Republique Algerienne Democratiqueet Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
UNIVERSITE MOHAMMED SEDDIK BENYAHIA
JIJEL
FACULTE DE SCIENCES EXACTES ET D'INFORMATIQUE
DÉPARTEMENT D'INFORMATIQUE

MEMOIRE DE MASTER

Présenté pour l'obtention du diplôme de :

MASTER EN INFORMATIQUE

Option : INFORMATIQUE LÉGALE ET MULTIMEDIA

Thème

Blockchain pour sécuriser un Feu de circulation intelligent

Réalisé par :
RECHEK Sara
TALEB Mina

encadré par :
Dr, SOUICI
Ismahane

Promotion : 2022

Remerciements

Tout d'abord, nous remercions et louons Allah Tout-Puissant pour la force, la santé, et le courage qu'il nous adonné afin de réaliser cette étude

Nous tiens à remercier vivement ***Dr SOUICI Ismahan****, pour ses précieux commentaires constructifs, ses orientations et son suivi pour mener bien cette étude*

Nous remercie aussi les membres de jury qui ont accepté d'examiner et de juger et d'évaluer notre travail.

Nos remerciements vont également à tous les enseignants de la spécialité ***Informatique légale et multimédia*** *et tous les responsables de la faculté* ***« sciences exacte et d'informatique »***

En fin nos remerciements sont dressés plus particulièrement à nos familles ; Nos ***pères, mères****, sœurs et frères et nos amis(es) qui ont su nous soutenir, nous encourager, nous aider tout au long des années.*

Dédicace

Je dédie ce modeste travail à :

*À **ma chère mère Massouda** , qui a œuvré et prié pour ma réussite, par son amour, son soutien, tous les sacrifices consentis et ses précieux conseils, pour toute son assistance et sa présence dans ma vie. Reçois à travers ce travail aussi modeste soit-il, l'expression de mes sentiments et de mon éternelle gratitude, merci beaucoup maman.*

*À **mon cher père Sid Ali**, qui peut être fier et trouver ici le résultat de longues années de sacrifices et de privations pour m'aider à avancer dans la vie. Puisse Allah faire en sorte que ce travail porte son fruit. Merci pour les valeurs nobles, l'éducation et le soutient permanent venu de toi papa.*

*Mes très chèrs frères : **Hamza,Seifeddine et Yahia.***

*Mes très chères sœurs : **Aicha, Aziza et sa petite fille Nour AlYakkin, Soumia .***

Mes amis, Mes collègues de la promotion. Toute la promotion Informatique 2022. Tous ceux qui j'aime et ceux que m'aiment. Encore merci à tout le monde du fond du cœur.

SARA

Dédicace

Je dédie ce modeste ouvrage comme le fruit de nombreuses années d'études :
En tout premier lieu, je remercie le bon ***DIEU****, tout puissant, de m'avoir donné la force pour survivre, ainsi que l'audace pour dépasser tout les difficultés.*
Pour mon idéal éternel, mon soutien moral, et celle qui s'est toujours sacrifiée pour me voir réussir, car elle m'a soutenu moralement et matériellement jusqu'à ce jour, pour son amour et ses encouragements, à toi ***ma chère mère '' LOUADJ AKILA ''.***

A l'homme de ma vie, à mon épaule, la lumière de mes yeux à ***mon cher père '' MAHFOUD"*** *pour son soutien matériel et moral. Que ce travail soit pour vous un petit témoignage de mon profond amour, que Dieu Tout Puissant vous protège, et vous accorde santé et longue vie.*

A mes chers frères ***Ibrahim, Abd el Hakim.***

A mes sœurs ***Rahima, Samira et Fatima.***

A ma chère tante ***Nadia.***

A Mes amis ***Bouchra, Roukia, Ahlem et Soumia.***

A tous ceux que j'aime.

MINA

RÉSUMÉ

Les feux de circulation intelligents (Intelligent Traffic Light) sont l'une des solutions dont le monde a été témoin au cours des deux dernières décennies pour réduire le problème de la congestion du trafic.
Pour ce faire, nous proposons dans notre travail une solution issue d'un processus dynamique de régulation du trafic où le problème de partage sécurisé de cette solution (combinaison des temps verts) sur les différents nœuds du réseau d'intersections pour des fins de validation vis-à-vis des conditions de la route, est assuré via la technologie de blockchain qui intègre la décentralisation, le calcul distribué, le chiffrement asymétrique, le hachage, l'horodatage et le principe de consensus.

Mots-clés : Congestion, Intelligent Traffic Light, sécurité, Blockchain, transparence.

ABSTRACT

Intelligent Traffic Light is one of the solutions that the world has witnessed in the last two decades to reduce the problem of traffic congestion. For this purpose, we propose in our work a solution from a dynamic traffic control process where the problem of secure sharing of this solution (combination of green times) on the different nodes of the intersection network for validation purposes with respect to road conditions, is provided via blockchain technology that incorporates decentralization, distributed computing, asymmetric encryption, hashing, time stamping and consensus principle.

Keywords : Congestion, Intelligent Traffic Light, security, Blockchain, transparency.

TABLE DES MATIÈRES

TABLE DES FIGURES

LISTES DES ABRÉVIATIONS

TRANSYT Trac Network Study Tool

SCOOT Split Cycleand Oset Optimisation Technique

SCATS Sydney Coordinated Adaptative Trafic System

PRODYN PROgrammation DYNamique

IoT Internet of Things

ECDSA Elliptic Curve Digital Signature Algorithm

PoS Proof of Stake

PoW Proof of Work

INTRODUCTION GÉNÉRALE

Avec la croissance des villes modernes et l'utilisation croissante de la voiture comme principal moyen de transport, il est devenu nécessaire de trouver des moyens efficaces pour contrôler le flux de véhicules.
Il y a des avantages significatifs à tirer de l'amélioration du trafic routier en termes de réduction du temps imposé aux usagers de la route en raison de la congestion du trafic, ainsi la récupération d'une partie de leur journée améliorera la qualité de vie et réduira la congestion qui conduira à moins d'accidents et sauve des vies. Les trajets domicile-travail ont un impact sur le temps passé au travail.
En fait, la plupart des gens sont essentiellement limités à effectuer la tâche de conduire uniquement pendant leur trajet. Les marchandises doivent être déplacées et les prestataires de services doivent se rendre chez leurs clients.
De toute évidence, le ralentissement de la circulation affecte la productivité et l'efficacité économique.
Il y a aussi le problème de la pollution où les voitures sont généralement moins efficaces pour s'arrêter et démarrer dans un trafic dense, ce qui entraîne plus de gaz à effet de serre.
Les feux de circulation (traffic light) sont l'une des solutions proposées pour réduire ce problème, mais ils ne sont pas sans défauts, car ils fonctionnent traditionnellement

et ne correspond pas à l'énorme embouteillage sur les routes.
Avec les grands développements dont le monde a été témoin en termes de technologie, qui ont conduit à l'émergence de nombreuses technologies dans de nombreux domaines de la vie, ils ont contribué au développement du fonctionnement des feux de circulation, qui l'ont transformé d'une technologie traditionnelle à une technologie intelligente et plus moderne. De plus, la prise en compte de l'aspect et des services de sécurité dans un tel domaine est primordiale pour empêcher toute altération du système.
Dans ce contexte, une sécurisation par blockchain demeure très prometteuse. Elle est apparue pour la première fois en 2008 lorsqu'il a été proposé et publié pour permettre aux paiements en ligne d'être envoyés directement d'une partie à une autre sans passer par une institution financière centrale, en utilisant la crypto-monnaie "bitcoin". Elle intègre plusieurs technologies telles que la décentralisation, l'informatique distribuée, le chiffrement asymétrique, le hachage, l'horodatage et l'algorithme de consensus. Du fait de la multiplicité des fonctionnalités de la Blockchain, le champ de son utilisation s'est élargi et ne se limite plus aux seules monnaies numériques. C'est d'ailleurs cette technologie que nous avons utilisée pour proposer une solution appropriée capable de gérer de manière dynamique et adaptative le trafic et d'améliorer les performances du système de contrôle des feux de circulation.
Ainsi et hormis cette introduction et la conclusion générale qui reprennent les travaux de l'ensemble des chapitres, le manuscrit est divisé en trois chapitres. Dans le premier chapitre, nous présenterons les concepts généraux liés au domaine de gestion des feux de circulation classiques et intelligents. En effet, nous citerons quelques exemples de systèmes classiques de gestion des feux de circulation, pour résumer ensuite les avantages et les inconvénients de tels systèmes avant de parler des systèmes intelligents de gestion de feux de circulation.
Sur le deuxième chapitre, nous présenterons tout d'abord le concept général de Blockchain, pour illustrer par la suite son architecture et fonctionnement. La sécurité via la blockchain sera aussi abordée en plus des notions cryptographiques y impliquées.
Le troisième chapitre exposera notre proposition d'exploitation de Blockchain pour sécuriser la combinaison calculée pour gérer dynamiquement un feu de circulation.

CHAPITRE 1

GÉNÉRALITÉ SUR LES SYSTÈMES DE FEU DE CIRCULATION TRICOLOR

1.1 Introduction

Au cours des dernières décennies, le nombre d'usagers de la route dans le monde a augmenté entraînant des embouteillages et de longues files d'attente créant un mécontentement chez les usagers. Le phénomène de congestion du trafic routier est, ainsi, un problème socio-économique qui nécessite des solutions. Pour résoudre le problème de la congestion afin que la circulation devienne fluide, les pouvoirs publics propose plusieurs solutions, telles que l'aménagement des infrastructures, le développement du transport public pour la réduction du nombre de véhicules, et la large adoption des feux de circulation tricolores ou dans un meilleur cas des feux de circulation intelligents. Ces derniers contribuent à assurer une meilleure gestion du trafic.

Dans ce chapitre, nous décrierons les concepts généraux liés au domaine de gestion de feux de circulation classiques et intelligents.

1.2 Définition d'un feu de circulation tricolore

Un feu de circulation tricolore est un système utilisé pour contrôler la progression du trafic à une traversée. Les feux de circulation utilisent généralement trois feux de signalisation d'ombrage pour envoyer un message au conducteur d'un véhicule [1].

— **feux rouge :** la tonalité rouge informe le conducteur de s'arrêter à l'intersection.

— **feux doré :** l'ombrage doré indique au conducteur que le signe va être passé au rouge dans les instants suivants, soyez prêt à vous arrêter à l'intersection.

— **feux verte :** la tonalité verte permet au conducteur de traverser le carrefour en toute sécurité.

FIGURE 1.1 – Feu de circulation tricolor

1.3 Terminologie

La route se compose de plusieurs éléments ,dont les intersections ,phase d'un feu et cycle d'un feu ,ainsi que certain caractéristiques résumé comme suite :

1.3.1 Intersection

Une intersection est le point de rencontre de plusieurs rues, déterminant les halls d'entrée et les sorties. Les directions du véhicule sont soit des flux directs, soit des flux tournés vers la gauche, soit vers la droite. L'établissement d'un systéme de feux de signalisation à une convergence permet alors de coordonner après un certain temps la confirmation des différentes progressions des véhicules. [2].

1.3.2 phase d'un feu

Une phase d'un feu est une période pendant laquelle au moins un flux intelligible est concédé dans le carrefour. [4]

1.3.3 cycle d'un feu

Le cycle d'un feu traite du temps qui isole deux phases identiques de l'intersection. Elle se caractérise par une séquence de phases. [4]

1.3.4 Caractéristique d'un trafic routier

Ce système a les attributs d'accompagnement qui clarifient ses difficultés[2] :

— **Dynamique :** : les phénomènes de trafic sont fortement dynamiques, le nombre d'intervenants retenus dans le système variant largement dans le temps. Une petite influence déstabilisante peut, par exemple, s'intensifier et se transformer en congestion.

— **Distribution :** les phénomènes de trafic résultent de l'interaction de chaque client de la rue avec son environnement

— **Complexité :** un système est qualifié de complexe lorsqu'un spectateur ne peut pas prévoir sa façon de se comporter ou son comportement ou son évolution ou qu'un de ses composants essentiels (le conducteur) a, par exemple, un comportement imprévisible.

— **Hétérogénéité :** le systéme de la circulation routière comprend divers acteurs dont des conducteurs hétérogènes (débutants/expérimentés), qui peuvent utiliser, par exemple,véhicules de différentes caractéristiques (véhicules de marchandises lourds/légers), etc.

1.4 Histoire et développement des systèmes de gestion des feux tricolore

L'administration des feux de circulation est en amélioration permanente suivant les conditions préalables de la rue et l'intérêt sans cesse croissant des véhicules [3] :

1.4.1 Phase1 -L'apparition des feux de circulation

De 1868 à 1920, le premier feu de circulation à combustion interne dépendait des plans de chemin de fer et n'avait que deutons, rouge et vert .Les panneaux étaient surveillés physiquement par les flics. Le poteau carré mesurait 24 pieds de haut et pouvait être vu de tous les côtés du point de passage, pour travailler sur la perceptibilité du régulateur de la circulation.

1.4.2 Phase2 -L'introduction des plans temps Xe

Vers 1920-1980, cette phase a vu les véritables débuts de contrôle de trafic urbain (UTC), car la congestion croissante a conduit à une prise de conscience parmi les décideurs aux problèmes du trafic et par conséquent déni les objectifs de base pour tous les systèmes de gestion des feux tricolore.

1.4.3 Phase3 -Signal actionné par le véhicule

Des années1970 à nos jours le problème ennu yeux de congestion ested'actualité. Le gouvernement britannique a poursuivi ces recherches pour améliorer les technologiesactuelles, un nuancement a été accordé pour la recherche et le développement afin de trouverune meilleure solution au problème. Dans le but de promouvoir l'eccéité du réseau urbain le gouvernement a lancé plusieurs projets à Londres et à Glasgow, c'était la naissance desystème designal actionné parlevéhicule.

1.4.4 Phase4 –Systèmes de transport intelligents

Depuis 1997 à présent, les systèmes de gestion des feux tricolore les plus avancés sontdésormais intégrés de manière plus centralisée avec d'autres systèmes de gestion afin de réduirela congestion et d'améliorer l'eccéité du réseau. Cela a été rendu possible grâce à un certainnombredetechnologies avancées, la plupartsontdesaméliorationsdestechniquesdedétectionetl'intégrationd'outilsintelligents [3].

1.5 Systèmes classiques de gestion des feux tricolore

Pour montrer la diversité des approches classiques pour la gestion de feu de circulation, quatre systèmes sont décrits en ce qui suit[4] :

1.5.1 TRANSYT (Trac Network Study Tool)

Est l'un des premiers systèmes proposés basé sur une optimisation hors-ligne qui génère des plans de coordination optimaux entre les feux de signalisation d'un réseau pour une période donnée. Il exige beaucoup de paramètres d'entrées utilisés pour définir un modèle mathématique :

— géométrie des artères des intersections.

— débit des véhicules.

— temps de feu vert minimal.

— plans de feux initiaux.

— taux de véhicules sur chaque voie sortante de chaque intersection.

Ensuite, il va appliquer un algorithme Hill-Climbing,ce dernier est un algorithme itératif de recherche locale des plus simples, qui commence avec une solution aléatoire à un problème, puis tente de trouver une meilleure solution en changeant progressivement la solution, un paramètre à la fois. Si le changement produit une meilleure solution, une mise à jour de la solution est faite, répété jusqu'à ce qu'aucune autre amélioration puisse être trouvée. utilisé pour améliorant progressivement la solution en modifiant légèrement la durée des feux vert et des décalages entre intersections adjacentes. Cette phase est nommée "l'étape de l'optimisation".

1.5.2 SCOOT(Split Cycle and Oset Optimisation Technique)

Introduit dans de nombreuses communautés urbaines de la planète et pour la plupart en Grande-Bretagne, est un système décentralisé et totalement polyvalent aux circonstances de la circulation. Il optimise : les durées de feu vert pour chaque intersection indépendamment, les décalages entre intersections voisines, les cycles des feux entre les zones d'intersection. Il collecte les données (nombre de véhicules par intervalle de temps) à partir des détecteurs installés sur les routes, boucles magnétiques en amont du carrefour.

Fondamentalement le même que TRANSYT, mais fonctionnant en continu, il examine différents choix (par exemple pour les termes de cycle : imiter des plans similaires, ajouter ou soustraire quelques instants) et choisit celui qui le rapproche le plus de son objectif d'amélioration en utilisant la Colline -Calcul d'escalade. Il ajuste régulièrement les plans . Quatre approches de référence du fonctionnement des feux de circulation au vu des informations recueillies par les capteurs introduits dans les rues. Ces modifications comportent de petites variations dans :

— la longueur des durées de processus (0, 4 ou 8 secondes)

— les temps de feu vert (0 ou 4 secondes).

— les reports entre les points de passage (0 ou 4 secondes).

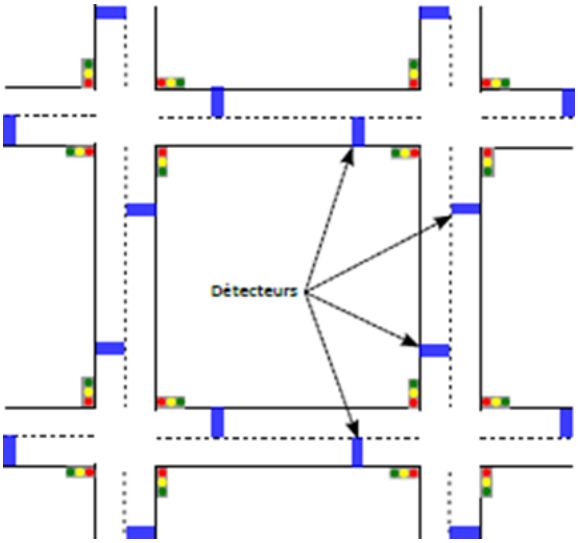

FIGURE 1.2 – Boucles magnétique Sénarmont
[4]

Ce cadre est introduit dans de nombreuses communautés urbaines sur toute la planète et principalement en Grande-Bretagne. Peu à peu, SCOOT reste un cadre faiblement polyvalent contrastant avec les autres, compte tenu de ses variétés peu lentes des étapes à chaque cycle. La figure suivante montre l'installation de ce système a la jonction de Archangelou-GrivaDigeni.

FIGURE 1.3 – SCOOT -Archangelou-GrivaDigeni
[5]

1.5.3 SCATS (Sydney Coordinated Adaptative Traffic System)

Installé dans beaucoup de villes dans le monde et principalement en Australie dans les villes contenant plus de 10 millions d'habitants, est un système partiellement décentralisé et adaptatif à la situation du trafic. SCATS utilise des bibliothèques prédéfinies qui stockent 10 ensembles de décalages et 4 ensembles de durées de feu vert à partir les données des capteurs installés sur les routes, en plus d'un algorithme temps réel de reconstruction de plan de feux pour intersection par cycle. L'algorithme compare plusieurs solutions et les données des capteurs avant d'appliquer la solution qui minimise la saturation des routes sachant que la variation ne peut excéder les 6 secondes. Donc SCATS est un système hiérarchique qui dépend fortement du choix des bibliothèques, des durées de feu vert et des décalages.

1.5.4 PRODYN (PROgrammationDYNamique)

Installé dans beaucoup de villes en France et en Belgique développé par le CERT ''Centre d'Etude et de Recherche de Toulouse" en France, est un système décentralisé d'optimisation de la circulation en ligne en minimisant les retards aux intersections sur un horizon futur de 80 secondes à l'aide d'une programmation dynamique. Ce dernier lui permet d'exprimer l'évolution des files d'attente en fonction des arrivées et des départs sur les tronçons. Pour les départs il utilise les données des capteurs installés sur les routes comme SCATS et SCOOT. La solution pour l'optimisation consiste à utiliser des prédictions établies au pas d'optimisation précédent tout en faisant l'hypothèse que la situation du trafic n'a pas beaucoup évoluée sachant que chaque intersection optimise séparément en fonction des données reçues de ses voisines. PRODYN est un système coûteux en communication.

1.6 Objectif et domaines d'utilisation

L'objectif des feux tricolore est de garantir la sécurité de tous les clients de la rue,promeneur set conducteurs, et de travailler avec la progression des flux de circulation denses [6] Comme exemples d'emploi, nous pouvons citer [7] :

- la gestion de la circulation aux intersections ;
- la traversée des piétons, autour des intersections gérées par des feux et les moments où la circulation est plus intense ou lorsque le sentiment d'insécurité des piétons est important ;
- l'exploitation par sens uniques alternés d'une section où le croisement est impossible ou dangereux (ouvrage d'art étroit, emprise de travaux, etc.) ;
- l'affectation de certaines voies d'une chaussée à un sens de circulation en fonction des besoins, ou leur condamnation momentanée ;
- le contrôle d'accès à certaines voies rapides ;
- la gestion d'un point de contrôle des personnes ou des véhicules nécessitant leur arrêt (péage) ;
- la protection d'obstacles intermittents (passages à niveau, traversées de voies de tramways, ponts mobiles, passages d'avions, avalanches, etc.).

1.7 Avantages et inconvénients des feux de circulation tricolore

Le feu tricolore permet de réguler les flux importants de véhicules et de piéton au niveau de la route à condition d'être utilisés avec pertinence, et il présente certain avantages et inconvénients, que nous résumons en ce qui suit :

1.7.1 Avantages

- En obligeant les clients enclins à se croiser à s'arrêter, les feux de circulation doivent permettre aux clients voyant le feu vert de traverser en toute sérénité

et à une vitesse inférieure à la plus grande vitesse autorisée les convergences de rues [6].

— La diminution des cycles de ralentissement (arrêt) augmentation de la vitesse agit sur le confort de conduite et diminue la consommation de carburant [6].

— La bonne synchronisation des feux sur un axe de circulation permet de créer des « ondes vertes » qui assurer une traversée facile et rapide de zones urbaines [7].

— Les conducteurs plus attentifs et prudents à l'approche d'un carrefour sans feux donc il augmenté la sécurité [7].

1.7.2 Inconvénient

Les principaux inconvénients des feux de circulation tricolores sont les suivants [8] :

— La forme circulaire uniforme des signaux lumineux entraîne une incertitude et des difficultés pour les usagers de la route atteints de daltonisme et de déficience visuelle, ce qui entraîne la nécessité de restrictions ou d'interdictions de délivrance de permis de conduire dans certains des pays. Cette incertitude devient particulièrement aiguë dans des conditions de faible visibilité.

— Le concept d'harmonie de forme et de couleur : une lumière verte seule correspond à la forme circulaire (sphérique) du signal. Les lumières rouges et ambrées se combien harmonieusement avec d'autres formes géométriques.

— Les feux de l'étape verte incitent les clients à dépasser la vitesse pour traverser l'intersection avant l'arrivée de l'étape verte,ce qui renforce la fragilité des clients plus lents, par exemple les cyclistes [6].

— Feux de circulation limitée à contrôle de trafic et, sur certains axes au confort de conduite des usagers.

1.8 Systèmes de feu de circulation tricolore intelligents

Dans cette section, nous présentant juste quelques exemples de systèmes intelligents de gestion des feux de circulation pour avoir une idée sur des exemples de mécanismes utilisés.

1.8.1 Système intelligent de gestion de feux de circulation par denso corparation

Dans ce système particulier, les données sont communiquées entre le feu de circulation et le véhicule entrant. Par cela , de meilleures décisions concernant le moment de changer la Signalisation aideront à maximiser le débit global des véhicules à une intersection. Ce système nécessite des émetteurs sans fil à courte portée montés dans les véhicules et également une connexion GPRS supplémentaire à des fins de communication entre les deux entités. Cela donnerait aux feux de circulation plus d'informations sur les prochains véhicules et pourraient changer dynamiquement en fonction de leur vitesse, du type de véhicule et du volume relatif de véhicules en approche. Le principal Inconvénient est la nécessité d'un équipement GPRS et d'émetteurs sans fil qui doit être facilité à l'intérieur du véhicule. Cela rend le système peu pratique et coûteux. [9].

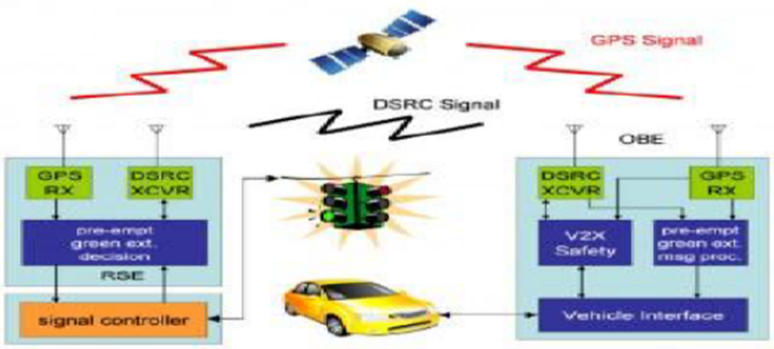

FIGURE 1.4 – Système de feux de circulation intelligent par denso corparation [9]

1.8.2 Système intelligent de gestion de feux de circulation basé sur la logique floue

L'effort connu à l'origine pour appliquer une logique duveteuse dans les feux de circulation a été établi par « Pappis et Mamdani' ». Ils ont reconstitué un point de passage signalé désengagé composé de deux routes à sens unique avec deux chemins vers chaque chemin sans détourner le trafic. De nombreux efforts ont été transférés dans ''Fuzzy Logic", car il se rapproche de la façon dont les individus pensent, offrant un plus grand nombre d'avantages que la logique booléenne. De plus, il n'est pas difficile à réaliser. La plupart des Framework ITS (intelligente trafic system) qui réalisent la logique floue sont pragmatiques dans une convergence solitaire [10]

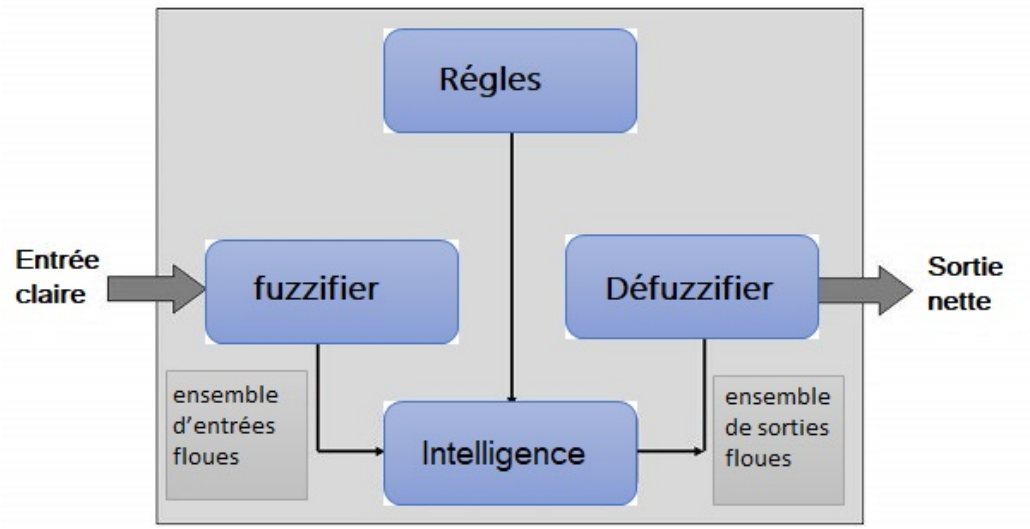

FIGURE 1.5 – Logique floue

1.8.3 Système intelligent de gestion de circulation basé sur l'IoT (Internet of Things)

Est un Système composé de trois couches fonctionnant comme illustré sur la figure 1.6 [11] :

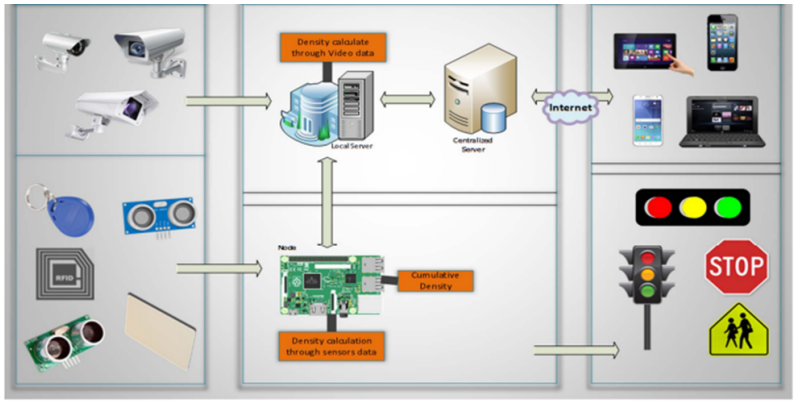

FIGURE 1.6 – Couches de système
[12]

1. **Couche d'acquisition et de collecte de données :**
   Les données de trafic sont collectées à partir des capteurs à ultrasons, **RFID**, des capteurs de fumée et des capteurs de flamme, des caméras de surveillance, etc. Ensuite, l'algorithme de détection de gouttes est appliqué au flux vidéo sur le serveur local en raison de ses performances et de sa capacité de réduction du bruit. Après détection du trafic, un serveur local envoie la densité mesurée par traitement d'images au micro-contrôleur respectif.
2. **Couche de traitement des données et de prise de décision :**
   Le système gère le trafic routier en fonction des conditions de circulation résumé on deux cas : une circulation normale où chaque signal passe au vert à leur tour pendant quelques secondes, et le reste des signaux à ce moment-là reste rouges. Le deuxième cas correspond à une circulation encombrée où un module de gestion du trafic basé sur la densité est ajouté qui alloue le temps de manière dynamique.
3. **Couche d'application et d'actionnement :**
   Le système calcule l'intervalle de pointe en utilisant l'algorithme d'arbre de régression sur les données enregistrées sur le serveur local et met à jour ce rapport sur le serveur centralisé quotidiennement.

1.9 Conclusion

Dans ce chapitre, nous avons présenté des concepts liés aux systèmes de gestion de feux de circulation. En effet, nous avons présenté une définition de ce système, la terminologie liée au domaine en plus des principales caractéristiques des systèmes de gestion de feux de circulation. De même, une histoire de développement de tels systèmes a été dressée suivi d'une présentation de leurs principaux avantages et inconvénients. Nous avons, aussi, parlé des systèmes classiques et intelligents de gestion de feux de circulation en présentant des exemples de systèmes développés dans ce sens.

CHAPITRE 2

TECHNOLOGIE BLOCKCHAIN

2.1 Introduction

Notre monde avance au rythme des développements et des innovations technologiques, qui certes, facilitent et améliorent l'échange et le partage d'informations et des données entre les personnes, mais qui créent de sérieux problèmes, tel que le problème de sécurité des données échangées ou partagées. La technologie Blockchain est l'une des percées technologiques émergentes qui devrait révolutionner la façon dont les transactions sont effectuées, affectant ainsi une grande variété de domaines d'application potentiels.

Dans ce chapitre nous présentons la technologie de Blockchain, en faisant le tour des principaux concepts impliqués (architecture, fonctionnement, ...etc.).

2.2 Concept générale de Blockchain

2.2.1 Qu'est-ce que la technologie blockchain ?

La blockchain est une innovation de stockage et de communication de l'information inventée à la fin des années 2008 par une personne ou un groupe anonyme sous le nom de satoshi nakamato [12].

La blockchain est une technologie permettant de stocker et de transmettre des informations sans organe de contrôle Techniquement, il s'agit d'une base de données distribuée dans laquelle les informations envoyées par les utilisateurs et les liens internes à la base de données sont scannées et agrégées à des intervalles spécifiés. Organisation en blocs Tout est sécurisé par cryptage et ainsi une chaîne est formée [13].

2.2.2 Architecture de la blockchain

La technologie de blockchain réunie plusieurs composants, tels que : transaction, bloc, consensus et Smart Contrat (contrat intelligent) [14], que nous présentons ci-après.

Bloc

Est une structure de données fondamentale (fichier) dans la blockchain. Des blocs sont liés entre eux pour former une chaîne de blocs. Ainsi, un bloc est un enregistrement de certaines transactions valides qui n'ont pas encore été enregistrées dans les blocs déjà chaînés. Chaque bloc est composé de plusieurs éléments tels que :

- **Bloc :**l'indice de bloc.
- **Hash du bloc précédent :** champ contient l'empreinte de bloc précédant (bloc d'indice numéro 90 dans notre exemple).
- **Transaction :** la partie qui contient la liste des transactions.

— **Horodatage :** temps de la création de bloc.

— **Hash :** l'indentant du bloc actuel.

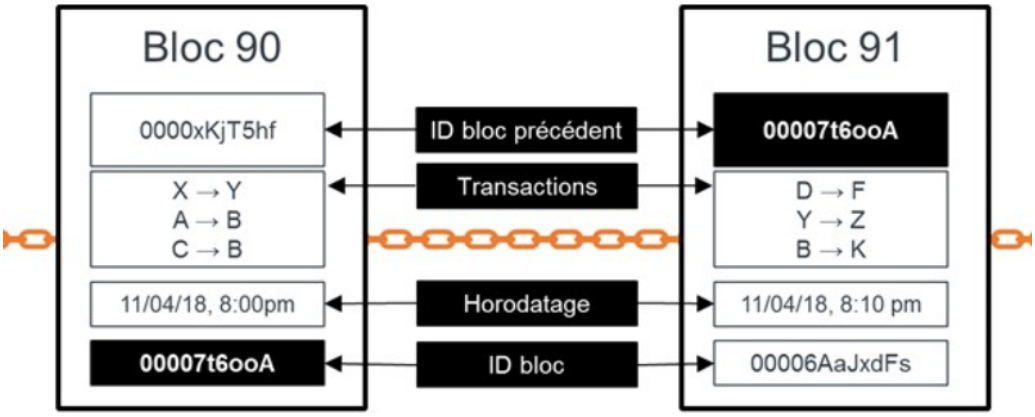

FIGURE 2.1 – Structure des Blockchain
[15]

Transaction

Une transaction est l'unité fondamentale d'une blockchain qui représente un échange d'argent (pièce électronique) entre deux entités ou utilisateurs à travers le réseau. Chaque transaction valide est enregistrée dans un bloc par les mineurs, qui peut contenir plusieurs transactions, pour plus d'efficacité [16].

Une pièce électronique est caractérisée comme une chaîne de signatures numériques. Chaque échange est caractérisé par un hachage soigneusement marqué de l'échange passé et de la clé publique du propriétaire suivant. La clé privée est utilisée pour signer l'échange et la clé publique est utilisée pour la confirmation de l'échange, comme illustré à la figure 2.2. La clé publique est conservée dans le portefeuille, qui peut être exécuté dans la programmation, l'équipement ou sur le Web [17].

Chaque sortie de la transaction ne peut être utilisée qu'une seule fois comme entrée dans l'ensemble de la blockchain sinon La tentative de référencer deux fois la même sortie conduit au problème de la double dépense et est interdite dans le réseau [17].

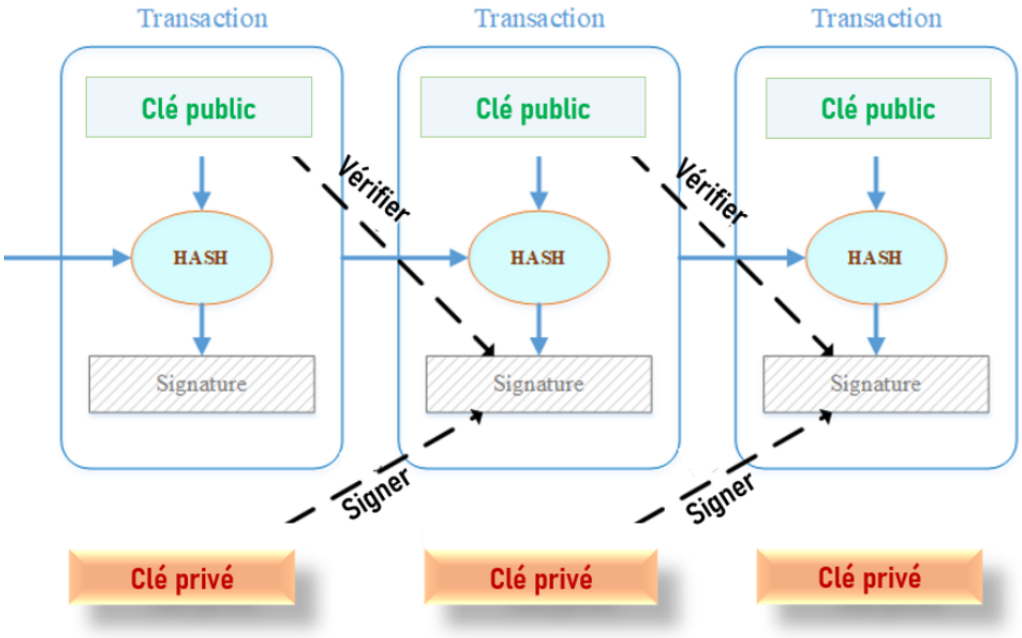

FIGURE 2.2 – Structure de transaction dans une blockchain Bitcoin

Consensus

La particularité principale de blockchain est la décentralisation c'est-à-dire, qu'il n'y a pas d'entité centrale pour décider quels nouveaux blocs sont valides. Donc chaque nœud doit décider s'il accepte ou non un nouveau bloc reçu. C'est la notion de consensus [18]. La blockchain utilise une variété d'algorithmes de consensus pour garantir la cohérence des données et la capacité de tolérance aux pannes du grand livre partagé entre les nœuds distribués, ''Proof of Work" (POW) et ''Proof of Stake'' (POS)sont les algorithmes les plus utilisé.

— **Proof of Work (POW) :** est un protocole d'élection de leader qui désigne parmi les participants au réseau (mineurs) un leader qui ajoutera le bloc suivant à la chaîne, Pour attirer plus de participants à rejoindre et à maintenir le réseau, et en même temps les décourager de tricher, un mineur honnête peut être élu pour recevoir une récompense très attrayante s'il peut résoudre un chalenge informatique ardu [19].

POW est sécuritaire et aide a protéger le réseau contre de nombreuses attaques différentes, une attaque réussi nécessiterait beaucoup de puissance de calcul et beaucoup de temps pour faire les calculs, et donc elle serait inefficace car le cout encouru serait supérieur aux récompenses potentielles pour attaquer le réseau [13].

— **Proof of Stake (POS) :** La méthode de POS est différente que POW où un mineur doit miser des montants d'actifs numériques prédéfinis pour obtenir un consensus [20].

Il consiste à choisir, au hasard, un mineur dans le pool de minage requis pour résoudre un problème mathématique simple. Deux cas sont à distinguer, si le mineur résout le problème avec succès, un bonus est accordé sur sa mise, sinon le mineur suivant est choisi au hasard [20].

Minage et Mineur

L'exploitation minage est la méthode de production de nouveaux blocs dans les systèmes de Blockchain le principalement des crypto-monnaies telles que Bitcoin, consistant à la validation d'un bloc par les mineurs (nœuds spécifiques) avant d'ajouter quoi que ce soit à la structure de la blockchain. Cela oblige les mineurs à résoudre un problème mathématique en calcul pour lier crypto graphiquement un nouveau bloc au bloc précédent dans la Blockchain [21]. Les mineurs qui réussiront à ajouter un nouveau bloc à la blockchain recevra une récompense en bitcoin. Les travailleurs ont été récompensés, en commençant par 50 bitcoins, et ils ont été divisés par deux environ tous les quatre ans (ce qui équivaut au 6.25 BTC en 6 mai 2020) [14].

Réseau pair à pair (décentralisé)

L'un des propriétés principales de la Blockchain est " Décentralisé " c'est-à-dire basé sur un réseau pair à pair, au lieu de dépendre d'un serveur central auquel de multiples utilisateurs se connectent pour effectuer des requêtes, les utilisateurs sont connectés directement entre eux sans intermédiaire. Ce réseau composé des plusieurs nœud, est un ordinateur lié au réseau de la Blockchain et représente un utilisateur particulier [22]. Chaque nœud va à la fois jouer le rôle de client et de serveur. Ici,

chaque nœud est capable auprès des autres nœuds d'effectuer des requêtes vers eux mais aussi de traiter des requêtes émanant d'eux. Cette modalité de mise en réseau particulière qui permet de ne pas dépendre d'un unique nœud est au cœur de la technologie blockchain.

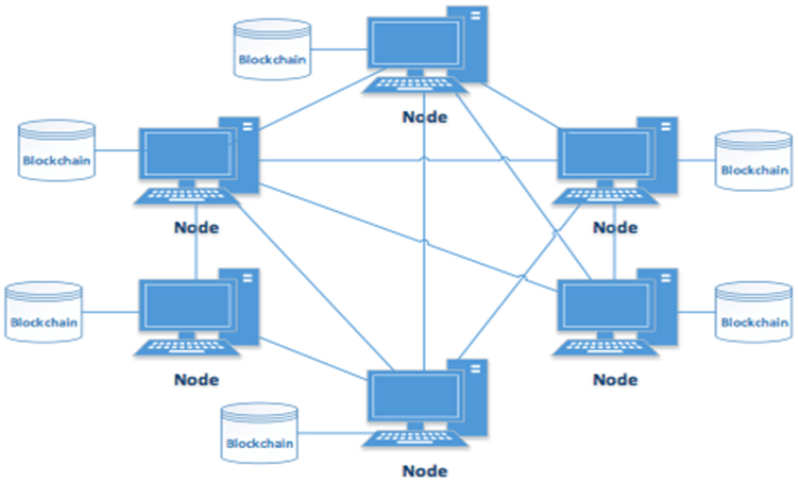

FIGURE 2.3 – Réseau pair à pair (décentralisé)

2.3 Classification de Blockchain

La technologie blockchain continue d'évoluer en ce qui concerne la façon dont les chaînes sont construites, nous pouvons classer les blockchains comme suite [23] :

Blockchain publique

Sont de nature sans autorisation, permettent à n'importe qui de se joindre et sont complètement décentralisées et permettent à tous les nœuds de la blockchain d'avoir des droit signaux pour accéder à la blockchain, créer de nouveaux blocs de données et valider des blocs de données.

À ce jour, les blockchains publiques sont principalement utilisées pour l'échange et l'extraction de crypto-monnaie. Vous avez peut-être entendu parler de blockchain

publique populaire est elles que Bitcoin, Ethereum et Litecoin.Surces Blockchains publiques, les nœuds « Minent » la crypto-monnaie en créant des blocs pour les transactions demandées sur le réseau en résolvant des équations cryptographiques.

Blockchain consortium

Sont des Blockchains autorisées régies par un groupe d'organisations, plutôt qu'une entité, comme dans le cas de la blockchain privée. Les Blockchains du consortium bénéficient donc de plus décentralisation que les Blockchains privées, ce qui entraîne des niveaux de sécurité plus élevés. Cependant, la création de consortiums peut être un processus ardu car il nécessite une coopération entre un certain nombre d'organisations. De plus, certains membres des chaînes d'approvisionnement peuvent ne pas avoir la technologie ni l'infrastructure nécessaires pour mettre en œuvre des outils de blockchain, et ceux qui le font peuvent décider que les coûts initiaux sont un prix trop élevé à payer pour numériser leurs données et se connecter à d'autres membres de la chaîne d'approvisionnement.

Blockchain privée

Également appelées blockchains gérées, sont des blockchains autorisées contrôlées par une seule organisation, l'autorité centrale détermine qui peut être un nœud et n'accorde pas nécessairement à chaque nœud les mêmes droits pour exécuter des fonctions. Elles ne sont que partiellement décentralisées car l'accès du public à ces blockchains est restreint. Quelques exemples de Blockchains privées sont le réseau d'échange de devises virtuelles internet reprises Ripple et Hyperledger, un projet cadre d'applications de blockchain open source.

Les blockchains privées et publiques ont des inconvénients - les blockchains publique sont tendance à avoir des temps de validation plus longs pour les nouvelles données que les blockchains privées, et les blockchains privées sont plus vulnérables à la fraude et aux mauvais acteurs. Pour remédier à ces inconvénients, des blockchains de consortium et hybrides ont été développées.

Type de blockchain / Propriété	Blockchain public	Blockchain privé	Blockchain à Consortium
Qui peut la consulter ?	Tout le monde	Seulement les utilisateurs invités	Cela varie
Centralisé	Non	Oui	Partiel
Vitesse de transaction	Lente	Rapide	Rapide
Immutabilité	Presque impossible à falsifier	Pourrait être falsifié	Pourrait être falsifié
Anonymat des utiisateurs	Oui	Non	Non
Détermination du consensus	Tous les noeuds	Une organisation	ensemble de nœuds sélectionné
Permission	Sans autorisation	autorisé	autorisé

FIGURE 2.4 – Comparaison entre blockchain public, privé, consortium [14]

2.3.1 Fonctionnement de Blockchain Bitcoin

Pour ajouter une transaction dans Blockchain Plusieurs étapes interviennent, ces derniers diffèrent selon le type de Blockchain tels que Bitcoin, il utilise la blockchain et son principe du peer to peer pour échanger des fichiers entre ordinateurs sans autorité centrale. Voici un exemple d'une transaction sur Bitcoin : Au début chaque personne possède un portefeuille Bitcoin pour envoyer et re- cevoir les transactions de bitcoin. Ce portefeuille est composé de deux partie : une « clé privée » qui est un numéro secret entre 0 et 2256-1 généré aléatoirement, permettant au propriétaire de signer les transactions à l'image d'un mot de passe secret ; et une « clé publique » utilisée comme adresse publique personnelle gérée par un algorithme de cryptographie asymétrique appelé ECDSA (Elliptic Curve Digital Signature Algorithm ou algorithme de signature numé- rique sur courbes elliptiques) [24].

— **Étape 1 :**Pour qu'Alice envoie du Bitcoin à Bob, elle se connecte d'abord à son portefeuille à l'aide de sa clé secrète et précise le montant et l'adresse de Bob comme adresse de destinataire [25].

— **Étape 2 :**La transaction est regroupée dans un bloc [25].

— **Étape 3 :** : authentifie la transaction par un acteur du réseau que l'on appelle des "mineurs". à l'aide de la clé publique d'Alice et vérifier qu'Alice a les moyens de réaliser cette transaction, avant qu'elle ne soit inscrite dans la blockchain [25].

— **Étape 4 :**Une fois la transaction sera validée par les mineurs, la mise à jour de la blockchain sera diffusée à tous les mineurs pour assurer le consensus distribué [25].

— **Étape 5 :**bob reçoit notification de la transaction de Alice.

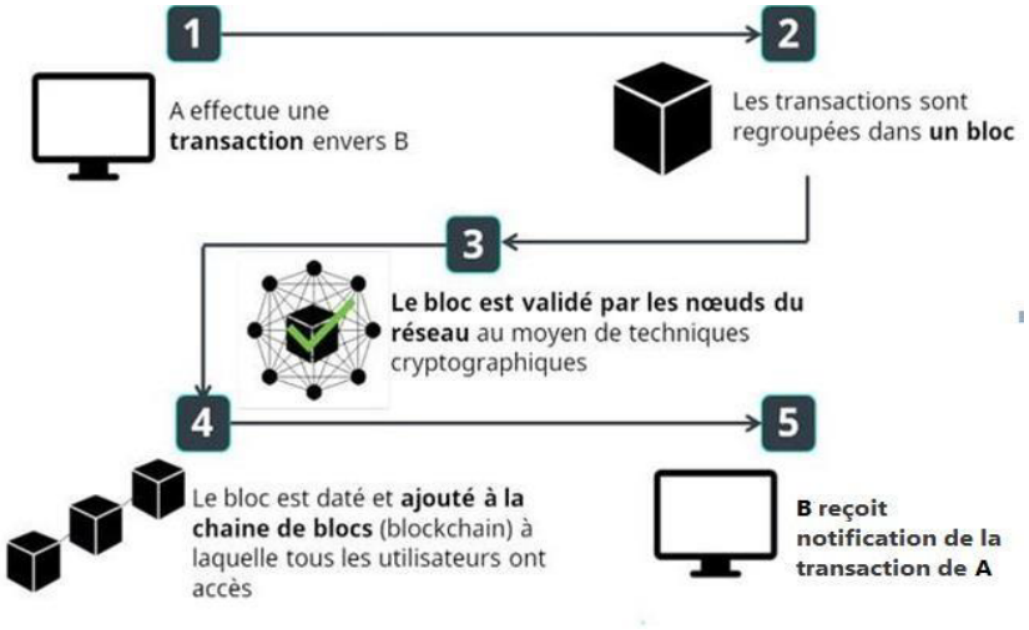

FIGURE 2.5 – Fonctionnement d'une blockchain
[14]

2.3.2 Caractéristique de la blockchain

Maintenant que nous savons ce qu'est une blockchain, nous passerons en revue certaines de ses caractéristique clés :

1. **Décentralisation :** : La Blockchain rend concevable d'échanger des données et des qualités et peut gérer et approuver les tâches accomplies sans l'intercession d'une autorité centrale car chaque nœud du réseau à une autorité et un accès égal sur les enregistrements [26]. En outre, chaque nœud a une copie du grand livre, et a le droit de vérifier ou d'effectuer une transaction [14].

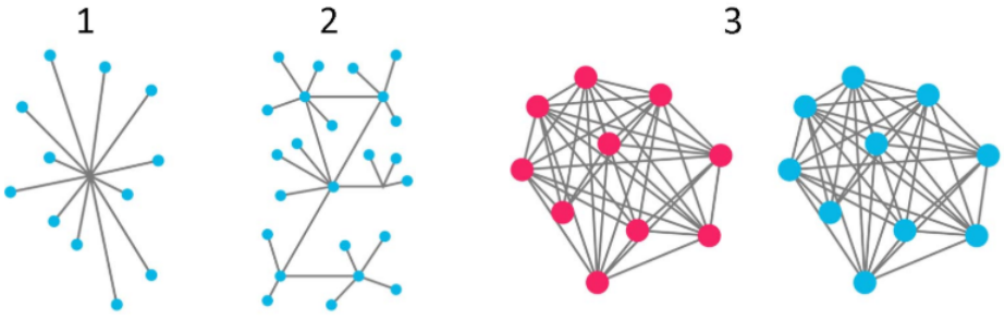

FIGURE 2.6 – Structure d'un système centralisé (1) et décentralisé (2) et (3)

2. **Anonymat :** : Dans le réseau de blockchain, chaque utilisateur peut interagir avec la blockchain avec une adresse personnelle créé, qui maintient la confidentialité de l'identité de l'utilisateur [14].
3. **Auditabilité :** étant donné que chacune des transactions sur la Blockchain est validée et enregistrée avec un horodatage, les utilisateurs peuvent facilement vérifier et retracer les enregistrements précédents [14].
4. **Simplicité (transparence) :** la Blockchain est transparente, car n'importe qui peut la télécharger complètement et vérifier son authenticité à tout moment. N'importe qui peut voir les échanges, les échanges actuels et passés, permettant à chacun de vérifier la légitimité de la chaîne [26].
5. **Persistance :** étant donné que chacune des opérations d'épandage à travers le réseau doit être confirmée et enregistrée dans des blocs répartis dans l'ensemble du réseau, il est presque impossible de les falsifier. En outre, chaque bloc serait diffusé validé par d'autres nœuds et les transactions seraient vérifiées. Donc, la falsification pourrait être détectée facilement [26].

6. **Sécurité :** l'information n'est pas facilitée par un serveur solitaire mais par une partie des clients, ce qui rend inconcevable l'annulation de tous les doublons des rapports [26].
7. **Indépendance :**le pouvoir d'enregistrement et l'espace de facilitation sont donnés par les centres d'organisation, par exemple les clients réels. Il n'y a donc pas d'exigence de cadre focal, au motif qu'il est diffusé à tous les clients [26].

2.4 Sécurité dans Blockchain

2.4.1 Notion de cryptographie

Les blockchains sont sécurisées par différents mécanismes, notamment par des techniques cryptographiques avancées. Donc, il est important de comprendre les concepts de base et les mécanismes qui assurent une protection efficace de ces systèmes à savoir les signatures numériques, et les fonctions de hachage et tout d'abord, il faut passer par les modes cryptographiques dits asymétrique.

Cryptographie Asymétrique

La cryptographie asymétrique est un élément fondamental de la technologie blockchain. Elle exige que chacun des correspondants possède une clé publiée dans un annuaire utilisée par tout le monde pour chiffrer des messages destinés à un individu particulier, et l'autre privée que cet individu est seul à détenir et qui lui permet de déchiffrer les messages qu'il reçoit [27]. Pour mieux comprendre le fonctionnement de la cryptographie asymétrique, nous retraçons ses principales étapes sur un exemple. Considérons une communication entre deux personne SARA et MINA illustrée à la figure 2.9 :

— SARA écrit un message, et souhaite l'envoyer à un destinataire en s'assurant qu'aucun intermédiaire ne puisse le lire.

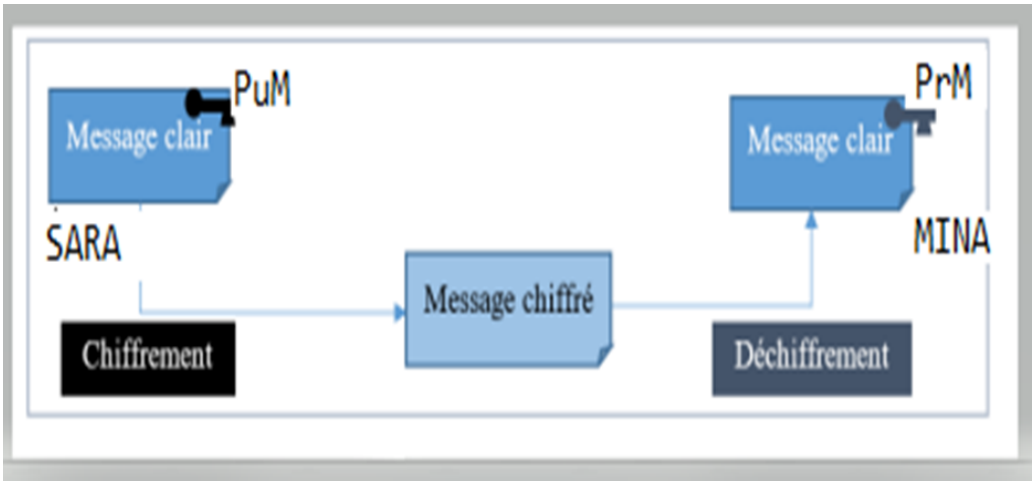

FIGURE 2.7 – Principe de la cryptographie asymétrique

— SARA et MINA génère leurs paires de clés (publique, privée) : (PuM,PrM) et (PuS,PrS).

— SARA chiffre son message avec la clé publique de MINA afin de garantir que seul MINA pourra déchiffrer le message.

— Ainsi pour lire le massage de SARA, MINA décrypte le message chiffré à l'aide de sa clé privée.

Utilisation de cryptographie asymétrique dans Blockchain La cryptographie Asymétrique permet à [28] :

— Un client de signer un échange effectué sur le registre public de la Blockchain.

— Confirmer qu'il en est bien le créateur.

L'expression « inégale » vient de l'idée de la donnée fondamentale pour le chiffrement de l'information :

— Une section est privée (la clé privée ou clé de chiffrement, connue distinctement du client)

— Une section est publique (la clé publique ou clé de décryptage, connue de toute l'organisation).

Chaque client dispose, en relation avec son porte-monnaie électronique, d'une clé privée et d'une clé publique. Solidement, le cryptage des échanges est simple pour la plupart des entreprises clientes puisqu'il est robotisé par des portefeuilles électroniques.

Signature numérique

Les signatures numériques permettent au bénéficiaire de vérifier l'authenticité de l'information, son point de départ, mais aussi de garantir qu'elle est irréprochable. En conséquence, les signatures numériques assurent la confirmation et l'honnêteté des informations. Ils donnent en outre une utilité de non-renoncement. Une signature informatisée répond à un besoin similaire à une signature manuscrite. Dans tous les cas, une marque transcrite peut être efficacement imitée, tandis qu'une marque informatisée est pratiquement infalsifiable. De plus, il garantit la substance des données, tout comme l'identifiant du signataire [29].

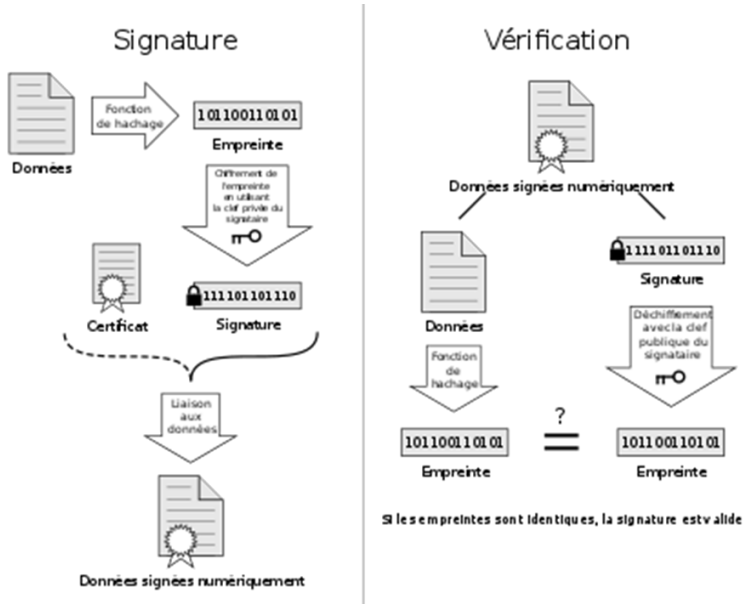

FIGURE 2.8 – Signature numérique
[30]

Utilisation de signature numérique dans Blockchain La signature numérique est l'une des primitives cryptographiques les plus importantes qui rend la blockchain publiquement vérifiable et avec un consensus réalisable, il utilisés dans presque toutes les blockchains pour signer la transaction, assurer trois aspecte de sécurité principale sont authentification, l'intégrité ainsi que la non-répudiation [31].

— **Intégrité :** récepteur peut confirmer que la transaction d'expéditeur n'a pas été modifiée entre envoyer et recevoir.

— **Confirmation (authentification) :** tant que la clé privée d'expéditeur reste secrète, le récepteur peut utiliser sa clé publique pour affirmer que les transactions avancées ont été faites par expéditeur qui plus est personne d'autre.

— **Non-répudiation :** Une fois la transaction, expéditeur ne peut nier l'avoir appliquée plus tard, sauf si sa clé privée est compromise d'une manière ou d'une autre [32].

Hachage

Une fonction de hachage est un algorithme permettant de calculer une empreinte de taille fixe à partir d'une donnée de taille quelconque [33]. L'utilisation de fonctions de hachage permet par conséquent d'accélérer des opérations comme le tri, l'insertion ou l'accès à un élément, Elle possède deux caractéristiques essentielles [34] :

— Ces fonctions sont à sens unique car il est impossible de retrouver les données initiales à partir de l'empreinte.

— Une fonction est « sans collision » lorsqu'il est réputé très difficile de trouver deux sources différentes conduisant à un même résultat (même empreinte).

Utilisation de hachage dans Blockchain

Chaque bloc possède un identifiant (signature) qui prend la forme d'un « hash» permettant de relier les blocs les uns aux autres, le hachage est effectué à partir du contenu du bloc c'est-à-dire le hash du bloc précédent, un certain nombre de transactions et un horodatage comme l'on montre dans la figure 2.10. Cet hash est toujours le résultat du « hachage » du bloc précédent C'est le condensé électronique

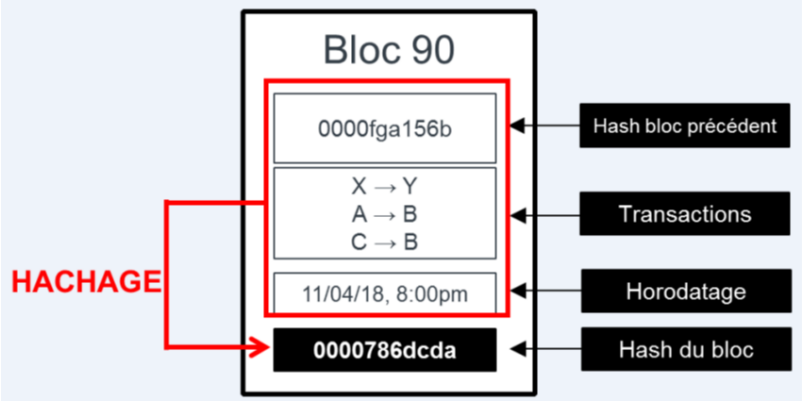

FIGURE 2.9 – Rôle de hash dans les blocs

de 256 bits d'un bloc de données de la blockchain, Cette signature électronique (empreinte) de 256 bits est obtenue grâce à un algorithme de chiffrement dit asymétrique (Exemple : SHA 256, Keccak-256) [35].

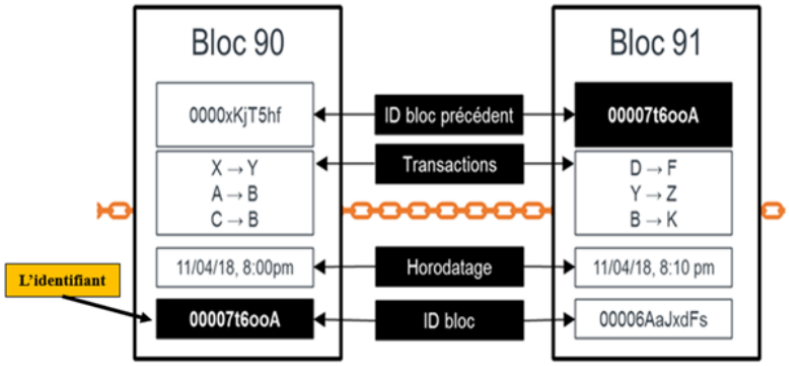

FIGURE 2.10 – Deux blocs relié et le rôle des haschs [39]

La particularité "transparente" de Blockchain mettre les tout modifications étant visible dans l'ensemble des blocs suivants et les blocs sont tous liés entre eux crypto graphiquement, donc chaque fois modifier le contenu d'un bloc suppose de recalculer les haschs de tous les blocs qui le suivent [36].

2.5 Contrat intelligent (Smart Contrat)

Smart contrat a été définie en 1994 par l'informaticien et cryptographe américain Nick Szabo ‘’ un smart contrat est un protocole de transaction informatique qui exécute les termes d'un contrat" [37].

Les smart contrats dans le contexte de la blockchain constituent juridiquement des « programmes autonomes, codés sur la blockchain, qui exécutent automatiquement tout ou partie d'un contrat sans intervention humaine. Dès lors qu'une des conditions préprogrammées du smart contrat se réalise, la clause contractuelle lui correspondant est automatiquement exécutée » [37].

La mise en œuvre du smart contrat fait par trois étapes [37] :

— **Étape 1 :** programme le smart contrat, de sorte qu'il transpose une ou plusieurs clauses du contrat traditionnel (par exemple, la rémunération) dans le langage de programmation du système blockchain.

— **Étape 2 :** sauvegarder le programme informatique associé au smart contrat dans une blockchain.

— **Étape 3 :** exécute le programme informatique, qu'il s'agisse d'une exécution immédiate de la transaction comme le paiement électronique ou d'une exécution déclenchée plus tard par un événement interne au smart contrat ou externe.

Avantages de smart contrat

Le smart contrat fourni certain avantage tels que :

— **Impartialité et sa rapidité d'exécution :** Une fois inscrit dans la blockchain, le contrat est immuable et s'exécutera sans aucun biais. Par exemple La Blockchain "Ethereum" utilise la preuve de travail, à savoir qu'un mineur propose un nouveau bloc contenant des obligations des contrats contenus dans la blockchain, Si jamais il tente de favoriser une partie dans l'exécution d'un contrat, alors le bloc qu'il propose ne sera pas accepté par les autres mineurs.

— **Coût de gestion très faible :** Bien que les mineurs des blockchains soient payés pour confirmer les blocs, le coût d'exécution d'un contrat est infime com-

paré à un contrat qui demanderait l'intervention d'un notaire ou d'un avocat. Plus le code qui représente le contrat est complexe, plus le coût est élevé.

2.6 Conclusion

Au cours de ce chapitre, nous avons fait un résumé sur la technologie de blockchain, défini la blockchain, ses principales caractéristiques, son fonctionnement ainsi que son utilité dans la sécurité. La blockchain a dépassé largement son application classique de monnaie électronique sans autorité centrale. Cette technologie a apporté des nouveaux concepts qui assurent l'immutabilité et renforce la sécurité.
Ces caractéristiques rendent la technologie de blockchain appropriée pour plusieurs domaines, tels que : les systèmes de vote, de santé et de gestion sécurisée des ITL sous laquelle s'inscrit notre travail décrit sur le prochain chapitre.

CHAPITRE 3

ITL SÉCURISÉ PAR BLOCKCHAIN

3.1 Introduction

L'utilisation intensive des véhicules sur les routes appelle des solutions efficaces. Afin d'améliorer la sécurité routière, des méthodes populaires telles que le GPS et l'Internet des objets (IoT) se sont avérées efficaces pour prévenir les accidents de la route en utilisant des données fiables.
La blockchain est devenue une approche prometteuse car elle implémente la solution distribuée au sens le plus vrai en utilisant l'algorithme de consensus et le registre distribué. Dans notre cas, nous proposons un nouveau système qui utilise la technologie Blockchain pour sécuriser le partage des informations relatives au fonctionnement des intersections qui soient de grande importance.
La validation de l'intégrité des solutions calculées est appliquée avant le consensus dans Blockchain et est effectuée à l'aide de techniques de cryptage et de signature électronique. Ainsi, notre proposition peut protéger de manière robuste le partage d'informations sur le trafic contre le vandalisme.
Au niveau de ce chapitre nous allons décrire notre solution décentralisée intelligente pour améliorer la sécurité de traffic light sur quatre intersection qui s'appuie sur la

technologie blockchain, afin d'assurer la sécurisation de systèmes de feu de circulation contre certaines attaques.

3.2 Conception

Afin de résoudre le problème de contrôle des feux de circulation, nous l'avons formulé comme suite :

3.2.1 Formalisation du problème de traffic light

On considère que chaque intersection est caractérisée par les propriétés suivantes :

1. une intersection est supposée être formée de quatre routes etiquetées en Route0, Route1, Route 2et Route3 comme le montre la figure suivante.

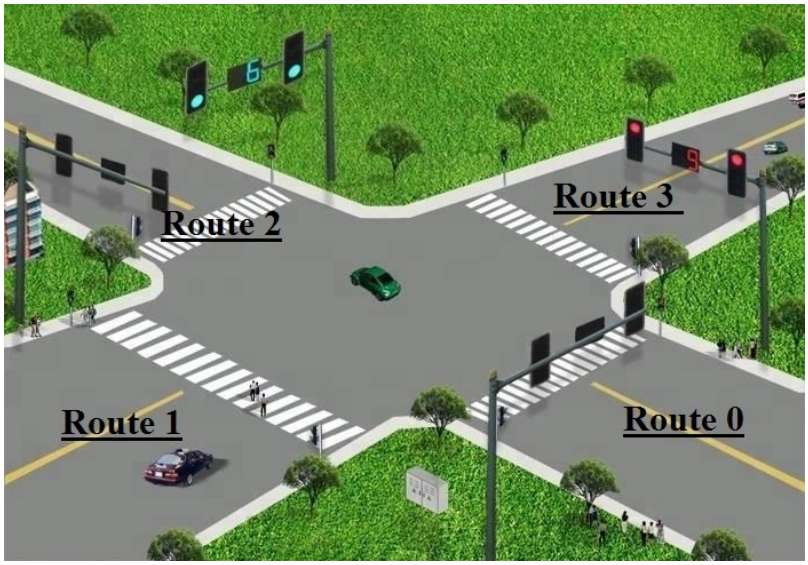

FIGURE 3.1 – Etiquetage de routes dans une intersection.

2. Chaque route est supposée être formée de deux lignes étiquetées en : ligne 1 et ligne 2. (Figure 3.2).
3. Nous considérons quatre intersection intersection 0,1,2,3.

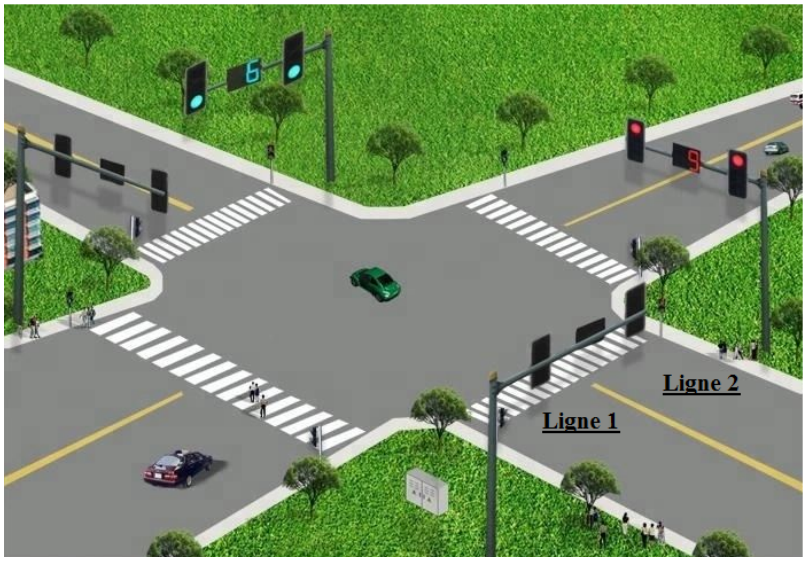

FIGURE 3.2 – - Etiquetage des lignes dans une intersection.

4. chacune des quatre intersections est contrôlée par un traffic light.
5. Le même temps est attribué aux lignes opposées dans une intersection. Par exemple, sur la Figure 3.3, la ligne 2 (l2) sur la route 0 (R0) et la ligne 1 (l1) sur la route 2 (R2) sont des lignes opposées :

   Sur une intersection, les véhicules se déplacent sur les routes suivant trois directions (figure 3.4) :

   — Soit tourner à droit .
   — Ou passe tout droit .
   — Ou tourner à gauche .

6. **Combinaison verte**

Elle représente le temps accordé aux différentes routes des quatre intersections (valeurs des temps verts). Dans notre cas, et en considérant l'état de la route à un instant donné, nous calculons une combinaison de temps permettant de faire passer le maximum de voitures engagées sur les différentes intersections en vérifiant les contraintes nécessaires (lignes opposées). Cette combinaison est appelée Combinaison verte. Elle est représentée par un vecteur de 16 valeurs tel que :

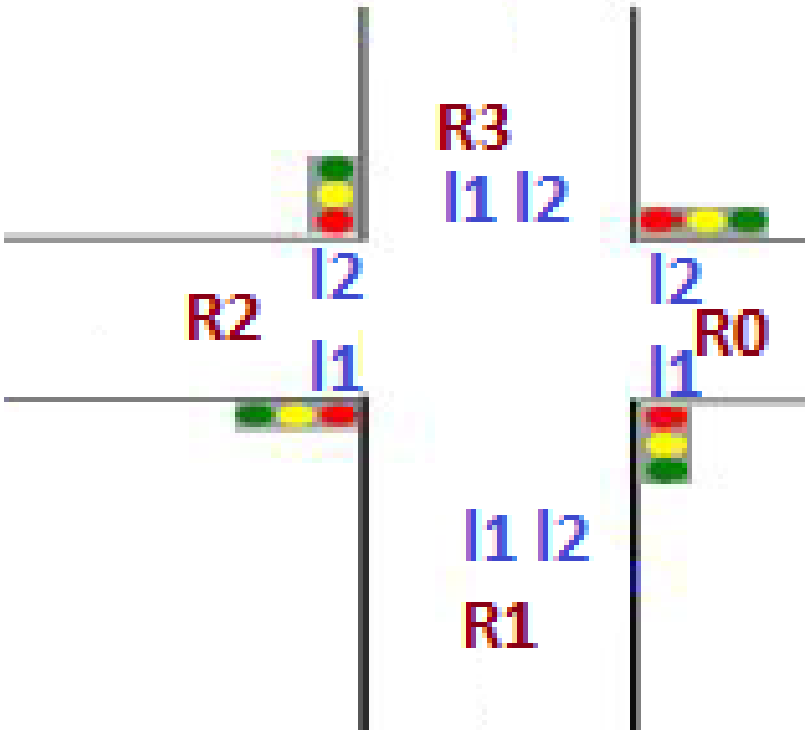

FIGURE 3.3 – les feux synchrones à une intersection.

— De gauche à droite, chaque quatre valeurs consécutives représentent les temps verts attribuées aux quatre routes d'un intersection

— Le temps vert est calculé en fonction du nombre de voitures sur une intersection, ce qui signifie que la route la plus encombrée sera la première à libérer en plus de sa route opposée. Cela permet d'adapter de manière dynamique le temps vert accordé à une route en fonction de son état.

— Les valeurs de G,I,J,K indique (figure 3.5) :

tel que : G I J K : est le temps vert accordé à l'intersection I, route J et ligne K.

Pour calculer ce dernier, nous utilisons l'algorithme appelé calculateur chargé de calculer le nombre de voitures sur la route pour les deux lignes opposées, de sorte

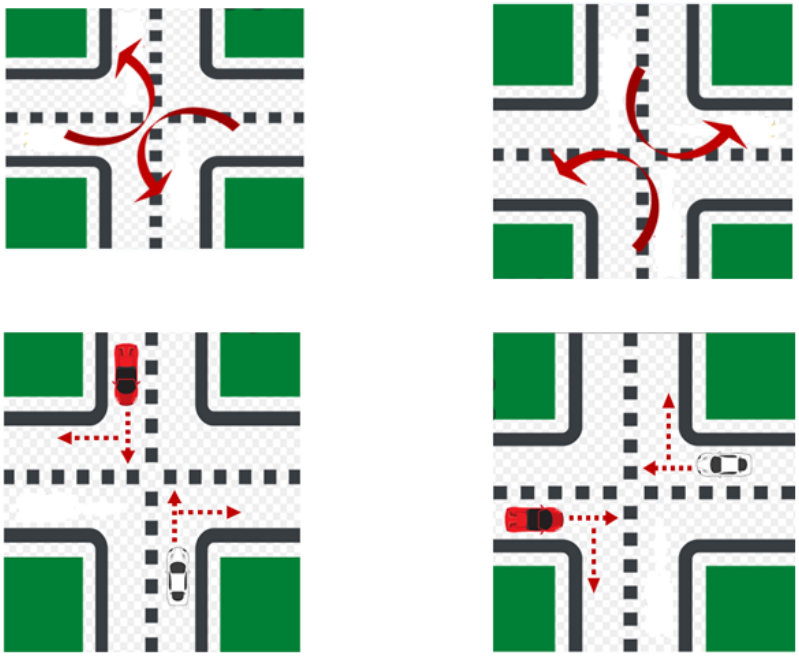

FIGURE 3.4 – – les itérations possibles des véhicules dans quatre intersections.

G 1.1.1	G 1.1.2	. . .	G 2.4.2	G 3.1.1	. . .	G4.4.1	G 4.4.2

FIGURE 3.5 – – Combinaison verte.

qu'il prenne le plus grand nombre de voitures dans la ligne et le fixe comme temps pour le feu vert. L'algorithme appelé Applicateur se charge de l'application de la combinaison verte suivant les plans de routes illustrés sur les matrices présentées sur la section 3.6.

Algorithm 1 Calculateur

```
if interin =0 then
    inter = self.monde.inter1
else
    if interin =1 then
        inter = self.monde.inter2
    else
        if interin =2 then
            inter = self.monde.inter3
        else
            inter = self.monde.inter4
        end if
    end if
    r1 = 0
    j = 14
end if
for iin range(10) : do
    if inter.cases[10][j] = 1 then
        r1 = r1 + 1
    end if
    j = j + 1
end for
r2 = 0
j = 9
for iin range(10) : do
    if inter.cases[13][j] = 1 then
        r2 = r2 + 1
    end if
end for
j = j − 1
if r1 > r2 then
    returnr1
else
    returnr2
end if
```

Les variable inter, r1, r2, j indique :

— inter : Déterminer l'intersection à laquelle se trouve la voiture .

— r1,r2 : Sont des compteurs utilisé pour calculer le nombre de voiture dans la route.

— j : Représente les coordonnées pour rechercher des voitures dans la ligne .

Algorithm 2 Applicateur

```
while (True) : do
  if  self.inter.sol.sol[0] > 6) : then
    self.inter.sol.solAct = 0
  end if
  if (self.inter.sol.sol[1] > 6) : then
    self.inter.sol.solAct = 1
  end if
  if (self.inter.sol.sol[2] > 6) : then
    self.solAct = 2
  end if
  if  (self.inter.sol.sol[3] > 6) : then
    self.inter.sol.solAct = 3
  end if
  time.sleep(0.5)
  if (self.inter.sol.solAct == 0) : then
    self.inter.sol.stop[10][14] = 0
    self.inter.sol.stop[13][9] = 0
  end if
  if  (self.inter.sol.solAct == 1) : then
    self.inter.sol.stop[11][14] = 0
    self.inter.sol.stop[12][9] = 0
  end if
  if (self.inter.sol.solAct == 2) : then
    self.inter.sol.stop[9][10] = 0
    self.inter.sol.stop[14][13] = 0
  end if
  if (self.inter.sol.solAct == 3) : then
    self.inter.sol.stop[9][11] = 0
    self.inter.sol.stop[14][12] = 0
  end if
  time.sleep(self.inter.sol.sol[self.inter.sol.solAct]/3)
  self.inter.sol.solAct = self.inter.sol.solAct + 1
  if (self.inter.sol.solAct == 4) : then
    self.inter.sol.solAct = 0
  end if
end while
```

3.3 Solutions proposées

Notre but est de créer un système de contrôle intelligent sécurisé des feux de circulation, où la fonction principale de ce système est d'assurer une transmission sécurisée par blockchain de la combinaison des temps verts accordées aux quatre intersections .
Basant sur le code trouvé dans [38], qui est le code d'une version simplifiée d'une blockchain.

3.3.1 Architecture de blockchain adoptée

Dans cette section, nous présentons l'architecture de la blockchain adaptée pour assurer la sécurisation des traffic light. Nous présentons, ainsi, les concepts relatifs à : transaction, bloc, consensus, etc.

— – **a- Noeud :** Dans notre application, nous étudions le trafic à quatre intersections.Par conséquent, chaque intersection est un nœud dans notre réseau blockchain.

— – **b- Transaction :** C'est la solution calculée à chaque intersection, qui, comme nous l'avons mentionné précédemment, est un vecteur à 16 valeur contenant les valeurs du temps vert accordées aux quatre intersections. Les transactions entre les noeuds sont envoyées et reçues via ce que l'on appelle le portefeuille électronique.

— – **c- Portefeuille électronique** Chaque nœud possède un portefeuille et il est considéré comme un compte composé des éléments suivants :

— – • **Clé publique :** elle est générée de manière aléatoire et est une valeur hachée. Elle est considérée comme une adresse publique personnelle pour chaque nœud (intersection).

— – • **Clé privée :** elle est générée de manière aléatoire, et considérée comme le mot de passe du nœud utilisé pour signer les transactions, donc, qui doit être gardée secrète. Elle est créée comme suit :

```
random_gen = Crypto.Random.new().read
self.clePrv = RSA.generate(1024, random_gen)
self.clePub = self.clePrv.publickey()
self.clePrv = binascii.hexlify(self.clePrv.exportKey(format='DER')).decode('ascii')
self.clePub = binascii.hexlify(self.clePub.exportKey(format='DER')).decode('ascii')
```

FIGURE 3.6 – – génération de clé publique et privée.

— – **d- Bloc :** Chaque bloc est constitué de plusieurs champs :

– **Index :** l'indice de bloc.

– **HashPr :** champ contient l'empreinte du bloc précédant.

– **Transaction :** la partie qui contient la liste des transactions. Pour notre cas, on dispose d'une seule transaction représentative de la combinaison verte..

– **Signe transaction :** la signature de transaction est codé comme suit :

Algorithm 3 signeTransaction(self,transaction) :

$private_key = RSA.importKey(binascii.unhexlify(self.portfeille.clePrv))$
$signer = PKCS1_v1_5.new(private_key)$
$h = SHA.new(str(transaction.to_dict()).encode('utf8'))$
$returnbinascii.hexlify(signer.sign(h)).decode('ascii')$

– **Nbr Transaction :** le nombre total de transactions confirmées. Pour notre cas ce nombre est fixe à un car chaque bloc contient une seule transaction validée.

— – **e-Mineur, Minage :** Le processus de minage est utilisé pour valider le bloc. Une fois la transaction propagée dans les intersections, les mineurs vérifient la validité de la transaction en effectuant une comparaison de la transaction envoyée par le nœud émetteur, avec la transaction calculée par le mineur récepteur.
donc l'algorithme de vérification :

Algorithm 4 verify$_t ransaction_s ignature(self, signature, transaction)$:

$public_k ey = RSA.importKey(binascii.unhexlify(transaction.cle Pub))$
$verifier = PKCS1_v1_5.new(public_k ey)$
$h = SHA.new(str(transaction.to_d ict()).encode('utf8'))$
$returnverifier.verify(h, binascii.unhexlify(signature))$

— – **f- Consensus :** : Le but du processus de consensus permet de s'assurer que la transaction a été vérifiée et validée par les trois mineurs correspondant aux trois intersections avant de l'insérer sur un nouveau bloc qui sera rajouté à la blockchain. Ainsi, si un mineur ne valide pas une transaction donnée, elle sera rejetée et un nouveau calcul de combinaison verte sera lancé. Plus de détails sur l'enchainement des différentes étapes et rôles seront donnés sur la figure 3.7. .

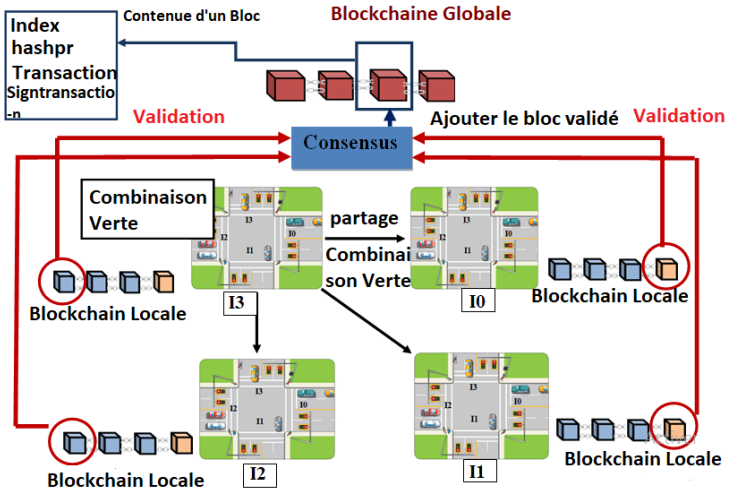

FIGURE 3.7 – –Architecture générale de notre application.

La figure ci-dessus résume les différents composants et étapes de calcul et de transfert sécurisé de la combinaison verte assurant une gestion dynamique de quatre intersection via la technologie de blockchain. En effet, un calculateur est attribué pour chacune des intersections qui joue un double rôle de calculateur de combinaison verte et de mineur chargé de valider localement (à son niveau) une transaction reçue

et calculée par un calculateur délégué (choisi aléatoirement) parmi les quatre disponibles. A ce niveau, une blockchain locale est impliquée comportant à la fois une copie des transactions précédemment validées localement ou meme globalement à travers le processus de consensus. Ce dernier représente un dernier stade de validation global d'une transaction à rajouter à la fin du compte à la blockchain principale.

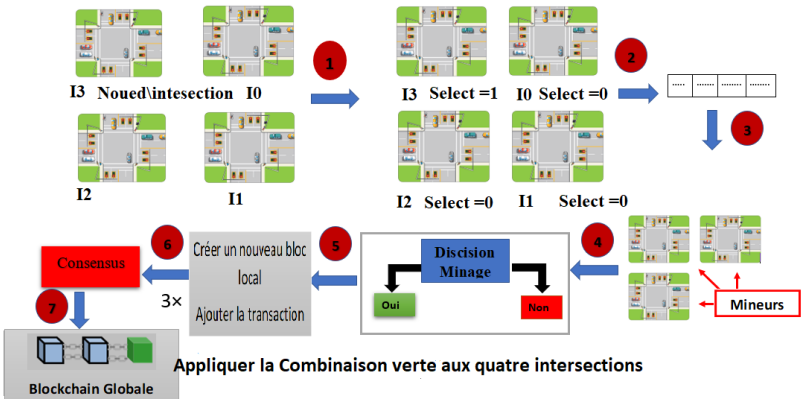

FIGURE 3.8 – -Schéma fonctionnel du système proposé.

Tel que : Select =1 => Ii = calculateur de combinaison verte.
Select = 0 => Ii = Mineur .

1. => : Choisir un calculateur aléatoirement parmi les quatre.
2. => Calculer et signer la combinaison verte par le calculateur choisi.
3. =>Partager la combinaison calculée aux trois autres calculateurs (mineurs).
4. => Minage : Vérifier la signature Calculer localement une autre combinaison verte. Comparer les deux combinaisons reçue et calculée.
5. => :Si la combinaison est validée (décision minage=oui), la transaction correspondante sera rajoutée à un nouveau bloc créé pour la contenir. Et enfin, ce dernier sera rajouté à la blockchain locale (propre au calculateur local). Le même processus est appliqué au niveau des trois calculateurs récepteurs (Mineurs).
6. => Consensus : c'est la validation globale de la transaction. Autrement dit, il consiste à vérifier la validation de la transaction par l'ensemble des mineurs.

7. => Si le consensus se termine par validation de la transaction, cette dernière sera rajoutée via un bloc à la blockchain globale et la transaction sera exécutée réellement (appliquer la combinaison verte aux quatre intersections).

3.4 Analyse et discussion

Notre proposition permet de sécuriser un intelligent Traffic light basé sur la technologie de blockchain. Dans cette partie nous présenterons, interpréterons et discuterons les principales fonctionnalités offertes par notre système.

Intérêt de blockchain dans notre système :

— • Les systèmes de cryptage, les portefeuilles électroniques et la signature électronique garantissent que nous maintenons et protégeons la sécurité des transactions, Cette protection consiste à empêcher les entités non autorisées d'accéder aux transactions dans le système afin de les détruire et d'empêcher toute altération abusive du système.

— • Outre l'importance du principe de consensus.

— • Accès facile à l'historique de la blockchain en accédant à la liste des transactions qui ont été effectuées.

3.2. Sécurisation contre les falsifications de la combinaison verte

Une attaque contre la combinaison verte calculée par l'une des intersections, doit strictement falsifier cette combinaison au niveau de toutes les intersections à la fois car elle doit etre approuvée (validée) par toutes les intersections avant d'être appliquée réellement sur les feux de circulation. En étendant cet effet à des villes comptant un grand nombre d'intersections, il devient plus compliqué de le réussir sur le plan effort et temps.

3.5 Environnement de développement

3.5.1 Language utilisé

Python

Il s'agit d'un langage de programmation interprété, qui ne nécessite donc pas d'être compilé pour fonctionner, orienté objet et de haut niveau avec une sémantique dynamique. Un programme interpréteur » permet d'exécuter le code Python sur n'importe quel ordinateur. Ceci permet de voir rapidement les résultats d'un changement dans le code, L'interpréteur Python et la bibliothèque standard étendue sont disponibles sous forme source ou binaire sans frais pour toutes les principales plates-formes, et peuvent être librement distribués. En tant que langage de programmation de haut niveau, Python permet aux programmeurs de se focaliser sur ce qu'ils font plutôt que sur la façon dont ils le font. Ainsi, écrire des programmes prend moins de temps que dans un autre langage. Il s'agit d'un langage idéal pour nous comme étudiant. Le langage Python doit sa popularité à plusieurs avantages qui profitent aussi bien aux débutants qu'aux experts. Tout d'abord, il est facile à apprendre et à utiliser. Ce qui permet de créer des programmes rapidement et avec peu d'efforts. De plus, sa syntaxe est conçue pour être lisible et directe. Enfin, même s'il est principalement utilisé pour le Scripting et l'automatisation, ce langage est aussi utilisé pour créer des logiciels de qualité professionnelle. Qu'il s'agisse d'applications ou de services Web, le Python est utilisé par un grand nombre de développeurs pour créer des logiciels.

Pycharm

Vu que Pycharm est l'API Python est la plus complète, nous avons choiside travailler avec. C'est un bon environnement de développement dédire au langagePython.

3.6 Structure de notre application

Nous présentons dans cette section une description de la structure de notre application contenant les classes suivantes :

3.6.1 La classe Règles Conduite Inter

```
def __init__(self):
    self.sort=[[0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,0,0,0,0,0,0,0,0,0],
               [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
               [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
               [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
               [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
               [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
               [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
               [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
               [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
               [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
               [1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
               [1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
               [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1],
               [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1],
               [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
               [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
               [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
               [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
               [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
               [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
               [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
               [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
               [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
               [0,0,0,0,0,0,0,0,0,0,1,1,0,0,0,0,0,0,0,0,0,0,0,0]]
```

FIGURE 3.9 – -Une matrice représentant les premières entrées de voitures à un carrefour.

Cette matrice, illustrée sur la figure 3.9,est utilisée pour repérer les entrées des voitures (les lignes sur les intersections) à partir des valeurs qui égalent à 1. Nous utilisons aussi d'autres matrices qui indiquent les directions de la voiture (gauche / droite / continuer tout droit). Par exemple, la matrice donnée sur la figure 3.10 illustre les positions à entreprendre pour tourner à gauche.

Cette matrice aide la voiture à changer sa position vers la gauche de sorte que si la position dans laquelle elle est plus petite que la position suivante prend ses nouvelles coordonnées et détermine la trajectoire de la voiture.

La matrice donnée sur la figure 3.11 est utilisée pour déterminer les positions d'arrêt de voitures sur les différentes lignes de l'intersection, de sorte que si la valeur vaut 1, cela signifie que la voiture s'arrête au signal Sinon, si elle vaut 0, cela signifie que le feu vert de la ligne correspondante est allumée, permettant ainsi aux voitures de passer.

Cette matrice (figure 3.13) aide la voiture à changer sa position vers la droite de

```
self.reglelgauche=[[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,11,10,9,8,7,6,5,4,3,2,1],
                   [0,0,0,0,0,0,0,0,0,0,0,0,12,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,13,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,14,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,15,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,16,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,17,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,18,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,19,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,20,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,21,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,22,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,23,0,0,0,0,0,0,0,0,0,0,0,0]]
```

Figure 3.10 – -Matrice indiquant que la voiture va tourner à gauche.

```
self.stop=[[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
           [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
           [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
           [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
           [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
           [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
           [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
           [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
           [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
           [0,0,0,0,0,0,0,0,0,0,1,1,0,0,0,0,0,0,0,0,0,0,0,0],
           [0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0],
           [0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0],
           [0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
           [0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
           [0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,0,0,0,0,0,0,0,0,0],
           [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
           [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
           [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
           [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
           [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
           [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
           [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
           [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
           [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]]
```

Figure 3.11 – -Matrice indiquant l'arrêt des voitures sur les feux de circulation.

sorte que si la position dans laquelle elle se trouve est plus petite que la position suivante, elle prend ses nouvelles coordonnées.

```
self.regle1direct=[[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [24,23,22,21,20,19,18,17,16,15,14,13,12,11,10,9,8,7,6,5,4,3,2,1],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]]
```

FIGURE 3.12 – - Matrice indiquant que la voiture va continuer tout droit.

```
self.regle1droite=[[0,0,0,0,0,0,0,0,0,0,0,0,0,21,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,20,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,19,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,18,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,17,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,16,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,15,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,14,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,13,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,12,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,11,10,9,8,7,6,5,4,3,2,1],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
                   [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]]
```

FIGURE 3.13 – Matrice indiquant que la voiture va tourner à droite

3.6.2 La classe intersection

Cette classe contient les informations relatives au numéro de l'intersection et des routes en plus de la manière dont les voitures roulent au niveau de la route, ce qui nous permet de localiser une voiture ou d'ajouter une nouvelle voiture sur la route suivant les méthodes illustrées ci-dessous :

nextVoiturePos :définit la position suivante d'une voiture sur la route. Elle peut se déplacer si et seulement si cet emplacement est vide.

ajtVoiture : permet de générer (insérer) des voitures au niveau des quatre entrées comme indiqué sur la figure 3.9.

3.6.3 La classe voiture

Cette classe contient les coordonnées d'une voiture, à savoir la route (ligne) et l'intersection sur laquelle elle se trouve, et la direction à entreprendre. Elle utilise également les méthodes de la classe intersection afin de déterminer sa position exacte.

3.6.4 La classe Monde

C'est un thread dans lequel on retrouve la forme générale de la fenêtre introduite à travers une matrice carrée de 48*48 contenant les quatre intersections. Les règles de conduite sur route sont exprimées à travers les méthodes suivantes :

Passvoiture(self,v) : Ici, nous définissons comment la voiture passe d'une intersection à une autre intersection en précisant le numéro de route et la direction visée.

affMat (self) : Permet l'identification et la division des intersections en dégageant, ainsi, la forme générale de la route.

Run(self) : c'est un groupe de Thread assurant la génération de voitures au niveau de la route sur une durée fixée à 30 secondes .

3.7 Présentation des interfaces

L'objet de notre application est de simuler un système intelligent de feux tricolores dont l'échange des informations de gestion (combinaison des feux verts) est sécurisé par l'exploitation de la technologie de blockchain. Nous présentons dans cette section quelques captures d'écran des interfaces principales de notre application.

3.7.1 L'interface Main

L'interface de main de notre application présente un état initial de la route. Elle englobe quatre intersections sans véhicules, car à ce moment les clés publiques et privées sont calculées pour chaque intersection. Cela prend environ 30 secondes.

FIGURE 3.14 – -L'interface Main.

3.7.2 Interface Instance-trafic

L'interface donnée sur la figure 3.13 illustre une instance de la route calculée par notre système où les véhicules traversent la route en exploitant les quatre intersections de manière ordonnée et sans embouteillages.

FIGURE 3.15 – – Exemple d'une instance de trafic.

3.7.3 L'interfaceBlockchain

La fenêtre relative à l'affichage des résultats obtenus suivant les principes de la blockchain proposée contient les informations suivantes :

— • Création du premier bloc "Genesis bloc"

— • Liste des transactions.

— • Nœuds (intersections) responsables du calcul des solutions.

— • Valeur de chaque transaction (combinaison des temps verts).

— • Le nombre total de blocs dans la blockchain.

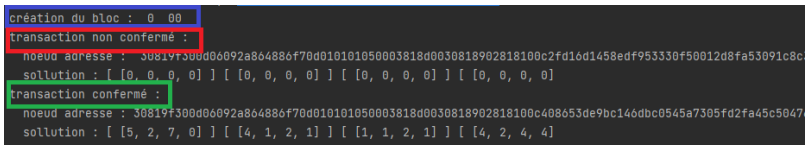

FIGURE 3.16 – – - affichage blockchain..

FIGURE 3.17 – -création d'un nouveau bloc.

3.8 Conclusion

Dans ce chapitre, nous avons présenté puis discuté notre proposition pour sécuriser un Intelligent Traffic light en basant sur la technologie de blockchain pour empêcher des attaques malveillantes contre certains ou à l'ensemble des nœuds (intersections) pour envahir ou entraîner l'effondrement de l'ensemble du système (la ville).
Nous avons, tout d'abord, calculer dynamiquement la combinaison des temps verts assurant une meilleure gestion d'un ensemble d'intersections. Cette combinaison calculée sur l'une des intersections sera déployée aux autres intersections pour validation via les principes de la blockchain.
Ainsi, l'attaque d'altération des feux de signalisation par des personnes non autorisées sera considérablement compliquée en considérant des instances plus importantes du problèmes (ville avec grand nombre d'intersections) grace au processus de double validation proposé (locale et globale).

CONCLUSION GÉNÉRALE

La congestion du trafic sur les routes urbaines est l'un des problèmes sociaux,économiques et environnementaux rencontrés par la plupart des pays du monde qui doivent être résolus pour soutenir le développement de la société. A cet effet de nombreuses méthodes ont été développées pour gérer et améliorer le trafic tels que les feux de circulation intelligents.

Le but de ce travail était d'étudier l'applicabilité de la technologie Blockchain pour sécuriser un Intelligent trafic light. Plus précisément, il s'agit de sécuriser le transfert d'une combinaison calculée de temps verts accordés aux différentes intersections considérées.

En effet, un des calculateurs associés aux différentes intersections sera désigné de manière aléatoire pour calculer, de manière la plus adéquate possible à l'état de la route, la combinaison des temps verts. Cette dernière sera communiquée aux autres calculateurs considérés comme mineurs pour validation locale. Un deuxième stade de validation est confié au processus de consensus de la blockchain. Il s'agit d'une validation globale et finale de la combinaison, a l'issue de laquelle cette proposition sera ajoutée à la blockchain principale avant d'être finalement appliquée en réalité.

Le système, ainsi proposé, a bénéficié de la transparence et de la fiabilité des opérations via blockchain tout en empêchant toute altération ou falsification de données

(combinaison verte).
Au cours de la réalisation de ce projet, nous avons découvert la technologie blockchain, son fonctionnement et sa conception de plus près. Toutefois, le système proposé représente juste un noyau à raffiner et à enrichir. Ainsi et en perspective au travail présenté dans ce mémoire et pour veiller à concrétiser un vrai aspect intelligent permettant de doter le traffic light de plus d'autonomie et de dynamisme, nous envisageons de régler ou d'adapter la sortie du système de gestion de feu de circulation exploitant les algorithmes génétiques proposé par[39]., à l'entrée de notre système. Dans ce cas, chacun des calculateurs situés sur les différentes intersections calcul via l'algorithme génétique, dont nous avons parlé précédemment, une combinaison verte. Le premier convergeant, mettra fin aux autres calculateurs génétiques où le processus de minage aura lieu et qui consiste à vérifier le degré de satisfaction de la combinaison proposée aux conditions de la route.
D'un autre côté, nous envisageons d'enrichir l'architecture de la blockchain proposée en introduisant d'autres nœuds pour garantir d'autres aspects de sécurité tels que l'authentification et pour gérer les différents rôles des nœuds et le passage d'information et de paramètres entre eux surtout dans le cas de systèmes couvrant de grandes villes.

BIBLIOGRAPHIE

[1] A. Wegener, H. Hellbruck, C. Wewetzer, and A. Lubke, "Vanet simulation environment with feedback loop and its application to traffic light assistance," in *2008 IEEE Globecom Workshops*, pp. 1–7, IEEE, 2008.

[2] B. Sammoud, *Contribution à la modélisation et à la commande des feux de signalisation par réseaux de Petri hybrides*. PhD thesis, Université de Technologie de Belfort-Montbeliard ; Université de Tunis El Manar, 2015.

[3] A. Hamilton, B. Waterson, T. Cherrett, A. Robinson, and I. Snell, "The evolution of urban traffic control : changing policy and technology," *Transportation planning and technology*, vol. 36, no. 1, pp. 24–43, 2013.

[4] M. Tlig, *Coordination locale et optimisation distribuée du trafic de véhicules autonomes dans un réseau routier*. PhD thesis, Université de Lorraine, 2015.

[5] A. Maimaris and G. Papageorgiou, "A review of intelligent transportation systems from a communications technology perspective," in *2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*, pp. 54–59, IEEE, 2016.

[6] B. R. guideke and M. onana, "étude simulation des feux de circulation : cas carrefour poste centrale de yaounde :cameroon," 2019.

[7] "Feu de circulation." wikipedia. https://fr.wikipedia.org/wiki/Feu_de_circulation. Page consultée le 25 fevrier 2022, 2022.

[8] Y. Kozin, "Road traffic light in new configuration," *Journal of road safety*, vol. 32, no. 1, pp. 52–54, 2021.

[9] "Intelligent traffic light system based on machine vision." Mahima.W. https://www.researchgate.net/publication/317869924. Page consultée le 25 fevrier 2022, 2012.

[10] G. R. Roberto Jacome, Manuel Augusto Pesantez Gonzalez, "A survey on intelligent traffic lights," 2018.

[11] S. Javaid, A. Sufian, S. Pervaiz, and M. Tanveer, "Smart traffic management system using internet of things," in *2018 20th international conference on advanced communication technology (ICACT)*, pp. 393–398, IEEE, 2018.

[12] S. Nakamoto, "Bitcoin : A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[13] B. Singhal, G. Dhameja, and P. S. Panda, *Beginning Blockchain : A Beginner's guide to building Blockchain solutions*. Apress, 2018.

[14] H. Huang, W. Kong, S. Zhou, Z. Zheng, and S. Guo, "A survey of state-of-the-art on blockchains : Theories, modelings, and tools," *ACM Computing Surveys (CSUR)*, vol. 54, no. 2, pp. 1–42, 2021.

[15] M. C. Villani and M. G. Longuet, "les notes scientifique de l'office note numéro 4 : comprendre les blockchain," tech. rep., 2018.

[16] S. Gupta and M. Sadoghi, "Blockchain transaction processing," *arXiv preprint arXiv :2107.11592*, 2021.

[17] D. Vujičić, D. Jagodić, and S. Ranđić, "Blockchain technology, bitcoin, and ethereum : A brief overview," in *2018 17th international symposium infoteh-jahorina (infoteh)*, pp. 1–6, IEEE, 2018.

[18] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Computing Surveys (CSUR)*, vol. 52, no. 3, pp. 1–34, 2019.

[19] J. Bergquist, "Blockchain technology and smart contracts : Privacy-preserving tools„" 2017.

[20] S. Seibold and G. Samman, "Consensus : Immutable agreement for the internet of value," *KPMG< https ://assets. kpmg. com/content/dam/kpmg/pdf/2016/06/kpmgblockchain-consensus-mechanism. pdf*, 2016.

[21] "Blockchain architecture basics : Components, structure, benefits & creation." https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture.

[22] I. Bashir, *Mastering blockchain*. Packt Publishing Ltd, 2017.

[23] "Types of blockchain : Public, private, or something in between." https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between.

[24] R. Gennaro, S. Goldfeder, and A. Narayanan, "Threshold-optimal dsa/ecdsa signatures and an application to bitcoin wallet security," in *International Conference on Applied Cryptography and Network Security*, pp. 156–174, Springer, 2016.

[25] B. France, "La blockchain décryptée," *Les clefs d'une révolution. Paris, Netexplo*, 2016.

[26] M. Pignel and D. Stokkink, "La technologie blockchain une opportunité pour l'économie sociale ?," 2019.

[27] T. Ebrahimi, F. Leprévost, and B. Warusfel, "Cryptographie et sécurité des systèmes et réseaux," 2006.

[28] "Comprendre la technologie de blockchain." cryptoencyclopedie. https://www.cryptoencyclopedie.com/single-post/quest-ce-que-la-cryptographie-asymetrique. Page consultée le 17 fevrier 2022, 2018.

[29] A. Bakhoum, "La blockchain pour la sécurisation des e-livrets scolaires.," 2019.

[30] Guilieb, "Illustration de signature et vérification d'un message," 2015.

[31] M. Raikwar, D. Gligoroski, and K. Kralevska, "Sok of used cryptography in blockchain," *IEEE Access*, vol. 7, pp. 148550–148575, 2019.

[32] A. Serhrouchni and I. Hajjeh, "Intégrationfr de la signature numérique au protocole ssl/tls," in *Annales des télécommunications*, vol. 61, pp. 522–541, Springer, 2006.

[33] T. Fuhr, *Conception, preuves et analyse de fonctions de hachage cryptographiques*. PhD thesis, Télécom ParisTech, 2011.

[34] J. L. Parouty, R. Dirlewanger, and D. Vaufreydaz, "La signature électronique, contexte, applications et mise en oeuvre.," in *Journées Réseaux (JRES 2003)*, pp. 14–pages, 2003.

[35] P. 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.

[36] M. C. Villani and M. G. Longuet, "Les enjeux technologiques des blockchains (chaînes de blocs)," tech. rep., 2018.

[37] J. Pons, "La mise en œuvre de la blockchain et des smart contracts par les industries culturelles," in *Annales des mines-réalités industrielles*, no. 3, pp. 81–90, FFE, 2017.

[38] "Code python disponible sur." https ://github.com/adilmoujahid/blockchain-python-tutorial. Page consultée le 20 mai 2022, 2018.

[39] W. Bouzenoune, A. Feraga, and I. Souici, *Smart Traffic Light System For Smart Cities.* PhD thesis, University Mohamed Seddik Ben Yahia of Jijel, Algeria, 2021.