N° d'ordre : ....

UNIVERSITÉ MOHAMMED SEDDIK BENYAHIA
JIJEL
FACULTÉ DES SCIENCES EXACTES ET INFORMATIQUE

Memoire

Présenté pour l'obtention du diplôme de :

MASTER

En **INFORMATIQUE**

Option : Réseau et Sécurité

Par :

Aissani Okba et Mekideche Djahid

Thème

Vers un Système de Signalement Anonyme des Anomalies dans les Villes Intelligentes : une approche d'incitation basée sur la technologie de Blockchain

Soutenue publiquement, le 16 / 09 / 2021, devant le jury composé de :

Dr.	Khelifi Manel	Grade à institution	Président
Dr.	Alioua Ahmed	Maitre de coférence à l'univ de Jijel	Encadrant
Dr.	Benkiniouar Mouad	Grade à institution	Examinateur

Dédicace Okba

Je dédie ce travail :

À ma très chère mère et mon très cher père que je remercie pour l'éducation et le grand amour dont ils m'ont entouré depuis ma naissance. Et pour leurs patiences et leurs sacrifices.

À mes adorables sœurs.

À mon binôme Djahid.

À tous mes amis.

Dédicace Djahid

Je dédie ce travail :

À ma très chère mère et mon très cher père ALLAH YRAHMO que je remercie pour l'éducation et le grand amour dont ils m'ont entouré depuis ma naissance. Et pour leurs patiences et leurs sacrifices.

À mes adorables sœurs.

À mon binôme Okba.

À tous mes amis.

Remerciements

Tout d'abord nous remercions ***ALLAH****, le tout puissant qui a illuminé notre chemin et qui s'est armé de courage et de patience pour accomplir ce travail.*

Nous remercions notre encadreur ***Dr. Alioua Ahmed****, qui a été très disponible tout au long de la réalisation.*

Nous remercions également toutes les personnes qui ont participé de près ou de loin à la réalisation de ce travail, sans oublier les membres du jury pour avoir accepté de la juger.

Résumé

L'introduction des technologies de l'information et de la communication au cours des dernières décennies à créé une tendance à doter les objets de quotidien d'intelligence, dans le but de rendre la vie humaine plus confortable.

Les villes intelligentes sont souvent vulnérables à des enjeux et à des défis comme les vols, les problèmes routiers, les agressions ainsi que les accidents. En effet les autorités ne peuvent pas contrôler tous et à tout moment. Ainsi, la collaboration intelligente entre les citoyens peut améliorer la vie collective et la gestion de la ville et permet aussi aux autorités d'intervenir à fin de résoudre certains enjeux et défis. Parmi les techniques de collaboration intelligente collective on trouve, les systèmes de signalement.

Dans un système de signalement, il est difficile de faire des signalements fiables sans révéler l'identité des citoyens, et ces citoyens ne sont pas généralement motivés à faire des signalements à cause de la peur et le manque de motivation. Mais aussi par rapport au fonctionnement des systèmes qui sont centralisés et restent inquiétant au niveau de la sécurité et de la fiabilité et ne garantissent pas la non-divulgation des informations privées des signaleurs. Avec l'apparition de la technologie de la Blockchain les systèmes de signalement sont devenus plus performent grâce à l'anonymat, l'immuabilité et la nature décentralisée. Dans ce memoire, nous proposons un nouveau système de signalement anonyme distribué et incitatif basé sur la technologie de la Blockchain, qui garantit la confidentialité de l'identité de l'utilisateur et qui permet de l'encourager à participer activement au processus de signalement.

Notre système est composé d'un protocole de signalement anonyme, avec un mécanisme d'incitation pour motiver les utilisateurs à participer activement et honnêtement au système. Pour cela, nous avons proposé une nouvelle stratégie de points virtuels, appelés jetons. Chaque utilisateur dispose d'un compte de crédit numérique pour stocker ses tokens, et chaque utilisateur participe au consensus de signalement obtient une récompense. Nous avons utilisé la théorie des contrats pour modéliser le problème d'incitation dans la signalisation avec des informations asymétriques. Nous avons aussi développé notre système et implémenté une application mobile pour mettre en oeuvre notre système de signalement et tester le mécanisme d'incitation dans des conditions réelles. Les résultats ont démontrés que notre système avec le mécanisme d'inictation basé sur la théorie des contats permet de garantir l'anonymat des signaleurs, d'augmenter le taux de participation dans le système et de distribuer les récompenses sur les utilisateurs plus équitablement selon le mérite.

Mots-clés : *villes intelligentes, systèmes de signalement, Blockchain, mécanisme d'incitation, théorie des contrats*

Abstract

The introduction of information and communication technologies in the last decades has created a tendency to endow everyday objects with intelligence, in order to make human life more comfortable.

Smart cities are often vulnerable to issues and challenges such as theft, road problems, assaults as well as accidents. Indeed, the authorities cannot control all and at all times. Thus, intelligent collaboration between citizens can improve community life and city management and also allow authorities to intervene in order to solve certain issues and challenges. Among the techniques of collective intelligent collaboration, we find the reporting systems.

In a reporting system, it is difficult to make reliable reports without revealing the identity of citizens, and citizens are generally not motivated to report due to fear and lack of motivation. But also because of the operation of the systems, which are centralized and remain worrying in terms of security and reliability and do not guarantee the non-disclosure of private information of the reporters. With the emergence of blockchain technology, reporting systems have become more efficient due to their anonymity, immutability and decentralized nature. In this paper, we propose a new distributed and incentive-based anonymous reporting system based on Blockchain technology, which guarantees the confidentiality of the user's identity and encourages the user to actively participate in the reporting process.

Our system consists of an anonymous reporting protocol, with an incentive mechanism to motivate users to actively and honestly participate in the system. For this, we proposed a new strategy of virtual points, called tokens. Each user has a digital credit account to store their tokens, and each user participating in the reporting consensus gets a reward. We used contract theory to model the incentive problem in signaling with asymmetric information. We also developed our system and implemented a mobile application to implement our signaling system and test the incentive mechanism in real-world conditions. The results showed that our system with the incentive mechanism based on the theory of contats can guarantee the anonymity of the flaggers, increase the participation rate in the system and distribute the rewards on users more fairly according to merit.

Keywords : *Smart cities, Reporting system, Blockchain, Internet of Vehicles, Incentive mechanism, Contract theory.*

TABLE DES MATIÈRES

TABLE DES FIGURES

LISTE DES TABLEAUX

LISTES DES ACRONYMES

STI	Les systémes de transports intelligents (Intelligent Transportation System)
TIC	Technologies de l'Information et de la Communication)
VANET	Les réseaux ad-hoc véhiculaires (Vehicular Ad-Hoc Network)
IoV	L'internet de véhicule (Internet of Vehicles)
OBU	Les unités embarquées au sein des véhicules (On Board Units)
RSU	L'infrastructure fixe de bord de la route (Road Side Unit)
V2V	Véhicule à véhicule (Vehicle to vehicle)
V2I	Véhicule à infrastructure (Vehicle to infrastructure)
V2X	Vehicle to Everything)
V2R	Véhicule à route (Vehicle to road)
V2P	Véhicule to Pedestrian)
V2S	Véhicule à capteur (Vehicle to sensor)
GPS	Global Positioning System
QoS	La qualité de service (Quality of Service))
WAVE	Wireless Access for Vehicle Environnent
DSRC	Dedicated Short Range Communication)
IoT	L'internet des objets (Internet of Things)
Mac	Medium Access Control
C-V2X	Cellular-Vehicular to Everything
PoW	Proof of Work
PoS	Proof of Stake
DPoS	Delegated Proof of Stake
PoA	Proof of Authority
PoET	Proof of Elapsed Time
TCP	Transmission Control Protocol
IP	Internet Protocol
P2P	peer-to-peer
CPU	Central Processing Unit
IC	Compatibilité incitative
IR	Rationalité individuelle
LDIC	Local Downward Incentive Constraints
LUIC	Local UpWard Incentive Constraints

INTRODUCTION GÉNÉRALE

0.1 Contexte et Motivation

Ces dernières années, nous observons une accélération du développement des nouvelles technologies. En effet, l'accroissement de la population, notamment urbaine et les problématiques environnementales accélèrent les investissements dans la recherche et l'innovation. Ceci a donné naissance à une nouvelle technologie qui est celle de la Smart City, ou ville intelligente en français. Smart city est une ville composés de réseaux interconnectés pour améliorer la qualité des services ainsi que la qualité de vie des citoyens. Les réseaux véhiculaires sont un des composants les plus importants d'une ville intelligente qui permet aux véhicules de communiquer entre eux. Et avec l'émergence des villes intelligentes, et la démocratisation de l'utilisation d'Internet dans les véhicules et l'apparition de nouveau concept de l'Internet des objets, les réseaux de véhicules se transforment petit à petit vers le paradigme de l'Internet des véhicules (internet of Vehicles, IoVs) avec plus de capacités et de meilleures performances.

Avec la propagation des appareils connectés à Internet, les utilisateurs mobiles peuvent demander et recevoir des messages à tout moment et n'importe où ce qui facilite la gestion des villes intelligentes. L'intelligence collective des citoyens construit une veille citoyenne, cette veille permet à chacun de trouver sa place et son rôle dans la vie, ainsi elle permet de développer la conscience du collectif et de l'intérêt général. Cela joue un rôle dans l'amélioration des services de la ville intelligente et aide les autorités à résoudre quelques problèmes, car les autorités ne peuvent pas tout contrôler et à tout moment.

Le signalement est devenu une forme concrète de retour d'information et de la gestion des villes intelligentes, ce qui contribuera à un environnement social plus sûr. Cependant, peu de personnes sont prêtes à réagir ou à signaler les événements qui se déroulent (les accidents, les problèmes de route, etc.) par peur de la vengeance des criminels et le manque de motivations, ces problèmes empêchent les utilisateurs de dénoncer un événement. Malgré l'existence de quelques systèmes de signalement anonyme, qui peuvent protéger la véritable identité du signaleur, mais qui sont des systèmes centralisés et qui possèdent des inquiétudes pour la sécurité et la fiabilité des données des signaleurs, et il n'y a aucune garantie qu'ils ne divulgueront pas les informations privées des signaleurs, ce qui

n'encourage pas les personnesà annoncer des signalements. Mais avec l'apparition de la technologie de la Blockchain, qui est très prométeuse en raison de son anonymat, de son immuabilité et sa nature décentralisée, les nouveaux systèmes de signalement anonymes basés sur cette technologie ont facilité les choses. Chaque personne lance un signal anonyme sans identité et sans aucune information personnelle et ce signalement sera stocké de manière distribuée.

0.2 Objectifs et contributions

Dans ce contexte, nous nous intéressons dans ce travail par présenter un nouveau système de signalement anonyme incitatif basé sur la technologie de la Blockchain dans la ville intelligente. Notre système garantit la confidentialité de l'identité de l'utilisateur et la fiabilité du message de signalement tout au long du processus de signalement. Pour cela :

- Nous avons fait une étude bibliographique sur les principaux travaux sur les systèmes de signalement anonymes existants.
- Nous proposons un mécanisme de signalement anonyme, dans lequel la technologie d'authentification de seuil améliore l'adaptabilité et l'exibilité des communications dans un environnement non-fiable et fournit un niveau plus élevé de confidentialité et de fiabilité pour la communication de signalements anonymes.
- Nous proposons un mécanisme d'incitation pour encourager les utilisateurs à participer activement dans notre système. Pour cela, nous proposons une nouvelle stratégie de jetons virtuals, appelée tokens. Chaque utilisateur possède un compte de crédit numérique pour stocker ses tokens. Au départ, le système distribue un ensemble de tokens à chaque utilisateur mobile qui possède un compte pour qu'il puisse participer en tant que témoin.
- Nous modélisons sur la base de la théorie des contrats les interactions entre un signaleur qui essaye d'offrir des contrats aux témoins pour participer avec lui avec des informations asymétriques, de telle sorte que chaque témoin soit incité à choisir le contrat destiné à son type qui est défini à la base sa réputation.
- Nous développons une application mobile destinée aux citoyens et les usagers de réseaux d'Internet des véhicule, dans laquelle, ils vont se connecter et signaler des éventement de façons anonyme et confortable.

0.3 Organisation du document

En plus de l'introduction et de la conclusion, notre mémoire est structuré en cinq chapitres. Dans ce qui suit nous détaillons le contenu des différents chapitres.

Dans le chapitre 1, nous fournirons une introduction à la ville Intelligente et l'internet des véhicules.

Dans le chapitre 2, nous présenterons la technologie de la Blockchain et ces ceoncepts fondamentaux.

Le chapitre 3 présente les principes fondamentaux des systèmes de signalisation annonymes, un survol bibliographique sur les différents systèmes de signalements basés sur la technologie de la Blockchain sera présenté aussi.

Dans le chapitre 4, nous proposerons et détaillerons notre système de signalement anonyme ainsi que le mécanisme d'incitation, ensuite, nous modéliserons à l'aide de la technique du contrat théorie notre système d'incitation.

Finalement, le chapitre 5 présente l'implémentation de notre conception du système de signalement par une application mobile.

CHAPITRE 1

INTRODUCTION À LA VILLE INTELLIGENTE ET L'INTERNET DES VÉHICULES

1.1 Introduction

L'évolutiondes technologies de l'information et de la communication au cours des dernières décennies à créé une tendance à doter les objets de quotidien de l'intelligence, dans le but de rendre la vie humaine plus confortable. Le paradigme des villes intelligentes est né en réponse à l'objectif de créer la ville du futur, où le bien-être et les droits des citoyens sont garantis, aussi que l'industrie et la planification urbaine sont évaluées d'un point de vue environnementale et durable. En outre, des villes du monde entier mettent en œuvre des caractéristiques des villes intelligentes pour améliorer les services ou la qualité de vie de leurs citoyens [1]. La ville intelligente résout une variété de problèmes liés à plusieurs domaines tels que la santé, la gestion des réseaux d'eau et d'énergie, le transport, etc.

Sur la base du "transport", l'internet des véhicules (internet of Vehicles, IoV) est en passe de devenir un axe de recherche et de dévellopement essentiel sur les systèmes de transport dans les villes intéligentes, fondé sur les réseaux ad-hoc de véhicules. Le but de ses systèmes est de réduire les accidents sur les routes, améliorer la gestion du trafic et l'expérience de voyage.

Dans ce chapitre, nous commencerons par présenter une vue d'ensemble sur les notions de bases de la ville intelligente, avant de survoler les concepts fondamentaux des réseaux de véhicules.

1.2 Ville intelligente

La création d'une ville intelligente est devenue une stratégie nécessaire pour atténuer les problèmes résultants de l'urbanisation rapide et de la croissance de la population urbaine. Malgré les coûts qui leur sont associés, les villes intelligentes, une fois mises en œuvre, peuvent rationaliser la consommation d'énergie, la consommation d'eau, les émissions de carbone, les besoins en transport et les déchets urbains, etc.

1.2.1 Définition

L'expression smart city ou ville intelligente fait désormais partie du vocabulaire courant des nouvelles théories de la vie urbaine. En effet, il n'y a pas de consensus clair sur la définition de ce concept et ils existent plusieurs définitions :

- IBM définit la ville intelligente comme l'utilisation des technologies de l'information et de la communication pour détecter, analyser et intégrer les informations clés des systèmes centraux des villes. En même temps, la ville intelligente peut apporter une réponse intelligente à différents types de besoins, y compris les moyens de subsistance quotidiens, la protection de l'environnement, la sécurité publique et les services municipaux, les activités industrielles et commerciales, les transports, etc. [2]

- La ville intelligente est l'approche réelle de la planète intelligente appliquée à une région spécifique, permettant une gestion informelle et intégrée des villes. On peut également dire qu'il s'agit d'une intégration efficace des idées de planification intelligente, des modes de construction intelligente, des méthodes de gestion intelligente et des approches de développement intelligent pour les villes [3].

- Une ville intelligente est une ville qui a intégré à grande échelle des technologies de l'information et des communications en vue d'améliorer l'efficacité de ses services, sa qualité de vie et de favoriser un changement de comportement chez les citadins, les gouvernants et les entreprises pour pouvoir croître d'une manière plus durable [4].

- La ville intelligente est une ville de réseaux interconnectés qui sont gérés à distance par un logiciel de gestion centralisé. L'ensemble des infrastructures et des services de la ville, contrôlés par ces capteurs, doivent être connectés à un réseau de télécommunications afin d'être pilotés à distance et optimisés à l'aide d'outils numériques.

1.2.2 Composant

Comme il est illustré à la figure 1.1, Une ville intelligente se compose des éléments fondamentaux suivant [5, 6] :

1) **La gouvernance intelligente :** grâce aux outils technologiques, la gouvernance à l'ère numérique est plus inclusive, connectée et ouverte. En d'autres termes, les nouveaux systèmes d'information et de communication servent d'intermédiaire entre les décideurs, les acteurs civiques et les citoyens. Pensons notamment à des tableaux électroniques dans des lieux publics qui peuvent afficher de l'information à l'intention des citoyens ou encore à une diffusion web simultanée des rencontres du conseil pour permettre à un plus grand nombre de personnes d'y assister.

2) **Le citoyen intelligent :** la ville doit être construite en fonction des préoccupations des habitants. La ville intelligente cherche à construire ses prestations autour des besoins de ses habitants qui ne sont plus considérés comme des consommateurs des

services, mais comme des partenaires et des parties prenantes de son développement. Un citoyen intelligent est celui qui utilisera les nouveaux outils technologiques, notamment pour participer aux débats publics et à la vie de ville.

3) **L'habitat intelligent :** la valeur élevée de l'immobilier dans les centres-villes combinée à la disponibilité limitée des terres rendent l'urbanisation complexe. Il faut réinventer des formes urbaines qui, à la fois, respectent une intimité indispensable, assurent un ensoleillement suffisant, permettent des évolutions et favorisent le "vivre-ensemble". Cette dernière notion consiste à améliorer la qualité de vie en termes de services, améliorer l'attractivité des touristes et promouvoir la cohésion sociale ainsi que la sécurité. La vie intelligente comprend les installations culturelles, la cyber-santé, les services et les outils de sécurité publique, tels que les systèmes de surveillance et réseaux de services inter-urgences.

4) **L'économie intelligente :** elle représente un pilier économique dont on se sert comme vecteur pour l'innovation et la création d'emplois durables pour la ville. Une économie intelligente est basée sur un esprit d'innovation et d'entreprenariat, sur la productivité et la flexibilité du marché. Elle possède aussi une aptitude à se transformer et à enchâsser le marché international.

5) **La mobilité intelligente :** la planification urbaine est la meilleure façon d'atteindre la mobilité intelligente. La planification urbaine met l'accent sur des modes de transports individuels et collectifs par l'utilisation extensive des Technologies de l'Information et de la Communication (TIC). L'un des défis consiste à intégrer différents modes de transport rail, automobile, cycle et marche à pied en un seul système qui est à la fois efficace, facilement accessible, abordable, sûr et écologique. Cette intégration permet une empreinte environnementale réduite, optimise l'utilisation de l'espace urbain et offre aux citadins une gamme variée de solutions de mobilité répondant à l'ensemble de leurs besoins.

6) **L'environnement intelligent :** dans une ville intelligente, les divers outils technologiques permettent notamment une protection et une préservation de nos ressources naturelles, comme par exemple, des capteurs pour détecter les fuites dans des réseaux, pour suivre le transport des matières résiduelles ou pour mesurer le niveau de pollution de l'air.

1.2.3 Domain d'application

Une ville intelligente comprend différents domaines d'application, parmi ces domaines les plus importants il y'a ceux résumés dans les points suivants [1] :

- **L'agriculture :** les villes et leur population augmentent à un rythme incontrôlable, ce qui a pour conséquence la réduction des terres utilisées pour l'agriculture. Les

FIGURE 1.1 – Les composants d'une ville intelligent [7].

villes ont fait face à ce problème potentiel avec différentes approches. Dans [8], les auteurs proposent l'agriculture Intelligente Climatique (CSA) comme un moyen de soutenir et de transformer les systèmes agricoles pour assurer la sécurité alimentaire tout en prenant en compte la problématique du changement climatique.

– **Les transactions commerciales :** l'une des principales caractéristiques des villes intelligentes est leur capacité à simplifier et à automatiser les processus pour les entreprises et le commerce local. Perera et al [9]. Ont étudié le concept de détection en tant que modèle de service. Dans ce dernier, les transactions sont d'une importance majeure, car elles enregistrent les communications entre les dispositifs, les entreprises étant l'une des parties prenantes impliquées.

– **La santé :** les villes intelligentes peuvent développer la capacité d'utiliser des technologies telles que le Big Data pour élaborer des prédictions ou identifier les points chauds de la santé de la population. La gestion intelligente des soins de santé convertit les données relatives à la santé en informations cliniques et commerciales, qui comprennent les dossiers médicaux numériques, les services de santé à domicile et les systèmes de diagnostic, de traitement et de suivi des patients à distance.

– **Le réseau intelligent :** dans plusieurs pays, l'infrastructure actuelle du réseau est encore unidirectionnelle. Cela entraîne une grande perte d'énergie en raison de la déperdition dans la distribution et du problème de rétention de l'énergie. Par conséquent, le développement du réseau intelligent apportera plusieurs avantages aux villes intelligents, il améliorait la sécurité des réseaux électriques en équilibrant l'offre et la demande, ils évitent le suréquipement des moyens de production et permettent une utilisation plus adaptée des moyens de stockage de l'électricité. Aussi, ils réduisent les pics de consommation d'énergie, ce qui atténue les risques de panne

généralisée.

- **Le transport :** le système de mobilité et de transport urbain est le service le plus développé dans les villes intelligentes. Ces villes ont mis en place un STI sophistiqué pour assurer la sécurité routière et améliorer la fluidité du trafic en utilisant des véhicules intelligents qui peuvent communiquer avec d'autres véhicules sur la route.

Les réseaux de véhicles sont considérés comme l'une des technologies les plus développées et les plus utilisées de la ville intelligente. Dans ce qui suit, nous détaillons le concept de base de cette technologie.

1.3 Réseau ad-hoc de véhicules (VANET)

Dans le monde des réseaux sans fil, les réseaux de véhicules (Vehicular Ad-hoc Networks) sont devenues l'un des domaines d'application concrète de la ville inteligente. Dans cette section, nous allons présenter les principes fondamentaux des réseaux de véhicules.

1.3.1 Définition

Les réseaux ad-hoc de véhicules, communément appellé VANETs pour Vehicular Ad-hoc Networks en anglais, est une nouvelle technologie émergente des réseaux Ad-hoc mobiles (MANETs), où les nœuds mobiles sont les véhicules intelligents, équipés de matériels à très hautes technologies (des calculateurs, des radars, des systèmes de Géo-localisation GPS, etc.). Les véhicules peuvent communiquer entre eux (pour échanger les informations sur le trafic par exemple), ou avec des stations de base placées tout au long des routes (pour demander des informations par exemple). Ces réseaux sont considérés comme la composante majeure des futurs systèmes de transport intelligents, dont le but principal est d'améliorer la sécurité sur les routes, le confort des voyageurs et l'efficacité de la gestion du trafic routier [10, 11].

1.3.2 Composants

Les réseaux de véhicules comprennent les composantes communicantes suivantes :

- **Les véhicules intelligents :** ils sont des véhicules équipés de terminaux tels que les calculateurs, les interfaces réseaux ainsi que des capteurs capables de collecter les informations et de les traiter. Les véhicules intelligents sont équipés d'une variété de technologies de communication sans fil. Toutes ces unités permettent aux véhicules d'effectuer des calculs, de localiser leur emplacement, de collecter et d'enregistrer des données sur leur environnement, et de communiquer avec d'autres véhicules ou équipements routiers [12].

- **RSU (Road Side Unit) :** ils sont des équipements externes aux véhicules installés au bord des routes, ils peuvent également jouer le rôle de stations de base, voir la

figure 1.2. Ils sont situés à des endroits spécifiques comme les carrefours ou près des places de parking. Leurs principales fonctions sont d'augmenter la zone de communication du réseau ad-hoc en réaffectant les informations à d'autres et d'exécuter des applications de sécurité comme l'alerte d'accident, etc. [11, 13]

- **OBU (On-Board Units) :** ils sont des unités embarquées dans les véhicules intelligents qui comprennent un ensemble de composants matériels et logiciels de haute technologie (le GPS, le radar, les caméras, les capteurs, l'unité de calcul, etc.), voir la figure 1.2. Leurs rôles consistent à assurer la localisation, la réception, le calcul, le stockage et l'envoie des données sur l'interface de réseau. ils sont les émetteurs-récepteurs qui permettent au véhicule de rester connecté au réseau [10].

- **L'équipement personnel :** les équipements personnels sont les équipements qui peuvent être emportés par les utilisateurs à l'intérieur du véhicule. Cela peut être un téléphone portable, un ordinateur portable ou encore un GPS autonome [14].

1.3.3 Architecture et mode de communication

L'objectif d'une architecture VANET est de permettre la communication entre les véhicules les uns avec les autres et aussi avec les véhicules et les équipements fixes au bord des routes menant aux trois possibilités suivantes (voir la figure 1.2) [10, 15] :

- **La communication de véhicule à véhicule (véhicule to Véhicule, V2V) :** ce mode de communication est un mode distribué, fonctionne à l'aide des OBUs. La communication entre deux véhicules se fait directement (les uns avec les autres) ou en mode multi-sauts en passant par des véhicules intermédiaires.

- **La communication véhicule à infrastructure (Vehicle to Infrastructure, V2I) :** dans ce mode de communication, les véhicules utilisent les RSUs qui représentent l'infrastructure fixe de la route pour communiquer en mode centralisé. Ce mode de communication assure une connectivité relativement forte par rapport à la communication en mode V2V.

- **La communication hybride (Vehicle to Everything, V2X) :** la combinaison des deux types cités ci-dessus (V2V et V2I) aboutit à un modèle hybride. Dans ce cas, les véhicules communiquent entre eux pour échanger des informations de trafic et avec l'infrastructure fixe au bord de la route pour demander des données spécifiques.

1.3.4 Caractéristiques et défis

Les VANETs sont des réseaux auto-organisés et distribués dans lesquels les véhicules se déplacent à des vitesses variables le long de chemins (i.e., routes) prédéterminés. Ces

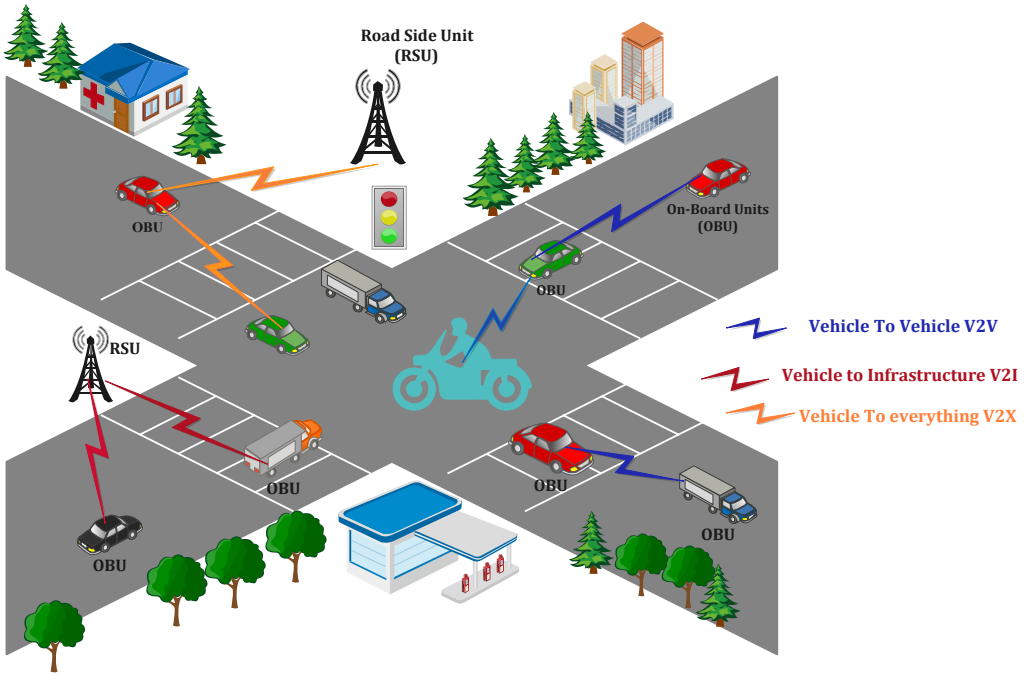


FIGURE 1.2 – Un exemple illustratif de l'architecture, composants et mode de communication des réseaux de vehicules.

réseaux présentent diverses caractéristiques, dont les suivantes [16, 17] :

- La forte mobilité et la topologie hautement dynamique du réseau.
- La grande capacité de traitement, d'énergie et de communication.
- La diversité de la densité avec une à variation spatio-temporelle.
- Une diversité des technologies de communications sans fil.
- Des exigences strictes en terme de délai de réponse (latence).

Les caractéristiques spécifiques des réseaux de véhicules génèrent plusieurs défis, parmi les plus importants, nous citons les suivants [18] :

- La dégradation de la qualité de service afece au grand nombre de véhicule et leur grande mobilité.
- Les risques de sécurité.

- Le problème accès au canal sans fil.

- Le problème de routage face à la connectivité intermittente et le partitionnement du réseau.

- Le problème de normalisation face à la grande diversité des tehcnologies de communications et aussi les fabricants.

1.3.5 Application

Les applications des réseaux VANETs peuvent être classifiées en trois grandes catégories [19, 20] :

- **Les applications de la sécurité routière :** les applications de cette catégorie visent à améliorer la sécurité routière et à réduire le nombre des accidents sur la route.

- **Les applications de la gestion du trafic :** les applications de cette catégorie visent à améliorer le trafic routier afin de réduire les embouteillages, contourner les obstacles, etc.

- **Les applications de confort :** cette catégorie définit l'ensemble des types d'applications visant à améliorer le confort du conducteur et à lui fournir les diverses ressources et connaissances nécessaires pour améliorer l'expérience de son voyage.

1.3.6 Technologie de communication

Les principales technologies de communication sans fil utilisées dans les VANETs sont :

- **DSRC (Dedicated Short Range Communications) :** c'est le premier standard défini pour les communications sans fil dans les STIs. Il représente un ensemble de protocoles et de normes définissant la communication à courte portée. Cette technologie a évolué à partir de la norme IEEE 802.11 a vers la norme IEEE 802.11 p afin de répondre aux caractéristiques des VANETs. [21].

- **WAVE (Wireless Access in Vehicular Environment) :** le groupe de travail IEEE a défini un standard dédié aux communications inter-véhicules, appelé WAVE. Cette norme utilise le concept de multicanaux afin d'assurer les communications pour les applications de sécurité et les autres services du STI. IEEE a défini le standard 1609.x comme une famille de protocole permettant l'accès au support sans fil dans les VANETs [22].

– **Cellular-Vehicular to Everything (C-V2X) :** il a été proposé par 3GPP (The 3rd Generation Partnership Project) come alternative de 802.11 p. Il utilise les réseaux cellulaires 4G LTE ou 5G pour les communications inter-véhicules. C-V2X est également conçu pour connecter directement les véhicules entre eux, ainsi qu'aux infrastructures et aux autres usagers de la route, même dans les zones où il n'y a pas de couverture de réseau cellulaire [14].

1.4 Réseau d'Internet de véhicules (Internet of Véhicules)

Le développement rapide des technologies de communication sans fil, l'expansion de l'utilisation de l'internet mobile dans les véhicules et l'introduction du véhicule intelligent ont contribué à l'émergence rapide d'une nouvelle génération de réseaux de véhicules dotés de capacités commerciales et de technologies avancées, connus sous le nom d'Internet des véhicules (Internet of Véhicules, IoV). Dans cette section, nous allons présenter les principes fondamentaux des réseaux d'Internet de véhicules.

1.4.1 Définition

L'IoV est un système de réseau ouvert qui intègre les réseaux VANETs, Internet of Things, et le Cloud computing mobile. Composé de multiples utilisateurs, de multiples véhicules, de multiples objets et de multiples réseaux. Les véhicules sont considérés comme des objets connectés ayant accès à l'internet via des réseaux sans fil qui permettent aux véhicules intelligents de collaborer entre eux ainsi qu'avec d'autres objets connectés pour la collecte et la communication de données. L'objectif idéal de l'IoV est de réaliser enfin une intégration approfondie de l'homme, du véhicule et de l'environnement, de réduire les coûts sociaux, de promouvoir l'efficacité des transports, d'améliorer le niveau de service des villes, etc [23].

1.4.2 Composant

En plus des éléments traditionnels des VANETs qu'on a détaillé dans la section précédente, autrement dit, les véhicules intelligents, OBU, les RSUs et les périphériques personnels. Les principaux éléments constitutifs de l'IoV en termes d'éléments de réseau expriment plus efficacement la signification et les fonctionnalités de l'IoV en tant qu'en semble complet de services. Ces éléments sont les suivants (voir la figure 1.3) [24] :

– **Cloud computing :** il représente le cerveau de l'IoV avec de très puissantes capacités de stockage et de traitement déployés sur des serveurs distants. Car les nœuds de l'IoV génèrent une quantité importante de données, qui ne peuvent être gérées que par des plateformes de grande capacité de calcul et de stockage similaires à celles proposée par la technologie du Cloud computing.

– **La connexion :** ils s'agissent de différents types de réseaux de communications (WiFi, DSRC, 4G 5G, etc.) qui fournirent de le support de connexion utilisée pour

établir et maintenir la communication entre le Cloud et les véhicules ainsi que les différents objets qui les entourent.

– **Les clients :** les services des serveurs intelligents déployés sur le Cloud sont utilisés par les applications clients des véhicules à l'aide de divers réseaux de communication. Chaque application client a des exigences de service qui peuvent être différentes de celles des autres clients.

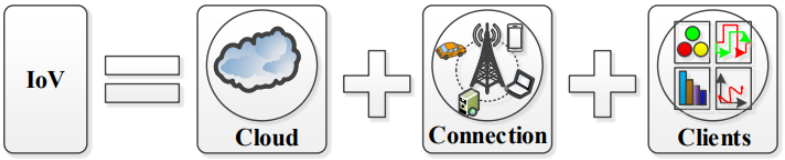


FIGURE 1.3 – Les trois éléments de base des réseaux de l'IoV [24].

1.4.3 Mode de communication

La communication dans l'IoV est le cœur du système IoV permet à tous les véhicules connectés de partager leurs données et reçoivent à leur tour des services du nuage Internet. Comme les différents appareils et les véhicules sont fabriqués par des fabricants différents, il est un peu complexe d'intégrer toutes les technologies de communication dans un seul réseau. L'IoV comprend les types suivants de communication entre ses nœuds connectés (voir la figure 1.4) [24].

– **Véhicule à véhicule (V2V) :** ce type permet au véhicule de communiquer directement avec une autre pour échanger des informations et des alertes de conduite dans un rayon donné.

– **Véhicule à Infrastructure (V2I) :** ce type permet au véhicule de communiquer avec les stations de base, les équipements de la route, etc.

– **Véhicule à route (véhicule to Road, V2R) :** ce type permet au véhicule de communiquer avec les infrastructures routières équipées de technologies de communication sans fil, telles que les feux de signalisation ou les panneaux d'avertissement pour les travaux routiers, etc.

– **Véhicule à piéton (véhicule to Pedestrian, V2P) :** ce type permet au véhicule de communiquer avec les dispositifs intelligents portés par les passagers, tels que les téléphones mobiles, les montres intelligentes, les ordinateurs de poche, etc.

– **Véhicule à capteurs (véhicule-to-Sensors, V2S) :** ce type permet au véhicule de communiquer avec les différents capteurs installés sur l'entourage de véhicule.

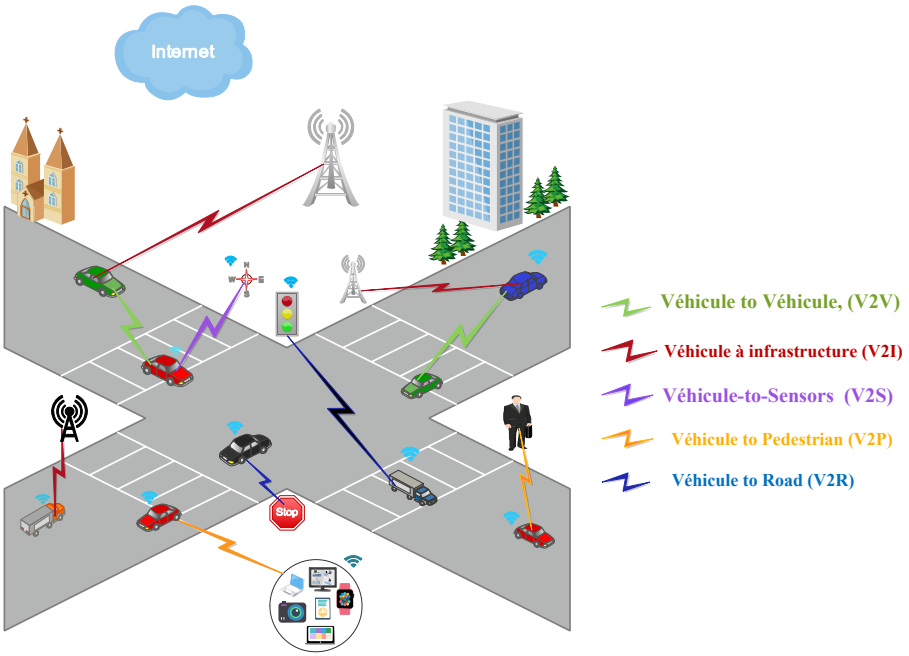


FIGURE 1.4 – le mode de communication dans un réseau d'Internet de véhicules.

1.4.4 Caractéristiques et défis

L'IoV est un réseau connecté de véhicules basé sur le système d'information des véhicules. Il a de nombreuses caractéristiques parmi eux [25, 26] :

- La forte mobilité.
- L'hétérogénéité des technologies et les équipements de communication.
- La forte évolutivité et la forte évolution du nombre de véhicules.

Ils existent de nombreux défis à relever dans l'IoV. Parmi ces défis, nous citons :

- **Big data :** un défi majeur est le traitement et le stockage des big data créés dans l'IoV en raison du grand nombre de véhicules connectés [22].
- **Les contraintes de délai :** les applications IoV requièrent des contraintes en termes de délai de réponse (la latence) très strictes, où il ne doit y avoir aucun ou un délai de service très faible [26].
- **La tolérance aux pannes :** les services de transport ont besoin d'une communication très fiable, capable de fournir une communication en temps même si certains des nœuds fonctionnent mal [26].

– **La sécurité et vie la privée :** le maintien d'un équilibre raisonnable entre la sécurité et la confidentialité est l'un des principaux défis de l'IoV. La réception d'informations fiables de la part de leur source est importante pour le récepteur. Cependant, ces informations fiables peuvent violer les besoins de confidentialité de l'expéditeur [22].

– La forte mobilité des véhicules et le changement rapide de la topologie du réseau qui affecte la disponibilité, la fiabilité et la robustesse des communications entre les objets communicants de l'IoV [27].

1.5 Conclusion

Dans la première partie de ce chapitre, nous avons abordé les villes intelligentes, notamment leur définition, leurs composants et quelques domaines d'application. Par la suite dans la deuxième partie, nous avons présenté les principes fondamentaux des réseaux de véhicules. Nous avons donc passé en revue leur architecture et leur style de communication, ainsi que leurs diverses caractéristiques et défis, les types d'application et quelque technologie de communication existante. Plus loin dans la dernière section, nous avons exposé la nouvelle technologie des réseaux d'Internet de véhicules. Nous avons également décrit ces composants, leur mode de communications et leurs principales caractéristiques et défis.

Dans le prochain chapitre, nous présentons la nouvelle technologie de la Blockchain.

CHAPITRE 2

TECHNOLOGIE DE LA BLOCKCHAIN

2.1 Introduction

Les transactions entre personnes ou entreprises, qu'elles soient financières ou autres, sont souvent centralisées et contrôlées par un tiers fiable et de bonne réputation. Par exemple, pour effectuer un paiement numérique ou un transfert d'argent, une banque ou un fournisseur de carte de crédit doit agir en tant qu'intermédiaire pour s'assurer que la transaction est menée à bien. En outre, une transaction entraîne des frais auprès d'une banque ou d'une société de cartes de crédit. La même méthode peut être appliquée à de nombreux autres domaines, notamment les jeux, la musique, les logiciels, etc. Dans la plupart des cas, le système de transaction est centralisé, et toutes les données et informations sont contrôlées et gérées par un tiers, plutôt que par les deux parties principales impliquées dans la transaction [28]. La technologie Blockchain (la chaîne de blocs) a été créée pour résoudre ce problème.

La Blockchain une approche novatrice du problème humain persistant de la confiance, qui modifie fondamentalement la manière dont les transactions en ligne peuvent être effectuées en garantissant la confiance de parties inconnues [29]. Elle utilise la cryptographie pour protéger l'identité des utilisateurs, garantir que les transactions sont effectuées en toute sécurité, sécuriser les informations et le stockage des valeurs.

L'objectif de ce chapitre est de présenter les concepts généraux de la technologie Blockchain. Nous commencerons par présenter quelques notions fondamentales sur la Blockchain, telles que son histoire, sa définition et ses caractéristiques. Nous aborderons ensuite les composants, l'architecture et le fonctionnement de cette technologie, ainsi que ses types, ses applications, ses protocoles de consensus, et nous nous terminons par ses avantages et ses défis.

2.2 Généralités sur la Blockchain

2.2.1 Historique

La technologie de la Blockchain est apparue pour la première fois lors de l'introduction de la cryptomonnaie bitcoin en 2008, où un individu (ou un groupe) écrivant sous le nom de Satoshi Nakamoto a publié un article intitulé "Bitcoin : A Peer-To-Peer Eléctronic Cash System" [30], est aujourd'hui connu sous le nom de livre blanc de Nakamoto.

Ce document décrivait les technologies de soutien aux transferts de monnaie numérique ou d'argent électronique, notamment la possibilité d'envoyer des paiements en ligne directement d'une partie à une autre sans aucun établissement financier tierce [31].

Le point fort de cette cryptomonnaie, c'est qu'il est possible de créer une monnaie contrôlée collectivement sur un réseau paire à paire sans qu'aucune autorité n'ait la capacité d'intervenir, y compris la capacité d'émettre de nouveaux bitcoins, grâce à un arrangement minutieux de protocoles cryptographiques.

Le protocole de Nakamoto a été rendu possible grâce aux fonctions de hachage cryptographiques (qui garantissent l'intégrité d'un grand fichier de comptes), aux protocoles de signature à double clé (qui garantissent que seul le titulaire du compte l'utilise), et au concept de preuve de travail (qui organise un système d'incitation pour que de nombreux utilisateurs participent à la gestion et à la surveillance du système).

La technologie de la Blockchain est à la base de la grande majorité des cryptomonnaies (Bitcoin, Ethereum, etc.). Cependant, l'évolution de cette technologie ne se limite pas aux cryptomonnaies ; elle a trouvé son succès dans divers domaines tel que la finance, l'assurance, la santé et l'Internet des objets, etc.

2.2.2 Définition

La Blockchain regroupe en fait deux choses différentes : une technologie et un système qui utilise cette technologie. On trouve à l'heure actuelle plusieurs définitions pour la Blockchain, parmi ces définitions on cite les suivantes :

Un grand livre numérique inviolable et mis en œuvre de manière distribuée (c'est-à-dire sans dépôt central) et généralement sans autorité centrale (c'est-à-dire une banque, une entreprise ou un gouvernement). À leur niveau de base, elles permettent à une communauté d'utilisateurs d'enregistrer des transactions dans un grand livre partagé au sein de cette communauté, de telle sorte que dans le cadre du fonctionnement normal du réseau Blockchain, aucune transaction ne peut être modifiée une fois publiée [32].

Une Blockchain, ou chaîne des blocs est une technologie de stockage et de transmission d'informations sans organe de contrôle central. Techniquement, il s'agit d'une base de données distribuée dont les informations envoyées par les utilisateurs et les liens internes à la base sont vérifiés et groupés à intervalles de temps réguliers en blocs, l'ensemble étant

sécurisé par cryptographie, et formant ainsi une chaîne [33].

La Blockchain est un registre numérique incorruptible des transactions économiques qui peut être programmé pour enregistrer non seulement les transactions financières, mais aussi pratiquement tout ce qui a de la valeur [34].

En se basant sur les définitions précédentes, nous pouvons définir la Blockchain comme un grand registre distribué, décentralisé (aucune autorité centrale) et public. Permet de créer la confiance entre des individus sans faire appel à des intermédiaires, composé de nombreux nœuds. Chaque nœud conserve sa propre copie du grand registre. Ce registre contient des enregistrements de données qui sont sauvegardées dans des blocs (groupe de transactions) sous forme d'une chaîne (voir la figure 2.1). Son fonctionnement est basé sur les algorithmes de consensus qui vérifient les transactions avant de les valider et de les ajoutés à un bloc de la chaîne.

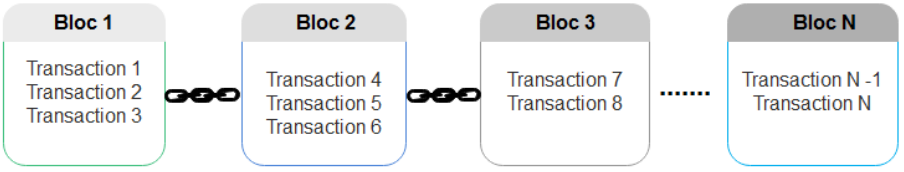


FIGURE 2.1 – Exemple simplifié d'une Blockchain.

2.2.3 Caractéristiques

La technologie de la Blockchain se caractérise principalement par les éléments suivants [35] :

— **La décentralisation :** la Blockchain permet de valider les transactions entre deux parties sans avoir besoin d'aucune autorité centrale ne supervise ou ne gère la Blockchain, mais les nœuds du réseau ont accès à toutes les transactions et peuvent les vérifier puisque chaque nœud possède une copie du grand livre public.

— **La transparence :** tout le monde peut voir les transactions et les échanges actuels et précédents, ce qui nous permet de vérifier la validité de la chaîne. Les données de la chaîne de blocs sont largement ouvertes à tout utilisateur qui peut accéder aux transactions de la chaîne et les vérifier.

— **La traçabilité :** chaque transaction enregistrée dans la Blockchain est assortie d'un horodatage. Par conséquent, les utilisateurs peuvent facilement vérifier et retracer les origines des éléments de données historiques.

— **L'immuabilité :** les enregistrements de la Blockchain sont dits immuables, car une fois stockés, ils sont archivés de manière permanente et ne peuvent pas être facilement modifiés.

— **L'anonymat :** lors de transfert des données entre nœuds, l'identité de l'individu reste anonyme, ce qui rend le système plus sécurisé.

— **La sécurité :** les données de la Blockchain ne sont pas stockées sur un seul serveur, mais plutôt par un groupe d'utilisateurs, ce qui rend impossible la suppression de toutes les copies des documents.

2.3 Composants, architecture et mode de fonctionnement de la Blockchain

2.3.1 Composants

La technologie de la Blockchain peut sembler complexe, mais il est possible de la simplifier en examinant chaque composant individuellement. Cette sous-section détaille chaque composant de la Blockchain [32, 36].

— **Les blocs :** les blocs sont des structures de données ayant pour but de regrouper un ensemble de transactions et d'être distribués à tous les nœuds du réseau. Chaque bloc contient (voir la figure 2.2) :
  — Un en-tête (block Header) composé de :
    — Index : la position du bloc dans la chaîne.
    — Hash : un hash SHA256 généré à partir des données contenues dans le bloc.
    — PreviousHash : le hash du bloc précédent.
    — Timestamp : le temps et la date de la création du bloc.
  — Corps du bloc (block Body) qui contient :
    — Une liste des transactions.
    — D'autres types de données peuvent être présents.

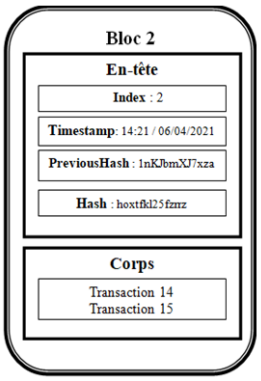


FIGURE 2.2 – la structure générale d'un bloc.

— **Fonctions de hachage cryptographiques(Cryptographic Hash Functions) :** l'utilisation de fonctions de hachage cryptographiques est un aspect essentiel de la

technologie Blockchain. Le hachage est une méthode qui consiste à appliquer une fonction de hachage cryptographique à des données qui calcule un résultat relativement unique pour une entrée de n'importe quelle taille (par exemple, un fichier ou un texte). Il permet à des individus de prendre indépendamment des données d'entrée, de les hacher et d'obtenir le même résultat, ce qui prouve que les données n'ont pas été modifiées.

— **Le compte ou porte-monnaie (Wallet) :** avec certains réseaux Blockchain, les utilisateurs doivent gérer et stocker de manière sécurisée leurs propres clés privées. Au lieu de les enregistrer manuellement, ils utilisent souvent un logiciel pour les stocker de manière sécurisée. Ce logiciel est souvent appelé portefeuille ou wallet. Il peut stocker des clés privées, des clés publiques et des adresses associées.

— **Les mineurs :** certains nœuds du réseau consacrent des ressources à la vérification des transactions et au maintien de la sécurité de la Blockchain. Ils sont appelés mineurs. Les mineurs sont payés par des récompenses de bloc. Pour chaque nouveau bloc, une récompense de bloc est attribuée à un seul mineur ou à un petit groupe de mineurs.

— **Le minage (Mining) :** afin de valider une transaction et de l'ajouter à la Blockchain, les ordinateurs du réseau doivent rivaliser pour résoudre un « puzzle » lié au bloc suivant, avant d'être ajouté à la Blockchain. Ce processus de résolution de l'énigme est connu sous le nom de minage ou mining. Le minage est donc le processus par lequel les transactions sont vérifiées par les mineurs et ajoutées au grand livre public.

— **Les transactions :** une transaction représente une interaction entre des parties. Avec les crypto-monnaies, par exemple, une transaction représente un transfert de la crypto-monnaie entre les utilisateurs du réseau Blockchain. Chaque demande de transaction dans la Blockchain doit être signer par l'émetteur pour être validé. Pour le signée elle va avoir besoin de généré à l'aide de son Wallet, une paire de clé de chiffrement, une clé privée qui ne doit être communiquer à personne et une clé public qui peut être communiquer à tout le monde.
Les transactions sont constituées d'une liste d'entrées qui contient une référence au résultat d'une transaction précédente et une signature qui vérifie l'authenticité de la transaction, ainsi que d'une liste de sorties qui contient l'adresse du destinataire et la donnée qu'il va envoyer.

— **Le consensus :** il signifie que tous les nœuds du réseau doivent se mettre d'accord sur une version identique de la Blockchain. Les mécanismes de consensus sont des protocoles garantissant que tous les nœuds conviennent des transactions légitimes à ajouter à la chaîne avant qu'un nouveau bloc ne soit ajouté. L'objectif est que chacun des participants au réseau convienne que le bloc a été assemblé et ajouté conformément aux règles du réseau.

— **Grands livres (Ledgers) :** un grand livre ou Ledger est un recueil de transactions distribué. Chaque nœud de réseau possède une copie de Ledger. À l'époque moderne, les grands livres sont stockés sous forme numérique, souvent dans de grandes bases de données détenues et gérées par un tiers de confiance centralisé pour le compte d'une communauté d'utilisateurs.

— **Les contrats intelligents (smarts contracts) :** sont des programmes informatiques irrévocables, le plus souvent déployés sur une Blockchain, qui exécutent un ensemble d'instructions pré-définies. Le smart contract propose en quelque sorte un équivalent informatique du contrat papier. Durant l'exécution du smart contract, toutes les étapes de validation sont enregistrées dans la Blockchain utilisée, ce procédé permet de sécuriser l'ensemble des données en empêchant leur modification.

— **Chaîne des blocs (Chaining Blocks) :** les blocs sont liés les uns aux autres, chacun contenant le hachage de l'en-tête du bloc précédent (voir la figure 2.3), formant ainsi la Blockchain. Si un bloc publié précédemment a été modifié, le résultat sera différent. Par conséquent, puisqu'ils utilisent le hachage du bloc précédent, tous les blocs suivants auraient des hachages différents.

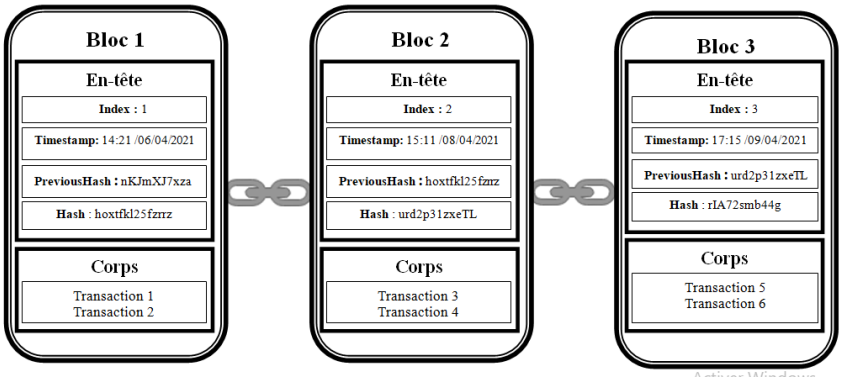


FIGURE 2.3 – la chaîne de blocs générique.

2.3.2 Architecture

La Blockchain relie la valeur de la même manière qu'Internet relie les informations. Comme la suite de protocoles Internet (TCP IP), la technologie de Blockchain peut être divisée en quatre couches : la couche de données, la couche de réseau, la couche de consensus et la couche d'application. L'architecture est présentée à la figure 2.4. Dans cette architecture, chaque couche joue son propre rôle [37].

— **La couche de données :** cette couche organise et stocke les données. Elle contient les blocs de données sous-jacents, les horodatages, etc. Elle stocke aussi toutes les données de transaction et les enregistrements d'informations sous forme de Blocs. Les différentes Blockchains adoptent des stratégies différentes pour organiser et stocker les données. Par exemple, la Blockchain adopte l'arbre de Merkle pour organiser

et stocker les informations sur les transactions.

— **La couche réseau :** la Blockchain est maintenue et gérée de manière autonome par un réseau P2P (Pair à Pair) composé de mineurs et d'utilisateurs. Dans un réseau P2P, il n'y a pas de centre et chaque nœud peut entrer ou sortir du réseau à tout moment.

— **La couche de consensus :** le consensus est essentiel dans la Blockchain, puisqu'elle est gérée par un réseau P2P, dans lequel chaque nœud détient son propre point de vue. L'obtention d'un consensus est une tâche non-triviale, et de nombreux algorithmes ont été proposés pour atteindre cet objectif, PoW, PoS, etc.

— **La couche d'application :** cette couche permet le développement d'applications décentralisées fonctionnant au-delà de l'algorithme de consensus. Les contrats intelligents et d'autres techniques sont utilisés pour rendre la Blockchain plus fonctionnelle.

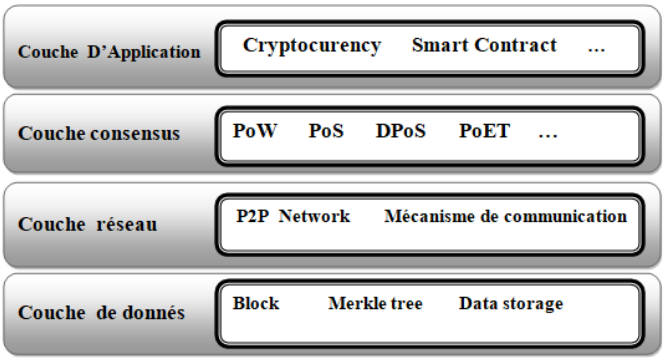


FIGURE 2.4 – l'architecture hiérarchique de la Blockchain.

2.3.3 Fonctionnement

La Blockchain fonctionne d'une manière distribuée sans aucun organe central de contrôle. La figure 2.5 illustre le mécanisme de fonctionnement des transactions dans le réseau Blockchain à travers un exemple de cas d'utilisation.

1. Un utilisateur A veut effectue une transaction vers B.
2. La transaction est regroupée avec d'autres transactions connexes au sein d'un bloc. Cette dernière ne peut s'exécuter que si tous les autres nœuds de réseau la vérifient comme une transaction valide.
3. La transaction est diffusée sur le réseau Blockchain.
4. Chaque nœud recevra une demande de vérification de la transaction en cours, qui sera vérifiée et validée par les mineurs du réseau à l'aide des techniques cryptographiques.
5. Une fois le nouveau bloc est validé, il est daté et ajouté à la Blockchain, sous une forme qui est permanente et inaltérable.
6. Enfin, la transaction sera effectuée avec succès et B reçoit la transaction.

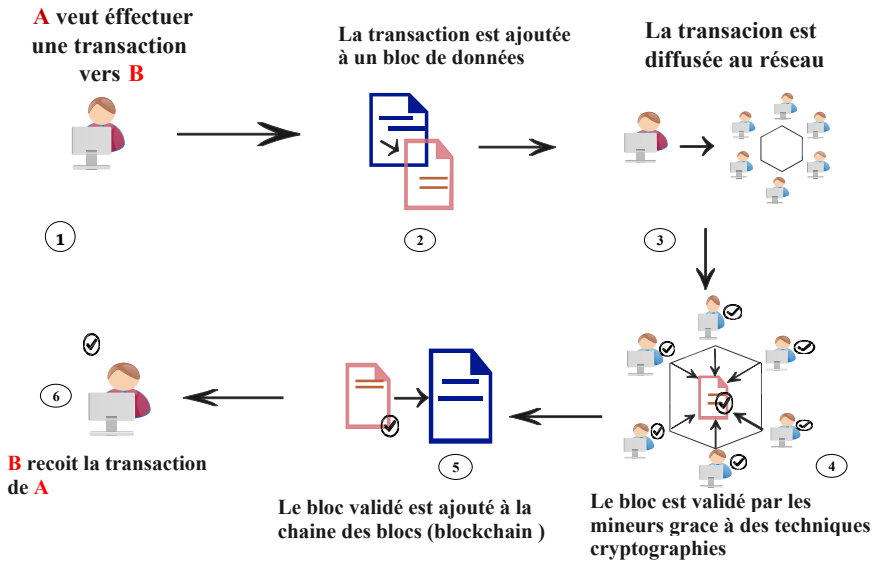


FIGURE 2.5 – Un scénario illustratif de mode de fonctionnement de la Blockchain

2.4 Types

Il existent différents modèles de conception de la Blockchain. Ces modèles sont classées en fonction des personnes autorisées à participer et à observer les données dans le réseau Blockchain. Essentiellement on distingue trois grands types de la Blockchain : la Blockchain publique, la Blockchain privée et la Blockchain de consortium [38].

2.4.1 Blockchain publique (permission-less Blockchain)

Elle est dite publique dans le sens où les réseaux sont ouverts au grand public, tous peuvent lire, écrire et participer au réseau (voir la figure 2.6). Une Blockchain publique est une Blockchain que tout utilisateur peut rejoindre sans condition. Sur une Blockchain comprenant des mineurs, n'importe quel utilisateur peut devenir mineur. Tous peuvent envoyer une transaction, qui aurait pour effet de modifier la Blockchain si la transaction est jugée légitime par les mineurs. L'accès à l'opération de vérification des transactions n'est soumis à aucune restriction ou condition [39].

Le plus grand avantage de ce type est qu'il n'est pas nécessaire de se faire confiance pour que le réseau puisse traiter et sécuriser les transactions. Aussi elle est ouverte et transparenet. Par contre, elles sont très lentes, pour traiter.
Les transactions d'un bloc prennent beaucoup de temps et consomment beaucoup d'énergie. Des exemples de la Blockchain publique : Bitcoin et Litecoin, etc.

2.4.2 Blockchain privée (permissioned Blockchain)

La Blockchain privée est limitée à un individu ou à une organisation (voir la figure 2.6). Une autorité est également responsable de l'octroi sélectif de l'accès en lecture-écriture aux utilisateurs, pour lire, écrire ou vérifier la Blockchain, les participants au réseau doivent d'abord obtenir une autorisation.

Ce type de Blockchain est principalement mis en place pour faciliter le partage et l'échange privés de données entre un groupe de membres connus au sein d'une même organisation. Cela incline davantage le réseau vers la centrali- sation, tout en dérogeant aux caractéristiques élémentaires de la Blockchain que sont la décentralisation complète et l'ouverture telle que définie [40]. Ce type est plus rapide : il permet de traiter un grand nombre de transactions pour chaque bloc dans un temps très court.

En effet, il est facile pour un individu indigne de confiance de prendre le contrôle du réseau et de menacer l'ensemble du réseau lorsque le nombre de nœuds est réduit, cela signifie que ce type est vulnérable au piratage et à la manipulation des données [41]. Des exemples de Blockchain privée : Hyperledger, Passcare, etc.

2.4.3 Blockchain de consortium

Ce type de Blockchain peut être considéré comme une Blockchain partiellement privée et semi-décentralisé, dans laquelle aucune organisation unique ne gère le processus de consensus et la validation des blocs, mais cette tâche sera réalisée plutôt par un ensemble de nœuds présélectionnés (voir la figure 2.6). Ces nœuds décident qui peut participer au réseau et qui peut prendre part au mécanisme de consensus. Il s'agit donc d'un système partiellement centralisé, en raison du contrôle exercé par certains nœuds de validation sélectionnés [42]. Des exemples de Blockchain de consortium : Ripple, R3, etc.

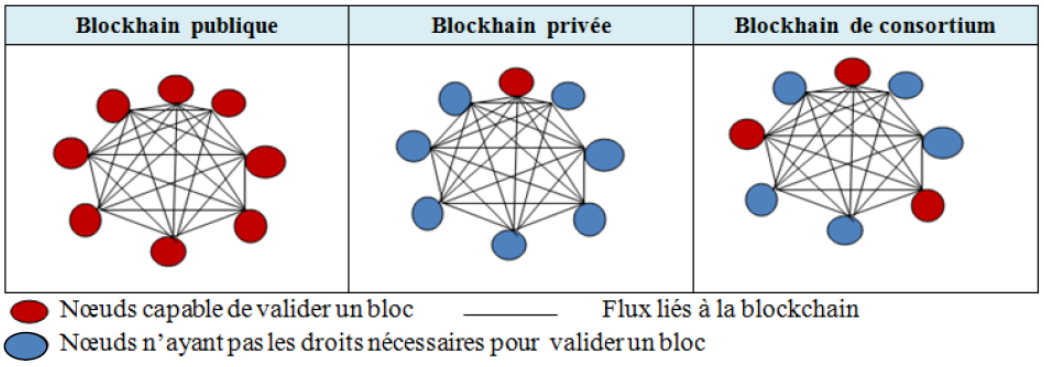


FIGURE 2.6 – les types de la Blockchains

Le tableau (2.1) fournit une étude comparative des différents types de la Blockchain.

Propriété	Blockchain publique	Blockchain privée	Blockchain consortium
Accès aux données en lecture	Aucune restriction	Avec ou sans restriction	Avec ou sans restriction
Accès aux données en écriture	Aucune restriction	Une entité unique	Aucune restriction ou uniquement des entités présélectionnées
Décentralisation	Décentralisé	Centralisé	Partiel
Transparence	Transparent	Opaque	Partiel
Flexibilité	Faible	Supérieure	Bien
Détermination par consensus	Tous les nœuds (mineurs)	Individu ou à une organisation	Ensemble de nœuds sélectionné
Exemple	Bitcoin , Litecoin	Hyperledger, PassCare	Ripple, R3

TABLE 2.1 – un tableau comparatif des types de la Blockchain [35].

2.5 Domaines d'application de la Blockchain

La Blockchain a été proposée pour être utilisée dans différentes applications et cas d'utilisation dont les plus importants sont résumés aux points suivants :

— **La santé :** les dossiers médicaux personnels sont des informations sensibles et doivent être traités avec une haute sécurité. Ces dossiers personnels peuvent être codés et stockés à l'aide de la Blockchain et fournir une clé privée qui ne permettrait qu'à des personnes spécifiques d'accéder aux dossiers [43].

La Blockchain pourrait permettre de gérer de manière transparente, sûre et infalsifiable les données des patients et restreindre le partage des données aux principaux tiers de confiances : les médecins, les hôpitaux, les laboratoires pharmaceutiques, etc.

Parmi ces projets : PassCar [44]. Un passeport de santé numérique personnel permettre aux patients de retrouver et de gérer toutes leurs informations de santé et de les partager avec les professionnels de santé de leur choix.

— **Le vote :** la Blockchain peut transformer le système de vote traditionnel sur papier en un système numérisé et peut fournir une plate-forme de vote sécurisée. Le protocole de Blockchain maintiendrait également la transparence du processus électoral, et en fournissant aux résultats immédiats [45].

La Blockchain distribue les informations relatives aux votes individuels par l'intermédiaire de milliers d'ordinateurs dans le monde, ce qui rend difficile la modification ou la suppression des votes. Cette approche favorise une plus grande confiance entre les citoyens et les gouvernements.

Public Votes est une application de vote simple et gratuite qui utilise la Blockchain Ethereum pour créer un système de vote transparent et équitable [45]

— **La finance et les banques :** les secteurs de la banque et de la finance sont fortement impliqués dans la technologie Blockchain. Divers fournisseurs de services et acteurs du secteur proposent des solutions de porte-monnaie électronique qui permettent des transactions financières rapides et sécurisées entre particuliers et entreprises, ainsi qu'entre institutions financières [46].

— **L'assurance :** tout actif de valeur ou correctement difficile à reproduire ou à détacher peut être enregistré dans la Blockchain. La demande d'assurance a été confrontée à plusieurs demandes frauduleuses. En outre, toute réclamation frauduleuse peut être détectée et abandonnée en toute confiance, car plusieurs participants doivent se mettre d'accord sur le montant de la réclamation. Cela garantit que les assureurs s'assurent que les assurances règlent rapidement et efficacement la réclamation qu'ils méritent [43].

— **La cyber sécurité :** les informations sur les menaces peuvent être partagées en utilisant la Blockchain entre les participants pour lutter contre les cyber-attaques futures. En utilisant la Blockchain avec l'aide d'une paire de clés publique et privée, les informations peuvent être partagées sans révéler d'informations identifiables à l'exception de la clé publique. [43].

— **Le Stockage :** dans n'importe quel domaine, la Blockchain offre la possibilité de stocker des documents à la fois sur la chaîne accessible à tous ou sur une sidechain qui n'est accessible par exemple qu'à la seule personne qui l'a créée. Avec cette option, la preuve générale de l'existence, l'authenticité ou les signatures peuvent être vérifiées par les parties concernées [47].

2.6 Apports et défis de la Blockchain

Quand on parle d'une technologie, on a besoin de connaître les avantages et les inconvénients de cette technologie [48, 49].

2.6.1 Apports

La technologie Blockchain a apporté de nombreux avantages, parmi ses avantages :

— **La distribution :** les données de la Blockchain sont souvent stockées dans des milliers de périphériques sur un réseau de nœuds distribués, le système et les données résistent très bien aux défaillances techniques et aux attaques malveillantes.

— **La sécurité :** la technologie de la Blockchain est plus sécurisée. Cela signifie qu'une Blockchain est beaucoup moins susceptible d'être la cible d'une tentative de piratage informatique, car il n'y a pas de point de défaillance unique.

— **La transparence :** toutes les transactions sur une Blockchain étant tracées et stockées publiquement sur plusieurs nœuds du réseau, la transparence est donc total.

— **Un système sans tiers de confiance :** un système de Blockchain élimine le risque de faire confiance à une seule organisation et réduit également les coûts globaux et les frais de transaction en éliminant les intermédiaires et les tiers.

— **L'authenticité et l'intégrété :** la Blockchain assure l'authenticité et l'intégrité des données par des techniques de cryptographie, telles que la signature numérique.

— **Une économie numérique décentralisée :** malgré le fait que la Blockchain ne pourra pas supprimer totalement les intermédiaires, mais elle permet l'émergence d'une nouvelle économie plus décentralisée.

2.6.2 Défit

Parmi les inconvénients de la technologie de la Blockchain, il y' a les suivants :

— **Les clés privées :** chaque compte Blockchain a deux clés correspondantes : une clé publique (partagée) et une clé privée (secrète). Les utilisateurs ont besoin de leur clé privée pour accéder à leurs fonds, ce qui signifie qu'ils agissent comme leur propre banque. Si un utilisateur perd sa clé privée, l'argent est alors concrètement perdu et il ne peut rien y faire.

— **L'espace de Stockage :** les registres de la Blockchain peuvent devenir très volumineux avec le temps. La croissance de la taille de la Blockchain devient supérieure à celle des disques durs, le réseau risque de perdre des nœuds si le registre devient trop volumineux pour être téléchargé et stocké par les utilisateurs, si l'on prend l'exemple du bitcoin, il contient actuellement en 2021 plus de 400 giga-octets (Go) de données de transaction [50].

— **L'augmentation du chômage :** grâce à la technologie de la chaîne de blocs, un grand nombre d'employés pourraient être envoyés au chômage. Car de nombreux systèmes financiers, comptables et administratifs pourraient être remplacés par cette technologie, et de nombreux emplois pourraient être supprimés.

— **Le temps de réponse :** l'un des plus grands inconvénients de la Blockchain est le temps nécessaire pour la prise en compte effective d'une transaction. Un temps qui peut aller jusqu'à plusieurs heures.

2.7 Protocoles de consensus

Les Blockchains sont des réseaux pair à pair, et il n'y a pas de nœud central qui garantit que les grands livres sur les nœuds distribués sont tous les mêmes. Pour s'assurer que tous les nœuds sont d'accord sur les transactions et l'ordre dans lequel celles-ci sont répertoriées sur le bloc validé, la Blockchain utilise des protocoles de consensus qui appliquent des

différentes méthodes. Il existe plusieurs protocoles de consensus ; nous allons présenter les plus connus ci-dessous.

2.7.1 Pow (proof of work)

Cette stratégie de consensus est utilisée dans le réseau Bitcoin en plus de nombreuses autres cryptomonnaies pour confirmer les transactions et produire de nouveaux blocs dans la chaîne. C'est le plus utilisé de tous les protocoles de consensus de la Blockchain. Depuis 2009, il a pu démontrer sa résistance et sa sécurité aux différentes tentatives d'attaques.

Le mécanisme PoW utilise la résolution de puzzle pour prouver la crédibilité des données. Le puzzle est généralement un problème mathématique complexe requérant une forte puissance de calcul pour y parvenir, difficile à calculer, mais facilement vérifiable. Lorsqu'un nœud crée un bloc, il doit résoudre un puzzle PoW. Une fois le puzzle résolu, il est diffusée aux autres nœuds pour les vérifier, afin d'atteindre l'objectif du consensus.

PoW sécurise efficacement le réseau en rendant les tentatives de piratage extrêmement difficile, mais il consomme une grande quantité d'énergie lors de la résolution du problème mathématique.

2.7.2 PoS (Proof of Stake)

Cette stratégie de consensus est une approche alternative au PoW qui nécessite moins de calculs CPU pour le minage. Au lieu d'une compétition entre les nœuds participants pour résoudre le prochain bloc, un nœud est choisi pour la tâche de minage sur la base de sa participation proportionnelle dans le réseau. Ce dernier utilisera alors une signature numérique pour prouver sa propriété sur la participation au lieu de résoudre un problème de hachage compliqué. Parallèlement, plus les faussaires détiennent de monnaie, plus ils ont de chances de générer le bloc suivant. De plus, dans cette méthode, toutes les pièces sont disponibles dès le premier jour et il n'existe pas de récompense pour le minage ou la création de pièces, au lieu de cela, les nœuds de minage sont récompensés uniquement par les frais de transaction. Bien que cette méthode élimine les exigences de calcul de la preuve de travail, elle crée de nouveaux problèmes, dans la mesure où elle dépend des nœuds ayant le montant de mise le plus élevé, ce qui rend en quelque sorte la Blockchain centralisée [40].

Proof of Stake possède une meilleure scalabilité, c'est-à-dire une meilleure vitesse pour gérer les transactions. Le principal avantage du PoS est que la validation d'un bloc ne dépend pas de puissants calculs algorithmiques qui consommeraient beaucoup d'énergie.

La simplicité du système pourrait engendrer une attaque de type "Nothing at stake" que l'on pourrait traduire par "Rien à perdre", la sécurité dans ce mécanisme est faible.

2.7.3 DPOS (Delegated proof of stake)

Le mechanism de Delegated Proof of Stake (DPoS) est une variante du Proof of Stake (PoS). La principale différence entre PoS et DPOS est que PoS est une démocratie directe

tandis que DPOS est une démocratie représentative. Les parties prenantes élisent leurs délégués pour générer et valider les blocs. Avec beaucoup moins de nœuds pour valider le bloc, celui-ci peut être confirmé rapidement, ce qui entraîne une confirmation rapide des transactions. Parallèlement, les paramètres du réseau, tels que la taille et l'intervalle des blocs, peuvent être réglés par les délégués. En outre, les utilisateurs n'ont pas à s'inquiéter des délégués malhonnêtes car ils peuvent être éliminés facilement [51].

L'avantage de ce type de construction, c'est qu'elle réduit les interactions entre les nœuds et permet dans un plus grand nombre de transactions et des validations plus rapides. Le principal inconvénient, c'est une plus grande centralisation, avec des risques de vulnérabilité, de censure et de cartellisation.

2.7.4 PoA(proof of authority)

Le modèle de consensus par preuve d'autorité (également appelé preuve d'identité) repose sur la confiance partielle des nœuds de publication grâce à leur lien connu avec des identités du monde réel. Les nœuds de publication doivent avoir leur identité prouvée et vérifiable au sein du réseau Blockchain (par exemple, des documents d'identification qui ont été vérifiés et notariés et inclus dans la Blockchain).

L'idée est que le nœud de publication met en jeu son identité pour publier de nouveaux blocs. Les utilisateurs du réseau Blockchain affectent directement la réputation d'un nœud de publication en fonction du comportement de ce dernier.

Les nœuds de publication peuvent perdre leur réputation en agissant d'une manière que les utilisateurs du réseau Blockchain désapprouvent, tout comme ils peuvent gagner en réputation en agissant d'une manière que les utilisateurs du réseau Blockchain approuvent. Plus la réputation est faible, moins la probabilité de pouvoir publier un bloc est grande. Par conséquent, il est dans l'intérêt d'un nœud de publication de maintenir une réputation élevée. Cet algorithme ne s'applique qu'aux réseaux Blockchain autorisés avec des niveaux de confiance élevés [32].

Le temps de transaction du PoA est sensiblement plus rapide que le temps de transaction des réseaux basés sur le PoW.
Les réseaux basés sur la preuve d'autorité n'exigent que très peu de puissance de calcul.

2.7.5 PoET (proof of elapsed time)

PoET vise à développer un algorithme de consensus équitable qui peut s'adapter à des milliers de nœuds et être économe en énergie. L'algorithme vise à reproduire un processus de génération de blocs équitable et aléatoire sans dépenser de ressources précieuses, telles que des pièces, de la puissance de calcul ou de l'électricité. Pour ce faire, il utilise de nouvelles instructions CPU et un environnement d'exécution de confiance [52]. Les nœuds validateurs demandent un temps d'attente à une fonction de confiance dans un processeur polyvalent. Le nœud ayant le temps d'attente le plus court produit le bloc. L'environnement vérifie si la demande de leadership est légitime selon le temps d'attente alloué. La

principale critique concernant cette approche est l'exigence de l'environnement développé par Intel, ce qui signifie que la confiance est toujours requise envers une seule autorité.

Le tableau 2.2 résumée une étude comparatif des différents protocoles de consensus de la Blockchain.

Propriété	Pow	PoS	DpoS	PoA	PoET
Année	2009	2012	2014	2017	2016
Gestion de l'identité des nœuds	Permissionless	Permissionless	Permissionless	Permissioned	Permissioned
Économie d'énergie	Non	Partiel	Partiel	Oui	Oui
Latence des transactions	Élevé	Faible	Faible	Élevé	Élevé
Blockchain	Public	Public, privé	Public, privé	privé ou consortium	Public, privé
Exemples d'applications	Bitcoin, Litecoin,	Ethereum, Peercoin,	Bitshares, Cardano	Swarm City, Kovan	Hyperledger, Sawtooth

TABLE 2.2 – un tableau récapitulatif and comparatif entre les protocoles de consensus de la blockcahin [37, 51].

2.8 Conclusion

Dans ce chapitre, nous avons présenté la technologie de la Blockchain qui est une nouvelle technologie révolutionnaire qui permet aux utilisateurs d'effectuer des transactions, garantir et auditables par tout le monde, sans avoir besoin d'un tiers de confiance. Tout d'abord, nous avons commancé par des généralités de cette technologie. Ensuite-nous avons mentionné ces types, quelques domaine d'applications, ces apports et ces défis et nous avons terminé par quelques protocoles de cette technologie.

Dans le prochain chapitre, nous présentons un survol bibliographique sur les différents systemes de signalemnts basés sur la tehcnologies de la Blockchain.

CHAPITRE 3

SYSTÈMES DE SIGNALEMENT

3.1 Introduction

Dans la vie, il y a des évenements sensibles qui affectent la gestion des villes dont les comportements illégaux ou dangereux de certains citoyens comme les griefs, la discrimination, la violation de la vie privée et les conditions de travail dangereuses, etc. Et comme les autorités ne peuvent plus contrôler et surveiller tout le monde à tout moment, les citoyens doivent collaborent ensemble à travers l'intelligence humaine pour améliorer la vie collective et la gestion de la ville. Parmi les outils de collaboration les systèmes de signalement qui sont des techniques qui peuvent améliorer la gestion de la ville. Les systèmes de signalement permet d'éviter quelques comportements où chaque personne avant de faire un comportement illégal ou dangereux doit savoir qu'il est contrôlé par des citoyennes et qui peuvent le signaler à tout moment aux autorités responsables même si ces autorités ne sont pas présentes au lieu de l'événement. Mais la peur de la vengeance certains citoyens évitent de signaler quelques comportements, cela a donné naissance à des systèmes de signalement anonyme basé sur la Blockchain qui encourage les citoyens de lancer des signaux sans aucune peur et doute qu'ils seront révélés.

L'objectif de ce chapitre est de présenter les principes fondamentaux d'un système de signalement. Nous commencons par passer en revue certains concepts de base, telles que la définition, l'architecture d'un système de signalisation, leur fonctionnement, ses avantages et ses inconvénients, ainsi que ses types, puis nous terminons sur quelque systèmes de signalements existants basé sur la technologie de la Blockchain.

3.2 Définition

Un signalement ou une alerte représente une alarme automatique d'avertissement d'un danger, ou tout dispositif qui signale l'occurrence d'un événement indésirable. Toute fois, il n'y a pas une définition universelle d'un système de signalement, plutôt des définitions dans des cadres spécifiques :

Un système de signalement médical est défini comme des dispositifs communiquant

qui sont capables de demander de l'aide, ou de déclencher une alarme lors de la détection automatique d'une situation anormale tel que : une augmentation de la chaleur ou une accelération anormale du rythme cardiaque [53].

Un système de signalement dans le domaine des réseaux des véhicules a pour rôle d'envoyer des avertissements sur les risques qui peuvent exister sur les routes tel que : le verglas, l'état de traffic. Il peut même être utilisé pour la diffusion des informations sur un site touristique ou un restaurant [54].

Dans notre cas, un système de signalement est un processus qui permet de signaler une anomalie (un évènement) ou un problème aux autorités concernées afin de les avertir d'une situation amorale ou dangereuse et leur permettre par la suite d'intervenir et réagir pour essayer de résoudre ses anomalies dans des meilleures délais.
La Figure 3.1, illustre un exemple d'un système de signalement dans le contexte des réseaux de véhicules. Dans ce système un véhicule qui a constaté un danger sur la route va lancer un signalement pour avertir l'autorité compétante et les autres usagers de la route. Ce signalement va être appuyer par d'autres témoins comme il peut être valider par un validateur à la demande de l'autorité, si elle se méfie de la bonne fois de signaleur.

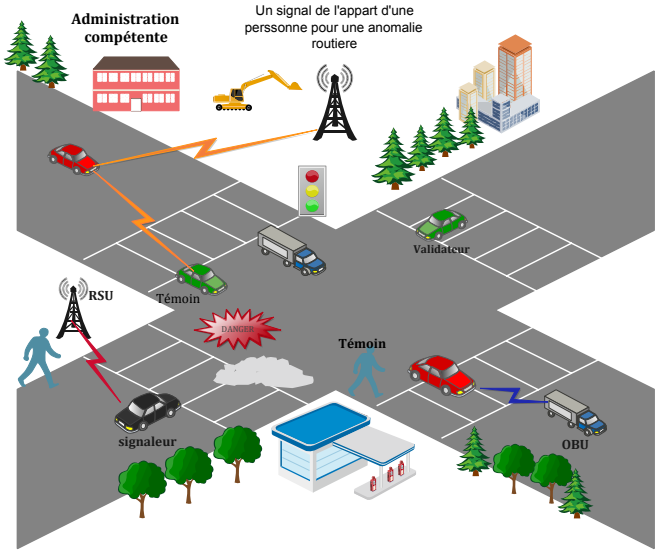


FIGURE 3.1 – un exemple illustratif d'un système de signalement dans les réseaux de véhicules.

La figure 3.2 montre un autre système de signalement des incidents criminels [55], ce système comporte trois groupes d'utilisateurs :

1. **Les rapporteurs** : c'est-à-dire les citoyens qui remplissent le rapport d'incident.
2. **Les officiers** : ils sont les policiers qui reçoivent le rapport d'incident.
3. **Les superviseurs** : ils sont les policiers qui gèrent le processus d'intervention pour régler l'incident.

Ce système permet aux citoyens de signaler des incidents criminels via une application mobile et aux agents de répondre au rapport via une application Web. Les données relatives aux incidents sont envoyées à un serveur et triées automatiquement en fonction de la

priorité de la situation ou du type d'incident, puis présentées aux agents. Ensuite, l'agent récupère le rapport et vérifie les détails de l'incident avec le rapporteur par téléphone [55].

L'application triera le rapport d'incident en fonction des règles de priorité définies et affichera les informations connexes afin de soutenir les opérations des agents d'intervention. Le rapport d'incident, le rapport de réponse à l'incident et les résultats seront automatiquement conservés dans la base de données et le système générera des rapports d'analyse pour les dirigeants à des fins d'évaluation et de planification future.

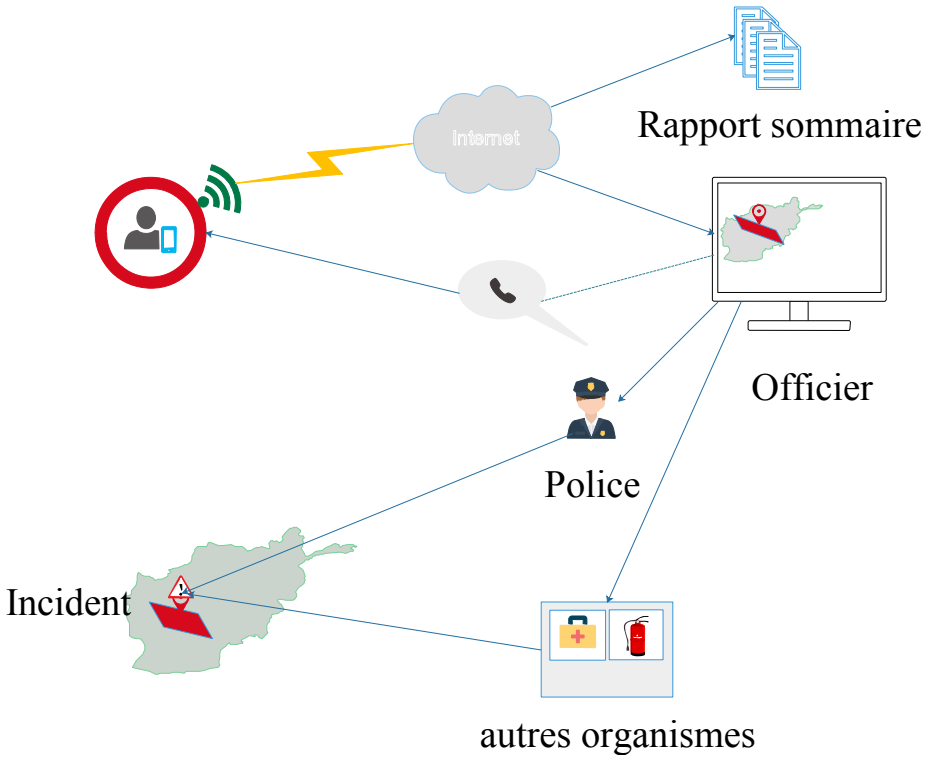


FIGURE 3.2 – un exemple illustratif d'un système de signalement.

3.3 Architecture typique d'un système de signalement

Un système de signalement est une collection d'entités interdépendantes, qui agissent ensemble et collaborent pour atteindre un objectif commun. En effet, un système de signalement se compose de :

1. **L'evénement :** c'est l'anomalie ou l'incident qui représente une situation anormale ou dangereuse qui peut représenter un risque ou causer des aléas pour la communauté des citoyens ou des usagers d'un système.
2. **L'autorité :** elle gère les identités et les clés de tous les usagers du système.
3. **Les signaleurs :** ils s'agissent des usagers ou des personnes qui ont constaté l'anomalie ou l'événement et qui ont décider de le faire signaler afin d'avertir l'autorité

compétente et protéger les autres utilisateurs.

4. **l'administration compétente :** elle représente des parties qui ont la responsabilité et la capacité de régler les anomalies dans un domaine de compétence donné.
5. **Les vérificateurs :** ils s'agissent d'un ou de plusieurs personnes (usagers) qui peuvent être chargé par l'administration compétente de vérifier l'existence de l'anomalie.
6. **Les témoins :** ils s'agissent des usagers du système qui sont dans le même périmètre de l'événement et qui peuvent témoigner avec le signaleur sur l'existence de l'événement pour donner plus de crédibilité au signalement.

3.4 Fonctionnement d'un système de signalement

Généralement, un système de signalement fonctionne de la manière suivante :

1. Un événement illégal, un incident dangereux ou une anomalie se produit.
2. Un signaleur qui est équipé d'une application observe cet événement et lance le processus de signalement.
3. Des témoins qui étaient présents sur le lieu de l'événement peuvent confirmer l'événement.
4. Le signaleur envoie le signalement approuvé par les témoins à l'administration compétente pour prendre les actions nécessaires.
5. L'administration compétente concernée reçoit le signal du l'événement.
6. L'administration compétente est responsable de la prise en compte de signalement et aussi de la mise en œuvre de l'ensemble des étapes pour régler le problème.
7. L'administration compétente peut contacter et envyoer des vérificateurs qui se trouvent dans l'entourage de l'événement pour vérifier le signalement avant de prendre les actions nécessaires pour régler le problème en question.
8. Plus le nombre des vérificateurs participants est élevés, plus la crédibilité de signalement est élevé, moins le besoin de faire appel à des vérificateurs par l'administration.
9. L'autorité reçoit la confirmation et passe à l'action pour essayer de résoudre le problème.

Le datagramme dans la Figure 3.3 décrit le fonctionnement d'une architecture typique d'un système de signalement et les différents flux de communication entre ses différentes composantes.

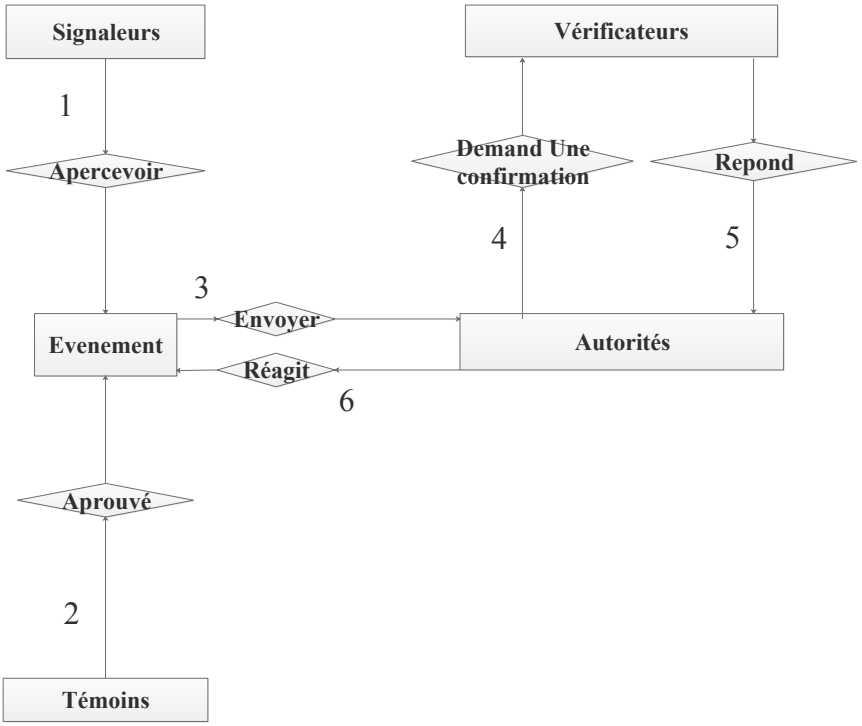


FIGURE 3.3 – le mécanisme de fonctionnement d'un système de signalement.

3.5 Apports et défis

Comme la plupart des systèmes, celui de signalement contient des avantages ainsi que des défis.

3.5.1 Apports

Un système de signalement apporte beaucoup d'avantages, parmi ses avantages, il y a [56] :

— Les systèmes de signalement contribueront à un environnement social plus sûr.

— Un système de signalement aide les autorités à réagir aux différents problèmes.

— Impliquer les citoyens dans l'amélioration de la gestion des villes intelligentes.

— Créer une intelligence collective de la communauté pour déjouer les aléas en signalant aux autres la présence d'un danger.

— Améliorer l'efficacité du trafic et réduire l'embouteillages et les accidents, etc.

3.5.2 Défis

Parmi les défis d'un système de signalement, il y a [57] :

— La protection de la vie privée, les gens peur de signaler des évènements avec leur réelle identité, car ils craignent de subir des représailles.

— La difficulté de transmettre des annonces fiables sans révéler l'identité.

— Difficile de garantir que le système de signalement est absolument sûr et fiable car tous les messages doivent être transmis de manière anonyme dans les réseaux.

— Manque de motivation pour les utilisateurs pour signaler quelqu'un et la crainte de recevoir des convocations des autorités qui demandent d'autres explications.

3.6 Types des systèmes de signalement

Les systèmes de signalement peut être divisés en deux grandes catégories selon le mode de fonctionnement : les systèmes de signalement centralisés et sytèmes distribués.

3.6.1 Systèmes de signalement centralisés

Un système de signalement centralisé, c'est un système ou toutes les entités du système sont connectées à une seule unité centrale [55] et chaque utilisateur qui veut signaler un événement doit envoyer son signalement à l'unité central. Dans ce type, l'unité ou l'autorité centrale va gérer toutes les informations des utilisateurs et leurs actions dans le système.

Parmi les exemples des systèmes de signalement centralisées existants : BetterStreet [58], YOUR VOICE et SAY SOMETHING.

A) **Avantages**

Les systèmes de signalement centralisés présentent plusieurs avantages [55] :

— Ils permettent de simplifier la configuration du système, car tous les dispositifs sont connectés à l'unité de calcul centralisée.

— Il est possible de partager des informations sans réseau supplémentaire, et les retards et les pertes d'informations dus à la communication sont minimes.

B) **Défis**

En plus des problèmes classiques des systèmes centralisés tel que :

— Le système centralisé nécessite une capacité de calcul élevée.

— Il est difficile de garantir une tolérance aux pannes fiable.

Les systèmes de signalement centralisés présentent d'autres types de problèmes parmi eux il y a :

— la vie privée et la crainte de divulger les informations personnels à une unité externe non digne de confiance.

— Le manque de confiance à une entité centralisée.

— Un modèle centralisé est facile à cibler par les attaquants [59].

3.6.2 Systèmes de signalement distribués

Un système de signalement distribué est une collection d'entités indépendantes qui apparaissent à l'utilisateur comme un seul système cohérent, chaque nœud collabore avec d'autres nœuds. Il n'y a pas de centre unifié, les données sont stockées de manière distribuée et chaque nœud est autonome [57].

Parmi les systèmes de signalement distribués existants il y a : Bouge Ma Ville [60], Voilà ! Signalement, coyotte, etc.

A) **Avantages**

Parmi les avantages d'un système de signalement distribué, il y a :

— Une grande crédibilité grâce aux grands nombres des signalements et l'existence de plusieurs entités (l'absence de l'autorité centralisée).

— Une amélioration considérable de l'efficacité et une solution au problème de point de défaillance uniques [59].

B) **Défis**

Parmi les défis d'un système de signalement distribué, il y a :

— Les messages de contrôles sont difficiles à gérer, car ses messages sont distribués sur plusieurs entités.

— La surcharge de réseau à cause du nombre des entités et la communication entre eux.

— Un accès aux données sans autorisation et protection de la sécurité des données [54].

— L'exigence d'assurer une synchronisation en temps réel [59].

Récemment, la technologie de la Blockchain a été adoptée par les systèmes de signalement distribués comme un outil efficace pour protéger les données des signaleurs.

3.7 Systèmes de signalement basés sur la technologie de Blockchain

L'intégration de la technologie de la Blockchain aux systèmes de signalement a attiré une attention croissante des chercheurs et des développeurs en raison des caractéristiques de la décentralisation, de l'anonymat et de la confiance de la Blockchain. en effet, les propriétés de la Blockchain répondent à toutes les exigences des nouveaux systèmes de signalement distribués et anonymes. Un système de signalement sécurisé, décentralisé et de confiance est établi par la Blockchain pour résoudre les problèmes de la sécurité des données de la confidentialité et de l'anonymat.

3.7.1 Apports de la Blockchain pour les systèmes de signalements

La Blockchain a ajouté beaucoup d'apports aux systèmes de signalement parmi eux [59] :

— Les systèmes de signalement anonymes basés sur la Blockchain sont plus sûrs, plus fiables et plus respectueux de l'environnement.

— L'anonymat et la sécurité, car la Blockchain garantit la sécurité de l'identité de l'utilisateur et la fiabilité des rapports.

— La Blockchain augmente la confiance entre les utilisateurs mobiles.

— Les réseaux basés sur la Blockchain sont ouverts, transparents, et prometteurs dans l'enregistrement des données avec les bonnes propriétés de résistance à la falsification et de la décentralisation.

— La Blockchain convertit la confiance entre les personnes ou les institutions en confiance gérée par le système et toute intervention humaine sera inopérante, garantissant ainsi la fiabilité des messages de déclaration anonyme.

— La Blockchain peut fournir un meilleur mécanisme d'incitation pour encourager les utilisateurs mobiles à effectuer des déclarations anonymes sans craindre la divulgation de leur identité.

— La Blockchain peut et maintenir un fonctionnement fiable même si certains nœuds sont envahis ou défaillants, ce qui permet de résister efficacement aux attaques.

3.7.2 Survol bibliographique sur les travaux des systemes de signalements annonymes

Des travaux sur les systèmes de signalement annonymes basés sur la Blockchain existent déjà. Parmi ces travaux, nous citons les suiveants :

1. **ReportCoin**
   Zou et al. dans le travail [61] ont proposé ReportCoin, un nouveau système décentralisé de signalement anonyme incitatif, basé sur la technologie de la Blockchain pour la gestion des villes intelligentes.
   À l'inverse des systèmes de signalement centralisés qui ne garantissent pas l'anonymat des signaleurs, ReportCoin a essayé de bénéficier des avantages de la Blockchain, autrement dit, la transparence, la décentralisation, l'anonymat, etc. pour protéger l'identité de signaleur et assurer la confidentialité ainsi que la distribution de système de signalement. En effet, ReportCoin permet aux utilisateurs de participer aux systèmes de signalement de manière anonyme sans craindre ni sur leur identité ni contre les vengeances.
   Le système de signalement proposé dans ReportCoin contient principalement deux parties [61] :

   (a) **Le Protocole d'annonce de rapport anonyme appelé ReportAnnouncement :** dans lequel la technologie d'authentification de seuil améliore l'adaptabilité et l'exibilité des communications dans un environnement non-fiable et fournit un niveau plus élevé de confidentialité et de fiabilité pour la communication de rapports anonymes dans ReportCoin. Les cinq phases de la communication des rapports announcement sont [61] :

      i. **La phase de mise en place initiale :** ReportCoin crée des paires de clés publiques et privées pour les utilisateurs ne utilisant la courbe elliptique.
      ii. **La phase de demande :** un utilisateur mobile transmet une requete comprenant ces informations aux autres témoins qui se trouvent dans le meme périmetre de l'évenement pour les inviter confirmer cette annonce.
      iii. **La phase de réponse :** après avoir reçu cette annonce, si le témoin est d'accord avec l'annonce de signalement de l'initialisateur de signal, il/elle

signera avec sa propre signature privée combinée avec les clés publiques des autres utilisateurs et renverra une réponse à l'initialisateur.

iv. **La phase d'annonce de publication :** une fois le seuil de témoins sera atteint, le signal sera diffuser aux autres utilisateurs mobiles des environs pour vérification.

v. **La phase de vérification :** tout utilisateur, qui reçoit le signal de vérification peut devenir vérificateur afin de vérifier l'authenticité et la fiabilité du signal. Lorsque le nombre de vérifications réussies atteint le seuil t, l'annonce de réponse est considérée comme valide et elle sera ajoutée au bloc.

(b) **Le mécanisme d'incitation basé sur la Blockchain :** ReportCoin [61] a proposé un nouveau mécanisme d'incitation pour encourager les utilisateurs à participer activement dans le système de signalement. Pour cela, il a proposé une nouvelle stratégie basée sur une monnaie virtuelle, appelé RCoins. Chaque utilisateur de ReportCoin possède un compte de crédit numérique pour stocker les points de réputation (Rcoins). Après que les annonces de signalement ont été vérifiées et ajoutées à la Blockchain, les rapporteurs (témoins) initiaux, les répondeurs et les vérificateurs de la Blockchain seront récompensés.

— Comme les utilisateurs ne disposent que d'une petite quantité de Rcoins au départ, ils n'ont que la possibilité d'agir en tant que témoins. L'utilisateur reçoit cinq Rcoins pour chaque réponse non-défaillante au la requete de témoinage.

— Après avoir conservé suffisamment de Rcoins, il peut choisir de travailler en tant que initialisateur et d'envoyer des requete de signalement (il peut lancer des signalements). et d'envoyer des RQP sur des événements de signalement plus tard pour gagner plus de Rcoins.

— Le lancement d'un signalement coûte des Rcoins (-10), ce qui empêche les utilisateurs malveillants d'envoyer des demandes inutiles ou frauduleuses dans le réseau ReportAnnouncement. Le signaleur gagne 20 Rcoins pour chaque signalement non defaillant et perde 10 si l'evenement s'averer faux.

— Les utilisateurs mobiles peuvent utiliser les Rcoin pour déduire une certaine quantité de leurs propres infractions, come ils peuvent également l'utiliser pour payer une place de stationnement par exemple.

Le systeme ReportCoin utilise le mécanisme de consensus de preuve de travail (PoW) [61] pour confirmer les transactions. Après avoir généré le nouveau bloc, le système va générer un problème mathématique. Tous ceux qui participent au processus de consensus sont en compétition pour être les premiers à trouver une solution à ce problème mathématique. Lorsque la bonne solution est trouvée, le réseau entier diffusera que l'utilisateur à le droit de générer un nouveau bloc et le récompensera avec une quantité de Rcoins.

2. **CreditCoin**

Li et al. dans [62] ont proposé CreditCoin, un système réseau d'annonces incitatif basé sur la Blockchain préservant la confidentialité dans les réseaux VANETs. Il est capable d'instaurer la confiance dans les communications des véhicules intelligents. CreditCoin utilise un réseau basé sur la Blockchain pour créer des comptes et enregistrer les transactions afin que le comportement des utilisateurs préserve la vie privée sans perte de fiabilité. Grâce à la Blockchain, les transactions et les informations de compte dans le CreditCoin sont inviolables. Ce réseau permet aux utilisateurs de générer des signatures et d'envoyer des annonces de manière anonyme dans un environnement sans confiance.

Le système de signalement proposé dans CreditCoin contient principalement deux parties [62] :

(a) Le protocole d'annonce, à savoir Echo-Announcement qui fournit un seuil d'authentification et un certain niveau de confidentialité pour garantir que les annonces anonymes sont fiables. Il permet aussi la fiabilité et l'anonymat des messages.

L'annonce de signalement d'Echo-announcement comporte cinq phases :

- **La mise en place :** l'autorité de confiance (T) génère des clés pour les utilisateurs basé sur la courbe elliptique.
- **La demande :** un utilisateur qui constate un accident devient un initiateur (I) avec sa volonté. Ensuite, I sélectionne des paramètres pour l'annonce et transmet des requêtes aux autres témoins pour les inviter à vérifier l'annonce.
- **La réponse :** un témoin renvoie une réponse à I, s'il est d'accord avec l'annonce de I.
- **L'annonce :** aprés atteindre un certain seuil de réponses favorales des témoins, l'initiateur envoie une autre fois une nouvelle reuqete à d'autres témoins dits vérificateurs pour validation.
- **Vérification :** tout utilisateur reçevant la requête de vérification va devenir un vérificateur pour vérifier la validité du signalement.

(b) Le mécanisme d'incitation dans le but de motiver les utilisateurs à transmettre honnêtement les vraies annonces (de manière anonyme et fiable) en utilisant la techonologie Blockchain qui fonctionne en parallele avec l'Echo-announnecement. Chaque utilisateur du CreditCoin possède un compte de crédit à plusieurs adresses. Le compte contient des points de réputation appelés pièces. Les utilisateurs récompensent les signaleurs en leur payant quelques pièces comme incitation. Ils peuvent également dépenser quelques pièces pour faire une annonce afin de augmenter leur réputation et gager plus de pièces [62].

- Un utilisateur peut comporter comme signaleur, témoins ou mem vérifiricateur dans le réseau. Si l'utilisateur est un nouveau, dans ce cas il/elle a peu de pièces en quantité initiale. Il n'a donc pas d'autre choix que de

se comporter comme témoins. Et chaque participation fiable recevra un nombre de pièces en tant que récompense.

— Après avoir accumuler un nombre suffisant de pièces, l'utilisateur est en mesure de signaler des événements et d'envoyer des signalements. Comme l'envoi d'une requête coûte des pièces, cela protège les utilisateurs honnêtes en réduisant le nombre de requêtes frauduleuses dans le réseau.

— Si la demande est valide, le signaleur recevra une récompense supérieure au coût de lancement de signalement.

Dans CreditCoin, les pièces non dépensées pendant une période de temps prédifinies seront réduites de moitié. Ce mécanisme empêche simplement l'accumulation des pièces qui pourraient être utilisées pour attaquer.

3. **Système d'annonces incitatives basé sur la Blockchain pour l'internet des véhicules**

Yang et al, Dans [63] ont proposé un nouveau système de signalement incitatif basé sur la Blockchain des échanges entre les utilisateurs de l'Internet de véhicules. Cette dernière est utilisée pour concevoir un mécanisme d'incitation préservant la confidentialité. Ce système permet aux participants d'annoncer anonymement leur message en utilisant la Blockchain dans un environnement non-fiable, et qui incite également les témoins à répondre à la demande d'informations sur le trafic grâce à un mécanisme d'incitation. Il garantit que tous les utilisateurs honnêtes peuvent obtenir une compensation, quelle que soit l'infraction commise par les autres utilisateurs malveillants.

Les utilisateurs transmettent des messages de manière anonyme et incitent les autres utilisateurs à partager des informations sur le trafic à l'aide de la Blockchain Ethereum sans avoir besoin d'une autorité de confiance pour réaliser un paiement équitable dans le système.

Le système se compose des entités suivantes [63] :

— **Requester (Demandeur R) :** un utilisateur qui est prêt à payer pour obtenir des informations sur une zone de la route.

— **Witness (Témoin Wi) :** un véhicule circulant à proximité de la destination correspondante qui fournit un message de témoinage à R.

— **RSUs :** les unités de bord de la route distribuées le long de la route et qui offrent aux utilisateurs la possibilité de communiquer entre eux (via l'Internet).

— **Blockchain (Chaîne de blocs) :** une Blockchain publique est adoptée pour appliquer les règles qui contiennent les informations sur le trafic sans dépendre d'une autorité de confiance.

Pour obtenir les informations sur une zone [63] :

— R envoie la demande aux RSUs et met la rémunération sur la Blockchain.

— Après avoir vérifié la demande et la rémunération, les RSUs diffusent la demande dans la zone et rassemblent suffisamment de témoins.

— Chaque témoin signe le message (msg) et l'insère dans le filtre de Bloom sur la Blockchain, de sorte que le message sera ancré sur la Blockchain comme un engagement.

— Pendant ce temps, W met un montant de dépôt sur la Blockchain pour l'empêcher de tricher. Lorsque toutes les signatures sont insérées dans le filtre, le témoin fournis le message et sa signature pour révéler son message sur la Blockchain.

— La signature du témoin sera vérifiée et authentifiée dans le filtre de Bloom.

— Après cela, la majorité du message sera calculée sur la base de ces msg. Si msg i est la majorité, Wi peut gagner les frais de message. Sinon, la phase de réclamation est effectuée si certains témoins ne révèlent pas le message ou si certains messages ne sont pas majoritaires. Dans ce cas, le témoin malveillant seronts sanctionnés.

4. **BB2AR**

Wang et al. dans [64] ont proposé un système de déclaration anonyme basé sur la technologie de la Blockchain (publique) avec récompense anonyme (BB2AR). BB2AR fournit un anonymat inconditionnel dans le sens où même un adversaire infiniment puissant ayant accès à un nombre illimité de signatures de messages ne peut pas deviner le dénonciateur, et ne peut pas lier des signatures supplémentaires au même signataire.

BB2AR fait appel aux techniques cryptographiques suivantes : la Blockchain, la signature numérique, la signature en anneau et la vérification par lot.

Ce système comprend trois entités différentes [64] :

— **Le dénonciateur :** qui soumettent les preuves du crime aux autorités. Il souhaite protéger la confidentialité de son identité tant dans la procédure de dénonciation que dans la procédure de récompense.

— **L'autorité :** qui encouragent les gens à exposer les preuves de s'incidents. L'autorité récompensera le dénonciateur s'il soumet des documents de valeur.

— **La Blockchain :** la procédure de récompense sera effectuée en utilisant la Blockchain. Le solde de la récompense sera transféré de l'autorité au dénonciateur sur la Blockchain.

BB2AR est fonction comme suite :

— Le dénonciateur s'inscrit sur la Blockchain et obtient des paramètres publics ; au même temps, l'autorité s'inscrit sur la Blockchain et stocke son argent sur la Blockchain.

— Tout d'abord, le dénonciateur soumet anonymement le matériel lié au crime à l'autorité, c'est-à-dire la déclaration anonyme.

— Lorsque les documents relatifs au crime soumis sont valables, l'autorité récompense le dénonciateur en utilisant la Blockchain. Cela correspond à la procédure de récompense anonyme.

— le dénonciateur obtient le solde de la récompense. Il peut utiliser les récompenses pour créer d'autres transactions sur la Blockchain.

5. **Un protocole évolutif BTCPS pour la gestion de la confiance dans l'Internet des véhicules avec Blockchain**

   La gestion de la confiance (TM) est considérée comme une mesure efficace pour résoudre les problèmes de confiance et de confidentialité dans les VANET. Liu et Huang dans [65] ont proposé un schéma de TM basé sur la Blockchain ainsi qu'un protocole d'annonce conditionnel préservant la confidentialité (appelé BTCPS) pour une communication véhiculaire sécurisée dans les VANET.

   BTCPS vise à construire un système d'annonce de TM sécurisé basé sur la réputation et préservant la vie privée pour les VANETs, dans ce système proposé il y a trois entités [65] :

   — **L**'autorité de confiance qui génère des clés basées sur l'identité et des adresses publiques (pseudonymes) pour chaque.

   — Les RSUs pour collecter les paquets d'agrégation des véhicules dans sa portée de communication pour évaluer la crédibilité des messages et mettre à jour les valeurs de réputation des véhicules.

   — Les véhicules : chaque véhicule est installé avec une unité embarquée (OBU).

   Le système est aussi composé de deux éléments [65] :

   (a) un protocole d'annonce anonyme qui maintient la fiabilité des annonces sans révéler la vie privée des véhicules dans l'environnement non entièrement fiable des VANET.

   (b) Le modèle de TM (gestion de la confiance) basé sur la Blockchain et fonctionne avec le protocole d'annonce anonyme agrégé des véhicules.

   Un algorithme de consensus mixte basé sur la preuve de travail PoW et l'algorithme PBFT a été proposé pour obtenir une meilleure efficacité par rapport aux algorithmes de consensus traditionnels de la Blockchain publique.

Le tableau 3.1 présente un résumé récapitulatif de quelques systemes de signalement présentés précédemment. Dans ce tableau, nous classifions les travaux selon les critères suivants : le type de la Blockchain, leprotocol de consensus utilisé, le mécanisme d'incitation, les techniques utilisé.

Travail	Type de la Blockchain	Protocol de consensus	Mécanisme d'incitation
ReportCoin	publique	PoW	Oui
CreditCoin	publique	PoW	Oui
BB2AR	publique	/	Oui
[63]	publique	/	Oui
[65]	publique	PoW, PBFT	Non

TABLE 3.1 – un tableau récapitulatif et comparatif entre les systemes de signalement.

3.8 Conclusion

Dans ce chapitre, nous avons passé en revue les principes fondamentaux des systèmes de signalement. Nous avons commencé par passer en revue certaines idées fondamentales, telles que la définition, l'architecture et d'un système de signalisation. Ensuit-nous avons vu leur fonctionnement, quelques avantages et inconvénients, ainsi que ses types. À la fin, nous avons conclu par un survol bibliographique sur quelques travaux des systèmes de signalements anonymes.
Dans le chapitre suivant, nous utilisant la technologie de la Blockchain pour proposer un nouveau système de signalement annonyme avec un mécanisme d'incitation pour les villes intelligentes.

CHAPITRE 4

PROPOSITION D'UN NOUVEAU SYSTÈME DE SIGNALEMENT ANONYME BASÉE SUR LA BLOCKCHAIN

4.1 Introduction

L'internet des objets est un nouvel outil de connectivité et de mobilité, qui transforme les affaires et la vie quotidienne à des objets connectés.

Les objets de notre vie de tous les jours deviennent actifs et intelligents, s'intégrant de façon transparente à un réseau mondial et sont en mesure de produire et d'échanger des données utiles. Avec l'explosion des objets intelligents, il devient important d'utilisé les technologies de l'Internet, que ça soit pour les véhicules intelligents ou pour les citoyens qui doivent collaborer ensemble pour améliorer la vie collective et la gestion de la ville intelligente. Parmi les techniques qui utilisent les technologies de l'internet pour une meilleure gestion de la ville, les systèmes de signalement qui sont des systèmes adaptable au contexte et aux besoins de la ville intelligente, mais en raison de la centralisation et du manque de motivation, les systèmes existants ont empêché les signaleurs de dénoncer ou de signaler un événement, avec l'apparition de la Blockchain, qui présente beaucoup d'intérêt par rapport à son autonomie, son anonymat et son immutabilité ainsi que la distribution des données stockées. La Blockchain a permet aux systèmes de signalement anonymes de devenir sûrs, fiables, transparents et inviolables.

Dans ce chapitre nous proposons un nouveau système de signalement anonyme avec un mécanisme d'incitation basé sur la Blockchain dans une ville intelligente. Nous commencerons par le protocole de d'annonce puis en passe au mécanisme d'incitation avant de terminer avec un modèle incitatif formel basé sur la technique de contrat theorie.

4.2 Objectifs de conception

Notre objectif est de concevoir un système de signalement anonyme sûr, fiable et inviolable pour les villes intelligentes. Notre système doit vérifier les propriétés suivantes :

— **L'anonymat :** nous utilisons la technologie d'authentification des utilisateurs pour

garantir la confidentialité des communications anonymes, les annonces et les transactions générées dans le réseau Blockchain. Ainsi, aucune information privée sur les sources du terminal mobile ne sera divulgué, ce qui répond à l'exigence d'anonymat.

— **La fiabilité :** nous utilisons la technique d'authentification par seuil et celle de la Blockchain, en faisant signer le rapport de signalement par plusieurs témoins honnêtes et nous stockant les signalements dans la Blockchain. De cette manière, chaque utilisateur peut gérer une copie de l'ensemble des chaînes de blocs de transactions, et chaque transaction est liée aux phases d'agrégation des annonces. Par conséquent, une source est incapable de nier l'envoi de messages (la non-réputation). De plus, les annonces et les transactions ne peuvent être modifiées sans l'autorisation de tous les autres utilisateurs (l'inviolabilité).

— **Les encouragements :** nous proposons un système d'incitation qui encourage et motive les utilisateurs mobiles à participer activement et efficacement au rapportement des signalements en utilisant des tokens numériques comme encourageants. Ces tokens une fois atteintes un certain seuil peuvent être converti et utilisés pour diverses situations telles que : le paiement d'une place de parking ou d'une amande. Si le signalement annoncé juste et valide, tous les utilisateurs qui ont participés au processus seront récompensés avec des degrés différents selon leur contribution.

— **La transparence et l'avertissement :** en raison des propriétés publiques et transparentes de la Blockchain, une fois que les informations de signalement anonyme sont vérifiées et confirmées avec succès, puis ajoutées à la Blockchain, peuvent être ouvertes à tout le monde, dans lequel les événements signalés serviront d'avertissement pour alerter les autres utilisateurs mobiles afin de prévenir des comportements inappropriés similaires.

4.3 Modèle du système

Nous proposons dans ce travail un système de signalement anonyme incitatif basé sur la Blockchain pour les villes intelligentes, où les utilisateurs mobiles (nous allons considères des usagers de réseaux véhiculaires e, particulier, mais notre system peut être généralisé pour d'autres cas d'utilisation) ne se connaissent pas et ne se font pas confiance. Ainsi, les utilisateurs mobiles susceptibles de participer à notre système de signalement d'un événement ne peuvent pas être distingués. En effet, même les messages doivent être transmis de manière anonyme pendant le processus de signalement, ce qui protège la confidentialité de l'identité des utilisateurs mobiles qui seront souvent des véhicules dans le scénario qu'on a choisi comme exemple de cas d'étude.Notre système comprend sept entités différentes, à savoir : le signaleur, l'événement,l'autorité de certifications, les vérificateurs et la Blockchain. En plus des administrations compétentes ainsi que les témoins, voir la figure 4.1. Leurs rôles sont décrits ci-dessous.

— **L'événement :** il représente toute situation anormale ou incident dangereux dans la ville intelligente. On peut citer à titre d'exemple, les accidents de la route, les obstacles, les vols, etc. Les utilisateurs sont mobiles et découvrent aléatoirement des événements ou des anomalies et collectent des données sensibles sur cet événement pour lancer un processus de signalement. .

— **Le signaleur :** il représente toute entité ou composante de la ville intelligente (les voitures, le citoyen, etc.) qui a la capacité d'observation et de signalement des événements aux administrations compétentes. Afin de se prémunir contre d'éventuelles vengeances ou représailles, le signaleur souhaite protéger la confidentialité de son identité tant dans la procédure de signalement que dans la procédure de récompense. Pour encourager les signaleurs à collecter des informations et à faire des signalements, nous proposons un mécanisme d'incitations dans la deuxième partie de ce chapitre.

— **L'administration compétente :** elle représente l'administration à laquelle revient l'autorité de règlement de l'évènement rapporté par le signaleur. Elle peut punir les criminels ou tout simplement intervenir pour résoudre les anomalies. L'administration si elle doute de la crédibilité des signaleurs, peut demander à certains utilisateurs appelées vérificateurs, d'aller valider le signalement avant de prendre toute action. A la fin l'autorité récompensera le signaleur et les vérificateurs s'il le signalement s'avère correcte et utile.

— **Les témoins :** ils sont des simples utilisateurs qui se trouvent dans la zone où l'événement a survenu. Le signaleur encourage les témoins à vérifier et à approuver son signalement en signant un contrat en contre parte d'un certain nombre de tockens en tant qu'encouragement. Plus des témoins signent le contrat, plus elle sera à crédibilité de signalement. Ce dernier, ne peut pas être annoncé à l'autorité si un certain seuil de signataire ne sera pas atteint.

— **Les vérificateurs :** ils sont des utilisateurs avec une bonne réputation qui se trouvent généralement dans une zone proche de l'événement signalé. Ces utilisateurs sont constamment sollicités par les administrations compétentes pour valider et confirmer les signalements en contrepartie d'un ensemble de tokens en tant qu'encouragement.

— **La Blockchain :** nous avons pensé à introduire la Blockchain pour sécuriser notre système à cause de deux raisons principales. La première est liée au fait que les réseaux basés sur la Blockchain sont ouverts et transparents, et prometteurs dans l'enregistrement des données de crédit avec les bonnes propriétés de résistance à la falsification et de décentralisation. La Blockchain convertit la confiance dans les personnes ou les institutions en confiance dans le système et toute intervention humaine sera inopérante, garantissant la fiabilité des messages de déclaration anonyme. La seconde est que la Blockchain peut fournir un meilleur mécanisme d'incitation pour encourager les utilisateurs mobiles à effectuer des déclarations anonymes sans craindre la divulgation d'informations de leurs identités [61].

— **L'autorité de certification :** elle est considérée comme une partie de confiance qui initialise le système. L'autorité de certification est responsable de la gestion, la génération et la révocation des clés de cryptage. Cette autorité est puissante et elle a un niveau de sécurité très élevé. À titre d'exemple, l'administration responsable de la gestion et la délivrance des permis de conduire ou des cartes grises des véhicules peut jouer ce rôle.

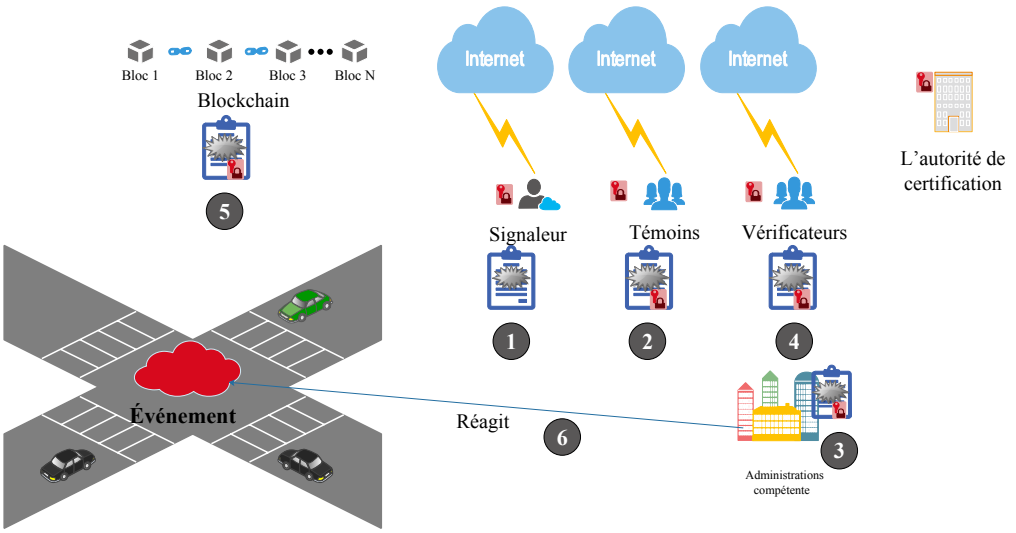


FIGURE 4.1 – les composantes du notre système de signalement étudié.

Notre système de signalement anonyme que nous avons proposé contient principalement deux parties :

— Un protocole de signalement anonyme dans un environnement non-fiable qui fournit un niveau plus élevé de confidentialité et de fiabilité pour la communication des rapports anonymes.

— Un mécanisme d'incitation basé sur la Blockchain pour encourager les utilisateurs a participé activement dans le système de signalement. Une nouvelle stratégie de points, appelés tokens est adoptée et chaque utilisateur possède un compte de crédit numérique pour stocker ses tokens.

4.4 Protocole de signalement anonyme

Dans cette partie, nous commençons par présenter notre protocole de signalement anonyme que nous appelons dorénavant PSA.

4.4.1 Mode opératoire

Le modèle du notre système est illustré dans la figure 4.2. Notre modèle est partiellement inspiré de celui proposé dans le travail [64], qu'on a amélioré en ajoutant trois autres entités : les témoins, les vérificateurs et l'autorité de certification des clés.

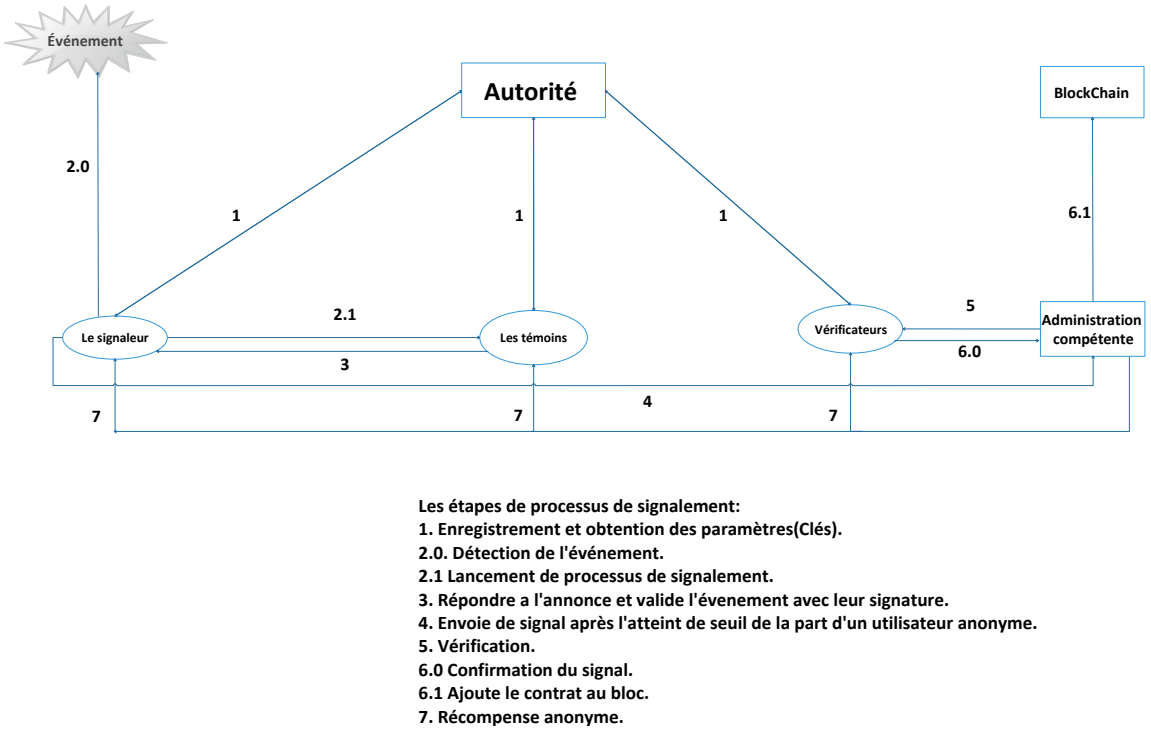


FIGURE 4.2 – le mode opératoire du système de signalement.

Le mode opératoire de notre système est représenté par :

— Au début, l'autorité distribue les clés aux utilisateurs.

— Le signaleur lance le processus du signalement.

— Les témoins participent au processus de vérification par leur réponse au signaleur.

— Après un certain seuil (S) sera atteint, le message est envoyé à l'administration.

— L'administration peut demander une vérification de la part des vérificateurs.

— Après la confirmation des vérificateurs l'administration ajoute le signal à la Blockchain et réagit pour résoudre le problème et aprés lancer le processus du récompense.

4.4.2 Type de paquets de signalement

Pour réaliser le protocole de signalement anonyme (PSA) dans la ville intelligente, les paquets de données transmis dans le réseau se présentent sous cinqu formes en fonction de leurs rôles [61, 62] :

— **Les paquets de type requête (RQT) :** ils sont générés par le signaleur et diffusés aux témoins dans un certain rayon de l'événement signalé. RQT contient un ensemble des informations de l'événement signalé tel que l'identité d'annonce (AID), le type d'annonce (RTYPE), l'horodatage, l'emplacement signalé, etc.

— **Les paquets de réponse (rQTR) :** ils sont générés par les témoins pour répondre au signaleur. Si un témoin honnête veut répondre positivement au paquet RQT, il procede à l'ajout de sa signature numérique au paquet RQT puis le renvoyer au signaleur.

— **Le paquet des rapports agrégés (AGP) :** ils sont générés par le signaleur et envoyés à l'administration compétente. Ce type de paquet contient le message de signalement et toutes les signatures de tous les témoins.

— **Le paquet de demande de vérification (ADrqt) :** ils sont générés par l'administration compétente et envoyés aux vérificateurs à proximité du lieu de l'événement pour le vérifier.

— **Le paquet de réponse de vérification (ADrqtR) :** ils sont générés par les validateurs pour répondre à la requête de l'administration compétente (i.e., si le signal est valide ou non).

4.4.3 Description des phases de lancement d'un signalement

Similaire à ce que a été proposé dans les travaux [61, 62] et afin de mieux détailler le mode opératoire de notre protocole de signalement anonyme, nous définissons un mode opératoire pour notre système autour de cinq grandes étapes qui sont brièvement décrites dans les points suivants :

1. **L'initialisation :** initialement l'autorité de certification des clés utilise la courbe elliptique pour enregistrer, générer et affecter une paire de clés (privée et public) pour chaque nouveau utilisateur de système. Ces clés seront utilisées plus tard pour le chiffrement des messages.
2. **Le signalement anonyme :** un utilisateur qui constate un événement anormale et il souhaite le signaler, il va commencer par formuler un message qui contient les détails de l'événement tel que le type d'événement, le lieu, la date, la photo de cet événement, etc. Le signaleur signe le message avec sa clé privée et diffuse ensuite ce message pour confirmation à un ensemble de témoins qui se trouvent dans une zone proche de l'emplacement de l'événement.
3. **La réponse des témoins :** après avoir reçu la requête de la part de signaleur, les témoins vérifie la signature et les informations de la requête afin de donner leurs réponses au signaleur.
4. **La vérification :** une fois, un seuil est atteint (un nombre minimum de signataire), le signaleur envoie le signalement à l'administration compétente. Cette dernière lorsqu'elle reçoit le message de la part de signaleur vérifie la signature et l'authenticité du message. Elle peut aussi lancer une étape de validation du signalement en l'envoyant à un ou plusieurs vérificateurs pour vérifications.
5. **La validation :** l'administration compétente contacte les vérificateurs afin que ces derniers valident l'événement. Si l'événement sera validé, l'administration va réagir et prendre toutes les actions nécessaires pour régler le problème.

Le tableau 4.1 montre un scénario de fonctionnement de notre système.

Phase	Etape	Signaleur	Témoins	Vérificateur	Administration compétente
Initialisation	1	Réception des clés	Réception des clés	Réception des clés	Réception des clés
Lancement de signalement	2	Faire un rapport d'un évènement et diffuse un message de signalement (RQT)	-	-	-
Réponse des témoins	3	Attendre	Vérifie l'évènement et réponde au signal (rQTR)	-	-
Agrégation des réponses des témoins	4	Envoi du message après avoir éteint le seuil des réponses (AGP)	Attendre	-	
Envoi du signal à l'administration	5	Attendre	Attendre	-	Réception d'un message de signalement (AGP), attends la validation du signal
Demand la validation du signal	6	Attendre	Attendre	Réception d'une demande de validation (ADrqt), réponde à cette demande (ADrqtR)	Attends la validité du signal.
Ajoute du signal à la Blockchain	7	Attendre la récompense	Attendre la récompense	Attendre la récompense	Ajoute le nouveau bloc à la BlockChain
La récompense	8	Réception des tokens	Réception des tokens	Réception des tokens	Réagit pour résoudre l'évènement

TABLE 4.1 – Un scénario de fonctionnement de notre système.

Les détails techniques de ces étapes sont résumés dans ce qui suit :

Étape 1-Initialisation

Pour la génération des clés, nous utilisons l'algorithme de cryptographie asymétrique ECDSA (Elliptic Curve Digital Signature Algorithm) [66] pour affecter à chaque utilisateur un couple de clés : privée et publique.

Supposons qu'il y ait n utilisateurs de terminaux mobiles, le système suit les étapes suivantes pour leurs générés les clés [61] :

1. Génèrer n nombre aléatoires de 256 bits de la chaînes d'octets $(k_1, k_2, \ldots, k_n)$ et calculer K tel que : $K_i = k_i P, i = 1, ..., n$
2. Sélectionner l'ensemble des clés privées $X = (k_1, k_2, \ldots, k_n) \leftarrow Zq*$ et définir le

vecteur des master key privées.

3. Sélectionner l'ensemble des clés public $Y = (K_1, K_2, \ldots, K_n)$ et définir le vecteur des master key public.
4. Sélectionner $SHA - 3$ comme fonction de hachage.
5. Définir (G, H, Y) comme les paramètres publics du système et diffuser ses paramètres.

En outre, les utilisateurs génères leur pseudonyme à partir de l'IMIE (International Mobile Equipment Identity) qui est défini sur le profile avec 20 octets.

Étape 2 -Signalement anonyme

Supposons que dans un scénario comprenant un événement, lorsque l'utilisateur (le signaleur) arrive à cet endroit et découvre l'événement, il suit les étapes suivantes [62, 65] :

1. Crée un message d'annonce ou de signalement (msg) anonyme qui contient :
   - Le type de l'événement.
   - L'identité du signaleur (Son pseudoname).
   - L'emplacement de l'événement (la localisation).
   - Une photo de l'évènement (optionnel).
   - L'heure et la date de l'événement.
   - Le degré de risque de cet évènement : nous définissons trois niveaux de risques :
     - 1^{er} degré : il représente tous les évènements sensibles aux délais tels que les cas d'urgence (les accidents de la route, les agressions, etc.).
     - 2^{em} degré : il représente les évènements pas urgents mais qui peuvent devenir dangereux tel que : le vandalisme d'une plaque de stop, etc.
     - 3^{em} degré : il représente les évènements non urgent ni dangereux tel que : l'effacement d'un passage de piéton, etc.
2. Sélectionner l'ensemble des ID $(ID_1, ID_2, ..., ID_{L-1})$ à l'exception de son propre ID), où la valeur de L est le nombre des utilisateurs (les témoins) qui vont s'afficher au signaleur lorsque il veut faire une sélection des témoins. Parmi ces utilisateurs mobiles, nous choisissons d'envoyer la requête de vérification aux utilisateurs les plus proches de l'emplacement de l'événement et de préférence aussi à ceux qui ont une réputation élevée.
3. Pour chaque $\in (ID_1, ID_2, ..., ID_L)$, le système génère les clés publiques (les PKI) de chaque utilisateur.
4. Pour chaque $ID_i \in (ID_1, ..., ID_L)$, le système génère la signature (Sig_i) basée sur le pseudonyme et la clé public tels que :

$$Sig_i = H(pseudonyme_i + pk_i) \tag{4.1}$$

tel que + et l'opérateur de la concaténation.

5. Choisir la valeur du seuil S et définir la requête (RQT) tels que :

$$RQT = \{< ID_1 >, \ldots, < ID_{L-1} >, msg, S, Sig_{signaleur}\} \tag{4.2}$$

6. Diffuser RQT pour inviter les témoins à confirmer l'évènement.

Etape 3 - Réponse des témoins

Après avoir diffusé la RQT initiale, le signaleur reste dans l'attente de recevoir les rQTR retournés par les témoins. Pareil comme il a été proposé dans [62], les témoins (T) effectuent les étapes suivant après la réception de RQT :

— T récupère la clé publique du signaleur $pk_{signaleur}$.

— Pour $ID_signaleur$, T vérifie l'équation suivante :

$$Sig_{signaleur} = H(pseudonyme_{signaleur} + pk_{signaleur}) \tag{4.3}$$

Si la signature de signaleur $Sig_{signaleur}$ ne satisfaite pas la relation 4.3, T n'acceptera pas la vérification de la RQT de signaleur. Si non (si elle vérifie la condition 4.3, T prend en compte la RQT puisque la signature qu'il contient le message est vérifié comme étant valide.

— T définit $m', Sig_{témoin}, pseudonyme$ comme rQTR. Ensuite, T transmet rQTR au signaleur. Tels que : $m' = msg + Sig_{témoin}$

Étape 4 -Vérification

Lorsque le signaleur reçoit les S (le seuil) rQTR, il exécute les étapes suivantes :

1. Le signaleur combine les rQTR pour générer un message agrégé (AGP) tels que :

$$AGP = \{< pseudonyme_1, m'_1 >, \ldots, < pseudonyme_S, m'_S >, S, msg, Sig_{signaleur}\} \tag{4.4}$$

2. Le signalement (AGP) sera transféré à l'administration compétente.

Lorsque l'administration compétente reçoit un AGP, elle confirme l'AGP comme suit :

1. Elle récupère et analysel'AGP.
2. Pour chaque $ID_i \in (ID_1, ..., ID_L)$, l'administration calcule :

$$V = H(pseudonyme_i + pk_i) \tag{4.5}$$

où V est la signature qu'on l'utilise pour la non répudiation des informations et elle peut empêcher la falsification de msg.

3. Pour chaque $ID_i \in (ID_1, ..., ID_L)$, l'administration vérifie la signature de chaque utilisateur(Sig_i)avec la signature qu'elle a calculé :

$$Sig_i = H(pseudonyme_i + pk_i) \tag{4.6}$$

Si le couple $< pseudonyme_i, m'_i >$ vérifie la relation 4.6, l'administration est prend en considération le msg, sinon le msg est immédiatement rejeter.

Étape 5 -validation

Après avoir validé l'authenticité de l'AGP reçu de la part du signaleur, l'administration effectue les étapes suivantes :

1. L'administration choisis les vérificateurs qui se trouvent à un endroit proche de l'événement et qui ont une réputation élevée, ce choix des vérificateurs peut-être :
   - Soit à un seul vérificateur avec une très bonne réputation. La réputation exigée doit être supérieur à un seul de confiance prédéfini.
   - Soit à un ensemble des vérificateurs de la zone de l'événement.
2. L'administration envoi aux vérificateurs concernés une requête (ADrqt).

$$ADrqt =< msg, degré, Sig_i > \tag{4.7}$$

Lorsque les vérificateurs reçoivent une ADrqt, ils confirment l'ADrqt comme suit :

- Ils analysent l' ADrqt.
- Ils vérifient la signature.
- Ils vérifient les informations de message s'il est vrai ou non, s'il est vrai ils envoient sur la requête ADrqtR une valeur rsp = true, si non ils envoient rsp = false.
- Ils envoient ADrqtR à l'administration compétente tels que :

$$ADrsp =< msg, degré, rsp, Sig_i > \tag{4.8}$$

4.4.4 construction de la Blockchain

Dans notre système, nous avons utilisé la Blockchain pour stocker de manière transparente et anonyme les événements et aussi les identités des utilisateurs de notre système. La Blockchain est aussi utilisée dans le mécanisme d'incitation pour encourager les utilisateurs à participer de manière plus active dans le processus de signalement.
La structure du bloc est décrite ci-dessous [61] :
$B = (B_h, B_t, B_u)$
Tels que :
B_h : L'en-tête de bloc
B_t : La transaction au sein du bloc (le signal)
B_u : La liste d'en-tête de bloc du nœud oncle
B_h est composé des éléments de données suivants :

1. Le numéro de bloc.
2. L'annonce (time stamp).
3. Data.
4. Le hash de bloc précédent.
5. Le hash de bloc.

La Blockchain est constituée d'un certain nombre de blocs, ce qui signifie que le nombre de blocs sur la chaîne maîtresse détermine la profondeur de la Blockchain, ce qui est illustré comme suit [61] :

$Blockchain := Block_1||Block_2||...||Block_k$

Une fois le consensus atteint, les mineurs extraient un nouveau bloc et enregistrent les transactions dans le bloc actuel, puis ajoutent le nouveau bloc à la Blockchain, en attendant une confirmation supplémentaire :

$Blockchain := Block_1||Block_2||...||Block_k||Block_{new}$

Afin d'encourager les utilisateurs à participer de manière active et efficace dans notre système de signalement, nous proposons un mécanisme d'incitation basée sur la technologie de la blockcahin. Les différents aspects de ce mécanisme d'incitation sont détaillés dans ce qui suit.

4.5 Proposition d'un mécanisme d'incitation basé sur la Blockchain pour un signalement plus efficace

Afin de résoudre le problème du manque d'enthousiasme dans le réseau de la part des signaleurs anonyme, nous proposons un mécanisme d'incitation basé sur la Blockchain. Un principe similaire à ce mécanisme a été déjà utilisé dans ReportCoin [61] et CreditCoin [62], cela en encourageant les utilisateurs mobiles à transmettre honnêtement les véritables annonces de signalement.

4.5.1 Etapes de mécanisme d'incitation

Les étapes de notre mécanisme d'incitation sont décrites dans ce qui suit :

Etape 1 - Initialisation : chaque utilisateur mobile est associé à un compte de crédit numérique indépendant (pour stocker les jetons (tokens)). Au début, un crédit de bienvenue qui est égale au nombre minimal de jetons virtuels de témoignage sera offert à chaque utilisateur pour encourager les utilisateurs de s'inscrire au système de signalement. Lors de lancement de système, on propose deux propositions pour contourner le problème manque de crédit minimum de signalement (il n'y a pas suffisamment ou il n'existe pas d'utilisateurs qui possèdent suffisamment de jetons pour lancer une alerte.) :

- Une période limitée de lancement de système ou de collecte des crédits / d'essai : ici, tous les utilisateurs ont le droit de signaler.
- Division des utilisateurs en plusieurs types avec différents degrés de confiance : ici, nous supposons que notre système contient différents types d'utilisateurs avec des degrés de confiance différents. Par exemple un véhicule spécial qui appartient aux autorités est supposé plus confiant qu'un véhicule de particulier. Aussi un véhicule de type taxi ou bus est supposé aussi plus confiant qu'un véhicule de particulier. Un véhicule de type confiant reçoit initialement un crédit minimum suffisant pour agir comme signaleur et les autres (non-confiant ou les véhicules normaux) peuvent agir uniquement comme des témoins.

Etape 2 -Lancement de signalement (alerte) : le lancement d'un signalement est payant. Cela veut dire que le signaleur va déposer un certain nombre de ses jetons afin de lancer un signalement. Si ce dernier s'avérait à la fin valide, le signaleur va gagner un nombre de jetons beaucoup plus grand que celui déposé et elle va partager une partie de ce gain avec les témoins. Dans le cas contraire, il va perdre tous les jetons déposés. Pareil pour les témoins.
Après la réception des réponses des témoins et si le seuil est attient, le signaleur génère un block candidat à l'ajout à la Blockchain qui contient toutes les informations sur l'événement ainsi que les informations sur les témoins qui ont approuvés le signalement.

Etape 3 - Réception de signalement de la part d'administration compétente : après que l'administration compétente reçoit le signalement (le block), elle va l'envoyer dans un message aux vérificateurs (validateurs). Si le signalement est validé, l'administration va ajouter le bloc à la Blockchain et elle va recevoir le gain de tous les jetons virtuels ou tokens. Nous supposons que l'administration est le nœud le plus fiable dans notre système, pour cela, l'administration va transférer tous les gains (jetons) au signaleur. Ce dernier va partager une partie de ce gain entre les témoins selon le rôle qui ont joué dans la vérification de l'événement de block. Bien sûr, le gain le plus important sera pour le signaleur.

Etape 4 : Stratégie de division des gains : dans notre stratégie d'incitation, l'administration compétente va initialement gagner tout le gain (reward, noté RWG), car il s'agit de l'entité qui va valider et ajouter le block. Après, elle va diviser ce gaine entre le(s) validateur(s) et le signaleur (l'initiateur de block). Le signaleur après va aussi partager une partie de son gain avec les témoins.

$$Ona : RWG = \alpha + \beta + \Omega \tag{4.9}$$

Tel que :

- α est le gain de signaleur.
- β est le gain total des témoins.
- Ω est le gain de(s) validateur(s) (auditeur(s)).

Sachant que $\alpha > \beta > \Omega$, $\alpha = \beta + \Omega$ et $\alpha >> \beta > \Omega$

Cela veut dire que le plus grand gain sera attribué au signaleur (par exemple 50% de gain). Après les témoins et les validateurs vont partager le reste du gain avec une petite préférence aux témoins. Par exemple 30% pour l'ensemble des témoins et 20% pour le(s) validateurs. Évidemment, dans notre application, on va laisser le choix à l'administrateur de notre système pour fixer de manière dynamique ces pourcentages de partage des gains.

Les utilisateurs mobiles peuvent convertir les jetons en services pour payer par exemple une place de parking ou une amende.

Si les jetons d'un utilisateur ne sont pas dépensés après une durée prédéfinie, une partie des pièces sera disparaître.

Après la validation de block par le validateur (l'administration compétente). Le block sera ajouté à la Blockchain et il sera diffusé pour une mise à jour de la Blockchain au niveau de tous les endroits de stockage répartie sur les RSUs et/ou les stations de base de réseaux cellulaires.

4.5.2 Stratégie de consensus

La stratégie de consensus Proof of Stake (PoS) à une meilleure évolutivité, c'est-à-dire une vitesse de traitement des transactions plus rapide, et la validation d'un bloc ne repose pas sur de puissants calculs algorithmiques qui consomment beaucoup d'énergie comme le cas de la stratégie Proof of Work (PoW).

Pour notre système de signalement, nous choisissons Delegated Proof of Stack (DPoS) comme algorithme de consensus, qui est une amélioration de PoS. DPoS est plus rapide que PoS et utilise moins d'énergie par rapport à PoS.

DPoS est plus adapté au partage sécurisé des données entre les pairs. Pour qu'il suit nous allons détaillér les étapes de DPoS appliqué à notre mécanisme d'incitation sont décrits dans ce qui suit [54, 67] :

Étape 1 -Initialisation du système : dans notre Blockchain, l'algorithme de signature numérique basé sur la courbe elliptique et la technique de la cryptographie asymétrique sont adoptées lors de l'initialisation du système. Chaque nouvelle entité devient légitime après avoir passé l'authentification de l'identité par l'autorité de confiance (Trusted Authority, TA). Chaque entité légitime obtient ses clés publiques et privées et le certificat correspondant pour le cryptage et le décryptage des informations. Une composante de système (le signaleur ou l'administration) qui souhaite être candidat à un poste de mineur (l'entité qui va gérer la création, la vérification et l'ajout d'un bloc) soumit tout d'abord ses informations d'identité à l'TA. Cette dernière n'accepte que les entités légitimes comme mineurs candidats.

Étape 2 - Adhésion du candidat mineur : chaque candidat mineur soumis un dépôt de stackes (Une partie de ces jetons virtuels (tokens)) sur un compte sous surveillance publique après avoir été candidat mineur. Ce dépôt sera confisqué par le système de Blockchain si le candidat a un comportement malveillant et cause des dommages pendant le processus de consensus, par exemple en ne produisant pas de bloc dans son créneau horaire.

Étape 3 - Calcul de la réputation : les parties prenantes peuvent calculer la réputation de tous les candidats mineurs. La réputation de chaque utilisateur est représentée par le nombre de tokens qu'il procède dans son compte. Ces tokens augmentent et diminuent après chaque participation au processus de signalement. Toute participation honnête et non falsifiée, l'utilisateur gagne des tokens à la fin de consensus par contre il perd une partie de ces tokens pour chaque participation frauduleuse ou malveillante.

Étape 4 - Sélection des mineurs (validateurs) : selon la réputation calculée à

l'étape 3, nous choisissons comme mineurs toutes les entités de système (les utilisateurs) qui possède une réputation supérieur ou égale à celle du signaleur actuel. Cela veut dire, les utilisateurs avec un nombre de tokens supérieur ou égale le nombre de tokens de signaleur seront choisis comme ensemble de mineurs actifs, les autres utilisateurs seront considérés comme des mineurs de réserve.

Étape 5 - Génération du gestionnaire de bloc : les mineurs actifs vont jouer à tour de rôle le rôle de gestionnaire de bloc pendant k tranches de temps du processus de consensus. Comme dans les schémas de consensus DPoS traditionnels, chaque mineur actif joue le rôle de gestionnaire de bloc pour effectuer la génération, la diffusion, la vérification et la gestion des blocs dans son intervalle de temps. Au début, le signaleur lance un signal aux témoins et devenir le premier gestionnaire de bloc avec un time slot qui égale au temps minimal de la réception des témoignages (une période de temps prédéfinie). Après la fin de la période de témoignage, si le seuil de témoignage est atteint, le signaleur envoi le bloc à l'administration compétente et cette dernière devient le nouveau gestionnaire de bloc avec un time slot égale au temps minimale nécessaire pour vérifier le bloc. Après, la fin de temps de vérification et si l'événement s'avère fiable, le bloc sera ajouté à la Blockchain par l'administration compétente et l'information sera diffusée à toutes les composantes de système pour mettre à jour leur copie de la blcokchain.

Étape 6 - Processus de consensus : dans un intervalle de temps, le gestionnaire de blocs génère d'abord un bloc non vérifié, puis diffuse ce bloc aux autres mineurs actifs pour vérification. Cependant, en raison du nombre limité de mineurs actifs, des mineurs actifs, malveillants peuvent lancer une attaque par collusion pour générer de faux résultats de vérification de blocs. Dans l'étape de vérification des blocs, plus il y a de vérificateurs, plus le réseau Blockchain est sécurisé. Par conséquent, pour se défendre contre cette attaque et améliorer encore les performances de sécurité du schéma de consensus DPoS proposé, un plus grand nombre de vérificateurs sont motivés et incités à participer à la vérification des blocs au lieu des seuls mineurs actifs qui terminent la vérification. En d'autres termes, les mineurs, y compris les mineurs actifs et les mineurs de réserve, peuvent agir comme vérificateurs et participer au processus de vérification des blocs, en particulier les mineurs à forte réputation, ce qui peut empêcher la collusion de vérification des blocs entre les mineurs actifs.

Étape 7 - Récompense et sanction : à la suite du processus de consensus, si le bloc et validé par les vérificateurs, le bloc sera ajouté à la Blockchain et l'administration compétente gagne la récompense. Après, elle va distribuer cette récompense à tous les participants au processus de signalement. Par contre, si le bloc ne sera pas validé les participants(le signaleur, les témoins et le validateur) perdent leurs tokens qui ont déjà soumis pour avoir le droit de participer au processus de signalement.

Pour encourager les témoins les plus fiables (avec une réputation élevée) à participer dans l'opération de vérification de block (ou l'événement), nous proposons un modèle d'incitation formel en utilisant la théorie des contrats comme outil de modélisation. Le modèle basé sur la théorie de contrat va servir aussi à distribuer les gains entres les vérificateurs.

À l'inverse des travaux existants (cités dans la fin du chapitre 3) qui répartit les gains entre les vérificateurs de manière égale quelque que soit leur degré de participation, notre système utilise un model basé sur la théorie des contrats afin de répartir les gains entre les témoins chacun selon sa participation (celui répond le plus vite reçoit plus de gain). Le modèle incitatif est détaillé dans la section suivante.

4.5.3 Approche basée sur la théorie des contrats pour l'incitation des témoignes de signalement

Sur la base du mécanisme d'incitation à la vérification de signalement présenté ci-dessus, nous considérons un scénario pratique avec des informations asymétriques au sein duquel les témoins peuvent être de différents types (différents depgrés de réputation) et ils sont inconnus du signaleur.

La théorie des contrats est une théorie économique qui décrit comment des personnes et des organisations établissent des accords juridiques dans des situations caractérisées par des conditions incertaines, des facteurs d'incertitude et une asymétrie d'information . Dans notre système, le contrat est décomposé de deux entités le signaleur qui va créer le contrat et les témoins qui vont signer ce contrat.

— **Le signaleur (contract designer) :** c'est lui qui va créer le contrat dans le but d'encourager les témoins pour un témoignage juste et rapide. Pour chaque témoin de type θ_k le signaleur définit un ensemble de contrats (R_k, L_k^{-1}) qui contient les informations de l'événement signalé, ici R_k et la récompense correspondante et L_k représente la latence de la vérification d'un bloc.

— **Les témoins :** qui sont classés de façon descendante selon leur réputation, c'est eux qui vont signer les contrats. Tout témoin qui réponde juste pendant un délai fixé par le signaleur, il sera recomposé le temps de réponse, le premier qui va répondre, prendre plus que le 2 ième et ainsi de suie. Et tout réponse qui le délai sera automatiquement ignoré et le contrat refusé.

4.5.3.1 Type des témoins

Nous définissons le type de témoin comme une représentation de sa réputation et sa volonté de participer à l'opération de vérification. Nous supposons qu'il existe au total N témoins de différents types et nous désignons l'ensemble des types par $\theta = \{\theta_1, ..., \theta_k, ..., \theta_N\}$. Tel que :

$$\theta_k = \alpha r_k + \beta D_k \tag{4.10}$$

Nous utilisons la réputation définie dans l'équation (4.10) pour représenter les types des témoins [68] qui sont triés par ordre croissant comme suivant $\theta_1 \leq ... \leq \theta_k \leq ... \leq \theta_N, \theta_k \in \{1, \ldots, N\}$. Un type supérieur implique une plus grande réputation par rapport au témoin d'un type inférieur. Veuillez noter qu'il s'agit d'un environnement d'information asymétrique où les valeurs exactes des types de témoin sont des informations privées [68], [69]. En effet, les informations véridiques de réputation sont nécessaires au signaleur pour

définir les contrats qui optimisent le bénéfice des témoins pour participer à l'opération de vérification. Ici, notre objectif est deconcevoir des contrats qui incitent les témoins de participer de manière honnête, juste et rapide. De ce fait, au lieu de fournir un contrat uniforme à tous les témoins, le signaleur propose un ensemble de contrats selon le type θ de témoin. Il est laissé à libre choix des témoins d'accepter ou de refuser tout type de contrats. Si un témoin refuse de vérifier (signer le contrat), ou il accepte de vérifier (il a signé) le contrat et l'envoyer avec un délai supérieure de L^{-1}, nous supposons que le témoin reçoit un contrat (R_1, L_1^{-1}) tel que le gain est nul $R_1 = 0$.

4.5.3.2 Modèle des utilités

Dans cette sous-section, nous présentons la fonction d'utilité de signaleur et des témoins basée sur le contrat signé. La fonction d'utilité est exprimée comme une fonction générale, telle que : Utilité = Gain - Coût [68].

1. **Utilité du signaleur**
   La fonction d'utilité de signaleur peut être définie par le gain qui va gagner à la fin de l'opération (reward) moins le coût qui va distribuer aux témoins, on not que :

$$U_s = G_s - C_s \tag{4.11}$$

   tel que G_s c'est le gain (reward) et C_s c'est le Coût.

   Le signaleur peut estimer la probabilité (ϕ_k) qu'un témoin appartienne au type- k malgré l'asymétrie de l'information qui peut être indiquée par ϕ_k et elle doit satisfaire la condition $\sum_{k=1}^{N} \phi_k = 1$. Dans ce travail, nous supposons que tous les types des témoins ont une probabilité égale à $\phi_k = 1/N$ [54, 70].

   Le Coût d'un signaleur représenté par les récompenses qui oufrir aux témoins qui participe avec lui dans un délai fixé L^{-1}. On note le Coût de signaleur C_s par :

$$C_{sk} = lR_k \tag{4.12}$$

   Où l est un paramètre de pondération prédéfini par rapport à l'incitation R_k du témoin de type k.

   Le gain du signaleur lié au type θ_k qui mesure le degré de satisfaction du signaleur. Le signaleur obtient un bénéfice plus élevé lorsque le θ_k est plus grand. En outre, un plus grand nombre de témoin avec une réputation élevée et une latence faible peuvent conduire à un type θ_k plus élevé. Un plus grand nombre de témoins participants peut conduire à une étape de vérification des blocs plus sûre [54]. Il est calculé par la fonction suivante :

$$G_s = \phi_k \theta_k L_k^{-1}, \forall L > 0 \tag{4.13}$$

   La fonction d'utilité globale de signaleur peut être formulée comme suit :

$$U_{SK} = \phi_k(\theta_k L_k^{-1} - lR_k) \tag{4.14}$$

L'objectif du signaleur est de maximiser son profit par la vérification des blocs comme suit :

$$argmax_{(R_k, L_k^{-1})} U_{Sk} = \sum_{k=1}^{N} \phi_k(\theta_k L_k^{-1} - lR_k), \forall L > 0 \tag{4.15}$$

2. **Utilité des témoins**

Pour un témoin de type θ_k, la fonction d'utilité de la vérification de blocs basée sur un contrat signé est représentée comme dans [70] par les récompenses reçues R_k moins le coût de ressources consommés es pour vérifier un bloc. On note :

$$U_T = R_{Tk} - C_{Tk} \tag{4.16}$$

Le gain de témoin noté par R_{Tk} représente le reword qui va gagner à la fin de cette opération. Il est calculé par la fonction suivante :

$$R_{Tk} = \theta_k \psi(R_k) \tag{4.17}$$

Tel que $\psi(R_k)$ est une fonction d'évaluation monotone croissante du témoin de type k en fonction de l'incitation [54]. L'évaluation est nulle lorsqu'il n'y a pas d'incitation, c'est-à-dire $\psi(0) = 0$.

Le Coût d'un témoin représente par les ressources qu'il perdre pendant cette opération de vérification. Nous définissons un paramètre l' qu'il va mesurer les ressources qui vont consommer par le témoin en termes d'énergie de calcul, etc. pour la vérification des blocs. Il est calculé par la fonction suivante [54] :

$$C_{Tk} = l' L_k^{-1} \tag{4.18}$$

Donc la fonction d'utilité d'un témoin de type k peut être désormais donnée par :

$$U_T(k) = \theta_k \psi(R_k) - l' L_k^{-1} \tag{4.19}$$

Tel que $\psi(R_k) = log(1 + R_k)$. elle va augmenter rapidement et aprés plus faiblement.

Le témoin de type k le plus élevé devrait avoir une utilité plus grande en raison de sa réputation plus élevée dans la vérification des blocs. Cependant, le témoin veut maximiser son utilité en minimisant la consommation de ressources dans la vérification des blocs. Plus précisément, l'objetctif du témoin de type θ_k est de maximiser l'utilité obtenue en rejoignant la vérification de bloc [54], exprimée par

$$argmax_{(R_k, L_k^{-1})} U_T(k) = \theta_k \psi(R_k) - l' L_k^{-1}, k \in \{1, \ldots, N\} \tag{4.20}$$

4.5.3.3 Solution de contrat

Dans cette sous-section, nous cherchons à formuler le contrat optimal qui va nous aider à réaliser et diviser la récompense entre les témoins chaucun selon son degré de contribution dans la vérification de contrat (le délai de répense et la i.e., réputation). Premièrement, nous décrivons les contraintes nécessaires qui peuvent garantir la faisabilité du contrat. Ensuite, nous formulons le problème de maximisation d'utilité de système basé sur les contraintes des faisabilités. Enfin nous cherchons à simplifier et calculer les valeurs optimales $(R_k, L_k^{-1})^*$.

A) **Contraintes de faisabilité d'un contrat**
Pour inciter les témoins à collaborer avec le signaleur dans la vérification d'un événement signalé, le contrat qu'un témoin a sélectionné doit respecter les contraintes de faisabilité qui sont la rationalité individuelle et la compatibilité de l'incitation pour tous les types de témoins [71].

1 - **Définition 4.1. La rationalité individuelle (Individual Rationaluty, IR) :** elle signifie que chaque témoin va accepter la vérification du bloc lorsqu'il recevra une utilité non négative. Le témoin choisit devrait garantir que son utilité soit toujours positive par rapport à son type [54,68]. IR peut-être exprimé comme suit :

$$U_T(k) = \theta_k \psi(R_k) - l^{'} L_k^{-1} \geq 0, k \in \{1, ..., N\} \tag{4.21}$$

Les contrats proposés par le signaleur doivent apporter des utilités non négatives aux témoins, ce qui encourage les témoins à participer activement au processus de témoignage. Il est défini dans la théorie des contrats que chaque témoin est rationnel. Il n'acceptera pas un contrat s'il reçoit une utilité négative pour son type.

2 - **Définition 4.2. Compatibilité incitative (Incentive Compatibility, IC) :** IC signifie qu'un témoin ne peut pas gagner plus d'utilité en acceptant une entrée de contrat qui n'est pas conçue pour son type [68]. IC être exprimé comme suit :

$$\theta_k \psi(R_k) - l^{'} L_k^{-1} \geq \theta_k \psi(R_{k'}) - l^{'} L_{k'}^{-1}, k, k' \in \{1, ..., N\}, k \neq k' \tag{4.22}$$

B) **Problème d'optimisation des contrats**
Au-delà des contraintes IR et IC et comme dans les travaux [68] et [54], le signaleur conçoit plusieurs contrats et chaque témoin choisit le bon contrat qui optimise son utilité. L'objectif du signaleur est de maximiser son utilité en offrant les entrées de contrat optimale $(R_k, L_k^{-1})^*, k \in \{1, \ldots, N\}$. Donc la conception du contrat optimal peut être formulée comme un problème de maximisation de l'utilité du signaleur,

comme suit [54] :

$$
\begin{aligned}
&(R_k, L_k^{-1})^* = argmax_{(R_k, L_k^{-1})} \sum_{k=1}^{N} \phi_k(\theta_K L_k^{-1} - lR_k) \\
&\text{S.}C.\ IR(4.21) : \theta_k \psi(R_k) - l^{'} L_k^{-1} \geq 0, k \in \{1, ..., N\} \\
&\text{IC}(4.22) : \theta_k \psi(R_k) - l^{'} L_k^{-1} \geq \theta_k \psi(R_{k'}) - l^{'} L_{k'}^{-1}, k, k' \in \{1, ..., N\}, k \neq k' \\
&\text{m}ax\{L_k\} \leq T_{max}, k \in \{1, \ldots, N\} \\
&\sum_{k=1}^{N} \psi(R_k) \leq R_{max}(k) \in \{1, \ldots, N\}
\end{aligned}
\tag{4.23}
$$

Ou T_{max} : est le seuil maximum de vérification en terme de temps.
et R_{max} : est la récompense totale de vérification des transactions (blocs ou évènement) par les utilisateurs de la Blockchain.

C) **Résolution de contrat optimal**

La principale difficulté pour résoudre le problème décrit à l'équation (4.23) est qu'il existe un grand nombre de contraintes IR et IC (k pour les contraintes IR et $k \times (k-1)$ pour les contraintes IC). Par conséquent, pour rendre (4.23) plus simple, nous simplifions premièrement les contraintes IR et IC, puis nous résolvons le problème.

i . **Simplification de contrat**

Afin de résoudre le problème dans (4.23), nous devons simplifier les contraintes IR et IC avant de les résoudre. En suivant la méthode standard décrite dans [68, 71], nous simplifions ces contraintes.

Lemme 1 : pour la solution optimale, étant donné que l'IC est satisfaite, la contrainte IR pour le type le plus bas est une liaison, c'est-à-dire :

$$\theta_1 \psi(R_1) - l^{'} L_1^{-1} = 0 \tag{4.24}$$

Preuve 1 : on a par définition des types des témoins : $\theta_1 \leq ... \leq \theta_k \leq ... \leq \theta_N$ Aussi, d'après les contraintes d'IC dans (4.23), nous avons $\theta_k \psi(R_k) - l^{'} L_k^{-1} \geq \theta_k \psi(R_1) - l^{'} L_1^{-1} \geq \theta_1 \psi(R_1) - l^{'} L_1^{-1}$. Tant que $\theta_k \psi(R_k)$ augmente strictement avec θ_k et si la contrainte d'IR de témoin de type 1 est satisfaite alors : $\theta_1 \psi(R_1) - l' L_1^{-1} > 0$. De plus, du point de vue de signaleur, afin de maximiser son profit, le signaleur souhaite obtenir une latence plus petite autant que possible. En fixant $\theta_1 \psi(R_1) - l' L_1^{-1} = 0$, le signaleur obtient le bénéfice maximal. Par conséquent, la condition dans (4.23) sera vérifiée lorsque le contrat est optimal.
Les contraintes IR peuvent être réduites par le lemme 1, qui indique que la latence pour le type le plus bas θ_1 doit être égal à l'évaluation du récompense R_1, c'est-à-dire, les gains de type θ_1 le plus faible ne réalisent aucun bénéfice, tandis que les bénéfices des autres témoins sont supérieurs à ceux du type θ_1 [68, 71]. Ensuite, nous prouverons que la contrainte IC : peut être réduite dans les lemmes suivants :

Lemme 2 : pour tout contrat (R_k, L_k^{-1}) de type θ_k : $R_k > R_{k'}$ si et seulement si $\theta_k > \theta_{k'}$ et $R_k = R_{k'}$ si et seulement si $\theta_k = \theta_{k'}$.
Preuve 2 : selon la contrainte d'IC, nous avons :

$$\theta_k \psi(R_k) - l^{'} L_k^{-1} \geq \theta_k \psi(R_{k'}) - l^{'} L_{k'}^{-1} \tag{4.25}$$

Et

$$\theta_{k'} \psi(R_{k'}) - l^{'} L_{k'}^{-1} \geq \theta_{k'} \psi(R_k) - l^{'} L_k^{-1} \tag{4.26}$$

Elle peut être réécrit comme :

$$\theta_k \psi(R_k) - \theta_{k'} \psi(R_{k'}) \geq l^{'} L_k^{-1} - l^{'} L_{k'}^{-1} \tag{4.27}$$

Et

$$\theta_{k'} \psi(R_{k'}) - \theta_{k'} \psi(R_k) \geq l^{'} L_{k'}^{-1} - l^{'} L_k^{-1} \iff \theta_{k'} \psi(R_k) - \theta_{k'} \psi(R_{k'}) \leq l^{'} L_k^{-1} - l^{'} L_{k'}^{-1} \tag{4.28}$$

En combinant les équations ci-dessus, nous avons :

$$\theta_k \psi(R_k) - \theta_k \psi(R_{k'}) > \theta_{k'} \psi(R_k) - \theta_{k'} \psi(R_{k'}) \tag{4.29}$$

$$\theta_k \psi(R_k) - \theta_k \psi(R_{k'}) - \theta_{k'} \psi(R_k) - \theta_{k'} \psi(R_{k'}) > 0 \tag{4.30}$$

$$(\theta_k - \theta_{k'})(\psi(R_k) - \psi(R_{k'})) > 0 \tag{4.31}$$

1) Si $\theta_k > \theta_{k'}$ alors : $R_k > R_{k'}$. $R_k > R_{k'}$ Cela implique $\theta_k > \theta_{k'}$. En divisant l'équation de (4.31) par $(\theta_k - \theta_{k'})$ il reste $(\psi(R_k) - \psi(R_{k'})) > 0$, Tant que $\psi(R_k)$ augmente strictement avec le type k, alors $\psi(R_k) > \psi(R_{k'})$ cela implique $R_k > R_{k'}$.

2) Si $R_k > R_{k'}$. Alors $\theta_k > \theta_{k'}$ Similaire au premier cas, nous commençons par la contrainte (4.31). Comme $R_k > R_{k'} > 0$ et $\psi(R_k)$ augmente strictement avec R_k nous pouvons déduire que $\psi(R_k) > \psi(R_{k'})$ Par conséquent, on obtient $\theta_k - \theta_{k'} > 0$, Ainsi, nous avons prouvé que $\theta_k > \theta_{k'}$ si et seulement si $R_k > R_{k'}$.

En utilisant la même méthode, nous pouvons facilement prouver que $\theta_k = \theta_{k'}$ si et seulement si $R_k = R_{k'}$. Cela implique que R_k augmente de façon monotone. Avec le type θ_k lorsque le contrat satisfait aux contraintes d'IC. Comme conclusion, nous pouvons dire qu'un témoin de type élevé devrait recevoir plus de récompense qu'un témoin de type faible. Si les deux témoin reçoivent les même récompense, ils doivent appartenir au même type, et vice-versa [68, 71]. Donc : Si $\theta_1 \leq ... \leq \theta_k \leq ... \leq \theta_N, \quad \theta_k \in \{1, \ldots, N\}$. Alors :

$$0 \leq R_1 \leq ... \leq R_{k'} \leq ... \leq R_N \tag{4.32}$$

Lemme 3 : si le contrat satisfait aux contraintes de IC, la condition suivante est vraie $R_k > R_{k'}$, si et seulement si $L_k^{-1} > L_{k'}^{-1}$.

Preuve 3 : si le contrat satisfait les contraintes d'IC indiquées en (4.22), c'est-à-dire : $\theta_{k'}\psi(R_{k'}) - l^{'}L_{k'}^{-1} \geq \theta_{k'}\psi(R_k) - l^{'}L_k^{-1}$, $k \neq k'$ qui peut être réécrit comme suit : $\theta_{k'}\psi(R_{k'}) - \theta_{k'}\psi(R_k) \geq l^{'}L_{k'}^{-1} - l^{'}L_k^{-1}$; Puisque $\theta_k\psi(R_k)$ est une fonction croissante par rapport à R_k et si $R_k > R_{k'}$ alors $\theta_{k'}\psi(R_{k'}) - \theta_{k'}\psi(R_k) < 0$; cela implique que $L_{k'}^{-1} - L_k^{-1} < 0$ donc $L_k^{-1} > L_{k'}^{-1}$
D'après le lemme 2 et le lemme 3, nous concluons que : « dans un contrat réalisable, un témoin d'un type supérieur θ_k peut gagne rune récompense R_k plus grande.
En combinant les lemmes 2 et 3, nous constatons que les conditions nécessaires aux contraintes d'IC, compte tenu des types $\theta_1 \leq ... \leq \theta_k \leq ... \leq \theta_N$ sont $0 \leq R_N \leq ... \leq R_{k'} \leq ... \leq R_N$ et $0 \leq L_1^{-1} \leq ... \leq L_k^{-1} \leq ... \leq L_N^{-1}$. Par conséquent nous pouvons facilement déduire ce qui suit :

$$0 \leq U_T(1) \leq ... \leq U_T(k) \leq ... \leq U_T(N) \tag{4.33}$$

Les témoins de type supérieur reçoivent plus d'utilité que les témoins de type inférieur. Si un témoin sélectionne le contrat conçu pour un type élevé, même s'il reçoit plus de récompense, le profit qui peut gagner ne peut pas compenser Par rapport à ce qui le perdu. Un témoin peut recevoir l'utilité maximale si et seulement s'il sélectionne le contrat qui convient le mieux à sa préférence. Ainsi, nous pouvons garantir que le contrat est honnetement révélé.

D'après [70] et pareil comme dans [71], les contraintes IC contiennent deux types de contraintes. La contrainte entre le type θ_i et le type θ_j, $j \in \{1, \ldots, i-1\}$ est appelée Downward Incentive Contraints (DIC). En particulier, la contrainte entre le type θ_i, et le type θ_{i-1}, est appelée Local Downward Incentive Contraints (LDIC). Au même temps, les contraintes entre les systèmes de type θ_i et de type θ_j, $j \in \{i+1, \ldots, N\}$ est appelé Up Ward Incentive Contraints (UIC), et la contrainte entre le type θ_i et le type θ_{i+1} est appelée Local Up Ward Incentive Contraints (LUIC).
Tout d'abord, nous montrons que les contraintes DICs peuvent être réduites [71] :

Lemme 4. (Réduire les contraintes LDIC (Local Downward Incentive Contraints)) : si les contraintes LDIC sont satisfaites pour un type θ_k de témoin, c'est-à-dire :

$$\theta_k\psi(R_k) - l^{'}L_k^{-1} \geq \theta_k\psi(R_{k-1}) - l^{'}L_{k-1}^{-1}, k \in \{1...N\} \tag{4.34}$$

Alors les contraintes d'IC seront valables pour tout $k' \leq k$, donc :

$$\theta_k\psi(R_k) - l^{'}L_k^{-1} \geq \theta_{k'}\psi(R_{k'}) - l^{'}L_{k'}^{-1} \tag{4.35}$$

Preuve 4 : nous avons deux contraintes LDIC comme suit :

$$\theta_k\psi(R_k) - l^{'}L_k^{-1} \geq \theta_k\psi(R_{k-1}) - l^{'}L_{k-1}^{-1} \tag{4.36}$$

$$\theta_{k-1}\psi(R_{k-1}) - l^{'}L_{k-1}^{-1} \geq \theta_{k-1}\psi(R_{k-2}) - l^{'}L_{k-2}^{-1} \tag{4.37}$$

$$\theta_{k-1}(\psi(R_{k-1}) - \psi(R_{k-2}) \geq l^{'}L_{k-1}^{-1} - l^{'}L_{k-2}^{-1} \tag{4.38}$$

Nous avons $\theta_k \geq \theta_{k-1}$ donc :

$$\theta_k(\psi(R_{k-1}) - \psi(R_{k-2})) \geq \theta_{k-1}(\psi(R_{k-1}) - \psi(R_{k-2})) \geq l^{'}L_{k-1}^{-1} - l^{'}L_{k-2}^{-1} \tag{4.39}$$

De plus, on a de (4.39) :

$$\theta_k(\psi(R_{k-1})-\psi(R_{k-2})) \geq l^{'}L_{k-1}^{-1}-l^{'}L_{k-2}^{-1} \iff \theta_k\psi(R_{k-1})-l^{'}L_{k-1}^{-1} \geq \theta_k\psi(R_{k-2})-l^{'}L_{k-2}^{-1} \tag{4.40}$$

On a :

$$\theta_k\psi(R_k) - l^{'}L_k^{-1} \geq \theta_k\psi(R_{k-1}) - l^{'}L_{k-1}^{-1} \tag{4.41}$$

Et,

$$\theta_k\psi(R_{k-1}) - l^{'}L_{k-1}^{-1} \geq \theta_k\psi(R_{k-2}) - l^{'}L_{k-2}^{-1} \tag{4.42}$$

Alors :

$$\theta_k\psi(R_k) - l^{'}L_k^{-1} \geq \theta_k\psi(R_{k-2}) - l^{'}L_{k-2}^{-1} \tag{4.43}$$

Par conséquent, si pour le témoin de type $k-1$, le LDIC détient la contrainte d'incitation par rapport au type $k-2$. Ce processus peut être étendu vers le bas du type $k-2$ à 1. Ce qui prouve toutes les contraintes LDICs. Compte tenu de la sélection aléatoire de θ, nous avons terminé la preuve [72].
Ensuite, nous montrons que toutes les contraintes UIC peuvent être réduites [71, 72] :

Lemme 5 (Réduire les contraintes LUIC (Local UpWard Incentive Contraints)) : si les contraintes LUICs sont satisfaites pour tous les types θ_k des témoins, c'est-à-dire,

$$\theta_k - \psi(R_k) - l^{'}L_k^{-1} \geq \theta_k\psi(R_{k+1}) - l^{'}L_{k+1}^{-1}, k \in \{1...N\} \tag{4.44}$$

Alors les contraintes d'IC seront valables pour tout $k < k'$, c'est-à-dire,

$$\theta_k\psi(R_k) - l^{'}L_k^{-1} \geq \theta_k\psi(R_{k'}) - l^{'}L_{k'}^{-1} \tag{4.45}$$

Preuve 5. la preuve est la même que lemme 4.

Lemme 6. (pour réduire les contraintes d'IC) : pour maximiser les bénéfices du signaleur, les contraintes d'IC peuvent être remplacées par :

$$\theta_k\psi(R_k) - l^{'}L_k^{-1} = \theta_k\psi(R_{k-1}) - l^{'}L_{k-1}^{-1} \tag{4.46}$$

Lemme 7 : soit (R_k, L_k^{-1}) un contrat réalisable, alors l'unique latence optimal

satisfait

$$(L_1^{-1})^* = \frac{\theta_k \psi(R_1)}{l'} \tag{4.47}$$

$$(L_k^{-1})^* = (L_{k-1}^{-1})^* + \frac{\theta_k(\psi(R_1) - \psi(R_{k-1})}{l'} \tag{4.48}$$

Preuve 7. compte tenu la récompense est fixe, l'utilité du signaleur est donc décidée par $\sum_{i=1}^{N} \phi_{i=1} \theta_i L_i^{-1}$ Supposons qu'il existe une autre latence possible $\{L_k^{-1'}, \forall k\}$ qui est considéré comme meilleure solution que $\{L_k^{-1*}, \forall k\}$ dans (4.48) Ainsi, il y a au moins une latence $L_k^{-1'} > L_k^{-1*}$ pour un type θ_k.

1) Si k = 1 : alors $(L_1^{-1})' > (L_1^{-1})^*$ et $(L_1^{-1})^* = (l^{-1})' \theta_k \psi(R_1)$. Par conséquent $(L_1^{-1})' > (l^{-1})' \theta_k \psi(R_1)$ qui ne respecte pas les contraintes IR pour le type θ_1.

2) Si k > 1 :$\{(L_k^{-1})', \forall k\}$ doit satisfaire le LDIC (4.35) alors :
$\theta_k \psi(R_k) - l'(L_k^{-1})' \geq \theta_k \psi(R_{k-1}) - l'(L_{k-1}^{-1})'$ ce qui implique : $(L_k^{-1})' \leq (L_{k-1}^{-1})' + l'^{-1} \theta_k(\psi(R_k) - \psi(R_{k-1}))$
En remplaçant $(L_k^{-1})^* = (L_{k-1}^{-1*}) + l'^{-1} \theta_k(\psi(R_k) - \psi(R_{k-1}))$ dans cette expression de comparaison $(L_k^{-1})' \leq (L_{k-1}^{-1})' + l'^{-1} \theta_k(\psi(R_k) - \psi(R_{k-1}))$ nous obtenons $(L_{k-1}^{-1})' \geq (L_{k-1}^{-1})^*$ qui implique par induction $(L_1^{-1})' \geq (L_1^{-1})^*$ qui ne respecte pas les contraintes IR pour le type θ_1 . Avec la démonstration par l'absurde, nous obtenons (4.48).
Après la simplification de (4.48), nous pouvons conclure que :

$$(L_k^{-1})^* = (l^{-1})'(\theta_1 \psi(R_1) + \sum_{i=2}^{k} W_i), \forall k \in \{1...N\} \tag{4.49}$$

Ou
$W_i = \left\{ \begin{array}{ll} 0 & \text{si i=1} \\ \theta_i(\psi(R_i) - \psi(R_{i-1}) & \text{si i=2 ... k} \end{array} \right\}$

ii . **Optimalité du contrat**
Compte tenu des contraintes de faisabilité d'un contrat, nous formulons ci-après le problème d'optimisation du système. En utilisant les lemmes dans la sous-section précédente, le problème d'optimisation dans (4.23) peut être réécrit comme :

$$\begin{array}{l} (R_k, L_k^{-1})^* = argmax_{(R_k, L_k^{-1})} \sum_{k=1}^{N} \phi_k \theta_k l^{-1}(\theta_1 \psi(R_1) + \sum_{i=2}^{k} W_i) - \phi_k l R_k \\ \text{S}C : 0 \leq R_1 \leq ... \leq R_{k'} \leq ... \leq R_N \\ \text{I}R(4.24)\ \theta_1 \psi(R_1) - l^{'} L_1^{-1} = 0 \\ \text{I}C(4.46)\ \theta_k \psi(R_k) - l^{'} L_k^{-1} = \theta_k \psi(R_{k-1}) - l^{'} L_{k-1}^{-1} \\ max\{L_k^{-1}\} \leq T_{max}, k \in \{1, \ldots, N\} \\ \sum_{k=1}^{N} \psi(R_k) \leq R_{max}(k) \in \{1, \ldots, N\} \end{array} \tag{4.50}$$

Où

$$W_i = \left\{ \begin{array}{ll} 0 & \text{si, i=1} \\ \theta_i(\psi(R_i) - \psi(R_{i-1}) & \text{si, i=2 ... k} \end{array} \right. \tag{4.51}$$

Afin de résoudre le problème (4.50), une approche standard consiste à ignorer la condition de monotonie (4.32) dans un premier temps, puis de vérifier si la solution remplit cette condition [72, 73]. Après avoir supprimé la condition de monotonie, on peut réécrire le problème d'optimisation en (4.50) comme suite

$$\begin{array}{l} (R_k, L_k^{-1})^* = argmax_{(R_k, L_k^{-1})} \sum_{k=1}^{e} U_s(k) \\ \text{S}C : 0 \leq R_1 \leq ... \leq R_{k'} \leq ... \leq R_N \\ \text{I}R(4.24)\ \theta_1 \psi(R_1) - l^{'} L_1^{-1} = 0 \\ \text{I}C(4.46)\ \theta_k \psi(R_k) - l^{'} L_k^{-1} = \theta_k \psi(R_{k-1}) - l^{'} L_{k-1}^{-1} \\ max\{L_k^{-1}\} \leq T_{max}, k \in \{1, \ldots, N\} \\ \sum_{k=1}^{N} \psi(R_k) \leq R_{max}, (k) \in \{1, \ldots, N\} \end{array} \tag{4.52}$$

Tel que :

$$U_s(k) = \phi_k l'^{-1} \theta_k((N-i)\psi(R_k)(\theta_k - \theta_{k+1})) - \phi_k l R_k \tag{4.53}$$

Nons calculons les dérivées partielles par rapport à R_k tel que k = 1,...,N

$$\frac{dU_s(k)}{dR_k} = (\phi_k l'^{-1} \theta_k((N-i)\psi(R_k)(\theta_k - \theta_{k+1})) - \phi_k l R_k)' \tag{4.54}$$

$$= \frac{\phi_k l'^{-1} \theta_k((N-i)\psi(R_k)(\theta_k - \theta_{k+1})) - \phi_k l R_k}{R_k} \tag{4.55}$$

Nous calculons la deuxième dérivée du signaleur par rapport à R_k :

$$\frac{d^2 U_s(k)}{d^2 R_k} = \frac{(\phi_k l'^{-1}((N-i)(\theta_k(\theta_k - \theta_{k+1})) - \phi_k l R_k}{R_k})" \tag{4.56}$$

$$\frac{d^2 U_s(k)}{d^2 R_k} = \frac{\phi_k l'^{-1}((N-i)(-\theta_k(\theta_k + \theta_{k+1}))}{R^2}) \tag{4.57}$$

$\frac{d^2 U_s(k)}{d^2 R_k} > 0$

Preuve : On a : $N > i$ et $N, \phi_k, \theta_k, l'^{-1} > 0$ Alors : $N\phi_k l'^{-1}(N-i) > 0$

D'après le lemme de la sous-section précédente on a : $\theta_{k+1} > \theta_k$
Donc : $N\phi_k l'^{-1}\theta_k(N-i)(-\theta_k + \theta_{k+1}) > 0$

Alors : $\frac{N\phi_k l'^{-1}\theta_k(N-i)(-\theta_k + \theta_{k+1})}{R^2} > 0$

Alors : $U_s(k) > 0$. On'a $U_s(k) > 0$ donc la fonction d'utilité de signaleur est une fonction convexe par rapport à $R_k, \forall k$. Le problème d'optimisation dans (4.52), est un problème d'optimisation convexe standard, qui peut être résolu par la méthode du multiplicateur lagrangien [68], [72] et [73]. Nous construisons la

fonction de Lagrange comme sui [75] :

$$L = \sum_{k=1}^{N} u_s k + (\partial^1 \sum_{k=1}^{N} R_k - 1) + \sum_{k=1}^{N} (\partial_k^2 R_k) \tag{4.58}$$

Où :∂ et ∂_k^2 sont les multiplicateurs de Lagrange.La valeur optimale du gain (R_k^*) est obtenue en appliquant la condition de Karush-Kuhn-Tucker. Pour cela, il suffit de mettre la première dérivée de L = 0. Ici R_k^*,k={1,2...,N} sont des solutions de :

$$\begin{cases} U_s'(k) + \partial^1 + \partial_k^2 = 0, & \forall k \in \{1, ..., N\} \\ \partial^1(\sum_{k=1}^{N} R_k - 1) = 0 & \\ \partial_k^2 R_k = 0, & \forall k \in \{1, ..., N\} \end{cases} \tag{4.59}$$

Où $U_s'(k)$ est la dérivée de premier ordre de $U_s(k)$ par rapport à R_K^*. En outre, nous devons vérifier si ces solutions sont réalisables. Si R_k^* satisfait à la condition de monotonie satisfait à la condition de monotonie (4.33) et les lemme(2) et (3), elle peut être considéré comme notre quantité optimale $R_k^* = R_k*, \forall k \in 1, ..., N$. Sinon, nous devons faire quelques ajustements, qui sont basés sur la proposition suivante [72, 75] :

Proposition : Soit $X_1(x)$ et $X_2(x)$ des fonctions concaves sur x. Si $\overline{x_1} \leq \overline{x_2}$ ou $\overline{x_1} = argmax_{x1} X_1(x)$ et $\overline{x_2} = argmax_{x2} X_2(x)$ alors $\overline{x_1} = \overline{x_2}$ Où :

$$\overline{x_1}, \overline{x_2} = argmax_{x_1,x_2} \sum_{i=1}^{2} X_i(x_i), S.C. x_1 \geq x_2 \tag{4.60}$$

Preuve : la preuve de la proposition est donnée dans [74].
La proposition peut être étendue à une forme plus générale : si $\overline{x_1} \geq \overline{x_2} \geq \overline{x_3} \geq ... \geq \overline{x_N}$ Où $\overline{x_k} = argmax_{x_1,x_2} \sum_{k=1}^{N} X_K(x_k)$ alors $\overline{x_1} = \overline{x_2} = ... = \overline{x_e}$ Où :

$$\overline{x_k} = argmax_{x_k} \sum_{k=1}^{e} X_k(x_k) s.c. x_1 \leq x_2 \leq ... \leq x_N \tag{4.61}$$

On note une sous-séquence de $(\overline{R_k^*})$ disons $(\overline{R_i^*}, \overline{R_{i+1}^*}, ...\overline{R_j})$ comme sous-séquence irréalisable, Si $\overline{R_i*} \geq \overline{R_i^*} \geq ... \geq \overline{R_j}$, par exemple : dans une récompense $\overline{R_k^*}$ = {1,3,3,2,6,5} il y a deux sous-séquences possibles, c'est-à-dire $\overline{R_1^*}, \overline{R_2^*}, \overline{R_3^*}$ et $\overline{R_5^*}, \bar{R}_6^*$ Selon la proposition 1, les valeurs ajustées satisfont $\overline{R_i^*} = \overline{R_{i+1}^*}...\overline{R_j^*}$. De plus, il devrait maintenir les contraintes d'appartenance à un type, c'est-à-dire :

$$\phi_i R_i^* + \phi_{i+1} R_{i+1}^* + ... + \phi_j R_j^* = \phi_i \overline{R_i^*} + \phi_{i+1} \overline{R_{i+1}^*} + ... + \phi_j \overline{R_j^*} \tag{4.62}$$

Donc :

$$R_i^* = R_{i+1}^* = ... = R_j^* = \frac{\phi_i \overline{R_i^*} + \phi_{i+1} \overline{R_{i+1}^*} + \phi_j \overline{R_j^*}}{\phi_i + \phi_{i+1} + ... + \phi_j} \tag{4.63}$$

En substituant la récompense optimale R_i^* en (4.49) nous obtenons la latence

optimal correspondant L_k^{-1*} comme suit :

$$L_k^{-1*} = l'^{-1}(\theta_1\psi(R_1) + \sum_{i=2}^{M} W_i^*), \quad \forall k \in \{1...n\} \tag{4.64}$$

pour k = {1,...,n}

$$W_i^* = \left\{ \begin{array}{ll} 0 & \text{si i=1} \\ \theta_i(\psi(R_i^*) - \psi(R_{i-1}^*) & \text{si i=2 ... k} \end{array} \right\} \tag{4.65}$$

Dans ce qui suit, nous donnons dans l'algorithme 1 l'ensemble des étapes qui permet le calcul de contrat optimal.

Algorithm 1 Algorithme de calcul de contrat optimal

Entrée : $N, \phi_k, \theta = \{\theta_1, \theta_2, ..., \theta_N\}$

Sortie : R, L^{-1}

Debut

i. **Pour chaque type {k = 1,...,N} Faire**

A. Calculer :
$U_s(k) = \phi_k l'^{-1}\theta_k((N-i)\psi(R_k)(\theta_k - \theta_{k+1})) - \phi_k l R_k$

B. Calculer :
$$R_i^* = \left\{ \begin{array}{ll} U_s'(k) + \partial^1 + \partial_k^2 = 0, & \forall k \in \{1, ..., N\} \\ \partial^1(\sum_{k=1}^{N} R_k - 1) = 0 & \\ \partial_k^2 Rk = 0 & , \forall k \in \{1, ..., N\} \end{array} \right.$$

FinPour.

ii. **Tant que R_i^* n'est pas faisable**

A. Trouver une sous-séquence infaisable $(\overline{R_i^*}, \overline{R_{i+1}^*}, ...\overline{R_j})$

B. Calculer $R_i^* = R_{i+1}^* = \dfrac{\phi_i\overline{R_i^*} + \phi_{i+1}\overline{R_{i+1}^*} + \phi_j\overline{R_j^*}}{\phi_i + \phi_{i+1} + ... + \phi_j}$

Fin Tant que.

iii. **Pour k = 1...N Faire**

A. Calculer $W_i = \left\{ \begin{array}{ll} 0 & \text{si, i=1} \\ \theta_i(\psi(R_i) - \psi(R_{i-1}) & \text{si, i=2, ... ,k} \end{array} \right.$

B. Définir : $L_k^{-1*} = l'^{-1}(\theta_1\psi(R_1) + \sum_{i=2}^{k} W_i)$

Fin pour

Fin.

4.6 Conclusion

Dans ce chapitre, nous avons proposé un nouveau système de signalement anonyme incitatif basé sur la technologie de la BlockChain. Notre système est composé de deux parties, dans la première partie qui contient le protocole d'annoncement ou bien le mécanisme de signalement, on a détaillé tout étapes pour le faire. Après, dans la deuxième partie, on a passé au mécanisme d'incitation pour incité les utilisateurs a participer, puis on a proposé une approche basée sur la théorie des contrats pour encourager les témoins à participer dans notre système. Nous avons décrit les fonctions d'utilité. Après, nous avons basé sur la condition d'optimisation contrainte de Karush-Kuhn- Tucker pour calculer les valeurs optimales du contrat. Et après, nous avons terminé par un algorithme pour définir le contrat optimal.
Dans le chapitre suivant nous présenterons l'implémentation de notre système de signalement annonyme basé sur la Blockchain.

CHAPITRE 5

IMPLÉMENTATION

5.1 Introduction

Dans ce chapitre, nous présentons l'implémentation de notre système de signalement qui représente la dernière étape de notre travail. Notre système est représenté par une application mobile sous android studio. Nous allons essayer de montrer les principaux éléments de notre application. Nous commençons d'abord, par une brève illustration de l'environnement de travail ainsi que l'ensemble des logiciels, utilisés dans la réalisation du système, ensuite en passe à présenter une conception de notre application par des diagrammes de séquence, puis nous passerons à un aperçu des interfaces de notre application.

5.2 Présentation des outils utilisés

Cette section présente les différents outils matériels et logiciels utilisés, tout le long de l'implémentation du projet.

5.2.1 Outils logiciels

5.2.1.1 Android Studio

Android Studio est l'environnement intégré (IDE) officiel pour le développement d'applications Android. Il peut être téléchargé sous les systèmes d'exploitation Windows, macOS, Chrome OS et Linux. En tant qu'environnement de développement intégré officiel de Google, Android Studio inclut tout ce dont le développeur besoin pour développer une application : un éditeur de code et un déboguer intelligents, des outils d'analyse des performances, des émulateurs, etc. Android Studio permet principalement d'éditer les fichiers Java et Kotlin et les fichiers de configuration XML d'une application Android. La figure 5.1 présente le logo de l'android studio.

FIGURE 5.1 – le logo d'android studio

5.2.1.2 Firebase

Firebase est une plateforme de développement d'applications mobiles de Google dotée de puissantes fonctionnalités pour le développement, la manipulation et l'amélioration des applications. Elle permet de développer rapidement des applications pour mobiles et pour le web. Elle est créée en 2011 par James Tamplin et Andrew Lee. Firebase n'est pas seulement une base de données, Il n'y a vraiment aucune limite aux types d'applications qui peuvent être aidées par les produits Firebase. Il n'y a que des limites aux plates-formes, sur lesquelles elle peut être utilisée. IOS et Android sont les principales cibles des SDK Firebase, nous avons utilisé cette plateforme dans notre application pour stocker les données des utilisateurs et des administrations. La figure 5.2 présente le logo de Firebase.

FIGURE 5.2 – le logo de Firebase.

5.2.1.3 Java

Java est à la fois un langage de programmation informatique orienté objet et un environnement d'exécution informatique portable créé par James Gosling et Patrick Naughton employés de Sun Microsystems, présenté officiellement le 23 mai 1995 au SunWorld. Le langage Java à la particularité principale que les logiciels écrits avec ce dernier sont très facilement portables sur plusieurs systèmes d'exploitation. Le langage reprend en grande partie la syntaxe du langage C++, très utilisé par les informaticiens. La figure 5.3 présente le logo de Java.

FIGURE 5.3 – le logo de JAVA.

5.2.1.4 XML

XML est un langage de structuration de document orienté texte, formé de balises, tags qui permettent d'organiser les données de maniere structuré. Chacune de ces balises définit le rôle et le sens des informations contenues dans le document décrit. XML est particulièrement souple et puissant. Il offre en effet la possibilité de définir des balises personnelles. Il est ainsi tout à fait possible de bâtir son propre métalanguage métier en incluant les spécificités propres à chaque secteur.

5.2.1.5 Entreprise Architect

Est un outil graphique multi-utilisateurs conçu pour aider les développeurs à construire des systèmes robustes et maintenables. Et en utilisant des rapports et une documentation intégrée de haute qualité, vous pouvez offrir une vision vraiment partagée facilement et avec précision, nous avons utilisé cet outil pour construire les diagrammes de séquences pour donner une idée de fonctionnement de notre application.

5.2.1.6 SDK Android

Le SDK Android (kit de développement logiciel) est un ensemble d'outils de développement utilisés pour développer des applications pour la plate-forme Android.

5.2.1.7 SDK Firebase

Le SDK Firebase (kit de comunication avec Firebase) est un API qui permet de conecter l'application android avec Firebase.

5.2.1.8 Bouncy Castle

Une implémentation java des algorithme cryptographique, les package est organisé de manière a contenue une API qui peut être utiliser dans n'importe quel environnement.

5.2.2 Outils matériels

Dans la réalisation de notre projet, nous avons utilisé nos deux ordinateurs portables personnels et nos smart-phones avec des caractéristiques qui sont présentées dans le tableau 5.1.

Caractéristique	PC 1	PC 2	Téléphone 1	Téléphone 2
Processeur	Intel Core I3-5005U CPU@2.00Ghz	Intel Core I3-6100U CPU @2.30Ghz	Intel MT6737 1.3 Ghz	SoC Exynos 7870 Ghz
RAM	4 Go	4 Go	2 Go	3 Go
Disque dure	500 Go	500 Go	16 Go	32 Go
Système d'exploitation	LuniX	Windows 10 X64bits	Android 6	Android 10

TABLE 5.1 – Caractéristiques des machines utilisées.

5.2.3 Spécification détaillée

Nous allons maintenant détaillée les étapes de notre application par des diagrammes de séquence (DSS). L'objectif du diagramme de séquence est de représenter les interactions entre les objets en indiquant la chronologie des échanges.

A) **DSS d'inscription (ajouter un compte)**

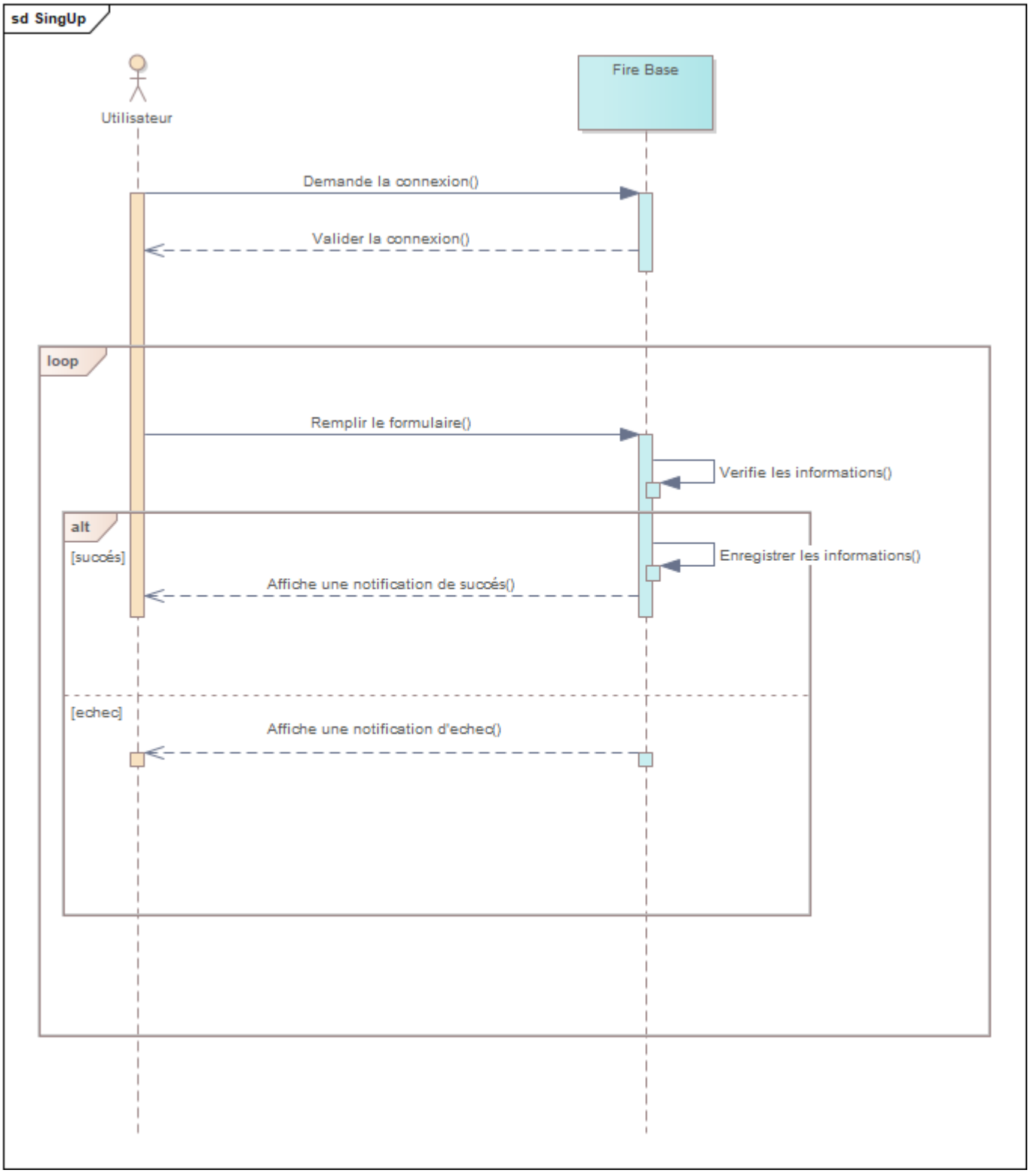


FIGURE 5.4 – DSS d'inscription.

B) **DSS d'authentification**

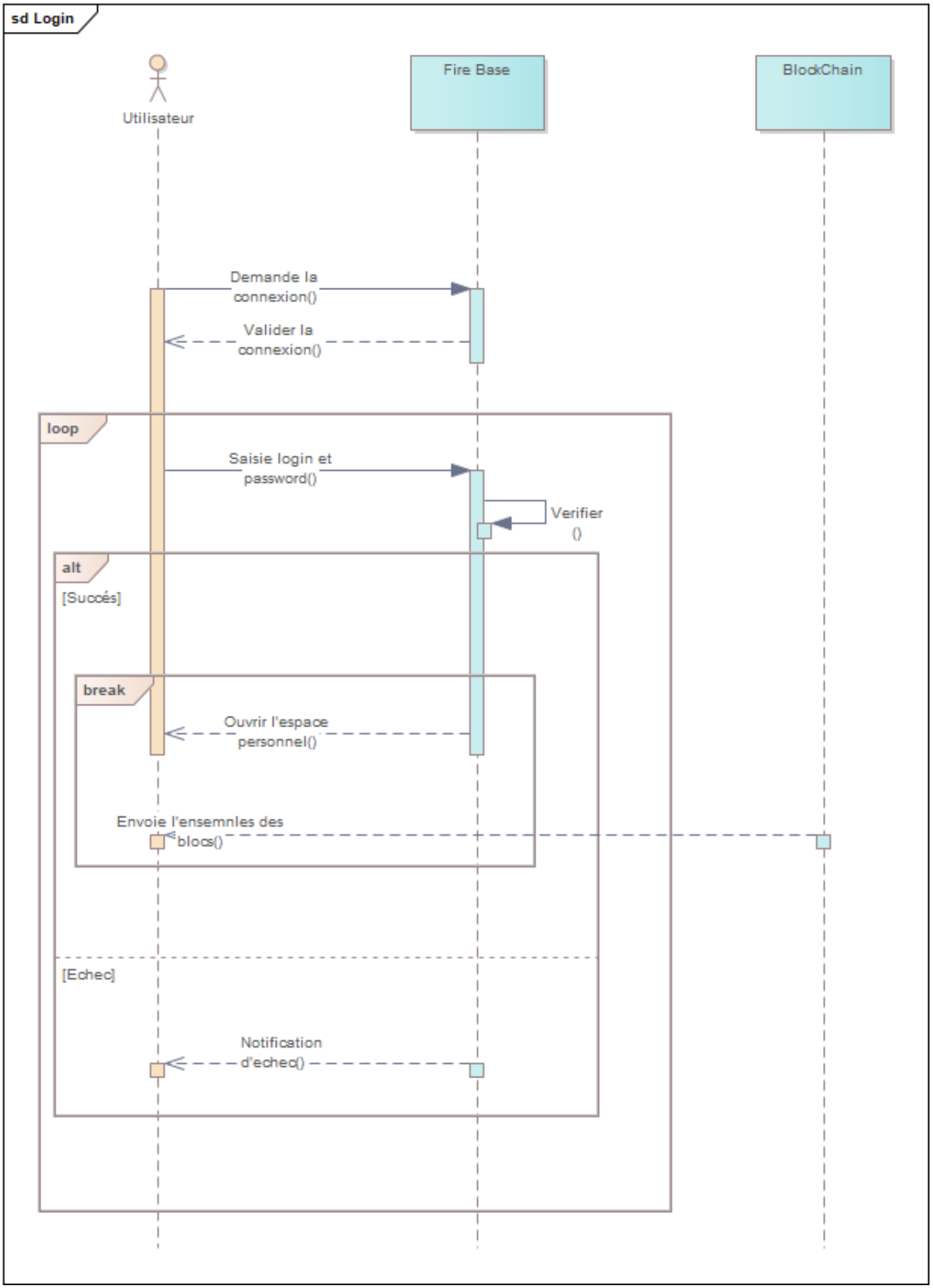


FIGURE 5.5 – DSS d'authentification.

C) **DSS d'ajout d'un signalement**

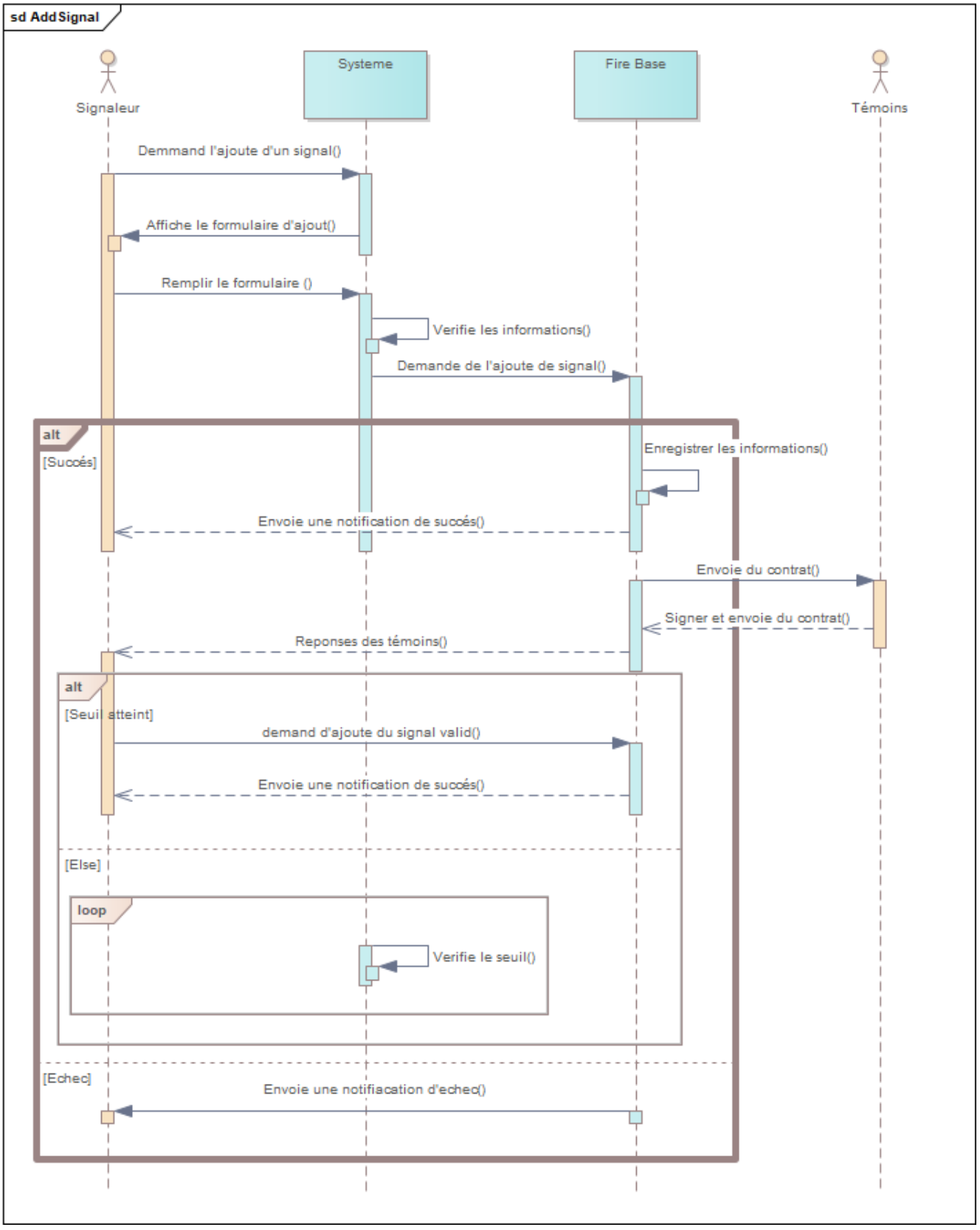


FIGURE 5.6 – DSS d'ajout d'un signalement.

D) **DSS d'ajout le signalement à la Blockchain**

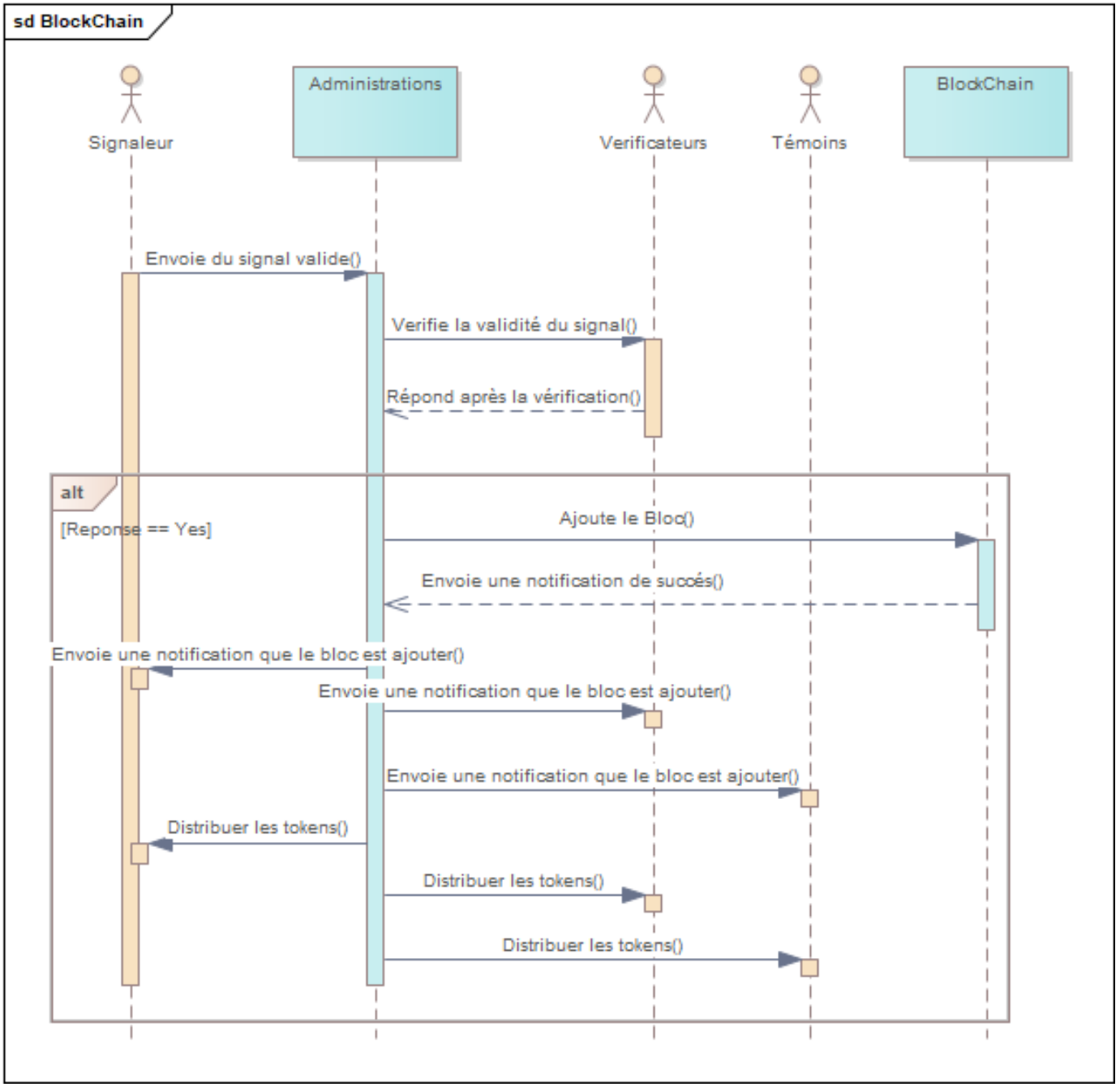


FIGURE 5.7 – DSS d'ajout le signalement à la Blockchain.

5.2.4 Présentation des IHMs

Notre application permet aux utilisateurs de signaler des événements qui se déroule dans la ville intellgente tels que : les accidents, les agressions, les problèmes de la route, etc. d'une manière anonyme et transparente. Un utilisateur peut être un signaleur, ou un témoin ou un validateur, chaque signal valide et juste va permettre à l'utilisateur qui a participé au conssesus de signalement d'être récompensé avec des tokens.

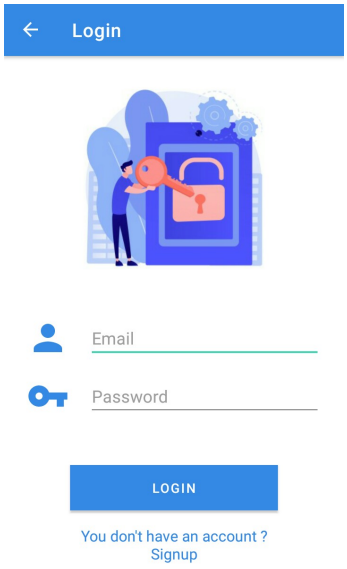
L'application comporte deux parties : une partie mobile destinée uniquement aux citoyens et une partie mobile pour l'administrateur, pour qu'il puisse modifier les paramètres de système.

Dans ce qui suit, nous allons détailler les interfaces de notre application mobile développée sous la plateforme android. Notre application est composée de deux IHM principaux dont chacune représente l'espace personnel de l'utilisateur (signaleur, témoins, vérificateur), et de l'administration compétente, ainsi qu'une application super-User dédiée à l'administrateur du système pour qu'il puisse modifier les paramètres du système. Dans cette partie, nous allons présenter les IHMs les plus importantes de notre application.

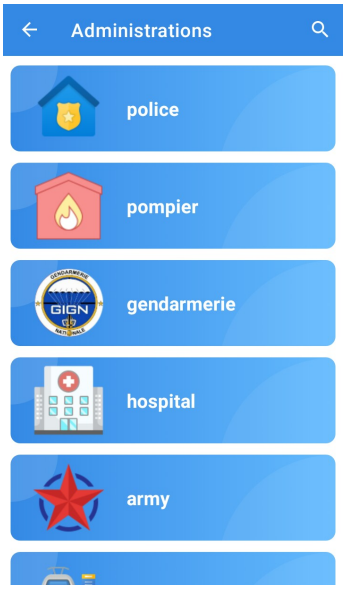
1) **IHM d'utilisateur et de l'administration compétente :** l'application possède une interface qui demande de choisir entre l'espace utilisateur et l'espace administration, la figure 5.8 représente cette interface.

FIGURE 5.8 – Fenêtre d'accueil de notre application mobile.

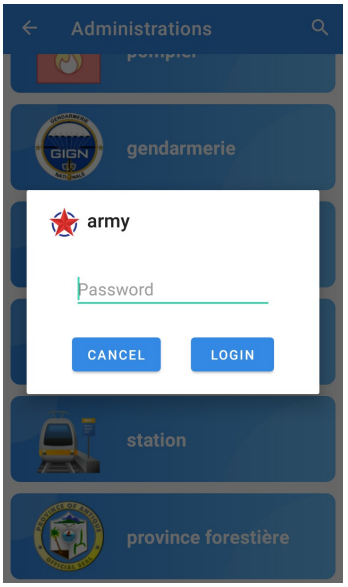
2) **IHM login de l'administration et des utilisateurs :** l'utilisateur se trouve sur l'IHM représenté dans la figure 5.9a , et l'administration se trouve sur les IHMs représentées dans les figures ci-dessous (les figures 5.9b et 5.9c) avant de saisir le mot de passe chaque utilisateur de l'administration doit choisir l'administration qu'il le concerne, apres l'interface de la saisie vas s'afficher à partir des quelles il peut accéder à son espace. Si le Nom ou le mot de passe sont erronés le système affiche une alerte, sinon il va ouvrir l'espace personnel.



(a) IHM login de l'utilisateur.



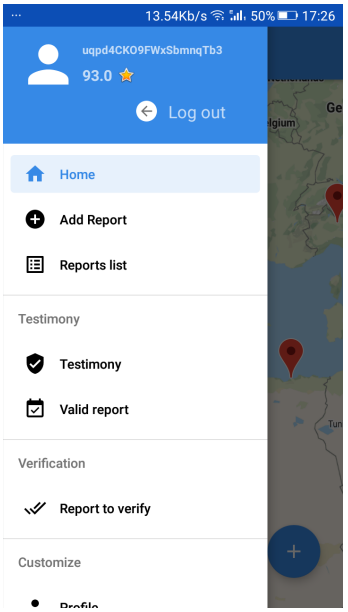
(b) IHM login de l'administration.



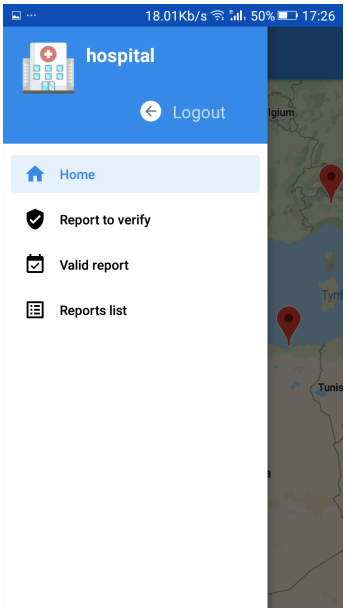
(c) IHM login de l'administration.

FIGURE 5.9 – IHM login administration et des utilisateurs.

3) **IHM de profile de l'administration et des utilisateurs :** l'image 5.10 présente les deux interfaces de l'utilisateur et de l'administration compétente. Chaque interface contient un menu et une Map qui contient les signalements déjà ajoutés à la Blockchain, lorsque on clique sur un signalement une fenêtre de dialogue s'affiche, cette fenêtre contient les informations du signalement.



(a) IHM de profile de l'administration



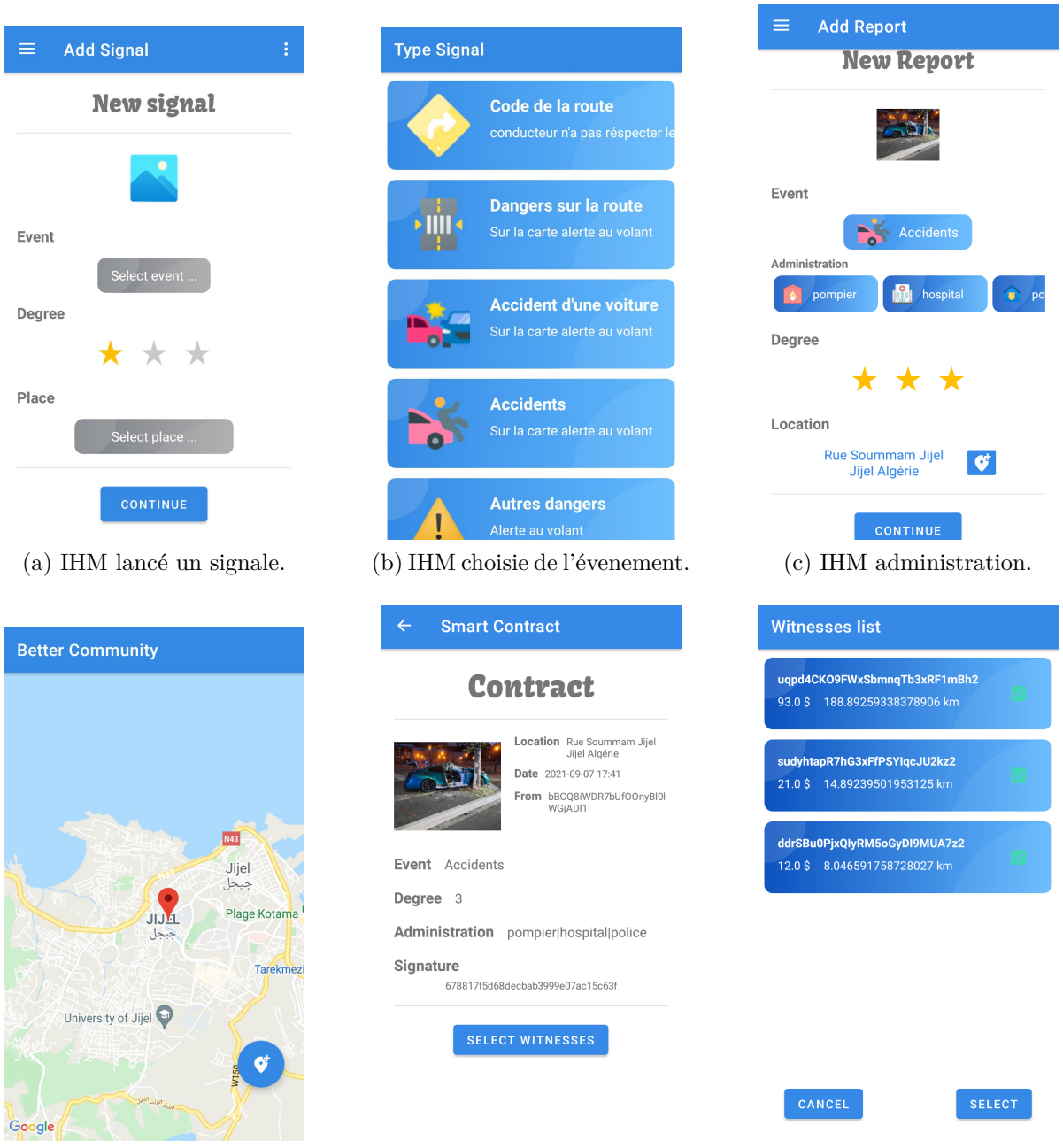
(b) IHM de profile des utilisateurs

FIGURE 5.10 – IHM de profile de l'administration et des utilisateurs.

4) **IHM d'ajout d'un signalement :** à partir de cette interface (voir la figure5.11a)

l'utilisateur peut lancer un signal, pour cela, il choisit un événement 5.11b dont les administrations responsables de cet événement seront sélectionnées automatiquement 5.11c, il peut choisir une image de l'événement (facultatif) que ça soit une image existante ou il peut prendre une image sur place, puis il doit sélectionner le lieu de l'événement 5.11d et le degré de danger de cet événement.

Une fois le signaleur clique sur le bouton continu , un contrat de signal s'affiche (voir la figure 5.11e) qui contient toutes les informations du signalement ainsi que le pseudo Name du signaleur et sa signature et la date de ce signalement. Le signaleur doit faire une sélection des témoins selon leur réputation et leur distance comme (voire la figure 5.11f), ce nombre des témoins est spécifié par l'administrateur du système (super-User).



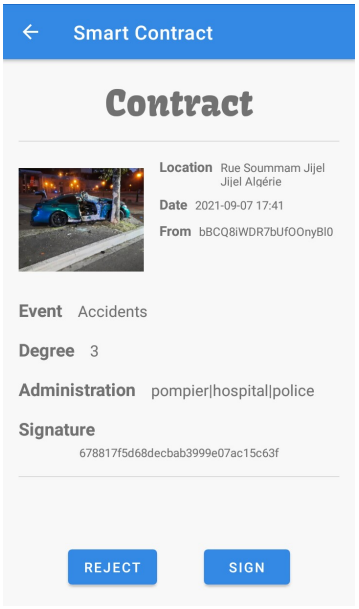
(a) IHM lancé un signale. (b) IHM choisie de l'évenement. (c) IHM administration.

(d) IHM GPS. (e) IHMdu contrat de signale. (f) IHM des témoins séléctioné.

FIGURE 5.11 – IHM d'ajout d'un signalement

5) **IHM témoignage :** Chaque témoin sélectionné va recevoir une notification lui indiquant qu'il est choisi par un signaleur à être témoin (voir la figure 5.12a), s'il accepte de participer, il aura un contrat à signer, sinon il rejet le contrat (5.12b).

(a) Reception d'une notification

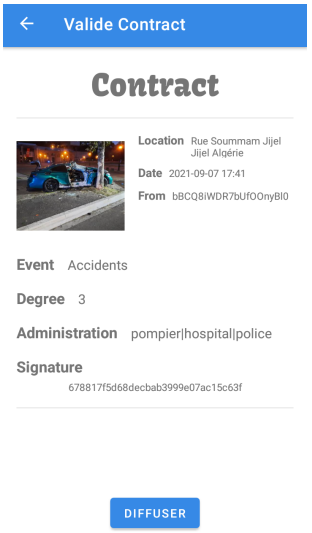


(b) L'acceptation ou le refus du contrat

FIGURE 5.12 – IHM de témoignage.

6) **IHM de l'envoi du signal à l'administration :** les témoins envoient leurs accord au signaleur, ce dernier attend une notification qui lui permet de savoir que le threchold est atteint 5.13a (nombre des témoins participé avec lui), puis il envoi le signal à administration compétent (voire la figure 5.13b).

(a)

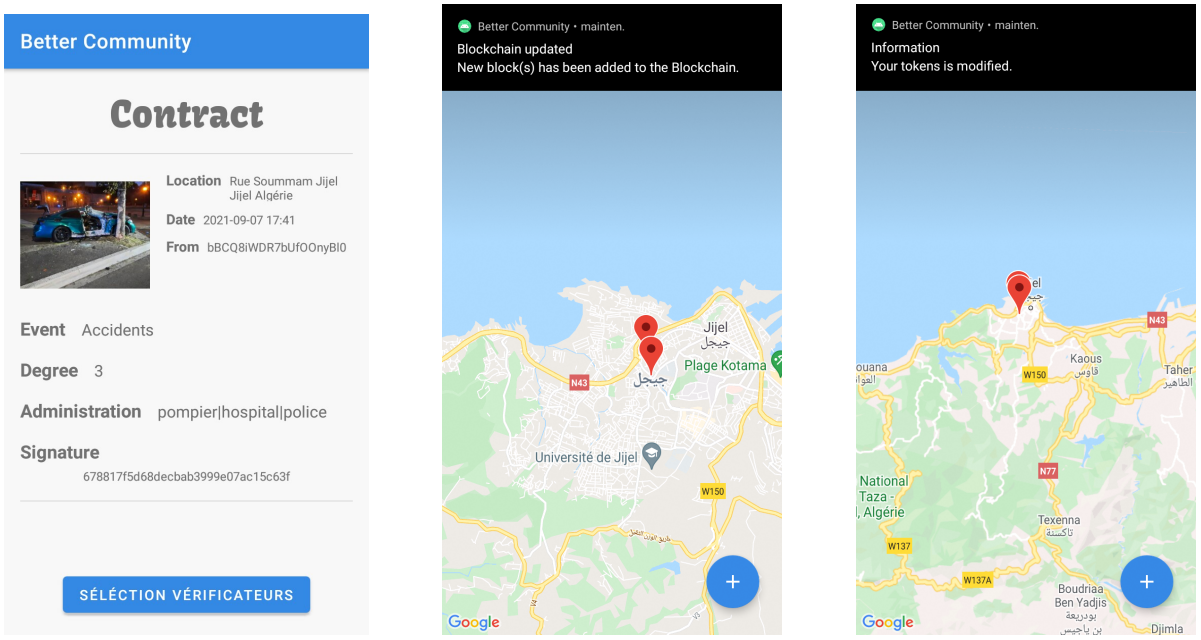


(b)

FIGURE 5.13 – IHM de l'envoi du signalement à l'administration.

7) **IHM du réception de signal de la part de l'administration compétente :** Lorsque l'administration compétente reçoit le signal de la part du signaleur elle

ouvre le contrat, puis elle sélectionne les vérificateurs (voir la figure 5.14a) pour qu'elle envoie ce contrat pour que ces derniers vérifient ce signal. Si les vérificateurs valide le signal, le processus de signalement se termine et le signal sera ajouter à la Blockchain et s'affiche sur la Map (voir la figure 5.14b), et tous les participents recevront une notification de leurs récompense et leur gain sera modifier (voir la figure 5.14c). Sinon le signalement sera rejeté.



(a) (b) (c)

FIGURE 5.14 – IHM du réception de signal de la part de l'administration compétente et l'ajoute de block

5.3 Conclusion

Dans ce chapitre, nous avons détaillé la réalisation de notre application tout en présentant, les outils logiciels et matériels utilisés. Ensuite, nous avons passé pour présenter une conception de notre application par des diagrammes de séquence, puis nous avons passé pour présenter les interfaces de notre application.

CHAPITRE 6

CONCLUSION ET PERSPECTIVES

6.1 Conclusion

La communication entre les gens est essentielle dans la vie humaine. Dans une ville intelligente, les gens vont signaler des événements et des anomalies entre eux pour l'avertissement et pour une meilleure vie. Mais, le manque de motivation et la peur de la vengeance des criminels à cause de la divulgation de l'identité du signaleur empêche les gens de signaler un événement. Malgré l'existence de quelques systèmes de signalement anonymes, qui peuvent protéger la véritable identité du signaleur, mais qui sont des systèmes centralisés et qui possèdent des inquiétudes au niveau de la sécurité et la fiabilité des données des signaleurs, et il n'y a aucune garantie qu'ils ne divulgueront pas les informations privées des signaleurs. Avec l'apparition de la technologie de la Blockchain, qui a beaucoup d'intérêt en raison de son anonymat, de son immuabilité et sa nature décentralisée. Nous pouvons protéger l'identité des signaleurs (anonymat) et motiver les gens pour faire des signalements.

Le travail que nous avons mené dans ce memoire vise à résoudre le problème d'anonymat et la crainte de la divulgation de l'identité de l'utilisateur au cours de mécanisme de signalement, ainsi que le problème de centralisation des systèmes de signalement ou toutes les informations de signalement et de la récompense sont stockées dans un seul serveur centralisé. Mais aussi le manque d'enthousiasme des utilisateurs à participer aux signalement. Nous avons proposé un système de signalement anonyme distribué basé sur la technologie de la Blockchain avec un mécanisme d'incitation. Notre système garantit la confidentialité de l'identité de l'utilisateur et la fiabilité du message de signalement tout au long du processus de signalement. Aussi, ce système motive les utilisateurs de participer grâce à ce mécanisme. Puis, nous avons utilisé la théorie des contrats pour modéliser le problème d'incitation à participer avec des informations asymétriques entre un signaleur et plusieurs témoins. Nous avons regroupé les témoins en plusieurs types selon leur réputation. Après, le signaleur va formuler des contrats spécifiques pour chaque type de témoin.

Nous avons développé une application mobile destinée aux citoyens, dans laquelle, ils vont se connecter et signaler des anomalies. Un utilisateur peut être aussi un témoin d'un

signalement et un validateur, un signalement valide va permet aux participants au processus de signalement d'avoir une récompense (Tokens), ce gain vas être utilisé après pour payer quelques amendes, aussi un signal valide vas être ajouté à la Blockchain et cette Blockchain sera distribué a tous les utilisateurs de système.

En guise de conclusion, sur la base de la discussion on peut dire que la veille citoyenne et l'intelligence citoyenne collective peut participer fortement à l'amélioration de la vie dans les futures villes intelligentes grâce aux nouveaux outils intelligents tels que les applications mobiles et les réseaux sociaux.

6.2 Perspectives

Les travaux présentés dans ce memoire peuvent être étendus pour accomplir d'autres objectifs. Comme perspectives futures de ce travail, nous envisageons de :

— Procéder à l'implémentation de notre modèle basé sur la théorie des contrats pour étudier les effets des différents paramètres du système (délais , le nombre d'utilisateurs, etc.) sur les performances de notre système. Aussi, comparer les performances de notre système avec d'autres travaux similaires.

— Compléter à implémenter les détails de notre système de signalement en ajustant et en améliorant notre application mobile.

Fem

BIBLIOGRAPHIE

[1] Ruben Sánchez-Corcuera, Adrián Nuñez-Marcos, Jesus Sesma-Solance, Aritz Bilbao-Jayo, Rubén Mulero, Unai Zulaika, Gorka Azkune, and Aitor Almeida. Smart cities survey : Technologies, application domains and challenges for the cities of the future. *International Journal of Distributed Sensor Networks*, 15(6) :1550147719853984, 2019.

[2] Honghua Qin, Hanqing Li, and Xia Zhao. Development status of domestic and foreign smart city. *Global Presence*, 9 :50–52, 2010.

[3] Kehua Su, Jie Li, and Hongbo Fu. Smart city and the applications. In *2011 international conference on electronics, communications and control (ICECC)*, pages 1028–1031. IEEE, 2011.

[4] Paul-Henri Richard. *Crise et ville intelligente au prisme de l'éthique appliquée à la sécurité civile*. PhD thesis, Troyes, 2016.

[5] Joëlle Simard. *La ville intelligente comme vecteur pour le développement durable : le cas de la ville de Montréal*. PhD thesis, Université de Sherbrooke, 2015.

[6] Gautier Aubourg. *La démarche Smart City comme nouveau cadre d'intégration des méthodes issues du génie industriel dans les chaînes logistiques de la fonction publique*. PhD thesis, 2017.

[7] Smart city : Les enjeux ÉnergÉtiques de la ville durable. `https://www.ifpenergiesnouvelles.fr/article/smart-city-les-enjeux-energetiques-ville-durable`.

[8] Leslie Lipper, Philip Thornton, Bruce M Campbell, Tobias Baedeker, Ademola Braimoh, Martin Bwalya, Patrick Caron, Andrea Cattaneo, Dennis Garrity, Kevin Henry, et al. Climate-smart agriculture for food security. *Nature climate change*, 4(12) :1068–1072, 2014.

[9] Charith Perera, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos. Sensing as a service model for smart cities supported by internet of things. *Transactions on emerging telecommunications technologies*, 25(1) :81–93, 2014.

[10] Kahina Moghraoui. *Gestion de l'anonymat des communications dans les réseaux véhiculaires Ad hoc sans fil (VANETs)*. PhD thesis, Université du Québec à Trois-Rivières, 2015.

[11] Ahmed Alioua. *Intégration du Software-Defined Networking (SDN) dans les réseaux de véhicules (VANETs)*. PhD thesis, 2019.

[12] Abdelwahab Boualouache. *Security and privacy in vehicular AD-HOC networks= Sécurité et vie privée dans les réseaux véhiculaires*. PhD thesis, 2016.

[13] Divya Chadha. Reena,"vehicular ad hoc network (vanets) : A review,". *Int. J. Innov. Res. Comput. Commun. Eng*, 3(3) :2339–2346, 2015.

[14] Ahmed Alioua. réseaux avancés, chapitre 5 : réseaux de véhicules, université de jijel, 2020.

[15] Rejab Hajlaoui. *Résolution à base d'heuristiques du problème de routage dans les réseaux ad hoc de vehicules*. PhD thesis, Bourgogne Franche-Comté, 2018.

[16] Moez Jerbi. *Protocoles pour les communications dans les réseaux de véhicules en environnement urbain : Routage et GeoCast basés sur les intersections*. PhD thesis, Evry-Val d'Essonne, 2008.

[17] Ram Shringar Raw, Manish Kumar, and Nanhay Singh. Security challenges, issues and their solutions for vanet. *International journal of network security & its applications*, 5(5) :95, 2013.

[18] Kahina Ait Ali. *Modélisation et étude de performances dans les réseaux VANET*. PhD thesis, Université de Technologie de Belfort-Montbeliard, 2012.

[19] Adel Berradj. *Contrôle de la diffusion multi-saut pour la dissémination de messages d'alerte dans les réseaux véhiculaires*. PhD thesis, Université de Toulouse, Université Toulouse III-Paul Sabatier, 2015.

[20] Walid Bouksani. *Gestion de la protection de la vie privée dans les réseaux véhiculaires (VANET)*. PhD thesis, Université du Québec à Trois-Rivières, 2017.

[21] Ines Chihi. *Étude de l'attaque «Black Hole» sur le protocole de routage VADD (Vehicule-Assisted Data Delivery)*. PhD thesis, Université du Québec á Trois-Rivières, 2017.

[22] Matthew NO Sadiku, Mahamadou Tembely, and Sarhan M Musa. Internet of vehicles : An introduction. *International Journal of Advanced Research in Computer Science and Software Engineering*, 8(1) :11, 2018.

[23] Fangchun Yang, Shangguang Wang, Jinglin Li, Zhihan Liu, and Qibo Sun. An overview of internet of vehicles. *China communications*, 11(10) :1–15, 2014.

[24] Omprakash Kaiwartya, Abdul Hanan Abdullah, Yue Cao, Ayman Altameem, Mukesh Prasad, Chin-Teng Lin, and Xiulei Liu. Internet of vehicles : Motivation, layered architecture, network model, challenges, and future aspects. *IEEE Access*, 4 :5356–5373, 2016.

[25] Joshua Joy, Vince Rabsatt, and Mario Gerla. Internet of vehicles : Enabling safe, secure, and private vehicular crowdsourcing. *Internet Technology Letters*, 1(1) :e16, 2018.

[26] Abdus Samad, Shadab Alam, S Mohammed, and MU Bhukhari. Internet of vehicles (iov) requirements, attacks and countermeasures. In *Proceedings of 12th INDIACom ; INDIACom-2018 ; 5th international conference on "computing for sustainable global development" IEEE conference, New Delhi*, 2018.

[27] Lylia Alouache, Nga Nguyen, Makhlouf Aliouat, and Rachid Chelouah. Nouveau protocole robuste pour les communications dans l'iov. *Internet des objets*, 1, 2017.

[28] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. Where is current research on blockchain technology ?—a systematic review. *PloS one*, 11(10) :e0163477, 2016.

[29] Nasser Al-Housni. *An Exploratory Study in Blockchain Technology*. PhD thesis, The University of Manchester (United Kingdom), 2019.

[30] Satoshi Nakamoto. Bitcoin : A peer-to-peer electronic cash system. *Decentralized Business Review*, page 21260, 2008.

[31] Michael Crosby, Pradan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman, et al. Blockchain technology : Beyond bitcoin. *Applied Innovation*, 2(6-10) :71, 2016.

[32] Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone. Blockchain technology overview. *arXiv preprint arXiv :1906.11078*, 2019.

[33] Bikramaditya Singhal, Gautam Dhameja, and Priyansu Sekhar Panda. *Beginning Blockchain : A Beginner's guide to building Blockchain solutions*. Springer, 2018.

[34] Arshdeep Bahga and Vijay K Madisetti. Blockchain platform for industrial internet of things. *Journal of Software Engineering and Applications*, 9(10) :533–546, 2016.

[35] Hong-Ning Dai, Zibin Zheng, and Yan Zhang. Blockchain for internet of things : A survey. *IEEE Internet of Things Journal*, 6(5) :8076–8094, 2019.

[36] Sophie Drame-Maigne. *Blockchain and access control : towards a more secure Internet of Things*. PhD thesis, Université Paris-Saclay (ComUE), 2019.

[37] Mingli Wu, Kun Wang, Xiaoqin Cai, Song Guo, Minyi Guo, and Chunming Rong. A comprehensive survey of blockchain : From theory to iot applications and beyond. *IEEE Internet of Things Journal*, 6(5) :8114–8154, 2019.

[38] Jonatan Bergquist. Blockchain technology and smart contracts : Privacy-preserving tools, 2017.

[39] Sylvain Tessierie. *Fonctionnement de la blockchain et son intèret pour le monde pharmaceutique*. PhD thesis, Université bordeaux, 2019.

[40] Asma Lahbib. *Distributed management framework based on the blockchain technology for industry 4.0 environments*. PhD thesis, Institut polytechnique de Paris, 2020.

[41] Understanding public vs. private blockchain. `https://selfkey.org/understanding-public-vs-private-blockchain/`.

[42] Muhammad Salek Ali, Massimo Vecchio, Miguel Pincheira, Koustabh Dolui, Fabio Antonelli, and Mubashir Husain Rehmani. Applications of blockchains in the internet of things : A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 21(2) :1676–1717, 2018.

[43] Danda B Rawat, Vijay Chaudhary, and Ronald Doku. Blockchain technology : Emerging applications and use cases for secure and trustworthy smart systems. *Journal of Cybersecurity and Privacy*, 1(1) :4–18, 2021.

[44] Comment innovhealth veut booster le déploiement de son passeport médical numérique. `https://www.ticsante.com/story/4684/%20comment-innovhealth-veut-booster-le-deploiement-de-son-passeport/%20-medical-numerique.html`.

[45] Kevin Curran. E-voting on the blockchain. *The Journal of the British Blockchain Association*, 1(2) :4451, 2018.

[46] Philippe Marrast. Blockchain : Éléments d'explication et de vulgarisation, pourquoi s' intéresser à la blockchain aujourd'hui ? In *Blockchain et Santé : Perspectives d'applications et enjeux juridiques (Séminaire IFERISS)*, 2018.

[47] Wesley van Nes. *Don't be fooled by the blocks that it got*. PhD thesis, Master thesis. CARU Containers, Erasmus University of Rotterdam. Erasmus . . . , 2017.

[48] Blockchain : avantages et inconvénients. `https://cryptoast.fr/blockchain-avantages-inconvenients/`.

[49] Mohamed Ahmed Mohamed, Chantal Taconet, and Mohamed Ould Mohamed Lemine. La traçabilité dans les chaînes logistiques en utilisant l'iot et la blockchain. In *Evolution des SI : vers des SI Pervasifs ?*, volume 2019, pages 1–10, 2019.

[50] `https://bitinfocharts.com/`.

[51] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An overview of blockchain technology : Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)*, pages 557–564. IEEE, 2017.

[52] What is proof of elapsed time. `https://themerkle.com/what-is-proof-of-elapsed-time/`.

[53] Juan Pablo Suarez Coloma. *TEMPAS-contribution à la qualité dans un système d'alertes contextualisées adaptable*. PhD thesis, Université de Grenoble, 2014.

[54] Jiawen Kang, Zehui Xiong, Dusit Niyato, and Dong In Kim. Incentivizing secure block verification by contract theory in blockchain-enabled vehicular networks. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, pages 1–7. IEEE, 2019.

[55] Kichun Jo, Junsoo Kim, Dongchul Kim, Chulhoon Jang, and Myoungho Sunwoo. Development of autonomous car—part i : Distributed system architecture and development process. *IEEE Transactions on Industrial Electronics*, 61(12) :7131–7140, 2014.

[56] Sébastien Faye, Claude Chaudet, and Isabelle Demeure. Contrôle du trafic routier urbain par un réseau fixe de capteurs sans fil. 2012.

[57] Karl Wüst and Arthur Gervais. Do you need a blockchain ? In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 45–54. IEEE, 2018.

[58] better street. `https://betterstreet.org/`.

[59] Honghua Qin, Hanqing Li, and Xia Zhao. Development status of domestic and foreign smart city. *Global Presence*, 9 :50–52, 2010.

[60] Bouge ma ville. `https://www.bougemaville.com/`.

[61] Shihong Zou, Jinwen Xi, Siyuan Wang, Yueming Lu, and Guosheng Xu. Reportcoin : A novel blockchain-based incentive anonymous reporting system. *IEEE Access*, 7 :65544–65559, 2019.

[62] Lun Li, Jiqiang Liu, Lichen Cheng, Shuo Qiu, Wei Wang, Xiangliang Zhang, and Zonghua Zhang. Creditcoin : A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 19(7) :2204–2220, 2018.

[63] Yang Yang, Jialiang Chen, Xianghan Zheng, Ximeng Liu, Wenzhong Guo, and Hairong Lv. Blockchain-based incentive announcement system for internet of vehicles. In *2019 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)*, pages 817–824. IEEE, 2019.

[64] Huaqun Wang, Debiao He, Zhe Liu, and Rui Guo. Blockchain-based anonymous reporting scheme with anonymous rewarding. *IEEE Transactions on Engineering Management*, 67(4) :1514–1524, 2019.

[65] Xingchen Liu, Haiping Huang, Fu Xiao, and Ziyang Ma. A blockchain-based trust management with conditional privacy-preserving announcement scheme for vanets. *IEEE Internet of Things Journal*, 7(5) :4101–4112, 2019.

[66] Don Johnson, Alfred Menezes, and Scott Vanstone. The elliptic curve digital signature algorithm (ecdsa). *International journal of information security*, 1(1) :36–63, 2001.

[67] Cong T Nguyen, Dinh Thai Hoang, Diep N Nguyen, Dusit Niyato, Huynh Tuong Nguyen, and Eryk Dutkiewicz. Proof-of-stake consensus mechanisms for future blockchain networks : fundamentals, applications and opportunities. *IEEE Access*, 7 :85727–85745, 2019.

[68] Tingting Liu, Jun Li, Feng Shu, and Zhu Han. Resource trading for a small-cell caching system : A contract-theory based approach. In *2017 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6. IEEE, 2017.

[69] Jiawen Kang, Zehui Xiong, Dusit Niyato, Shengli Xie, and Junshan Zhang. Incentive mechanism for reliable federated learning : A joint optimization approach to combining reputation and contract theory. *IEEE Internet of Things Journal*, 6(6) :10700–10714, 2019.

[70] Yanru Zhang and Zhu Han. *Contract Theory for Wireless Networks*. Springer, 2017.

[71] Patrick Bolton, Mathias Dewatripont, et al. *Contract theory*. MIT press, 2005.

[72] Tra Huong Thi Le, Nguyen H Tran, Phuong Luu Vo, Zhu Han, Mehdi Bennis, and Choong Seon Hong. Joint cache allocation with incentive and user association in cloud radio access networks using hierarchical game. *IEEE Access*, 7 :20773–20788, 2019.

[73] Weidang Lu, Bin Yin, Guoxiang Huang, and Bo Li. Edge caching strategy design and reward contract optimization for uav-enabled mobile edge networks. *EURASIP Journal on Wireless Communications and Networking*, 2020(1) :1–10, 2020.

[74] Lin Gao, Xinbing Wang, Youyun Xu, and Qian Zhang. Spectrum trading in cognitive radio networks : A contract-theoretic modeling approach. *IEEE Journal on Selected Areas in Communications*, 29(4) :843–855, 2011.

[75] Tra Huong Thi Le, Nguyen H Tran, Phuong Luu Vo, Zhu Han, Mehdi Bennis, and Choong Seon Hong. Contract-based cache partitioning and pricing mechanism in

wireless network slicing. In *GLOBECOM 2017-2017 IEEE Global Communications Conference*, pages 1–6. IEEE, 2017.