie 2020, Alger, Algérie.
MERLIN, P. & CHOAY, F. 1988. de l'article/du chapitre Dictionnaire de l'urbanisme et de l'aménagement, distributeur Presses Universitaires de France.
NAVARRO, A. 2003. Approche systémique des déchets, Ed. Techniques Ingénieur.
RAHMOUN, N. 2013. La planification urbaine à travers les PDAU-POS et la problématique de la croissance et de l'interaction villes/villages en Algérie. Référence empirique à la willaya de Tizi-Ouzou. Université de Tizi Ouzou-Mouloud Mammeri.
SABRINA, S. 2006. Comportement des bétons à base de granulats recyclés. Génie civil.
SEYRING, N., DOLLHOFER, M., WEIßENBACHER, J., BAKAS, I. & MCKINNON, D. 2016. Assessment of collection schemes for packaging and other recyclable waste in European Union-28 Member States and capital cities. Waste Management & Research, 34, 947-956.
TAHAR, B. 2017. Les bases de traitement des déchets solides.
TOMAS, F. 1998. Vers une nouvelle culture de l'aménagement des villes. Projet urbain. Ménager les gens, aménager la ville, Wavre: Mardaga, 15-34.
VAILLANCOURT, J. 1998. Evolution conceptuelle et historique du développement durable. RNCREQ (Regroupement National des Conseils Régionaux de l'Environnement du Québec), Rapport de recherche, mai.
VORBURGER, J. 2006. Écologie industrielle & valorisation des déchets. Université Laval.
ZHIJUN, F. & NAILING, Y. 2007. Putting a circular economy into practice in China. Sustainability Science, 2, 95-101.
ZOBEL, T. 2015. ISO 14001 adoption and industrial waste generation: The case of Swedish manufacturing firms. Waste Management & Research, 33, 107-113.

ANTONOPOULOS, A. M. 2017. Mastering Bitcoin: Programming the open blockchain, " O'Reilly Media, Inc.".
ATZORI, M. 2015. Blockchain technology and decentralized governance: Is the state still necessary? Available at SSRN 2709713.
BASHIR, I. 2017. Mastering blockchain, Packt Publishing Ltd.
BELFEDHAL, A. E. 2016. Etude et Implémentation des Fonctions de Hachage Cryptographiques Basées sur les Automates Cellulaires.
BERTONI, G., DAEMEN, J., PEETERS, M. & VAN ASSCHE, G. Keccak. Annual international conference on the theory and applications of cryptographic techniques, 2013. Springer, 313-314.
CASINO, F., DASAKLIS, T. K. & PATSAKIS, C. 2018. A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics and Informatics.
DE FILIPPI, P. & LOVELUCK, B. 2016. The invisible politics of bitcoin: governance crisis of a decentralized infrastructure. Internet Policy Review, 5.
DELAHAYE, J.-P. 2015. Les blockchains, clefs d'un nouveau monde'. Pour Sci, 80-85.
EYAL, I., GENCER, A. E., SIRER, E. G. & VAN RENESSE, R. Bitcoin-ng: A scalable blockchain protocol. 13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16), 2016. 45-59.
FEKKES, L., BATINA, L., PAPACHRISTODOULOU, L. & DE RUITER, J. 2018. Comparing Bitcoin and Ethereum. URl: https://www. cs. ru. nl/bachelorscripties/2018/Lotte_Fekkes___4496426___Comparing_Bitcoin_and_Ethereum. pdf.
GAETANI, E., ANIELLO, L., BALDONI, R., LOMBARDI, F., MARGHERI, A. & SASSONE, V. 2017. Blockchain-based database to ensure data integrity in cloud computing environments.

GERVAIS, A., KARAME, G. O., WÜST, K., GLYKANTZIS, V., RITZDORF, H. & CAPKUN, S. On the security and performance of proof of work blockchains. Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, 2016. ACM, 3-16.
GILBERT, H. & HANDSCHUH, H. Security analysis of SHA-256 and sisters. International workshop on selected areas in cryptography, 2003. Springer, 175-193.
HANNESSE, T., DE HERTAING, A. R. & DE BROQUEVILLE, O. Les banques doivent-elles craindre les blocktechs* et leur technologie blockchain?
KIBET, A. 2018. A Synopsis of Blockchain Technology.
LAMICHHANE, M., SADOV, O. & ZASLAVSKY, A. 2017. A smart waste management system using IoT and blockchain technology.
LELOUP, L. 2017. Blockchain: la révolution de la confiance, Editions Eyrolles.
LOPEZ, J. & DAHAB, R. 2000. An overview of elliptic curve cryptography.
LOTFI, I. 2017. Cryptographie à base de courbes elliptiques.
MUKHOPADHYAY, M. 2018. Ethereum Smart Contract Development: Build blockchain-based decentralized applications using solidity, Packt Publishing Ltd.
NAKAMOTO, S. 2008. Bitcoin: a peer-to-peer electronic cash system (2008).
NARAYANAN, A., BONNEAU, J., FELTEN, E., MILLER, A. & GOLDFEDER, S. 2016. Bitcoin and cryptocurrency technologies. s Princeton University Press.
ØLNES, S. Beyond bitcoin enabling smart government using blockchain technology. International Conference on Electronic Government, 2016. Springer, 253-264.
ØLNES, S., UBACHT, J. & JANSSEN, M. 2017. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. Elsevier.
PRASADH, S. & SIVASUBRAMANIAN, S. 2017. Multiple Securities for Cloud Computing Using RIPEMD-160. Available at SSRN 3078377.
SWAN, M. 2015. Blockchain: Blueprint for a new economy, " O'Reilly Media, Inc.".
VIDAKOVIC, D., PAREZANOVIC, D., NIKOLIC, O. & KALJEVIC, J. 2013. RSA Signature: Behind the Scenes. arXiv preprint arXiv:1304.3309.
WANG, B., CHEN, S., YAO, L., LIU, B., XU, X. & ZHU, L. A simulation approach for studying behavior and quality of blockchain networks. International Conference on Blockchain, 2018. Springer, 18-31.
YUAN, Y. & WANG, F.-Y. Towards blockchain-based intelligent transportation systems. 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), 2016. IEEE, 2663-2668.
ZHENG, Z., XIE, S., DAI, H., CHEN, X. & WANG, H. An overview of blockchain technology: Architecture, consensus, and future trends. 2017 IEEE International Congress on Big Data (BigData Congress), 2017. IEEE, 557-564.

ARUNADEVI 2019. SMART GARBAGE MONITORING SYSTEM USING INTERNET OF THINGS. International Research Journal of Engineering and Technology (IRJET) 06 Issue: 03 | Mar 2019.
BASAIAOCLU, H., CELENK, E., MARIULO, M. A. & USUL, N. 1997. SELECTION OF WASTE DISPOSAL SITES USING GIS 1. JAWRA Journal of the American Water Resources Association, 33, 455-464.
KIETZMANN, J. 2008. Interactive innovation of technology for mobile work. European Journal of Information Systems, 17, 305-320.
NAMEN, A. A., DA COSTA BRASIL, F., ABRUNHOSA, J. J. G., ABRUNHOSA, G. G. S., TARRÉ, R. M. & MARQUES, F. J. G. 2014. RFID technology for hazardous waste management and tracking. Waste Management & Research, 32, 59-66.
OFFENHUBER, D., LEE, D., WOLF, M. I., PHITHAKKITNUKOON, S., BIDERMAN, A. & RATTI, C. 2012. Putting matter in place: Measuring tradeoffs in waste disposal and recycling. Journal of the American Planning Association, 78, 173-196.

RADA, E. C., RAGAZZI, M. & FEDRIZZI, P. 2013. Web-GIS oriented systems viability for municipal solid waste selective collection optimization in developed and transient economies. Waste management, 33, 785-792.

ROVETTA, A., XIUMIN, F., VICENTINI, F., MINGHUA, Z., GIUSTI, A. & QICHANG, H. 2009. Early detection and evaluation of waste through sensorized containers for a collection monitoring application. Waste Management, 29, 2939-2949.

SCHOWENGERDT, R. 2007. Remote sens: models and methods for image processing. Elsevier/Academic Press, Oxford.

SHARMIN, S. & AL-AMIN, S. T. A cloud-based dynamic waste management system for smart cities. Proceedings of the 7th Annual Symposium on Computing for Development, 2016. ACM, 20.

WANT, R. 2006. An introduction to RFID technology. IEEE pervasive computing, 25-33.

XU, Y., HUANG, G. & XU, L. 2014. A fuzzy robust optimization model for waste allocation planning under uncertainty. Environmental engineering science, 31, 556-569.

YEONG, B. C., AHAMED, N. H., MALIM, H. & SINGH, M. M. NFC-based waste management tracking and monitoring system. Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing, 2017. ACM, 86.

ZAMORANO, M., MOLERO, E., GRINDLAY, A., RODRÍGUEZ, M., HURTADO, A. & CALVO, F. 2009. A planning scenario for the application of geographical information systems in municipal waste collection: A case of Churriana de la Vega (Granada, Spain). Resources, Conservation and Recycling, 54, 123-133.

COLLOMP, R., CHALINDAR, P., HOUSSEMAN, S., DELANOE, A., CRIDELICH, C., DANTIN, T.,

BÉRARD, O., MULLER, F., POITRAT, S. & SOCCOJA, G. Traçabilité et Déchets d'activités de soins à risque infectieux (DASRI): Evaluation de l'apport de la technologie RFID. Gestion et Ingénierie des SystèmEs Hospitaliers: GISEH 2010, 2010.

COLLOMP, R., CHALINDAR, P., HOUSSEMAN, S., DELANOE, A., CRIDELICH, C., DANTIN, T.,

BÉRARD, O., MULLER, F., POITRAT, S. & SOCCOJA, G. Traçabilité et Déchets d'activités de soins à risque infectieux (DASRI): Evaluation de l'apport de la technologie RFID. Gestion et Ingénierie des SystèmEs Hospitaliers: GISEH 2010, 2010.

DUCKETT, J. 2011. *HTML & CSS: design and build websites*, Wiley Indianapolis, IN.

FLANAGAN, D. 2006. *JavaScript: the definitive guide*, " O'Reilly Media, Inc.".

KUMAR BHOSALE, K. A., JADHAV DEEPAK, AWANI SANKHE 2019. Blockchain based Secure Data Storage. *International Research Journal of Engineering and Technology (IRJET)* 06**,** 5058.

MUKHOPADHYAY, M. 2018. *Ethereum Smart Contract Development: Build blockchain-based decentralized applications using solidity*, Packt Publishing Ltd.

SOLIDITY. 2019. *Solidity v0.5.9* [Online]. Available: https://solidity.readthedocs.io/en/v0.5.9/.

WOHRER, M. & ZDUN, U. Smart contracts: security patterns in the ethereum ecosystem and solidity. 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE), 2018. IEEE, 2-8.