République Algérienne Démocratique et Populaire
Université Abou Bakr Belkaid– Tlemcen
Faculté des Sciences
Département d'Informatique

Mémoire de fin d'études

pour l'obtention du diplôme de Master en Informatique

Option: *Réseaux et Système Distribue (R.S.D)*

Thème

Utilisation de la blockchain pour une gestion sécurisée du spectre dans les réseaux radios cognitifs

Réalisé par :

- **Benzellat Djamel Eddine**
- **Halabi Zakarya**

Présenté le 29 Juin 2022 devant le jury composé de MM.

- LEHSAINI Mohammed *(Président)*
- AMRAOUI Asma *(Encadrante)*
- BENMAMMAR Badr *(Examinateur)*

Année universitaire : 2021-2022

Remerciements

Nous remercions tout d'abord Dieu le tout puissant de nous avoir donné la force et la patience pour réaliser ce modeste travail, et d'exprimer ma profonde et sincère gratitude à tous ceux qui, de près ou de loin, ont œuvré pour la réalisation de cet ouvrage.

Nous voudrions dans un premier temps remercier notre encadrante madame Asma AMRAOUI pour le temps, pour sa patience, sa disponibilité et surtout ses judicieux conseils et qui est toujours à notre écoute et nous orienter dans la bonne direction.

Je remercie *Mr LEHSAINI Mohammed* d'avoir accepté de présider le jury, je remercie également *Mr BENMAMMAR Badr* pour avoir accepté de nous prêter leur attention et évaluer notre travail.

Sans oublier nos enseignants pour la qualité de l'enseignement qu'ils nous ont prodigué au cours de ces 5 années et aussi le département d'Informatique de la faculté des sciences.

Enfin, nous tenons à remercier tous les proches qui nous ont aidé et motivé pour l'élaboration de ce mémoire qui a été plein d'embûches.

Dédicaces

C'est avec profonde gratitude et sincères mots, que nous dédions

ce modeste travail de fin d'étude à nos chers parents,

qui ont sacrifié leur vie pour notre réussite

et nous ont éclairé le chemin par leurs conseils judicieux.

Nous espérons qu'un jour, nous pourrons leur rendre un peu de ce qu'ils ont fait pour nous, que dieu leur prête bonheur et longue vie.

Nous dédions aussi ce travail à nos frères et sœurs, nos familles, nos amis,

tous les professeurs qui nous ont enseigné et à tous ceux qui nous sont chers.

Table de matières

Liste des figures

Liste des tableaux

Liste des abréviations

- **BFT**: **B**yzantine **F**ault **T**olerance.
- **CSMA**: **C**arrier **S**ense **M**ultiple **A**ccess.
- **DAC**: **D**iscretionary **A**ccess **C**ontrol.
- **Dapp**: **D**ecentralized **App**lication.
- **DoS**: **D**isk **O**perating **S**ystem.
- **ERC**: **E**thereum **R**equest for **C**omments.
- **EVM**: **E**thereum **V**irtual **M**achine.
- **MAC**: **M**edia **A**ccess **C**ontrol.
- **POS**: **P**oint **O**f **S**ales.
- **POW**: **P**roof-**O**f-**W**ork.
- **PU**: **P**rimary **U**ser.
- **PUE**: **P**rimary **U**ser **E**mulation.
- **QoS**: **Q**uality **O**f **S**ervice.
- **RC**: **R**adio **C**ognitive.
- **RPoW**: **R**eusable **P**roof **O**f Work.
- **RRC**: **R**apid **R**esults **C**ollege.
- **RTT**: **R**ound-**T**rip **T**ime.
- **SDR**: **R**adio **L**ogicielle **R**estreinte.
- **SHA**: **S**ecure **H**ash **A**lgorithm.

- **SSDF**: **S**ecure **S**oftware **D**evelopment **F**ramework.
- **SSL**: **S**ecure **S**ocket **L**ayer.
- **SU: S**econdary **U**ser.
- **TCP**: **T**ransmission **C**ontrol **P**rotocol.
- **TLS**: **T**ransport **L**ayer **S**ecurity.
- **WLAN**: **W**ireless **L**ocal **A**rea **N**etwork.

Introduction générale

Le développement de la technologie sans fil est de plus en plus rapide d'une génération à une autre. Passer d'une génération à l'autre nécessite des vitesses plus élevées, des services élevés et de plus en plus avancés, ce qui signifie une forte demande du spectre électromagnétique qui est le terme désignant le support de transmission. Le problème de la vitesse de transmission est presque résolu, ceci dit, d'autres problèmes subsistent avec des paramètres tels que la protection des données et informations relatives à l'utilisateur, sécurité et optimisation des messages transmis l'utilisation des bandes de fréquences par les utilisateurs, car il y a d'importants blocage dû à la rareté du spectre.

Sur le dernier point, les chercheurs notent que l'utilisateur n'est pas connecté tout le temps il y a des temps qui n'utilise pas le spectre et dans cette absence il y a beaucoup temps et vitesse de connections est lente et gaspillée. Comment pourrions-nous alors utiliser ce potentiel au profit d'autres utilisateurs ? Comment réduire et résoudre le problème de saturation de spectre ? Comment distinguer entre un utilisateur honnête et malveillant ?

La radio cognitive (RC) est une nouvelle solution qui permet de répondre et résoudre le problème de limite de spectre. Cette solution consiste à voir si l'utilisateur primaire n'a pas besoin d'un canal pendant un temps alors il le passe à un utilisateur secondaire. Avec cette technique, on optimise la perte et le gaspillage de canaux vides, si l'utilisateur primaire a besoin de ce canal, il peut le récupérer à n'importe quel moment. Par conséquent, le réseau est optimisé et tous les utilisateurs sont satisfaits.

La radio cognitive répond également à la rareté du spectre et garantit de fournir aux utilisateurs une meilleure qualité de service.

La problématique de notre travail de recherche consiste à proposer une technique qui permet de protéger et sécuriser les utilisateurs dans les réseaux radio cognitive contre les attaques et nous avons choisi de traiter l'attaque PUE (Primary User Emulation) dans ce mémoire.

Le but de notre travail est d'utiliser le concept de la blockchain pour assurer que tous les utilisateurs sont honnêtes, puis, nous avons introduit la notion de jeton non fongible (ERC721) qui permet de sécuriser encore plus le réseau de radio cognitive.

Le document est décomposé en trois chapitres qui se répartissent comme suit :

Le premier chapitre est consacré à l'étude du concept de la radio cognitive. Nous avons commencé par donner l'historique et expliquer brièvement la notion de la radio cognitive. Ensuite, nous avons présenté les différents aspects de cette technique ; principe général, architecture, cycle cognitif et fonctions. Enfin, nous avons donné des détails sur la sécurité dans la radio cognitive et expliqué les attaques existantes.

Dans le deuxième chapitre, nous nous sommes concentrés sur le concept de la technologie blockchain. Nous étudierons en détails la blockchain : définition, historique, caractéristique, les modèles de la technologie, les applications et fonctionnement. Ensuite, nous allons introduire le contrôle d'accès et définir les différents aspects : système, politique, modèle, mécanisme et architecture. Après cela, nous avons abordé le contrôle d'accès basé sur la blockchain et contrats intelligents. Pour finir, nous donnons un petit état de l'art sur l'utilisation des blockchains dans la RC.

Le troisième chapitre portera sur la mise en œuvre de notre application web et comprendra l'environnement de conception et de développement. Nous présenterons en détail l'architecture et les différentes étapes utilisées. Enfin nous allons présenter les résultats obtenus.

Chapitre I:
Sécurité dans la radio cognitive

I. Chapitre I : Sécurité dans la radio cognitive

I.1 Introduction

Le monde actuel des réseaux et des télécommunications mobiles connait une évolution exponentielle vu la demande des utilisateurs de technologie sans fil qui est devenue importante et indispensable au quotidien. Chaque évolution s'accompagne toujours par une nouvelle technologie complexe pour subvenir à une forte recrudescence des demandes de clients en termes de débit et de disponibilité des services proposés basés sur l'allocation du nouveau spectre, ceci peut engendrer des problèmes appelés en Anglais **« Spectrum Scarcity »** ce qui signifie une insuffisance du spectre. Pour cela, la radio cognitive (RC) est apparue afin de résoudre le problème de gestion du spectre.

Dans ce chapitre, nous allons étudier la radio cognitive dans ses différents aspects : principes, architecture, cycle de cognition, fonctions, ainsi que la théorie de sécurité et les types de menace dans la RC.

I.2 Radio cognitive

i. Historique

L'histoire de la RC remonte à la fin des années 1990, lorsque Joseph Mitola III a inventé un nouveau concept de communication sans fil, Joseph Mitola Connu comme le **« Père de la radio logicielle»** Il combine son expérience de la radio logicielle et l'apprentissage automatique et l'intelligence artificielle pour mettre en place la technologie de la radio cognitive[2][3].

Après avoir analysé l'utilisation de la radio fréquence, les régulateurs d'un certain nombre de pays, notamment l'Allemagne, l'Italie, la France, le Royaume-Uni, l'Espagne.

Aux États-Unis et au Royaume-Uni en particulier, la conclusion a été qu'une grande partie du spectre est utilisée de manière inefficace. Comme le montre la figure I.1.

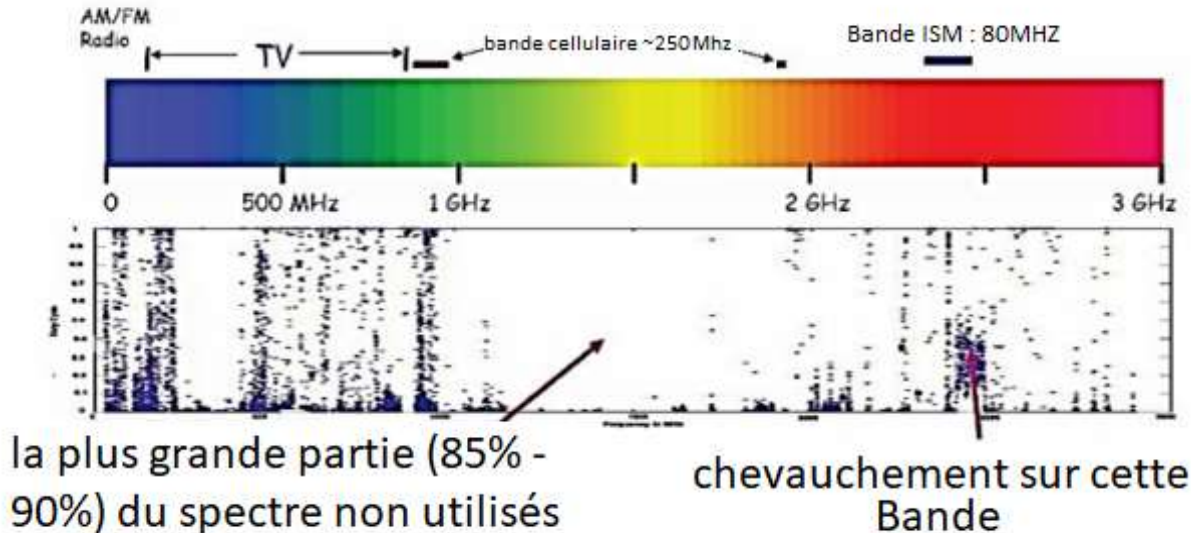

Figure I.1 : Exemple d'utilisation du spectre [1].

Les bandes pour les communications mobiles sont encombrées, mais pour les bandes de radio cellulaire ne le sont pas. En d'autres termes, l'utilisation du spectre dépend du lieu et du moment, et au-delà, les bandes sous licence ne peuvent pas être utilisées par des utilisateurs sans licence .Par conséquent, les appareils à courte portée étaient autorisés tant qu'ils ne provoquaient pas d'interférences et ne nécessitaient pas de protection contre les appareils fonctionnant de manière primaire (Utilisateur avec licence). Dans la recherche d'un moyen d'améliorer l'efficacité de l'utilisation du spectre, ainsi que d'assurer la connectivité, qui varie en fonction du réseau et des besoins des utilisateurs, il a été décidé

de recourir à des systèmes de communication cognitive, qui devraient fonctionner sans causant des interférences ou des problèmes de sécurité avec l'utilisateur primaire (PU)[4].

ii. Définition

Le radio cognitif est un système ayant les capacités nécessaires pour détecter automatiquement et reconnaître son cadre d'utilisation, ceci afin de lui permettre d'ajuster ses paramètres de fonctionnement radio de façon dynamique et autonome et d'apprendre des résultats de ses actions et de son cadre environnemental d'exploitation[5].

iii. Radio logicielle

Le concept de radio logicielle est issu des travaux de Joseph Mitola en 1991 pour définir une classe de radio reprogrammable et reconfigurable.

La radio logicielle est une radio dans laquelle les fonctions typiques de l'interface radio généralement réalisées en matériel, telles que la fréquence porteuse, la largeur de bande du signal, la modulation et l'accès au réseau sont réalisés sous forme logicielle. La radio logicielle moderne intègre également l'implantation logicielle des procédés de cryptographie, codage correcteur d'erreur, codage source de la voix, de la vidéo ou des données[5].

iv. Radio logicielle restreinte

La radio logicielle restreinte (SDR) est un système de radiocommunication configurable qui peut s'adapter à n'importe quelle bande de fréquence et recevoir n'importe quelle modulation en utilisant le même matériel qui va apporter la flexibilité, sa flexibilité permet de résoudre des problèmes de la gestion dynamique du spectre.

Les opportunités qu'offre le SDR lui permettent de résoudre des problèmes de la gestion dynamique du spectre. Les équipements SDR peuvent fonctionner dans des réseaux sans fil hétérogènes c'est-à-dire qu'un SDR idéal peut s'adapter automatiquement aux nouvelles fréquences et aux nouvelles modulations[6].

v. Le rôle de SDR dans la RC

La radio logicielle avec leur fonctionnalité est capable d'offrir la flexibilité avec les paramètres de la radio (fréquence porteuse, puissance, modulation, bande passante), que la radio cognitive requiert.

Dans ce modèle simple, les éléments de la radio cognitive utilisé et entourent le support radio logiciel restreint, autrement dit que le SDR c'est le cœur du RC comme la figure I.2 montre.

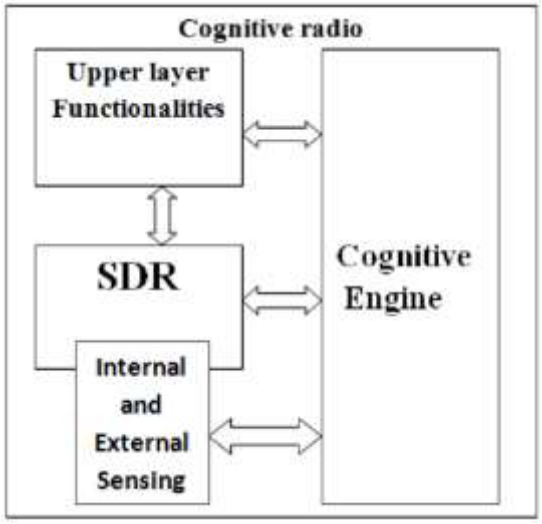

Figure I.2 : relation entre radio cognitive et le SDR[5].

vi. Principe général

Dans la RC, deux éléments sont omniprésents dans chaque communication reseau radio cognitif :

a) Utilisateurs primaires (PU) : Ce sont les utilisateurs licenciés qui détiennent une licence pour opérer sur cette Bande. Cette licence va donner à ce type d'utilisateurs des droits de communications qui permettent d'opérer à n'importe quel moment sur des bandes spectrales qui leurs sont réservées[7].

b) Utilisateurs secondaires (SU) : Ce sont les utilisateurs qui n'ont pas de licence pour opérer sur la bande spectrale. Cependant, grâce aux techniques d'accès dynamique au spectre, ces utilisateurs pourront partager la bande spectrale avec les utilisateurs primaires à condition de ne jamais interférer avec les utilisateurs primaires[7].

Dans un temps donné et à un emplacement géographique spécifique, il arrive qu'un PU n'utilise plus sa bande de fréquence, ainsi, un autre SU peut utiliser ces bandes grâce à des trous dans le spectre comme le montre la figure I.3 et ça, sans perturber les communications des utilisateurs primaires, et les utilisateurs secondaires peuvent profiter grâce aux trous du spectre une communication durant cette absence.

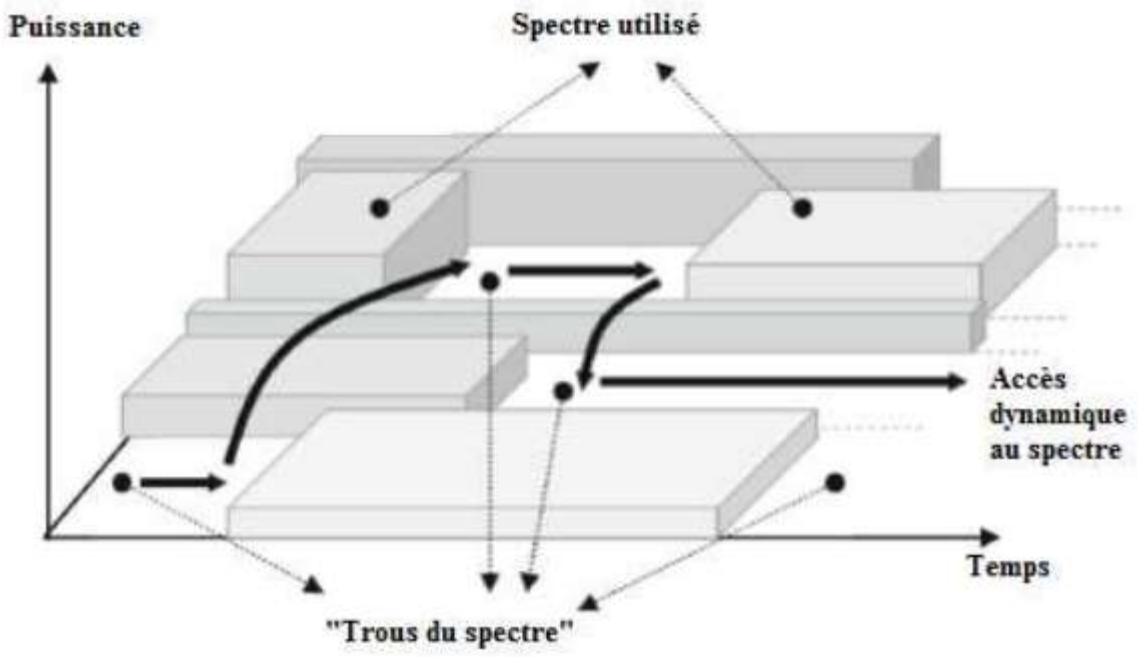

Figure I.3 : Le concept des trous du spectre [17].

Ci-dessous, et ça, sans perturber les communications des utilisateurs primaires, et les utilisateurs secondaires peuvent profiter grâce aux se trous du spectre une communication avec sa fréquence durant cette absence.

vii. Architecture de la radio cognitive

La radio cognitive contient six composantes fonctionnelles qui constituent son architecture:

- ✓ La perception sensorielle de l'utilisateur qui comprend les fonctions de capture « **Sensing** » et de perception visuelles et acoustiques.
- ✓ Les capteurs de l'environnement local (emplacement, température, accéléromètre, etc…)
- ✓ Les applications système (les services médias indépendants comme un jeu en réseau).
- ✓ Les fonctions qui incluent la détection RF et les applications radio de la SDR.
- ✓ Les fonctions de la cognition (pour les systèmes de contrôle et de planification, d'apprentissage).
- ✓ Les fonctions locales effectrices (synthèse de la parole, du texte, des graphiques et des affiches multimédias).[3]

La figure I.4 est une illustration de l'architecture de la radio cognitive, Le moteur cognitif représente la partie chargée de l'optimisation ou du contrôle du module radio logicielle restreinte .[3]

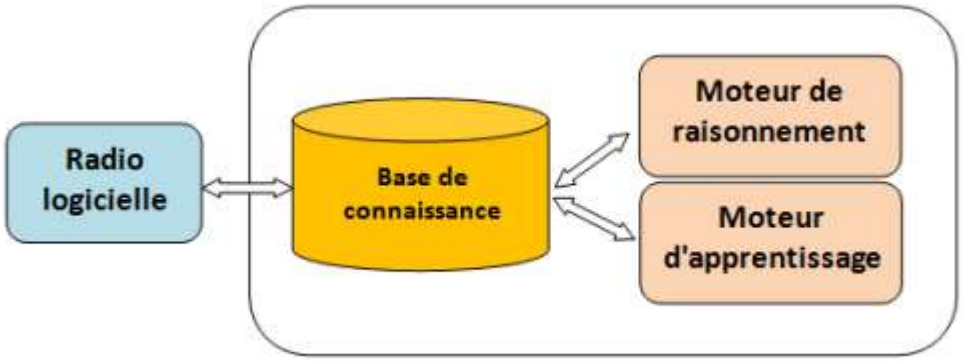

Figure I.4 : Architecture de reseaux radio cognitif

viii. Cycle de cognition

L'organisation temporelle, les processus d'inférence et les états de contrôle font tous partie de la composante cognitive de l'architecture de la radio cognitive. Ce cycle produit ce composant d'une manière évidente. Les stimuli entrent dans la radio cognitive sous forme de perturbations sensorielles qui sont transmises par le cycle de cognition dans l'espoir de susciter une réponse. Ce type de radio cognitive surveille son environnement, s'oriente, élabore des plans, prend des décisions, puis agit [5].

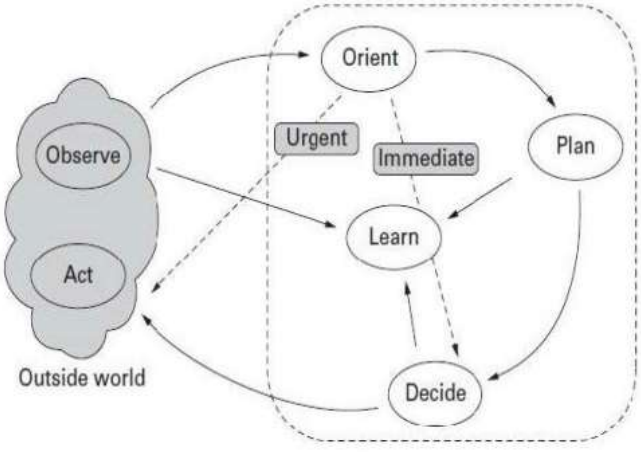

Figure I.5 : Cycle de cognition de Mitola

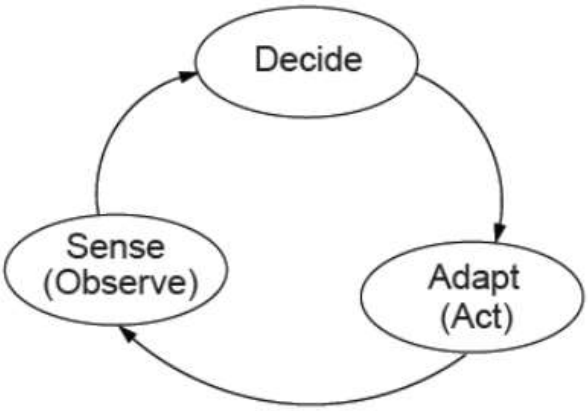

Figure I.6 : Cycle de cognition simplifié

Phase d'observation (détecter et percevoir)

La radio cognitive analyse le flux de stimuli et extrait plusieurs informations à partir de son environnement. La radio cognitive relie un certain paramètre comme l'emplacement, la température, le niveau de lumière des capteurs, etc. pour déterminer le contexte de communication pendant cette phase.

Phase d'orientation

La phase d'orientation détermine l'importance de la phase précédente (phase d'observation) en l'associant à un ensemble connu de stimuler de déterminer s'il y a besoin d'une action urgente ou une planification est plutôt nécessaire.

Phase de planification

Une phase qui fait un prétraitement sur les actions pour la phase suivante (phase de décision) pour identifier les actions alternatives à prendre.

Phase de décision

La phase de décision décidée entre les actions candidates ou les plans qui sont à planifier par la phase précédant en choisissant la meilleure d'entre elles.

Phase d'action

Agir sur l'environnement en effectuant, par exemple, des modifications au niveau de la fréquence radio.

Phase d'apprentissage

La perception, les observations, les décisions et les actions jouent toutes un rôle dans l'apprentissage. L'apprentissage initial se produit pendant la phase d'observation la figure I.7 montre les différentes composantes de la radio cognitive.

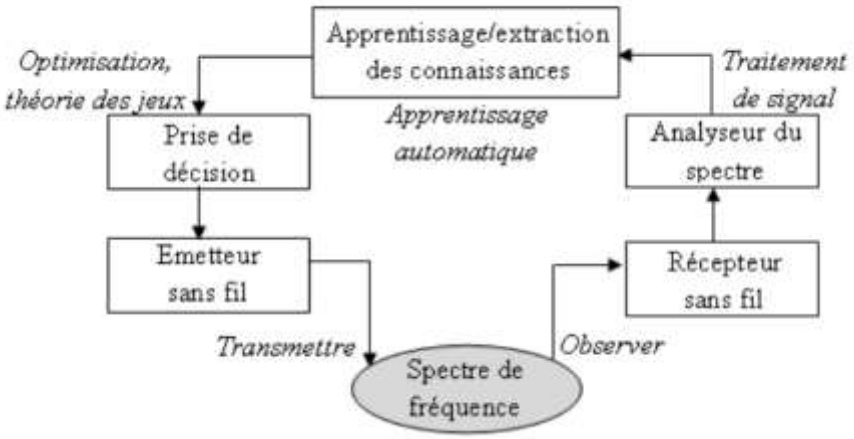

Figure I.7 : Composantes de la radio cognitif [3].

ix. Fonctions de reseaux radio cognitif

I.2.1.1 Détection du spectre « Spectrum sensing »

La radio cognitive doit détecter le spectre libre et le partager sans interférence avec d'autres utilisateurs, la façon la plus efficace pour détecter le spectre vide les espaces blancs du spectre par la détection de signaux d'utilisateurs primaires.

L'un des objectifs de la détection du spectre est d'obtenir le statut du spectre.

I.2.1.2 Gestion du spectre « Spectrum management »

La radio cognitive devrait capturer la meilleure bande de spectres pour fournit une meilleure qualité de service (QoS) aux utilisateurs avec des fonctions classées comme suit :

Analyse du spectre : Les résultats obtenus de l'étape précédant(la détection du spectre) sont analysés pour estimer la qualité du spectre qui peut être accédé par un utilisateur secondaire par rapport certains paramètres comme signal/bruit, la durée moyenne et la corrélation de la disponibilité des espaces blancs du spectre[5].

Décision sur le spectre : Après l'analyse des résultats obtenus et l'estimation en applique un modèle de décision pour l'accès au spectre, la complexité de ce Modèle devient plus complexe dans le cas ou un utilisateur secondaire a des objectifs multiples. On résoudre ça par des méthodes d'optimisation stochastique (le processus de décision de Markov)[5].

I.2.1.3 Mobilité du spectre « Spectrum mobility »

C’est le processus qui permet à l’utilisateur de la RC de changer sa fréquence de fonctionnement durant la communication. Les réseaux radios cognitifs utilisent le spectre de manière opportuniste et dynamique en permettant à des terminaux radio de fonctionner dans la meilleure bande de fréquence disponible et répondre aux exigences de communication transparentes.

- **Recherche des meilleures bandes de fréquence :**

  La RC doit garder une trace des bandes de fréquence disponibles de sorte que si nécessaire, il peut passer à d'autres bandes de fréquences immédiatement. Lors de la transmission par un utilisateur secondaire.

- **Auto-coexistence et synchronisation :**

  Quand un utilisateur secondaire effectue un transfert du spectre, deux questions doivent être prises en compte. Le canal cible ne doit pas être actuellement utilisé par un autre utilisateur secondaire (l'exigence d'auto-coexistence), et le récepteur de la liaison secondaire correspondant doit être informé de la non-intervention du spectre (la demande de synchronisation)[6].

I.3 Sécurité dans le reseau de radio cognitif

le réseau radio cognitif à résoudre le problème de la pénurie de spectres en permettant aux SUS d'utiliser la bande de fréquence sans causer d'interférence avec les PU. Par conséquent, cette méthode d'accès à certains utilisateurs malveillants peut accéder au réseau cognitif et lancer des attaques particulières d'attaques spéciales, telles que l'émulation de l'utilisateur principal, la falsification des données ou le déni de service. Qui causeront de sérieux dommages au le réseau de radio cognitif. En plus des menaces de sécurité spécifiques au réseau cognitif.

Nous catégorisons les attaques sur les Réseaux Radio cognitive en quatre (4) classes principales[8] :

1) Les attaques de la couche physique.
2) Les attaques de la couche de liaison.
3) Les attaques de couche de réseau.
4) Les attaques de la couche de transport.

x. Les attaques de la couche physique

Les principales vulnérabilités se situent dans la couche physique, car la détection du spectre est une étape cruciale des RRC. Les attaques qui falsifient la capacité de détection du spectre du spectre des SUS peuvent exploiter le système pour leur utilisation excessive ou pour bloquer les communications des utilisateurs légitimes. Les attaques les plus fréquentes et les attaques fréquemment utilisées visant la détection du spectre des RRC peuvent :

I.3.1.1 Emulation de l'utilisateur primaire

Cette attaque est généralement réalisée par un groupe d'utilisateurs secondaires malveillants, en transmettant des signaux spéciaux afin d'utiliser toutes les bandes de spectres inutilisées la figure I.8 montre comment un utilisateur malveillant envoyer des signaux avec les mêmes caractéristiques qu'utilisateur primaire pour prétend en entre le propriétaire de ces spectres.

Dans ce cas, les attaquants peuvent perturber l'utilisation opportuniste du spectre par les SUs et prendre l'avantage sur les autres utilisateurs et prendre l'avantage sur les autres SUs pour se réserver les ressources disponibles pour eux-mêmes[9].

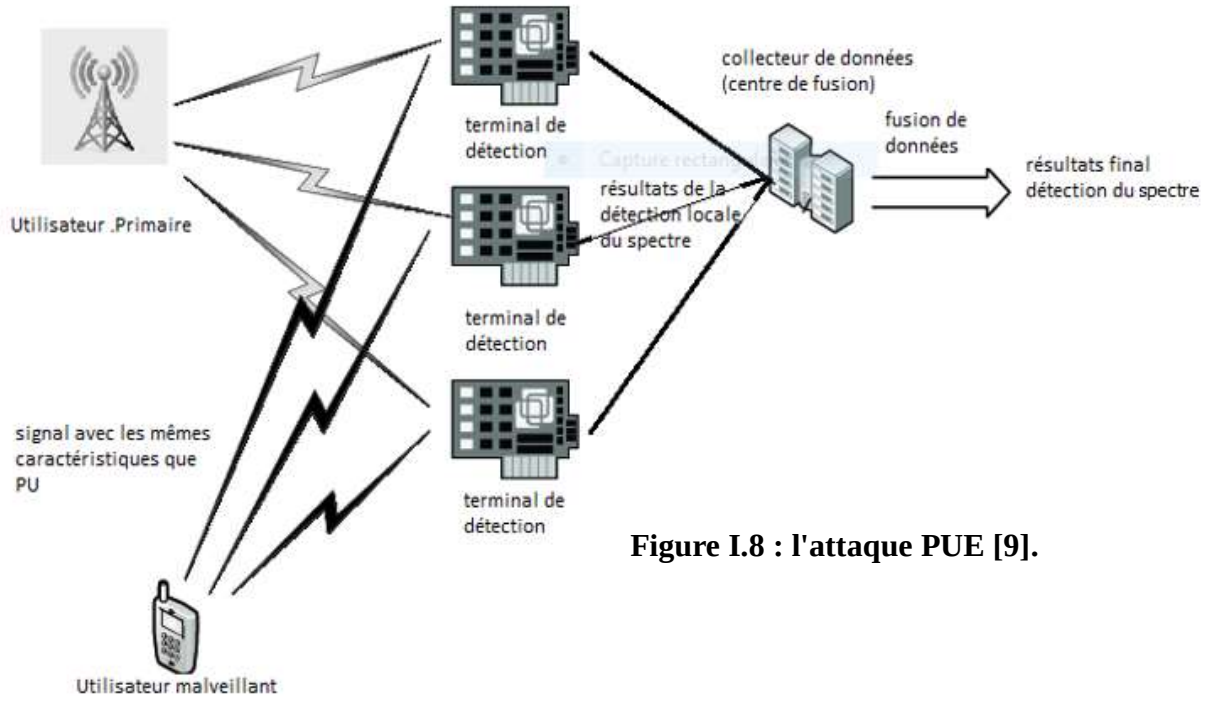

Figure I.8 : l'attaque PUE [9].

Types d'attaque PUE

- ***Attaques égoïstes de PUE***

Objectif de l'attaquant est de maximiser sa propre utilisation des ressources du spectre[10].

- ***Attaque de PUE malveillant***

Objectif de l'attaquant d'empêcher les SUs autorisé d'utiliser les espaces blancs d'un spectre[10].

I.3.1.2 L'attaque de la fonction objectif

Dans la radio adaptative, le moteur cognitif manipule ces paramètres radio au fil du temps dans le but de répondre à des exigences spécifiques telles qu'une faible consommation d'énergie, un débit de données élevé et une sécurité élevée. Ces attaques s'appliquent à tous les algorithmes d'apprentissage qui utilisent des fonctions objectifs, notamment diverses formes d'algorithmes génétiques.

Puisque ces attaques s'appliquent aux moteurs d'apprentissage, il s'agit d'attaques par manipulation de croyances.

$$f(P,R,S) = \alpha P + \beta R + \gamma S$$

La fonction objectif F utiliser par le moteur cognitif montre un exemple pratique détaillé tell que l'attaquant lance un brouillage sur la radio en réduisant le taux de transmission **R** et réduisant aussi la

fonction objectif F, tel que α,β,γ représente les poids de la force P, le taux de transmission R, la Sécurité S.

En supposant qu'un attaquant souhaite forcer le moteur cognitif à utiliser un certain niveau de sécurité S1, où $S1 < S2$.

Chaque fois quelle moteur cognitif essaie d'utiliser S2, l'attaquant peut brouiller le canal, en réduisant le R de R2 à R1 avec $R1 < R2$. Donc

$$\alpha P + \beta R2 + \gamma S1 > \alpha P + \beta R1 + \gamma S2$$

on peut résoudre R1 comme suit :

$$R1 < R2 - \frac{\gamma}{\beta}(s2 - s1)$$

Par conséquent à chaque fois qu'un niveau de sécurité plus élevé est tenté, la fonction objectif du système s'en trouve affectée[11].

I.3.1.3 L'attaque de Brouillage « Jamming »

La philosophie « ouverte » du paradigme de la radio cognitive rend le réseau RC vulnérable aux attaques par brouillage basées sur le brouillage par des utilisateurs malveillants intelligents.

Un attaquant peut parcourir les canaux, identifier les communications légitimes des SU et ensuite transmettre un signal de brouillage sur le même canal ou un fragment du canal, causant des interférences perturbatrices pour le SU.

Perturbant le SU, ce qui peut créer une situation de DoS (rendre le service indisponible) et bloquer complètement la transmission du SU légitime[12].

Ce type des attaques touche les couches physiques et même les couches de Liaison (MAC).

Pour illustrer l'effet du brouillage, SumanBhunia et ShamikSengupta[12]fait une expérience sur deux ordinateurs qui ont été configurés pour communiquer sur un canal 36 MHz (centré sur 5,180 MHz) du WLAN (IEEE 802.11-a).

Le figure I.9 montre comment l'attaquant exploite la vulnérabilité du MAC de l'IEEE 802.11, l'émetteur légitime sent qu'il y de l'énergie sur le canal, il s'abstient de transmettre. En effet, l'attaquant réussit à brouiller le canal avec un coût très faible[12].

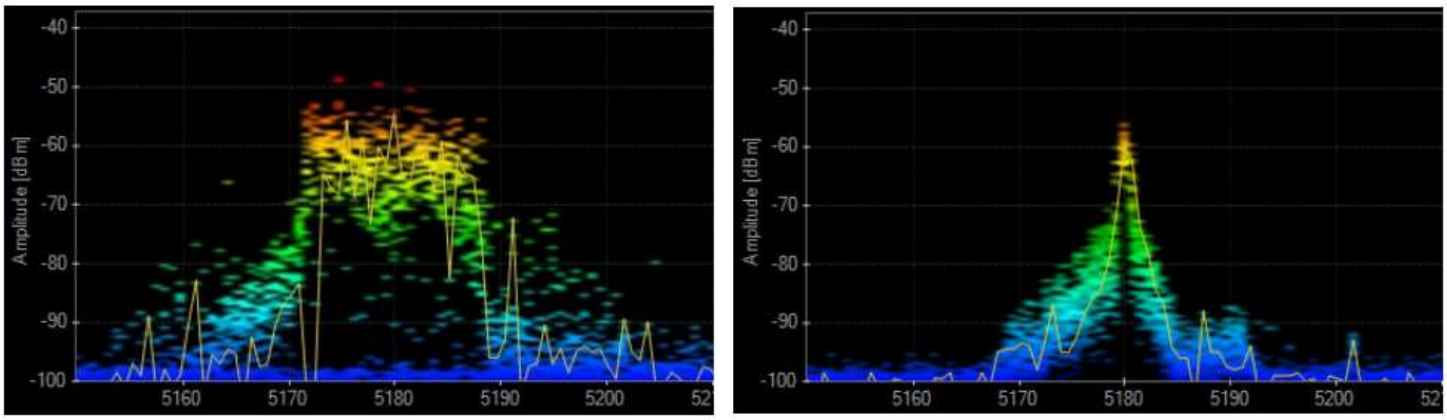

Figure I.9 : La densité spectrale de puissance et le signal du brouillage.

Types de brouilleurs

Brouilleur constant

Permet d'envoyer une suite de bits en continu sans tenir compte des protocoles de la couche MAC (CSMA) ce type d'attaque est inefficace sur le plan énergétique et facile à détecter.

Brouilleur trompeur

Transmets en continu des paquets réguliers au lieu d'émettre des bits aléatoires. Il trompe les autres nœuds pour qu'une transmission légitime soit en cours, de sorte à ce qu'ils restent en état de réception.

Brouilleur aléatoire

Transmets par intermittence soit des bits aléatoires ou des paquets réguliers. Il passe continuellement de deux états : la phase de sommeil et la phase de brouillage.

Brouilleur réactif

Ne commence à brouiller que lorsqu'il observe une activité sur un certain canal. Par conséquent, un brouilleur réactif vise à compromettre la réception d'un message. Il peut perturber les paquets de petites et de grande taille.

xi. Les attaques de la couche liaison « Link Layer Attack »

La gestion du flux de trafic et le contrôle des erreurs sur le support physique font partie de la responsabilité de la couche Liaison, cette couche prend en charge plusieurs utilisateurs sur un support partagé au sein du même réseau. Chaque utilisateur reçoit sa propre adresse MAC unique qui va identifier ce dernier au sein du réseau. La plupart des attaques ciblent les adresses MAC pour réaliser des falsifications pour perturber le Réseau[13].

I.3.1.4 Falsification de données de détection de spectre

Comme le montre la figure I.10, l'attaquant envoie de faux résultats de détection du spectre local à ses voisins ou au centre de diffusion, ce qui amène le récepteur à prendre une mauvaise décision de détection du spectre[8].

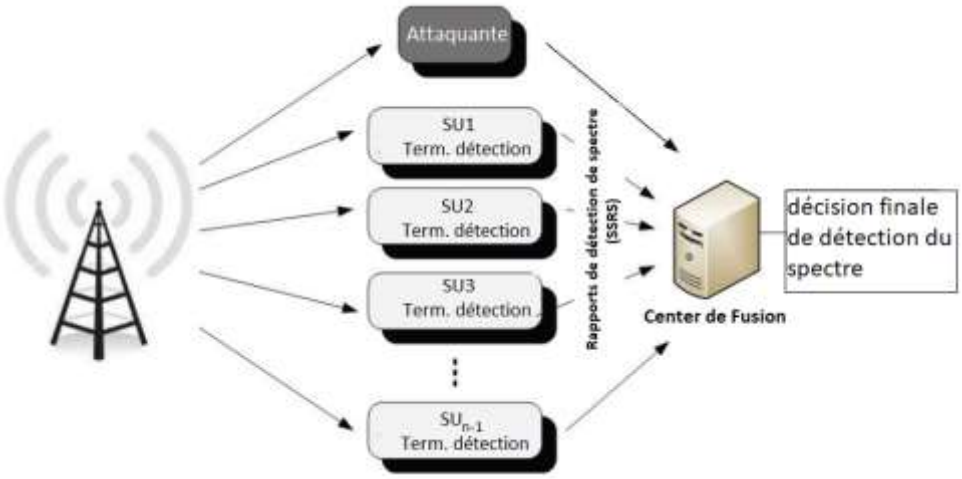

Figure I.10 : Exemple d'une attaque SSDF[9].

I.3.1.5 La saturation du canal de contrôle

Du point de vue de la sécurité, le canal de contrôle joue un rôle clé dans la disponibilité du réseau. Si les attaquants parviennent à saturer le canal de contrôle, ils peuvent gravement entraver le processus de négociation et d'allocation des canaux, provoquant ainsi un déni de service (DoS). Dans un protocole MAC RRC multi-sauts (multi-hop), un attaquant peut facilement falsifier les trames de négociation de canal pour lancer un déni de service[14].

xii. Les attaques de la couche Réseau (Network Layer Attack)

La fonctionnalité principale de cette couche consiste à acheminer les paquets de données d'un nœud source sur un réseau à un nœud à destination sur un autre réseau via des protocoles appelés protocoles de routage et avec la fragmentation et le réassemblage de paquets, si nécessaire. La RC

rencontre les mêmes problèmes de sécurité que les réseaux de communication sans fil classiques en raison des trois architectures qui sont : maillée (Mesh), ad hoc et infrastructure.

Les attaquants passent leur temps à cibler la fonctionnalité de routage, qui est la plus complexe et la plus vulnérable aux écoutes[13].

I.3.1.6 Attaque Hello Flood

Dans une attaque Hello Flood, un attaquant diffuse un message à tous les nœuds d'un réseau et jouant sur les paramètres du Réseau (ex. : niveau de puissance) pour indiquer la meilleure route vers un nœud de destination spécifique du réseau. Lorsque l'attaquant utilise un niveau de puissance élevé pour envoyer le message de diffusion, les autres nœuds recevront ce message avec une bonne intensité de signal et ils supposeront que ce nœud attaquant est très proche d'eux alors que ce n'est pas le cas en réalité.

Les nœuds du réseau transmettront leurs paquets destinés à un nœud particulier à travers ce nœud attaquant avec un niveau de puissance de signal régulier, mais les messages seront perdus en raison de la distance du nœud attaquant (le nœud de transmission)[13].

I.3.1.7 Attaques de puits (Sinkhole Attacks)

L'attaquant de type **« sinkhole »** prétend qu'il s'agit de la meilleure route pour le transfert des paquets. Par conséquent les nœuds voisins vont utiliser ce dernier pour transmettre leurs paquets. L'attaquant peut perpétrer l'attaque de transfert sélectif en transmettant, abandonnant ou modifiant les messages reçus. Cette attaque est particulièrement efficace dans les architectures maillées et les architectures d'infrastructure, car tout le trafic local qui cherche à être relayé vers un autre nœud est éliminé[15].

xiii. Les attaques de la couche transport (Transport Layer Attack)

Les responsabilités de la couche de transport comprennent le contrôle du flux, le contrôle de la congestion et la récupération des erreurs de bout en bout. La couche transport dans le réseau de radio cognitive est sujette à de nombreuses vulnérabilités qui affectent les réseaux ad hoc sans fil[15].

I.3.1.8 Attaque de Lion « Lion Attack »

L'attaque Lion est une attaque basée sur le PUE de la couche de transport, qui vise à dégrader le débit des connexions TCP (Transmission Control Protocol) au sein d'un réseau RC. Les attaques PUE permettent à l'attaquant de forcer facilement la fréquence, ce qui a un impact néfaste sur le débit TCP. De plus, si l'attaquant connaît ou peut deviner certains paramètres de connexion, il peut effectuer un déni de service facilement[16].

I.3.1.9 Attaque de suppression de clé « Key Depeletion Attack »

Les réseaux de radio cognitive souffrent de la courte durée de la couche transport en raison des temps d'aller-retour (RTT) élevés et des retransmissions fréquentes. Cela implique nécessairement qu'un grand nombre de sessions sont initiées. La plupart des protocoles de couche de transport, tels que le protocole SSL (secure socket layer) et Transport Layer Security (TLS), établissent des clés cryptographiques au début de chaque couche de transport. Il est plus probable qu'une clé de session soit répétée. L'attaquent va essayer de répéter les clés des sessions, cette répétition peut fournir une voie d'exploitation pour casser le système de chiffrement[15].

I.4 Conclusion

Dans ce chapitre, on récapitule que la radio cognitive est une solution efficace permettant aux SUs non autorisés d'accéder de manière opportuniste à la bande de fréquences détenue par les PUs, mais la philosophie qui est appliquée par ce dernier rend vulnérables aux attaques surtout les attaques de PUE.

Chapitre II : Blockchain

II. Chapitre II : Blockchain.

II.1 Introduction

Blockchain est une nouvelle façon de stocker et de gérer des données, ce qui en fait une technologie potentielle dans la société informatique. C'est pourquoi, en ce qui concerne les monnaies numériques, la blockchain peut potentiellement avoir un impact et transformer de nombreux domaines. Bien entendu, les bénéfices que l'on peut en tirer varient selon le domaine dans lequel on l'applique. Cependant, il est bien certain que l'assurance, l'immobilier, la logistique et bien sûr les entreprises peuvent être transformées grâce à la technologie blockchain.

La technologie de blockchain utilisée partout dans le système de communication sans fil, surtout dans le domaine des réseaux radio cognitive. La détection de spectre, un composant fondamental des réseaux radio cognitive est menacé par des attaques de sécurité. Le processus de détection de spectre est interrompu par des utilisateurs malveillants attaquant la détection du signal principal, ce qui affecte la précision des résultats de détection.

La présence de l'utilisateur malveillant dans le système envoyant de fausses données de détection peut dégrader les performances de la radio cognitive. Donc l'implémentation de cette technologie pour le but de la détection du spectre et d'amélioration de la sécurité tout en identifiant les utilisateurs malveillants présents augmente les performances de réseau.

Dans ce chapitre, nous allons étudier la chaine de bloc « Blockchain » dans ses différents aspects : historique, architecture, définition, fonctionnement, les caractéristique, les modelés ainsi que les applications.

II.2 Blockchain

II.2.1 Définition

Blockchain est une nouvelle technologie distribuée qui permet aux utilisateurs de réseau d'enregistrer, d'accéder et de modifier les informations échangées entre les deux sans aucun intermédiaire et de façon sécurisée et transparente en utilisant des outils cryptographiques et infalsifiables.

II.2.2 Historique

La technologie de Blockchain est l'une des technologies les plus avancées du 21e siècle, en raison de son effet sur divers domaines.

- **En 1991**

Les chercheurs Stuart Haber et W. Scott Stornetta [18] ont décrit l'architecture derrière la technologie blockchain cryptographiquement sécurisée où les individus ne peuvent pas modifier les horodatages des documents. En 1992, ils ont mis à jour leur système pour incorporer les arbres de Merkle, ce qui a permis un gain d'efficacité, permettant ainsi de rassembler les fichiers sur un seul bloc, mais cette technique a été oubliée.

- **En 1995**

Le NY Times met en place la première blockchain dans le journal, cette technologie qui est toujours active, est la plus longue blockchain de l'histoire[19].

- **En 2004**

L'informaticien et activiste en cryptographie Harold Thomas Finney a introduit un système appelé RPoW ("Reusable Proof of Work"). Le système fonctionne en recevant un jeton de preuve de travail non échangeable et non fongible basé sur le système Hashcash, qui à son tour crée un jeton avec une signature RSA, qui peut ensuite être transférée de personne à personne.

RPoW résout le problème de la double dépense en conservant un enregistrement de la propriété du jeton, qui est stocké sur un serveur de confiance et est conçu pour permettre à tout utilisateur dans le monde de vérifier son exactitude et son intégrité en temps réel.

Nous pouvons considérer RPoW comme le premier prototype et la première étape de l'histoire des crypto-monnaies[18].

- **En 2009**

La naissance de Bitcoin a marqué un tournant dans la blockchain. En fait, il s'agit du premier projet à mettre en œuvre cette technologie à grande échelle.

Le 3 janvier 2009, Satoshi Nakamoto a créé le premier bloc de la blockchain Bitcoin, donnant ainsi naissance à la première monnaie numérique alimentée par la technologie blockchain[18].

- **En 2013**

Le programmeur et co-fondateur de Bitcoin Magazine, Vitalik Buterin, a déclaré que Bitcoin avait besoin d'un langage de script pour créer des applications décentralisées.

A défaut de parvenir à un accord au sein de la communauté, Vitalik s'est lancé dans le développement d'une nouvelle plateforme informatique distribuée basée sur la blockchain : Ethereum, dotée de capacités de script appelées « contrats intelligents ». ".

Les contrats intelligents « Smart Contract » sont des programmes ou des scripts qui sont déployés et exécutés sur la blockchain Ethereum. Par exemple, ils peuvent être utilisés pour effectuer des transactions répondant à certaines conditions. Ils sont écrits dans un langage de programmation spécifique et compilés en bytecode, une machine virtuelle décentralisée "Turing-complete" appelée Ethereum Virtual Machine (ou EVM pour Ethereum Virtual Machine), qui peut ensuite les lire et les exécuter[18].

II.2.3 Caractéristique de blockchain

De manière générale, les caractéristiques de la technologie blockchain sont :

- **Immutabilité**

Les données stockées dans la blockchain sont immuables, permettant de garantir l'intégrité des données. Cette immuabilité est l'un des principaux aspects qui contribue à la fiabilité du système blockchain. De plus, les données sont ajoutées aux blocs après avoir été approuvées par tous les membres du réseau, permettant des transactions sécurisées.

- **Transparence**

Une recette obligatoire de certaines blockchains, spécialement publique.

La transparence de la blockchain garantit que toutes les transactions sont visibles sur l'ensemble de réseau. Par exemple, un portefeuille électronique et son solde. Ce solde représente l'addition ou la soustraction de toutes les transactions effectuées qui concernent l'adresse du portefeuille. Étant donné que ces mouvements sont inscrits dans la blockchain, qui est consultable à souhait, le solde exact peut être vérifié en tout temps. Dans le cas d'une blockchain privée, la transparence peut être délibérément limitée pour protéger la confidentialité[20].

- **Décentralisation**

La technologie Blockchain permet aux utilisateurs de réseau d'échanger les informations et contrôler et valider les opérations effectuées sans intervenir une autorité centrale et sans aucun point central qui gère le réseau.

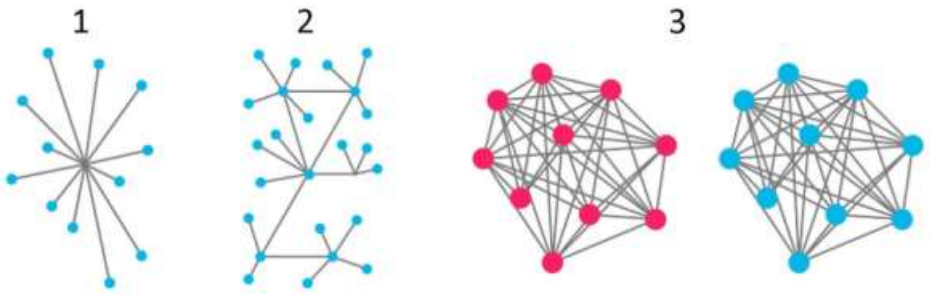

FIGURE II.1 : Différence entre système centralisé (1) et décentralisé (2) (3)[21].

- **Sécurité**

Les données ne sont pas stockées dans un serveur unique mais chaque utilisateur a une copie. Ce qui permet d'interdire la modification, la duplication et la suppression de données. Tout ça grâce à l'utilisation des fonctions cryptographiques sur lesquelles s'appuie la technologie blockchain.

- **Autonomie**

La puissance de calcul et l'espace d'hébergement sont fournis par les nœuds du réseau, c'est-à-dire les utilisateurs eux-mêmes. Il n'y a donc pas besoin d'une infrastructure centrale [22] car elle est répartie entre tous les utilisateurs.

II.2.4 Les modèles de la technologie Blockchain

La technologie de blockchain est divisée on trois grands types :

- **Blockchain privée**

Ce type de blockchain est considéré comme un réseau centralisé car il est contrôlé par une seule organisation. Dans une blockchain privée, le régulateur vérifie l'introduction de nouveaux membres et accorde des autorisations de lecture et d'écriture. Ce pouvoir peut être dirigé ou géré individuellement, il est composé de différents participants[24].Par conséquent, son accès et son utilisation sont réservés à certains participants. Aucun utilisateur ne peut participer sans autorisation, mais tout le monde peut consulter[23].

- **Blockchain publique**

Ce type de blockchain peut être visible et utilisé par tout le monde. Chaque utilisateur de réseau peut faire une consultation, suppression et modification sans aucune permission. Il est connu pour être totalement décentralisé.

En bref, n'importe qui peut voir et utiliser les chaînes de blocs publiques, telles que dans les blockchains Bitcoin et Ethereum.

- **Blockchain de consortium**

Une technologie de blockchain qui combine des éléments de blockchain privés et publics. Il permet aux organisations de créer un système privé basé sur des autorisations ainsi qu'un système public sans autorisation, leur permettant de contrôler qui peut accéder à des données spécifiques stockées sur la blockchain et quelles données seront mises à la disposition du public.

Le tableau II.1 suivant montre une comparaison entre les trois types de blockchain.

Type de blockchain / Propriété	Blockchain Publique	Blockchain Prive	Blockchain a Consortium
Permission de lire	Publique	Pourrait etre publique ou restreinte.	Pourrait etre publique ou restreinte.
Centralisé	Non	Oui	Partiel
Efficacite	Faible	Élevé	Élevé
Immutabilité	Presque impossible à falsifier	Pourrait être Falsifié	Pourrait être Falsifié
Anonymat Des utilisateurs	Oui	Non	Non
Détermination Du consensus	Tous les nœuds	Une Organisation	Ensemble des nœuds sélectionnés

Tableau II.1 : Comparaison entre les types de blockchain public, privé, consortium[20].

II.2.5 Les applications de Blockchain

En raison de la confiance et la fiabilité de la blockchain en termes de sécurité et transparence des transactions, elle est utilisée dans plusieurs domaines d'applications. Ci-dessous, nous mentionnons les plus connu.

II.2.5.1 Blockchain dans la finance

A. Bitcoin

Le Bitcoin ou monnaie numérique a été introduit pour la première fois par une personne ou un groupe anonyme sous le pseudonyme de Satoshi Nakamoto en 2008 [25].

Le Bitcoin utilise un registre public Blockchain pour effectuer des transactions à travers un réseau peer to peer. Des exemples de Bitcoins sont Bitbond, BitnPlay, BTC Jam, Codius et DeBuNe. DeBuNe.

B. Ripple

Ripple est un système d'échange de devises, de transfert de fonds et de règlement brut (RTGS) [26] en temps réel qui utilise le protocole Ripple via un réseau peer-to-peer et est un échange décentralisé axé sur le marché bancaire. Les systèmes d'échange et de remise incluent Coinbase, BitPesa, Billion, Stellar, Kraken et CryptoSigma.

II.2.5.2 Blockchain dans la non finance

A. Ethereum

Le chercheur et programmeur en crypto-monnaie Vitalik Buterin a créé la prochaine génération de contrats intelligents et de plates-formes d'applications décentralisées. Cette plateforme est également la base d'une monnaie virtuelle connexe, appelée Ether[27].

Il utilise une plate-forme informatique distribuée basée sur la blockchain et un langage de script Turing complet qui peut traiter des contrats intelligents « Smart Contract » sur la blockchain.

B. Hyperledger

Hyperledger est un projet de la fondation Linux qui développe des technologies Blockchain pour les entreprises, ne supportant que les membres enregistrés. Hyperledger est un effort de collaboration open source créé pour faire progresser les technologies Blockchain interindustrielles. Il s'agit d'une collaboration mondiale, hébergée par la Fondation Linux, qui comprend des leaders dans les domaines de la finance, de la banque, de l'Internet des objets, des chaînes d'approvisionnement, de la fabrication et de la technologie[28].

II.2.5.3 Blockchain dans la santé

Dans le domaine de la santé, la technologie blockchain permet le partage de données cliniques en stockant les données elles-mêmes ou en indiquant qui peut y accéder, en protégeant les identités et les informations des patients et des prestataires, et en optimisant la gestion des données. Dans le domaine de la santé, la technologie blockchain permet le partage de données cliniques en stockant les données

elles-mêmes ou en indiquant qui peut y accéder, en protégeant les identités et les informations des patients et des prestataires.

Les prestataires de soins de santé peuvent utiliser la blockchain pour le stockage des dossiers médicaux de leurs patients.

II.2.5.4 Blockchain dans le vote

Les systèmes de vote traditionnels sur papier présentent de nombreux inconvénients, tels que les dossiers perdus et fraude électorale. La blockchain peut transformer les systèmes de vote traditionnellement servi par un système de vote numérique avec une plateforme sécurisée pour soutenir l'ensemble du processus (vote, suivi et dépouillement).

Le système de vote basé sur la technologie blockchain est transparent car les votes peuvent être comptés et vérifiés qu'aucun vote n'a été supprimé, modifié ou adapté par l'homme.

II.2.5.5 Les contrats intelligents « Smart Contract »

Inventés par Nick Szabo en 1994, les contrats intelligents sont des protocoles ou des ensembles de règles qui régissent les transactions interentreprises. C'est une excellente idée pour automatiser l'exécution des contrats entre les parties. Les contrats intelligents peuvent inclure différentes conditions contractuelles, qui peuvent être directement applicables et/ou auto-exécutoires en tout ou en partie. Ils sont conçus pour offrir une sécurité supérieure tout en réduisant les coûts et la latence par rapport aux contrats traditionnels.

La figure II.2 suivant montre une structure de contrat intelligent.

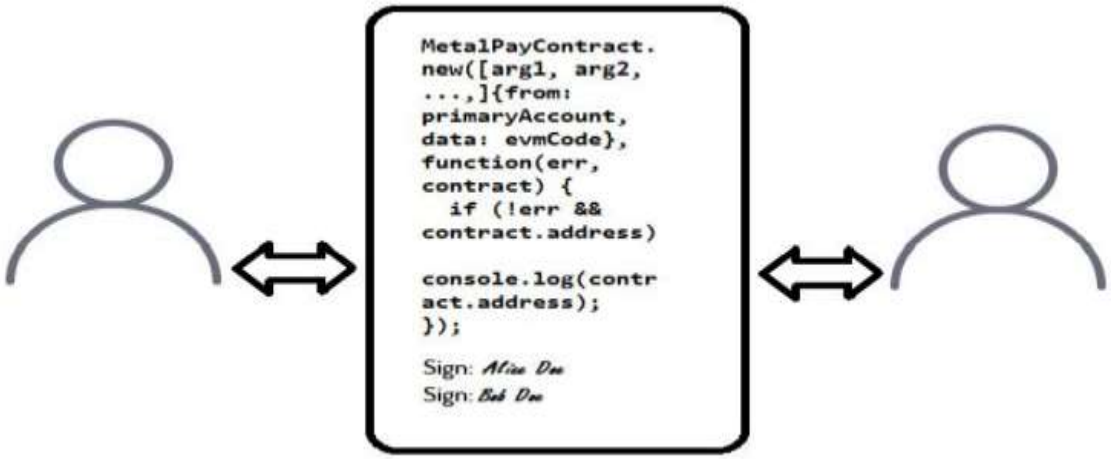

FIGURE II.2 : Structure contrat intelligent[39].

II.2.6 Fonctionnement de Blockchain

II.2.6.1 Principe fonctionnement de Blockchain

Selon [19], le protocole blockchain est essentiellement un registre numérique distribué composé de transactions numériques et partagé sur le réseau. Le protocole est basé sur une architecture peer-to-peer, où chaque participant constitue un nœud dans le réseau. Ces participants stockent des copies identiques du grand livre, puis travaillent ensemble dans le processus de validation et d'authentification des transactions numériques, en ajoutant de nouvelles transactions au grand livre. Le processus "mineurs" d'ajout de transactions consiste à traiter les transactions proposées et à les soumettre au vote. Si la transaction est considérée comme valide par une majorité de participants, elle est ajoutée au grand livre, qui la relie aux transactions précédentes, formant une chaîne qui ne peut être modifiée sans détruire son intégrité. Chaque transaction qui passe par le processus de chaînage est regroupée dans un bloc qui contient en outre le hachage cryptographique du bloc précédent, puis ajoute une relation linéaire avec le grand livre dans l'ordre chronologique.

Les modifications apportées au grand livre sont répliquées sur le réseau, de sorte que chaque participant dispose d'une copie complète du grand livre mis à jour. Cela signifie également qu'aucun participant n'a la capacité d'attaquer facilement l'ensemble du réseau distribué. Bien que le concept de transactions existe toujours, les données associées à n'importe quel type, car la blockchain n'est qu'un lien vers les données qui y sont stockées.

Le format des transactions est défini par le réseau sous-jacent qui sous-tend la blockchain, tandis que les données qu'elles contiennent sont définies par les participants qui les ont créées. Ces données peuvent être cryptées et signées numériquement, offrant des avantages supplémentaires au système tels que l'authenticité, l'intégrité et la non-répudiation. Lorsqu'une transaction est ajoutée à la chaîne, le mécanisme de consensus spécifique est vérifié.

En résumé, le fonctionnement d’une transaction en 5 étapes :(Figure II.3)

1. A effectue une transaction vers B.
2. Regroupe plusieurs transactions dans un bloc.
3. Le bloc est validé par les nœuds du réseau au moyen de techniques cryptographiques.
4. Apres validation de bloc, il est daté et ajouté à la chaîne de blocs à laquelle tous les utilisateurs ont accès.

5. B reçoit la transaction de A

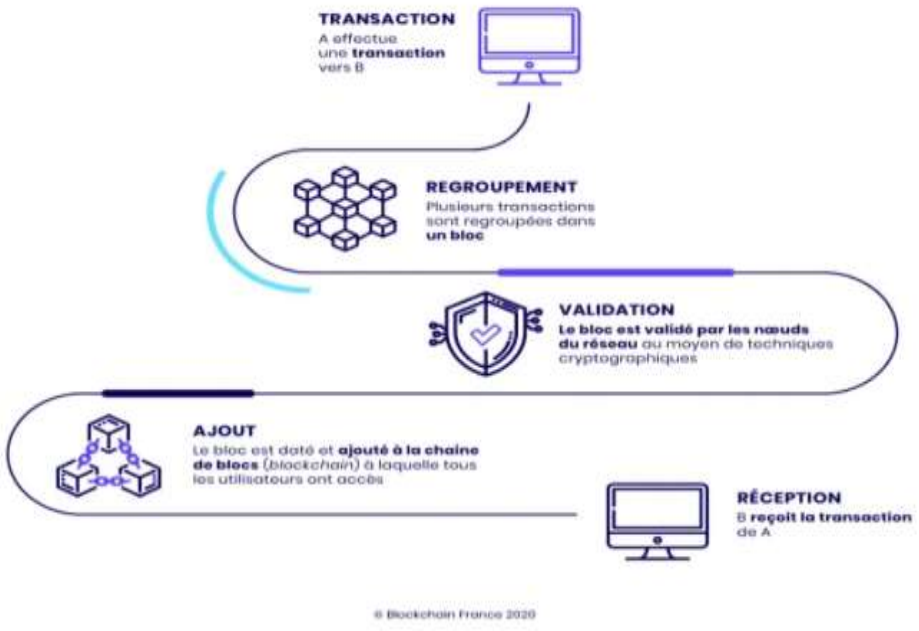

FIGURE II.3 : Fonctionnement de blockchain[29].

II.2.6.2 Architecture de Blockchain

Ce sont les principaux composants de l'architecture de la blockchain :

- **Le bloc**

Les blocs d'une blockchain peuvent contenir différents types de données, des enregistrements de transactions (Bitcoin), des images, du texte, des applications.

Ces données peuvent être cryptées ou enregistrées en texte clair.

Les en-têtes de bloc sont des données techniques et des métadonnées (horodatage, propriétaire, signature électronique, lien, etc.).

Le premier bloc d'une blockchain est appelé bloc genèse qui n'a pas de bloc parent.

La figure 2.4 suivant montre une structure de bloc.

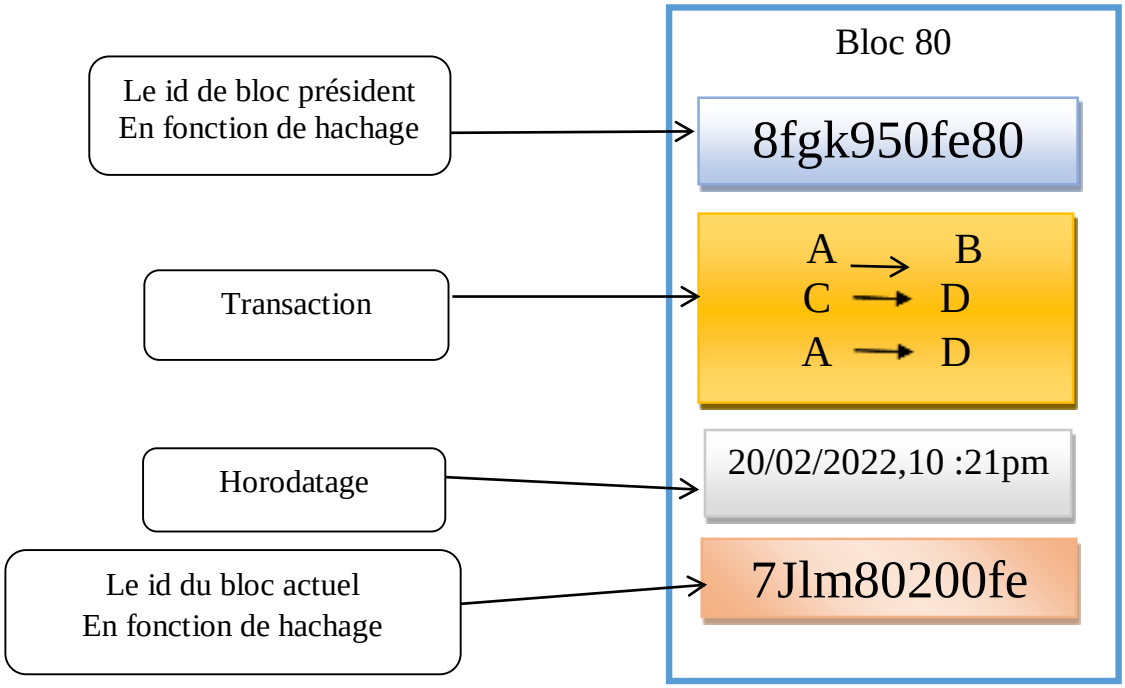

FIGURE II.4 : Structure de bloc.

- **La chaine**

La chaine est une séquence des blocs, qui contient une liste complète d'enregistrement de transactions. L'ensemble des blocs sont reliés entre eux par la signature numérique. Cette signature appelée hash cryptographique.

Chaque bloc contient le hachage(hash(ID)) du bloc précèdent pour former la chaine de cette façon.

Le hash(ID) est un résumé électronique de 256 bits d'un bloc de données blockchain. C'est la robustesse de cette chaîne qui garantit la fiabilité de la blockchain.

La figure II.5 suivant montre une structure d'une chaine.

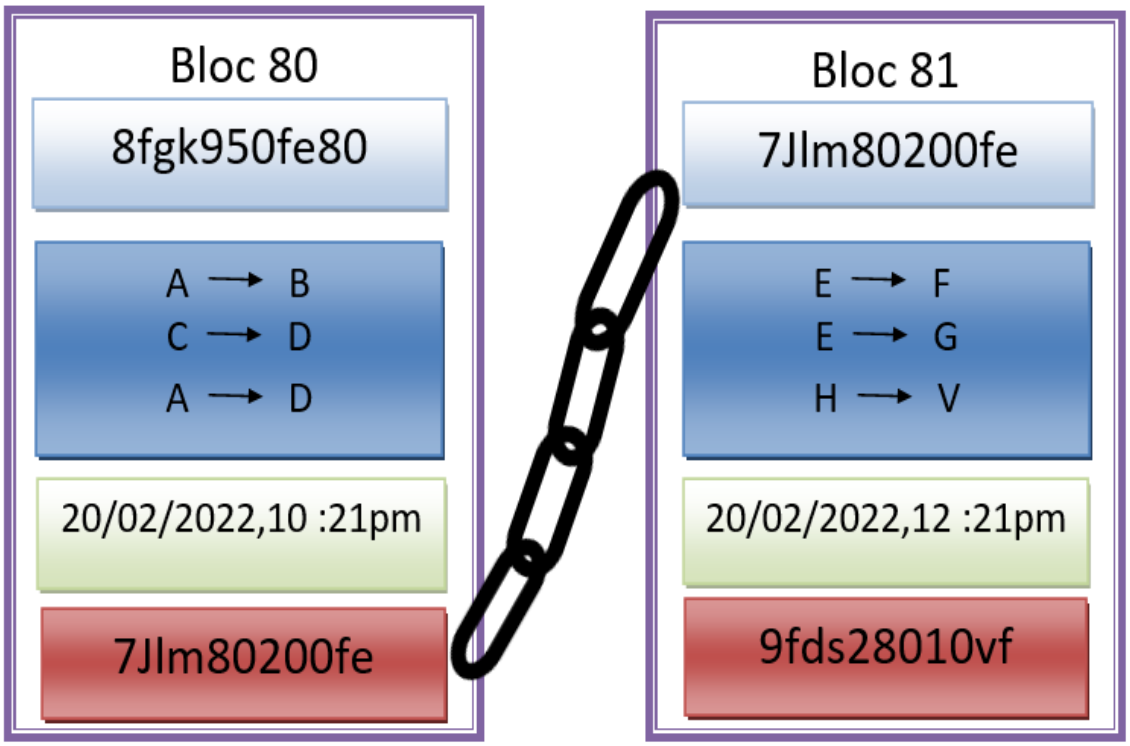

FIGURE II.5 : Structure d'une chaine.

Cette signature électronique de 256 bits est réalisée à l'aide d'un asymétrique(SHA 256, Keccak-256).

L'algorithme a les caractéristiques suivantes :[30]

- Il est déterministe, si on applique la fonction sur une donnée deux fois, on obtient le même résultat.

- Il est rapide.

- C'est irréversible car on ne retrouve pas la donnée d'origine quand on connaît sa signature, sauf avec le temps de calcul prohibitif de la technologie actuelle.

- Il est anticollision. Deux données différentes, même très légères, produisent deux signatures complètement différentes.

- **Réseau décentralisé**

Un réseau blockchain se compose de nombreux nœuds répartis dans le monde entier, chacun conservant une copie locale de la blockchain avec un enregistrement complet de toutes les transactions. Pour atteindre son objectif d'immuabilité des données, le protocole s'exécute généralement de manière décentralisée ou distribuée. Il s'agit d'un réseau peer-to-peer distribué qui permet à deux nœuds de communiquer entre eux sans avoir besoin d'une autorité centrale. Dans un système de blockchain, le réseau partage de manière proéminente les données des ressources, à savoir la blockchain.

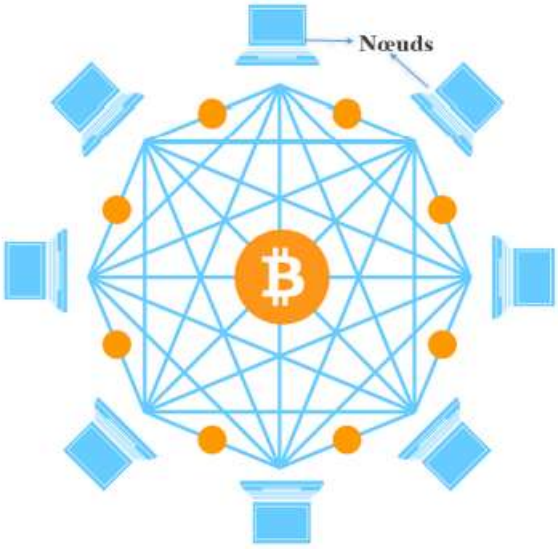

FIGURE II.6 : Un réseau décentralisé (P2P)[20].

- **Transaction**

Chaque transaction est déterminée avec sa valeur de hachage représentant un identifiant de transaction et un ensemble d'entrées et de sorties.

Lorsqu'un utilisateur initie une transaction, elle est envoyée à la blockchain et attend la vérification par les mineurs. Les transactions seront enregistrées dans le carnet et ne pourront pas être supprimées ou modifiées. Ce dernier est un horodatage automatique, qui permettra à la blockchain d'être dans l'ordre chronologique. L'une des grandes caractéristiques de la blockchain Bitcoin est qu'il s'agit d'un cahier public que tout le monde peut consulter via Internet. La transaction est publique, mais elle reste anonyme : c'est-à-dire que le montant est visible, mais pas l'identité de l'auteur. Ce sont des adresses cryptées complexes qui identifient l'expéditeur et le destinataire.

La clé privée est utilisée pour signer la transaction, et La clé publique est utilisée pour la vérification des transactions[31], comme le montre la figure II.6.

Avant l'avènement de la blockchain, le problème de la double dépense était résolu par un tiers de confiance.

La figure II.7 suivants montre une structure de transaction.

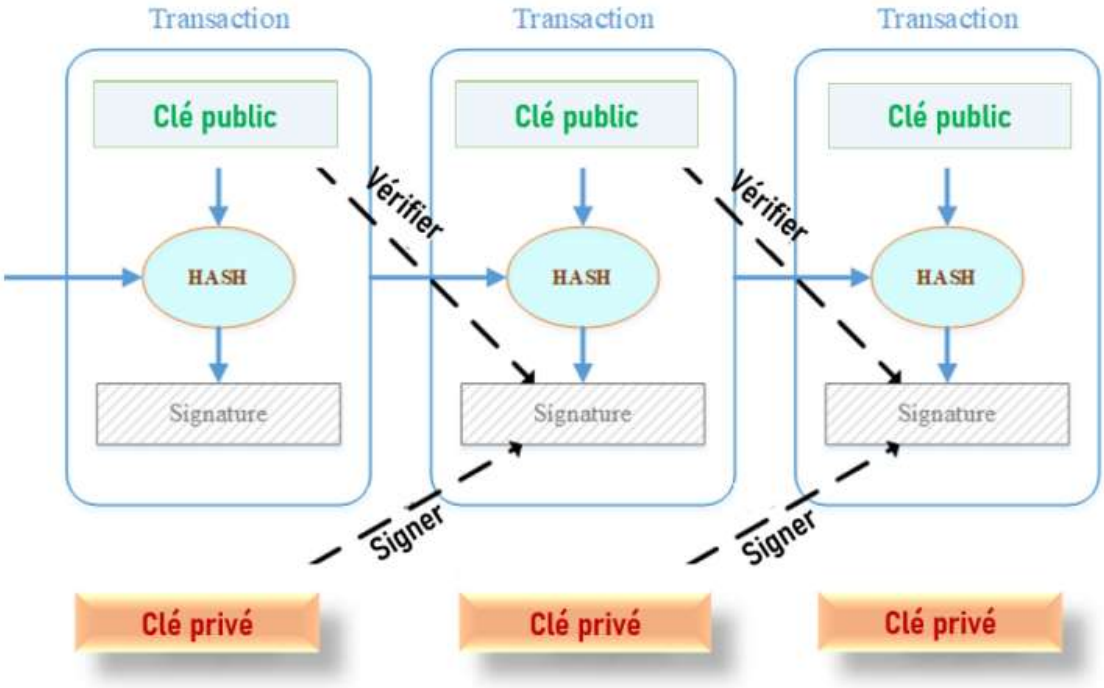

FIGURE II.7 : Structure de transaction[28].

- **Le consensus**

Le troisième module correspond au consensus distribué de la blockchain et est au cœur du modèle de gouvernance de la blockchain, c'est-à-dire le consentement de l'opinion publique le plus étendu. Cette conception consensuelle met en avant un mode de fonctionnement décentralisé Le concept d'aucun intermédiaire a été mentionné précédemment, où les mineurs mettent en œuvre un système de preuve de travail « Proof-of-Work » qui permet de valider les transactions et de générer de nouveaux bitcoins. Par conséquent, la modification de la blockchain nécessite le consentement de la majorité, soit 51% du réseau.

Le consensus peut être défini comme l'épine dorsale de la blockchain (système de grand livre distribué), car la sécurité de la blockchain sont garanties à cette couche, qui est généralement la couche de base de la plupart des systèmes de blockchain. Dans un réseau blockchain (par exemple Bitcoin) le consensus est utilisé pour vérifier les transactions (simple) + algorithme de consensus (PoW, Pos...) (complexe). Il existe de nombreuses variantes différentes de protocoles de consensus tels que Preuve d'enjeu (PoS), Preuve de travail (PoW), Preuve d'autorité (PoA), Tolérance aux pannes byzantines (BFT).

II.3 Contrôle d’accès

II.3.1 Définition

Une exigence fondamentale de tout système dont le but de protéger les données et les ressources contre la divulgation et la modification non autorisé, tout en garantissant leur disponibilité pour les utilisateurs légitimes. Par conséquence, pour assurer la protection il est nécessaire de contrôler chaque accès au système et ses ressources. Le contrôle d’accès déterminé qui peut accéder à quoi, comment et selon quelles règles.

II.3.2 Système de contrôle d’accès

Il existe deux types de systèmes de contrôle d'accès : le contrôle d'accès logique et le contrôle d'accès physique.

- **Contrôle d’accès physique**

Les systèmes de contrôle d'accès physique ont trois composantes principales : le contrôle d'accès, la surveillance et les tests.

Le contrôle d'accès physique étudie les solutions permettant de réguler l'accès aux lieux physiques et aux ressources physiques pour les entreprises qui souhaitent gérer le contrôle d'accès à leurs ressources physiques privées et sensibles.

- **Contrôle d’accès logique**

Le contrôle d'accès logique concerne la gestion du contrôle d'accès aux systèmes logiciels et aux données. Les systèmes actuels de contrôle d'accès se concentrent souvent sur le contrôle d'accès logique et ils stockent les données sur un serveur centralisé, qui serait géré par les administrateurs du serveur, qui ont un accès total à tout et les processus de contrôle d'accès sont exécutés de manière centralisée.

II.3.3 Politique de contrôle d’accès

Une politique de contrôle d'accès est définie comme un plan ou un plan d'action prescrit pour un système ou une organisation conçue pour influencer et guider les décisions et les actions des composants. Par conséquent, les politiques de contrôle d'accès sont le plus souvent définies par une organisation ou une application et sont liées à qui doit accéder à qui, sur la base d'une logique dépendante de l'utilisation. Voici des exemples de politiques de contrôle d'accès courantes : contrôle d'accès discrétionnaire (Discretionary AC (DAC)), contrôle d'accès obligatoire (Mandatory AC (MAC))[41].

- **Contrôle d'accès discrétionnaire (DAC) :** Les ressources appartiennent à leurs créateurs, et ils ont toute liberté pour déterminer les autorisations qui doivent leur être associées. Les politiques contrôlent l'accès en fonction de l'identité du demandeur et des règles d'accès qui spécifient ce que le demandeur est autorisé (ou non) à faire[41].

- **Contrôle d'accès mandataires (MAC) :** Dans le même temps, des politiques définies de manière centralisée sont appliquées pour toutes les ressources système. MAC est le meilleur pour les organisations. Cependant, il est écrit et nécessite des règles définies au préalable pour toutes les ressources pouvant être prises en compte dans le système. Les politiques contrôlent l'accès conformément aux réglementations obligatoires déterminées par une autorité centrale [41].

II.3.4 Modèles de contrôle d'accès

Le modèle de contrôle d'accès fournit une représentation formelle de la politique de contrôle d'accès sur laquelle il opère. Cette représentation formelle fournit un cadre pour prouver que les propriétés de sécurité d'une politique de système de contrôle d'accès conçue peuvent être étendues au fil du temps pour s'adapter à de nouvelles exigences ou à des changements organisationnels.
Exemple : RBAC [42], ABAC [43], VBAC [44], TBAC [45], TMAC [46] et ORBAC [47].

II.3.5 Mécanisme de contrôle d'accès

Les mécanismes de contrôle d'accès définissent les fonctions de bas niveau (logiciel et matériel) qui mettent en œuvre les contrôles imposés par la politique et formellement énoncés dans le modèle. Des exemples de mécanismes de contrôle d'accès bien connus : Les listes de contrôle d'accès (ACL) [48] et les capacités [49].

II.3.6 Architecture

Toutes les solutions de contrôle d'accès remplissent la même fonction : protéger les systèmes contre les accès non autorisés. Ils utilisent donc tous les mêmes blocs de construction de base. Ces blocs représentent des fonctions logiques. La façon dont ils sont répartis entre les participants et combien de fois ils sont répliqués est ce que nous utiliserons pour définir l'architecture.

Point de décision politique (PDP) [50] **:** Le point où les décisions politiques sont prises.

Point d'application de la politique (PEP) [50] **:** Le point où les décisions politiques sont effectivement appliquées.

Point d'information sur les politiques (PIP) [43] **:** Une entité qui sert de source d'extraction des attributs, ou des données requises pour l'évaluation des politiques afin de fournir les informations nécessaires au PDP pour prendre les décisions.

Point d'administration de la politique (PAP) [51] **:** l'entité du système qui crée une politique ou un ensemble de politiques.

D'abord, le PAP définit cette règle et l'impose au PDP. Supposons que nous sommes lundi matin et que Belinda se rend au travail. Elle appuie son badge sur la porte du parking, le PEP. Le PEP récupère

d'abord son identité à partir de son badge. Il interroge ensuite un serveur situé quelque part dans le bâtiment qui fait office de PDP. Le PDP interroge une base de données agissant comme un PIP pour demander si Belinda est une employée. Le PIP confirme que Belinda est bien une employée. Une réponse positive est renvoyée au PEP qui lui ouvre la porte[52].

La figure II.8 suivant montre une instance de demande de contrôle d'accès.

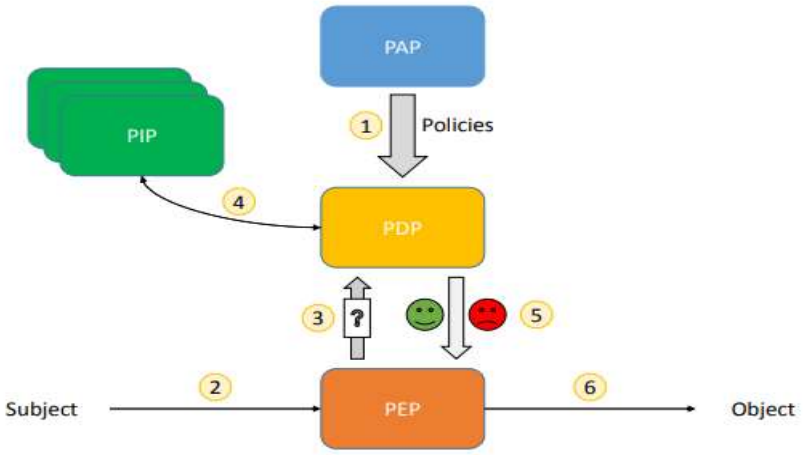

FIGURE II.8 : Instance de demande de contrôle d'accès[52].

II.3.7 Contrôle d'accès à base de blockchain

Les systèmes de contrôle d'accès sont appliqués à la sécurité informatique pour vérifier les conditions et la mise en œuvre de l'octroi ou de la révocation de l'accès aux ressources logiques ou physiques. L'application de la blockchain aux systèmes de contrôle d'accès est l'un des domaines indemnes d'utilisation de cette nouvelle technologie. Les caractéristiques uniques de la blockchain telles que la durabilité, l'immuabilité, la fiabilité, l'audibilité et la sécurité, en font une solution parfaite pour les systèmes de contrôle d'accès pour une variété d'application. La blockchain peut être considérée comme une base de données distribuée pour gèrer le contrôle d'accès et comprend l'historique permanent des transactions qui sont inviolables et indélébiles. En outre, la blockchain élimine la part des tiers du système et par conséquence, elle assure la confidentialité.

MedRec [53] est l'une des premières études à mettre en place un système de contrôle d'accès pour le partage de données médicales basé sur la blockchain Ethereum. Le système décentralisé permet le partage des données médicales avec le patient qui est le véritable propriétaire des données. MedRec utilise une solution de récompense minière pour inciter les participants médicaux à participer au système et authentifier les transactions en tant que mineurs. Ainsi, le MedRec permet l'émergence de l'économie des données en fournissant aux chercheurs des mégadonnées tout en engageant les patients.

MedShare[54] est un autre cadre basé sur la blockchain pour le partage des grandes données médicales entre des services en cloud afin d'obtenir la provenance et la vérification de donnée. MedShare surveille les entités qui accèdent aux données pour une utilisation malveillante à partie d'un système de dépositaire de donnée. Les transactions et le partage des données d'une entité à l'autre, ainsi que toutes les actions effectuées sur le système MedShare sont enregistrées de manière inviolable.

Dans [55], les auteurs présentent une application de contrôle d'accès basée sur la blockchain qui utilise la blockchain publique Bitcoin pour exprimer les échanges d'autorisations d'accès à une ressource entre les utilisateurs. Puisqu'il utilise une blockchain publique, tout le monde peut voir qui accède à quelles ressources. Il offre une audibilité et une sécurité tout en compromettant la confidentialité.

Les auteurs de [56] font des études de contrôles d'accès basé sur la blockchain qui considèrent le contrôle d'accès dans le contexte de l'IoT. Leur solution FairAccess comme un cadre de gestion des autorisations entièrement décentralisé, pseudonyme et préservant la vie privée, qui permet aux utilisateurs de posséder et de contrôler leurs données.

II.3.8 Contrôle d'accès basé sur des contrats intelligents

L'utilisation de contrats intelligents pour le contrôle d'accès présente plusieurs avantages, notamment : premièrement, la décentralisation garantit qu'aucune entité ne contrôle l'exécution. Par conséquent, l'exécution du code est fiable et toutes les modifications qui en résultent sont approuvées par consensus. Deuxièmement, en raison du consensus et de la preuve de travail, le code ne peut pas être changé ou modifié.

Un modèle d'accès est présenté dans [57] où le contrôle d'accès est basé sur les rôles (RBAC) utilisant des contrats intelligents (RBAC-SC), une plate-forme qui utilise la technologie de contrat intelligent Ethereum pour permettre l'utilisation de rôles dans toutes les organisations. RBAC-SC utilise des contrats intelligents et la technologie blockchain comme cadre général pour exprimer les relations de confiance et d'approbation qui sont essentielles dans RBAC, et implémente un protocole d'authentification defi-response qui vérifie la propriété du rôle de l'utilisateur.

Un schéma est proposé dans [58] pour faciliter le contrôle d'accès multi-autorisations basé sur les attributs à l'aide de contrats intelligents Ethereum. Dans ce schéma, les contrats intelligents Ethereum sont créés pour définir les interactions entre les propriétaires de données, les utilisateurs de données et les autorisations d'attributs multiples. Les utilisateurs de données présentent leurs attributs à différentes autorisations d'attribut et, une fois la vérification d'attribut réussie, ils obtiennent des jetons d'attribut pour leurs autorisations d'attribut respectives. Une fois que suffisamment de jetons de propriété ont été collectés, un contrat intelligent est exécuté pour transmettre la clé à l'utilisateur de données afin qu'il puisse accéder à l'objet de requête.

MedShare [54] discute également de la conception de l'utilisation de contrats intelligents et de mécanismes de contrôle d'accès pour suivre efficacement le comportement des données et révoquer l'accès aux entités fautives lorsque des violations d'autorisation de données sont détectées.

II.4 Blockchain pour le réseau radio cognitif

Ces dernières années, la blockchain a été largement utilisée dans l'Internet des objets, les réseaux de brouillard, les réseaux cloud et les réseaux cellulaires à large bande. Un nombre limité de documents de recherche sont disponibles sur les blockchains avec les réseaux CRN. Par conséquent, la combinaison de la technologie blockchain et du CRN est cruciale pour améliorer la détection du spectre avec des contraintes de sécurité. La technologie blockchain généralisée avec CRN est illustrée à la figure II.8.

Clé privée s'agit de la clé d'identité de chaque bloc du CR de l'utilisateur. Les utilisateurs CR ne connaissent que la clé privée. Dans la méthode proposée, une clé générée de 16 bits est considérée comme une clé privée. Signification résultat Il est défini comme la partie données du bloc.
Il s'agit du détail des résultats finaux de la détection basée sur la technique d'identification de l'énergie.

Hash est défini comme une clé unique qui est créée à l'aide de la fonction sha256.
Chaque utilisateur possède une clé unique qui est également appelée clé publique de l'utilisateur en question. Cette clé est présentée au bloc suivant de l'utilisateur. Cette clé peut être partagée avec les considérations du réseau.

Dans les CRN utilisant la technologie blockchain, la détection des utilisateurs malveillants est une tâche importante pour améliorer les performances du système. Dans la méthode proposée dans [32], la détection des utilisateurs malveillants ainsi que la gestion de la détection du spectre sont considérées comme les principaux objectifs du réseau CRN adoptant la technologie blockchain.

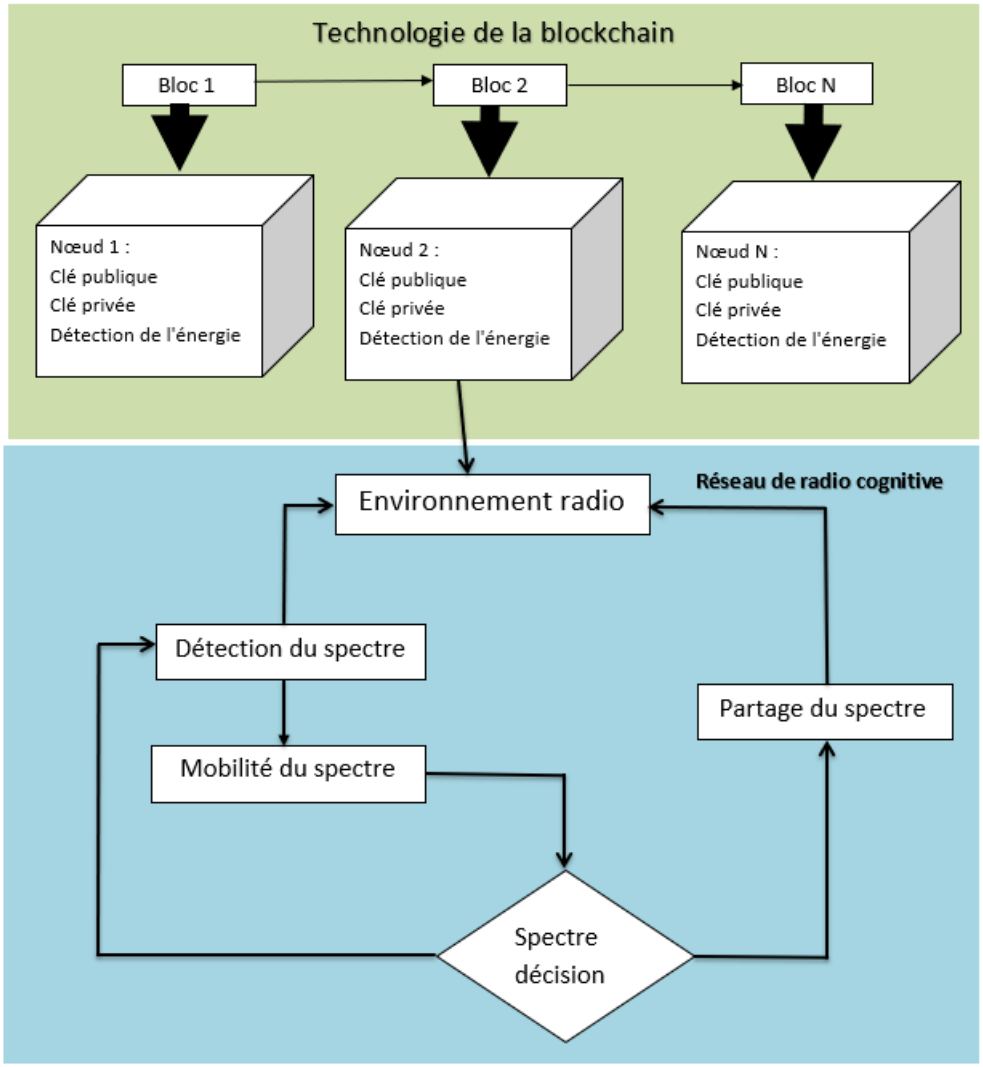

FIGURE II.9 : Blockchain avec conception de réseau CRN[32].

II.4.1 Blockchain pour la détection du spectre

Dans la première étape du processus, les utilisateurs primaires (PU) et les utilisateur secondaire (SU) sont convertis en blocs de blockchain. Dans le réseau CRN, le registre distribué des nœuds avec les données SU et PU est initialisé. Dans le bloc, les clés privées et publiques sont générées. Une clé privée se compose d'informations secrètes sur un nœud, telles qu'un code d'authentification et son emplacement. De même, la clé publique est constituée d'informations générales qui dépendent de différentes parties du CRN, telles que l'état du réseau de transport, segments dans le CRN, tels que le statut PU ou SU[32].

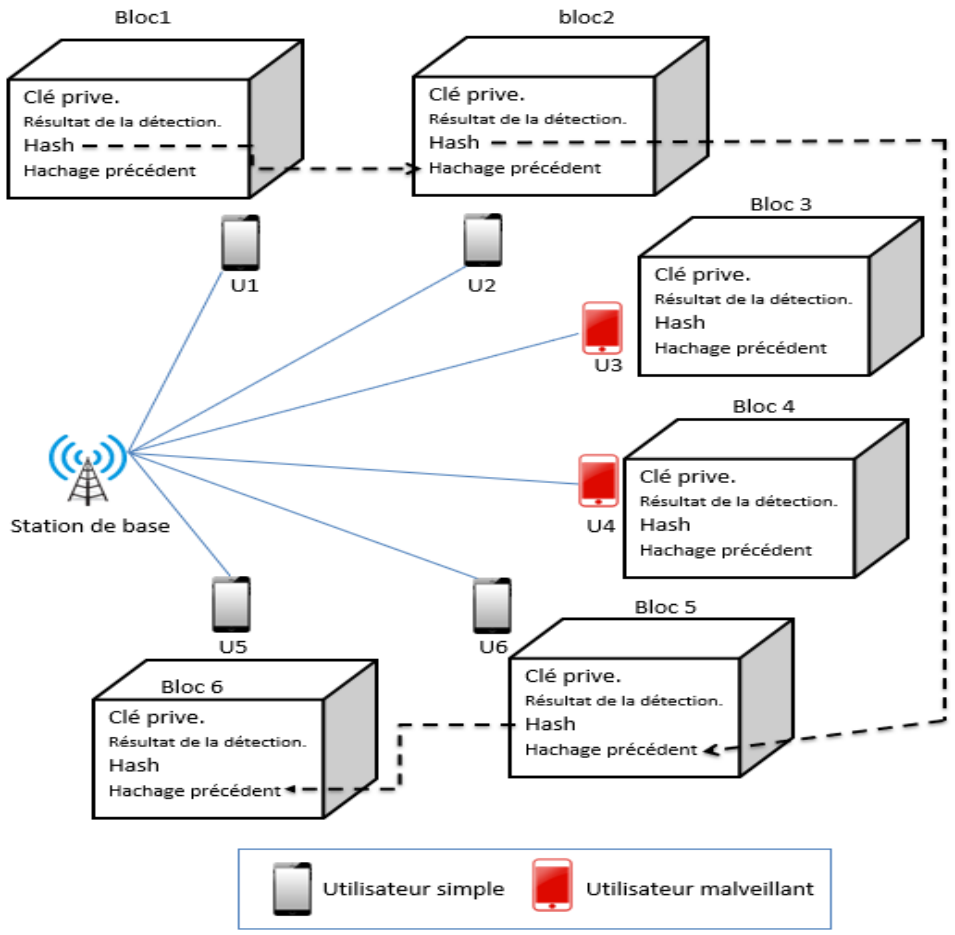

FIGURE II.10 : Blockchain avec détection d'un utilisateur malveillant[32].

II.4.2 Blockchain pour la gestion du spectre

Récemment, les régulateurs des télécommunications ont mis l'accent sur l'application de la technologie blockchain pour améliorer la qualité du service, comme la gestion des numéros de téléphone et la gestion du spectre. Au Royaume-Uni, Ofcom a lancé un projet pour étudier comment utiliser la blockchain pour gérer les numéros de téléphone [33].

Plus précisément, la technologie blockchain peut être utilisée pour créer une base de données décentralisée, améliorer l'expérience client lors du transfert de numéros entre fournisseurs de services, réduire les coûts réglementaires et prévenir les appels importuns et la fraude. D'autre part, la blockchain devrait également offrir de nouvelles opportunités pour la gestion du spectre.

Selon un récent discours de la commissaire de la FCC, Jessica Rosenworcel, la blockchain peut être utilisée pour contrôler et gérer les ressources du spectre afin de réduire les coûts de gestion et d'accélérer le processus d'enchères du spectre [34].

Tout utilisateur intéressé peut accéder à l'utilisation du spectre en temps réel qui y est enregistrée, de sorte que la fréquence de la bande peut être allouée dynamiquement en fonction de la demande

dynamique soumise par l'utilisateur, améliorant ainsi l'efficacité de l'utilisation du spectre. Basé sur les requêtes dynamiques soumises par les utilisateurs utilisant la blockchain.

II.4.2.1 Blockchain comme base de données sécurisée

La base de données de géolocalisation classique pour l'utilisation des bandes de spectre, comme les espaces blancs de télévision, peut être réalisée par la blockchain avec une sécurité, une décentralisation et une transparence accrues.

En outre, d'autres informations telles que les résultats historiques de détection, les résultats des enchères de spectre et les enregistrements d'accès peuvent également être stockés dans la blockchain et les enregistrements d'accès peuvent également être stockés dans la blockchain.

II.4.2.2 Marché du spectre auto-organisé

Un marché du spectre auto-organisé est souhaité avec son efficacité améliorée et son coût réduit dans l'administration par rapport à la dépendance à une autorité centralisée pour gérer les ressources du spectre.

Grâce à la combinaison de contrats intelligents, de crypto-monnaies et d'algorithmes cryptographiques pour la vérification des identités et des transactions, la blockchain peut être utilisée pour établir un marché du spectre auto-organisé.

Par exemple, les enchères traditionnelles de spectre nécessitent généralement une autorité de confiance pour vérifier l'authentification des utilisateurs, décider de l'utilisateur gagnant et régler le processus de paiement. Avec la blockchain, et plus précisément avec le contrat intelligent, les ventes aux enchères de fréquences peuvent être organisées de manière sécurisée, automatique et non controversée.

En outre, grâce à la sécurité offerte par la blockchain, des transactions peuvent être effectuées entre les utilisateurs sans qu'ils aient confiance les uns dans les autres. Ainsi, la barre élevée pour obtenir les ressources du spectre peut être réduite. Outre le droit d'accès au spectre, d'autres biens/services liés à la gestion du spectre, tels que la détection du spectre, peuvent également être échangés entre utilisateurs par des contrats intelligents.

II.4.2.3 Déploiement de la blockchain

L'algorithme de consensus, tel que Proof of Work (PoW), grâce auquel un nouveau bloc contenant des transactions peut être ajouté à la chaîne de blocs. Par lequel un nouveau bloc contenant des transactions peut être ajouté à la blockchain, est généralement gourmand en ressources de calcul.

Il est donc nécessaire de prendre en compte la capacité de calcul et la batterie limitées des utilisateurs mobiles lors du déploiement de la blockchain sur le réseau radio cognitif traditionnel.

Sur cette base, nous proposons trois méthodes

- Permettre aux utilisateurs de maintenir directement une blockchain,
- Utiliser une blockchain dédiée maintenue par une autorité tierce,
- Permettre aux utilisateurs de utilisateurs de décharger simplement la tâche de calcul à des fournisseurs de services de calcul en périphérie (ECSP) tout en conservant la propriété de la blockchain. (ECSP) tout en conservant l'autorité de vérification et de validation pour eux-mêmes.

II.4.3 Smart Contract dans la radio cognitive

Il existe de nombreuses méthodes différentes pour gérer la détection du spectre et maintenir la sécurité dans le réseau CRN avec la technologie blockchain, l'une des méthodes c'est les contrats intelligents. L'utilisation de ce dernier dans La radio cognitive fournit une solution efficace pour certaine attaque comme l'attaque spectrum sharing data falsifcation (SSDF) et d'autres.

II.4.3.1 Détections de spectre à base de contrats intelligents

Selon [40], le SU émet une tâche de détection de spectre et propose des exigences de tâche y compris le temps d'acquisition, le budget, les restrictions d'emplacement géographique, la gamme de bandes de fréquences, etc., puis utilise un langage de programmation pris en charge par des chaînes de blocs telles que ***« Solidity »*** pour écrire la tâche et écrire le code du contrat intelligent. Publier le contrat intelligent écrit, les mineurs le conditionnent et l'écrivent dans la blockchain. Bien que le contrat intelligent soit publié sur la blockchain, il ne s'exécutera pas automatiquement et devra répondre aux conditions de déclenchement correspondantes. Dans cet article, la condition de déclenchement est que le SU choisit d'accepter la tâche après avoir vu le contenu de la tâche et l'enregistre sur le contrat intelligent. Une fois le contrat intelligent publié sur la blockchain, la station de base de l'unité de stockage diffuse l'adresse du contrat intelligent en blockchain.

Les nœuds de détection locaux intéressés peuvent récupérer le contenu du contrat par adresse et le visualiser. Affichez le contenu du contrat par adresse et consultez les exigences relatives aux tâches de découverte. Il calcule sa propre utilité en fonction de ses préférences, de l'énergie restante, de l'emplacement géographique, des récompenses estimées et d'autres facteurs. Si l'utilité est supérieure à l'utilité moyenne de tous les SU, le SU accepte la tâche de détection du spectre et s'inscrit au contrat intelligent. Le contrat intelligent choisit ensuite un nœud enregistré en fonction de son budget, du prix demandé par le SU et de sa réputation. Les nœuds sélectionnés démarrent la tâche de découverte et téléchargent les résultats de la découverte vers la station de base de l'unité de stockage avec leurs signatures numériques.

La station de base SU décrypte et fusionne les données de détection, et paie la récompense.

La figure suivante montre la détection du spectre basée sur un contrat intelligent.

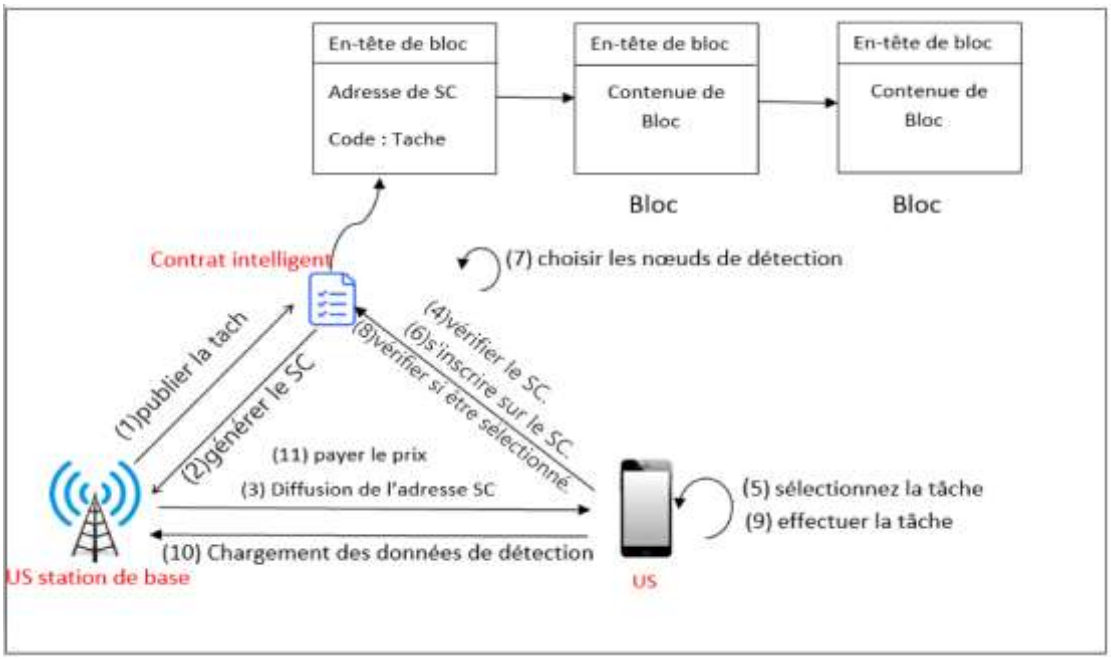

FIGURE II.11 : Détection du spectre basée sur un contrat intelligent[40].

II.4.3.2 Utilisation des contrats intelligent dans le partage coopératif primaire

Les contrats intelligents pourraient exiger qu'un utilisateur se soumette à une vérification et ses appareils répondent à certains critères qui contrôleraient la clé de signature privée nécessaire pour appliquer certaines actions dans le contrat. En plus de la flexibilité et de l'automatisation des contrats fournir un enregistrement transparent, auditable et unifié des transactions[37].

II.4.3.3 Utilisation des contrats intelligents dans le partage primaire,non coopératif

Dans ce type de partage, les utilisateurs ne coordonnent pas leur utilisation du spectre à l'avance et ils sont équivalents pour transmettre et recevoir. L'exemple le plus simple de ce type de partage serait le spectre en libre accès tel qu'il est caractérisé par les bandes ISM sans licence (même si certaines utilisations de ces bandes mettent en œuvre une certaine coopération dans leur protocole d'accès au support). Il existe deux sous-catégories de partage primaire non coopératif : Espaces Communs en accès libre (Open Access Commons), Communs privés (Private Commons).

Dans un bien commun privé, le respect des normes de coordination est exigé par le gestionnaire du bien commun. Donc, l'application n'est pas seulement une question d'exigences de base par les régulateurs, mais des conditions spécifiques fixées pour le privé. Parce que chaque appareil devrait

s'enregistrer et être identifié, des contrats intelligents pourraient être utilisés pour établir le paiement mécanismes des appareils au gestionnaire de biens communs. Ils pourraient également fonctionner comme un « kill switch » pour les appareils qui ne parviennent pas à répondre aux exigences applicables.

II.4.3.4 Utilisation des contrats intelligent dans le partage secondaire,non coopératif

Le partage secondaire, non coopératif est un cas de partage opportuniste caractérisé par les radios cognitives, où les utilisateurs ne coordonnent pas leur utilisation à l'avance avec les utilisateurs principaux. Cette approche a été largement étudiée.

Les contrats intelligents pourraient encore améliorer un tel système. Ils pourraient être utilisé pour mettre en œuvre des masques de transmission géospécifiques pour limiter la capacité des appareils secondaires à interférer avec les utilisateurs, tout en leur laissant la flexibilité de transmettre quand, où et comment ils choisissent. Si les utilisateurs principaux rencontrent interférence, un registre basé sur la blockchain enregistrant les activités des dispositifs secondaires pourraient être utilisés pour évaluer les violations, ou même imposer des pénalités par le biais de contrats intelligents.

II.4.4 Les jetons non fongibles dans le reseau radio cognitif

II.4.4.1 Une analyse approfondie sur les jetons digitaux

Les jetons digitaux ou bien les jetons crypto sont les plus utilisés dans les crypto-monnaies. Et on peut dire techniquement qu'un cryptomonnaie est un jeton mais pratiquement ce sont deux choses différentes.

Ils sont utilisés pour décrire les actifs (asset en anglais) numériques qui fonctionnent sur la base d'une infrastructure de blockchain ,en général, les jetons sont créés pour un objectif spécifique dépend de l'organisation ou de l'individu qui a créé ce dernier, et peut être de toute nature : il peut s'agir de collecter des fonds ou de donner l'accès à des services.

Ces jetons sont complètement décentralisés, ils constituent un moyen d'échange (dépend de la blockchain utilisée) et utilisent des signatures cryptographiques à des fins de sécurité et d'enregistrement, de la même façon que les autres actifs crypto. Toutefois, ils présentent des différences fondamentales.

II.4.4.2 La différence entre les jetons digitaux crypto et cryptomonnaies

Comme nous venons de le dire : les deux sont similaires paracerque les deux sont décentralisés et ayant une valeur dans les systèmes, mais leur structure est différente, les cryptomonnaies font partie de la blockchain elle-même par exemple Ethereum ou Bitcoin, même leur structure et les moyens de manipulation (d'échange, création ..), par contre les jetons Digitaux ne font pas partie intégrante d'une

blockchain, leurs structures sont définis par l'organisation ou de l'individu et leur comportement est plutôt régulé par des contrats intelligents qui déterminent comment les transactions s'effectuent.

II.4.4.3 Les jetons non fongibles

Les jetons non fongibles (NFT) représentent des actifs numériques qui permettent aux personnes d'acquérir des actifs et d'enregistrer leur propriété exclusive (par exemple, une voiture dans un jeux public). Grâce à la blockchain, la partie « non fongible » qui signifie que ces derniers sont uniques et ne sont pas interchangeables. Par exemple, l'argent est fongible, on peut échanger des dollars, mais une œuvre d'art (pièce de Mona Lisa) est non fongible, car elle est unique.

Les NFT n'ont réellement touché le grand public qu'à partir de 2017, lorsque la plateforme Ethereum a pris de l'ampleur. C'est sur cette blockchain que les projets CrytoPunks et CryptoKitties (utilisant des NFT) sont nés.

Les NFT sont utilisée dans plusieurs domaines grâce aux propriétés de ce dernier et la flexibilité de manipulations via les contrats intelligents par exemples :

- ✓ Une peinture digitale ;
- ✓ Une vidéo, comme les vidéos de basket de « NBA Top Shot » ;
- ✓ Un mème ;
- ✓ Une photographie ;
- ✓ Un objet de collection, une carte par exemple.

II.5 Conclusion

Dans ce chapitre, nous examinons de manière générale la blockchain et ses concepts qui est une nouvelle technologie qui a retenu l'attention des chercheurs et des innovateurs dans le monde. Nous démontrons que plusieurs domaines bénéficient de cette technologie par exemple le réseau de la radio cognitive qui utilise cette technologie pour gérer le spectre et identifier les utilisateurs malveillants pour augmenter et améliorer les performances de réseau.

Chapitre III : Contribution et Résultats

III. Chapitre III : Contribution et résultats

III.1 Introduction

Dans ce chapitre, nous allons présenter notre travail pour sécuriser l'accès aux spectre dans les réseaux de radio cognitive. En effet, nous avons choisi de traiter l'attaque PUE présentée dans le chapitre I qui est réalisée par un groupe d'utilisateurs malveillants qui veulent prendre la place d'un utilisateur primaire et partager les bandes de fréquences libres avec les utilisateurs secondaires.

Dans ce travail, nous pensons que l'intégration des NFT (ERC721) est une solution potentielle car il y a la possibilité de garantie que il y a un seul propriétaire de l'active par retourner l'adresse de le propriétaire qui est unique.

III.2 Les acteurs du système

Nous avons trois différents acteurs dans notre système qui sont décrit dans ce qui suit :

1. ***Autoritaire :*** c'est le responsable général qui va gérer les manipulations des bandes de fréquences qui sont représentés comme des jetons non fongibles dans notre système.

2. ***Utilisateur primaire :*** ce dernier va acheter une bande de fréquence et va créer des sous-bandes de fréquence et les publier pour que les utilisateurs secondaires puissent les utiliser.

3. ***Utilisateur secondaire*** : cet utilisateur va acheter des sous-bande de fréquence qui sont publiées par les utilisateurs primaires.

III.3 Scénario

Dans ce chapitre nous allons étudier le cas où il y a un seul autoritaire et quatre (4) PU et aussi 4 SU. Nous travaillons sur une blockchain locale (Hardhat) pour stocker les transactions, metamask pour affecter le payement et transformation d'argent entre les utilisateurs.

a) Côté Autoritaire et PU

Dans cette figure nous avons présenté le scenario d'autoritaire qui doit créer les bandes de fréquence (NFT) est publié aux PUs ce dernier doit choisir la bande de fréquence (NFT) selon son choix (prix, start band, end band, localisation, date périmassions) puis affecte le paiement à l'Autoritaire.

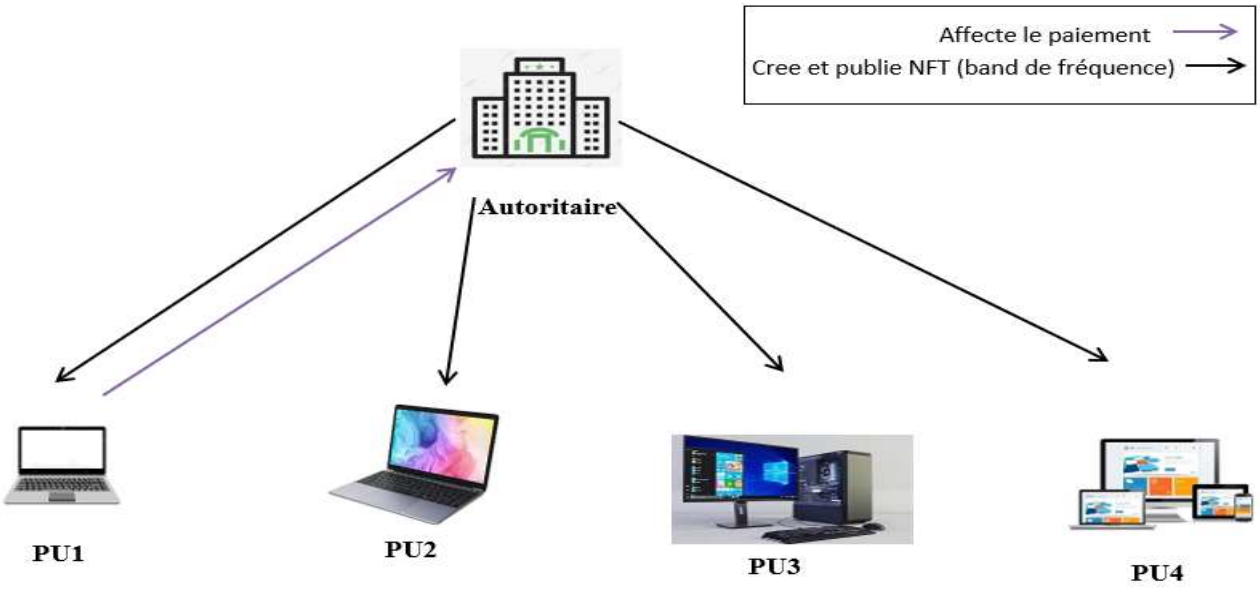

Figure III.1 : Scenario entre Autoritaire et PU.

b) Côté PU et SU

Dans cette figure nous avons présente le scenario de PU qui acheté la bande de fréquence a le choix de crée des sous bandes de fréquence non utilise et publié aux SU ce dernier doit choisir la bande de fréquence selon votre choix (prix, start band, end band, localisation, date périmassions) puis affecte le paiement aux PU.

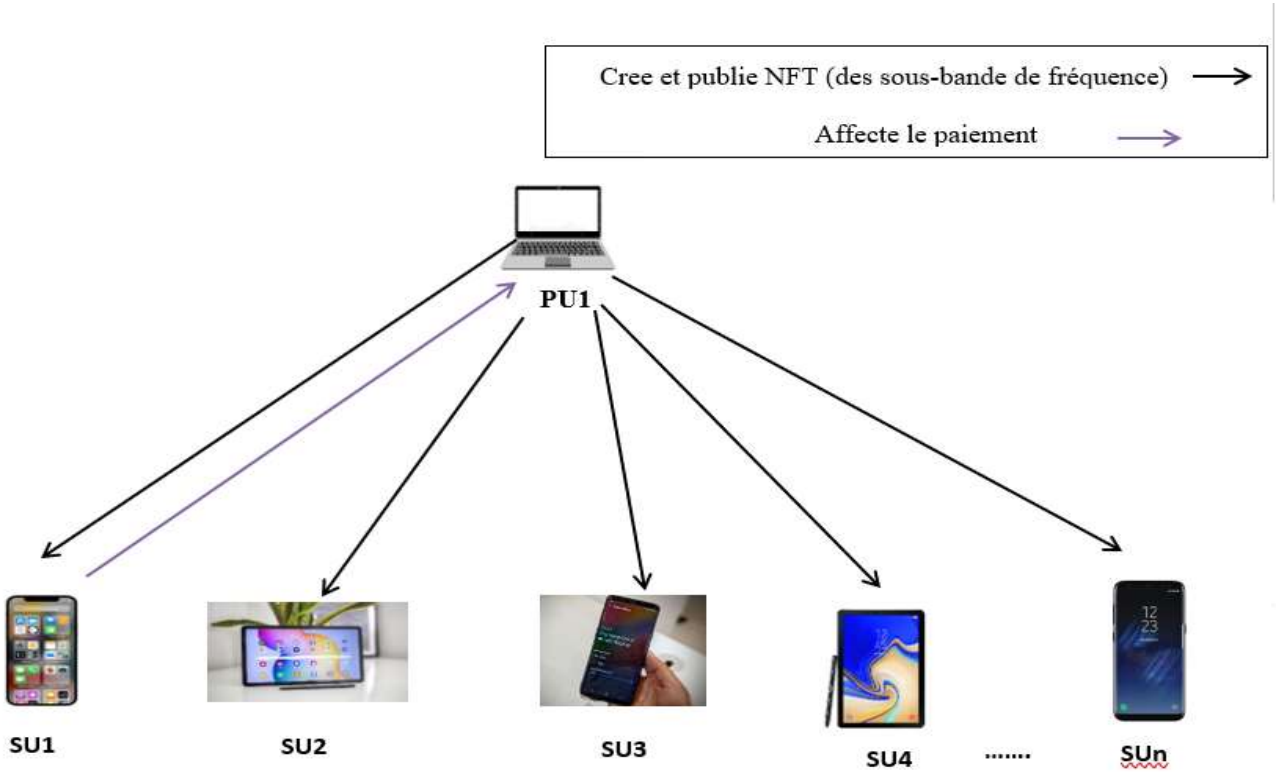

Figure III.2 : Scenario entre PU et SU.

III.4 Travaux relatifs

Les chercheurs ont étudié l'application de la blockchain dans la gestion du spectre. Par exemple, dans [35], les auteurs ont associé différents modes de partage du spectre avec différents types de blockchain.Dans [36], les auteurs présentent les avantages de l'application de la blockchain aux schémas de partage du spectre du Citizens Broadband Radio Service (CBRS).

Dans [37], l'accès dynamique au spectre permis par les enchères du spectre est assuré en utilisant la blockchain.Dans [38],des contrats intelligents soutenus par une blockchain sont utilisés pour fournir des services de détection du spectre fournis par des capteurs aux utilisateurs secondaires pour un accès opportuniste au spectre.

Essentiellement, il est nécessaire de dériver certains principes de base pour étudier pourquoi et comment l'application de la blockchain à la gestion dynamique du spectre peut être bénéfique.

Plus précisément, nous pouvons utiliser la blockchain :

- ✓ Comme une base de données sécurisée
- ✓ Pour établir un marché du spectre auto-organisé.

III.5 Contribution

Dans ce travail, nous avons utilisé la blockchain pour assurer que tous les utilisateurs sont fiables, puis nous avons protégé la communication entre les utilisateurs contre l'attaque PUE par la notion de jeton non fongibles (ERC721) qui garantie que chaque bande de fréquence a un jeton unique et gagnant la meilleure utilisation de la bande de fréquence sans interférence.

Le PU doit s'assurer que la bande de fréquence qu'il va acquérir est bel et bien fiable c'est-à-dire qu'elle provient de l'autoritaire et ceci grâce aux NFT.

Le SU à son tour doit aussi s'assurer que les sous bandes proviennent de chez un PU fiable.

III.6 Conception système (les diagrammes)

Nous avons donné un nom à notre application « SOLIDROMO ». En effet, ça signifie

SOLID =>Solid.

R => Rapid.

OMO => Organization for allocation and management spectrum of cognitive radio.

Dans cette partie on va décrire la conception de l'application « Solidromo », qui fournit une Plateforme riche pour manipuler l'allocation du spectre.

xiv. Spécification des besoins de système

III.6.1.1 Besoins non fonctionnels

L'application réponde à un ensemble des besoins non fonctionnels qui caractérisent le système. On résume ces besoins dans les points suivant :

- L'application doit être facile à utilisé, les interfaces simples et adapte à l'utilisateur.
- L'application doit être Scalable et fiable.
- Les taches doivent être indépendantes (multitâche).
- L'application doit être disponible à tout moment.
- L'application doit être sécurise.

III.6.1.2 Besoins fonctionnels

Dans cette section, nous proposons un ensemble des besoins fonctionnelles qui devraient satisfaire notre application Web. Permis c'est un ensemble des besoins fonctionnelles exprimées comme suit :

- L'authentification des utilisateurs par un adresse et clé prive pour accéder aux diffèrent fonctionnalité.

- Crée les bandes des fréquences, publie, renouveler, retirer et supprimer par l'Autoritaire.
- Acheté, demande des bandes des fréquences, Cree des sous-band de fréquence, publie et retirer par PU.
- Acheté des sous-bandes de fréquence par SU.

xv. Modélisation des besoins

III.6.1.3 Conception générale

1. Diagramme de cas d'utilisation : Il sert à modéliser les fonctionnalités du système dans une vue globale.

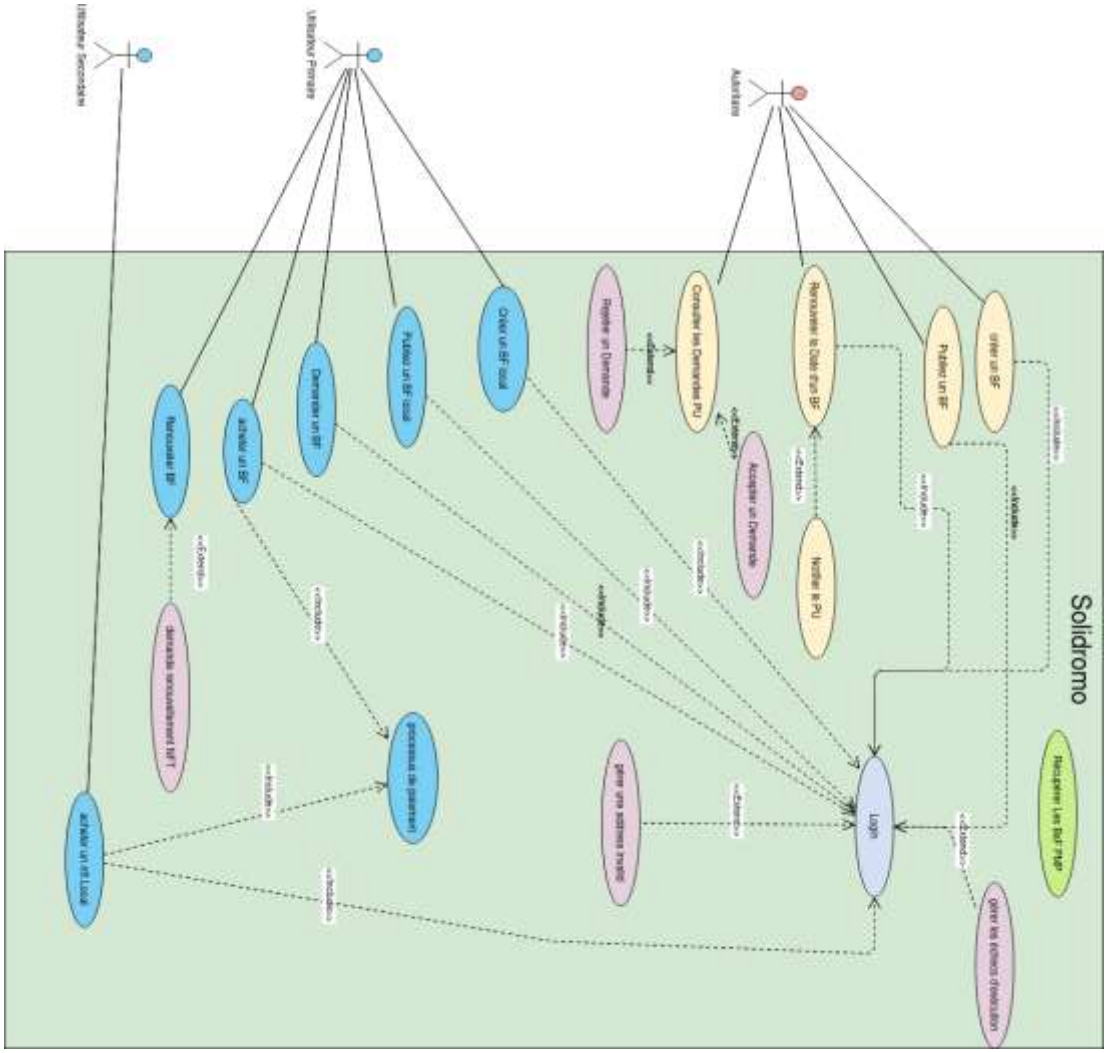

Figure III.3: Diagramme de cas d'utilisation.

2. Diagramme de séquence du cas « Demande d'une BF » :

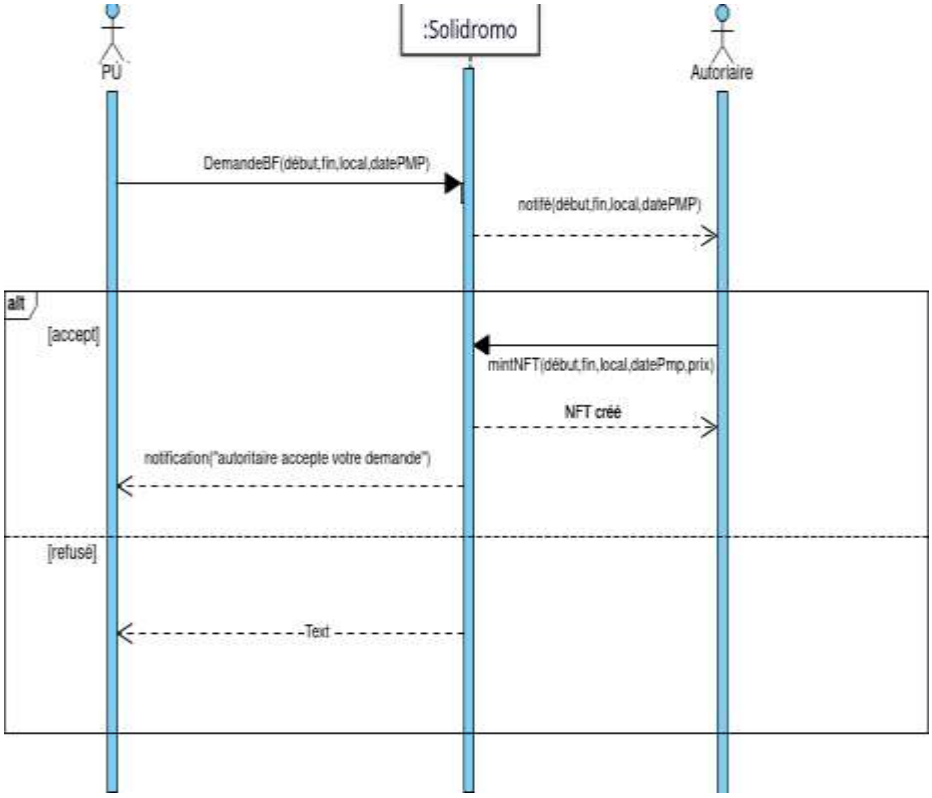

Figure III.4 : Diagramme de séquence du cas (Demande d'une BF).

1. Diagramme de séquence du cas « PU Acheter une BF »

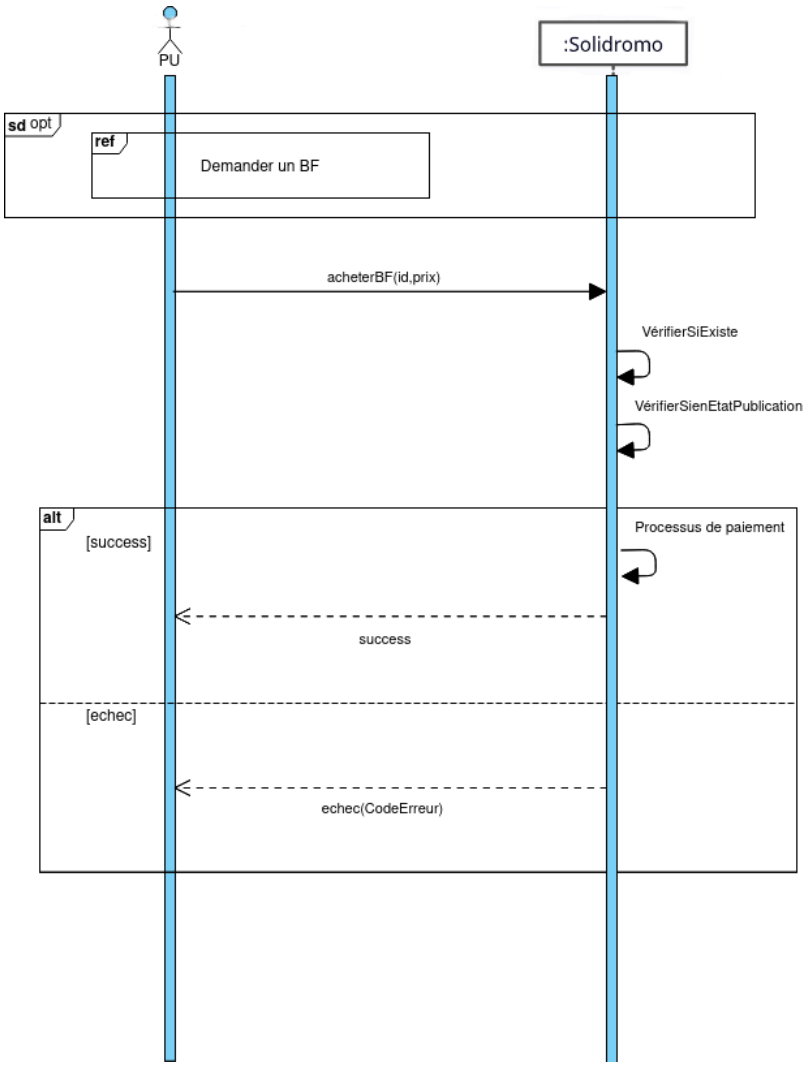

Figure III.5 : Diagramme de séquence du cas (PU Acheter une BF).

2. Diagramme de séquence du cas « Renouveler la date EXP d'un BF » :

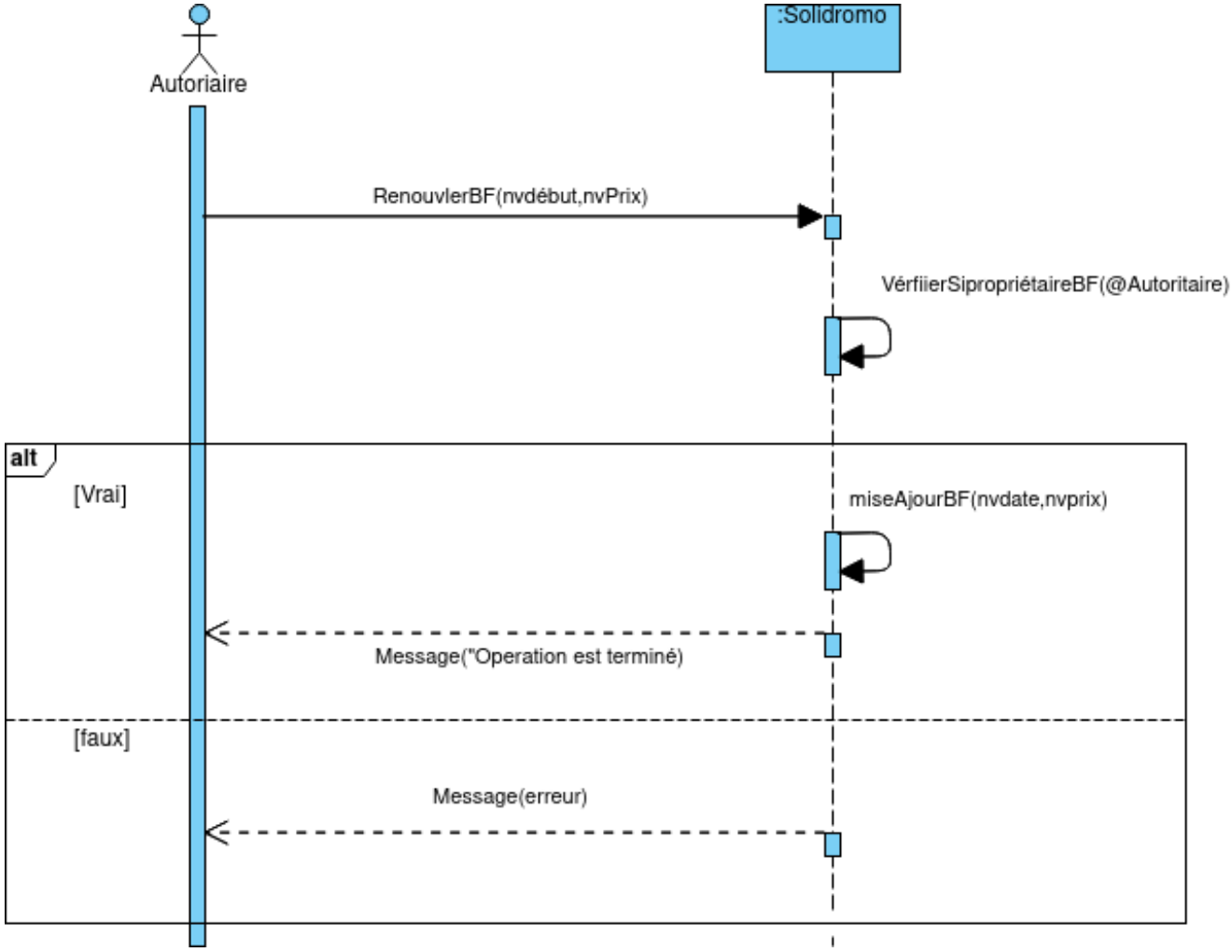

Figure III.6 : Diagramme de séquence du cas (Renouveler la date d'un BF).

3. Diagramme de séquence du cas « Renouveler une BF » :

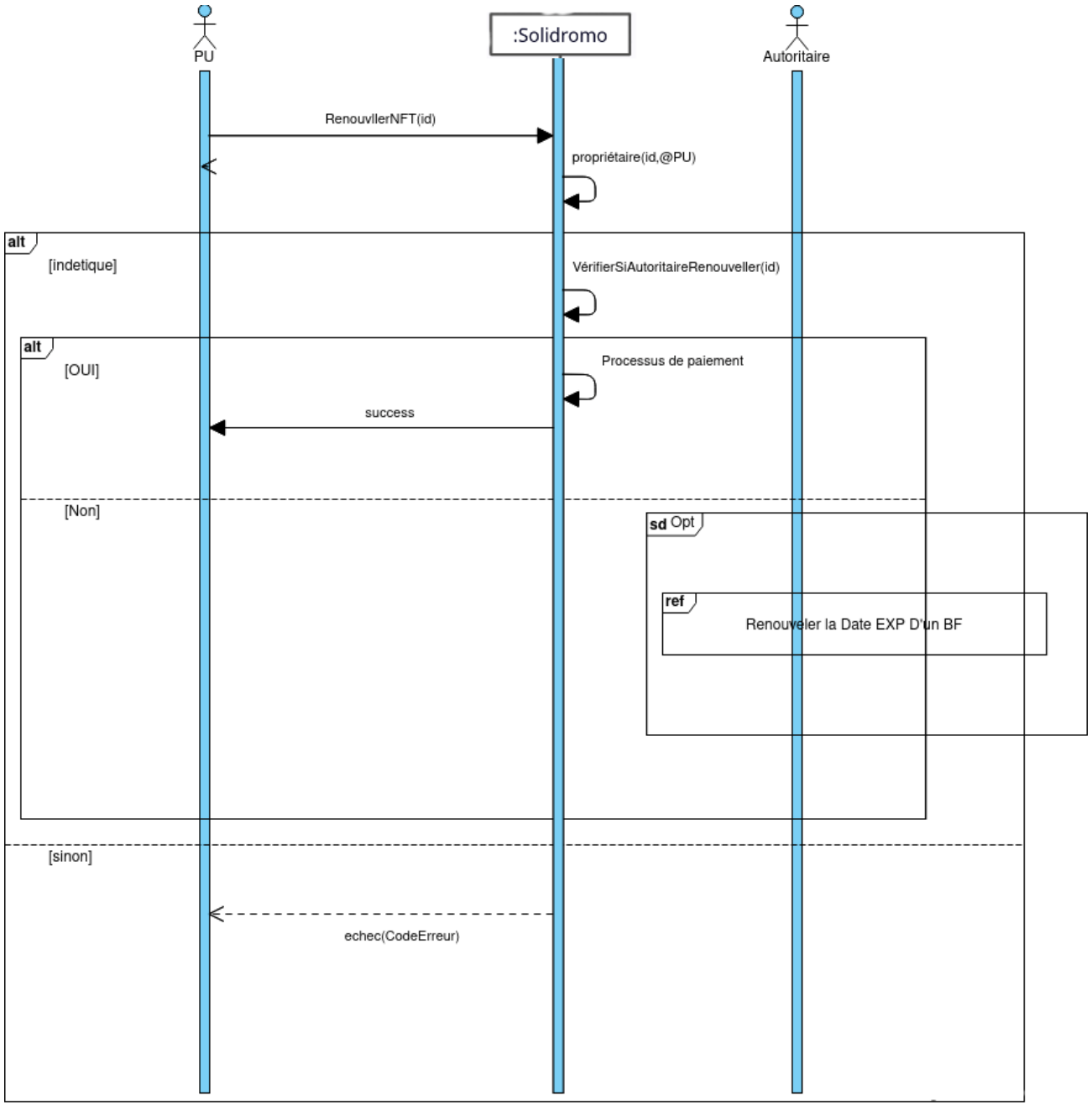

Figure III.7 : Diagramme de séquence du cas (Renouveler une BF).

4. Diagramme de séquence du cas « SU Acheter une BF » :

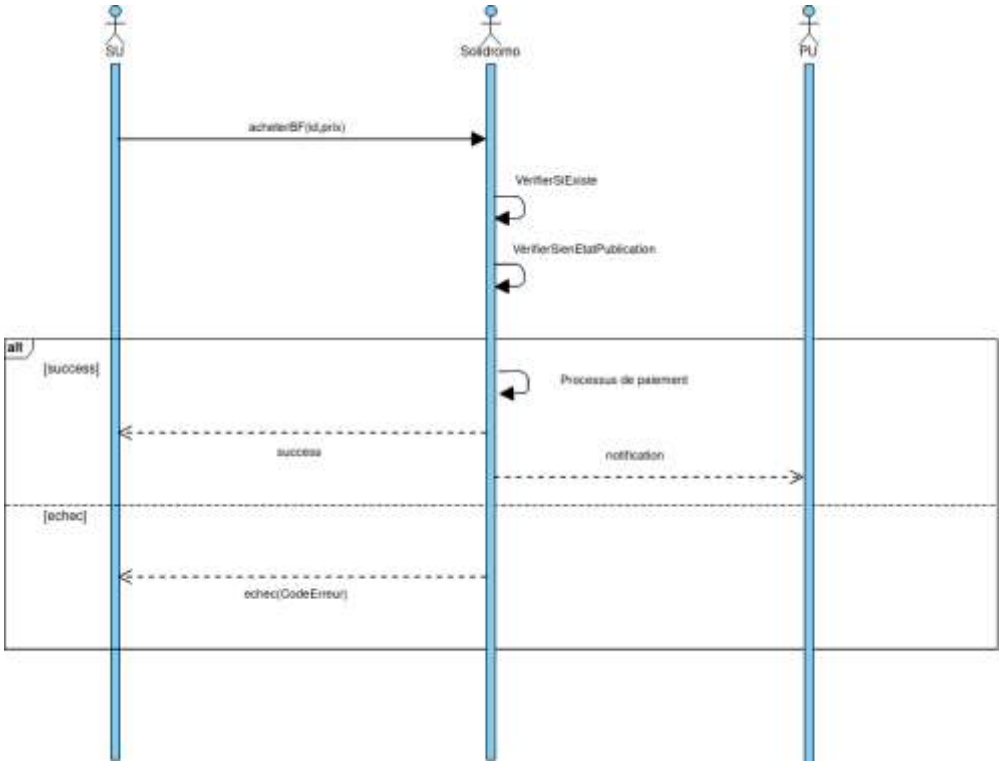

Figure III.8 : Diagramme de séquence du cas (SU Acheter une BF).

III.6.1.4 Conception détaillée

III.6.1.4.1 Architecture logique du système

1. Diagramme de composants

Le diagramme de composants permet de représenter les composants logiciels d'un système ainsi que les liens existants entre ces composants. [Référence de UML 2]

- **Navigateur :** Permet aux utilisateurs d'accès aux page Web (l'application).
- **Serveur Web :** C'est un logiciel qui permet de traité les requêtes qui récit par navigateur et fournit la page web correspondant.
- **App Web :** C'est un site web crée par les développeurs stocke dans un serveur web et accessible par Navigateur.
- **Blockchain :** dans notre application blockchain jouée une rôle d'une base des données décentralise qui permettre de stocke les données.

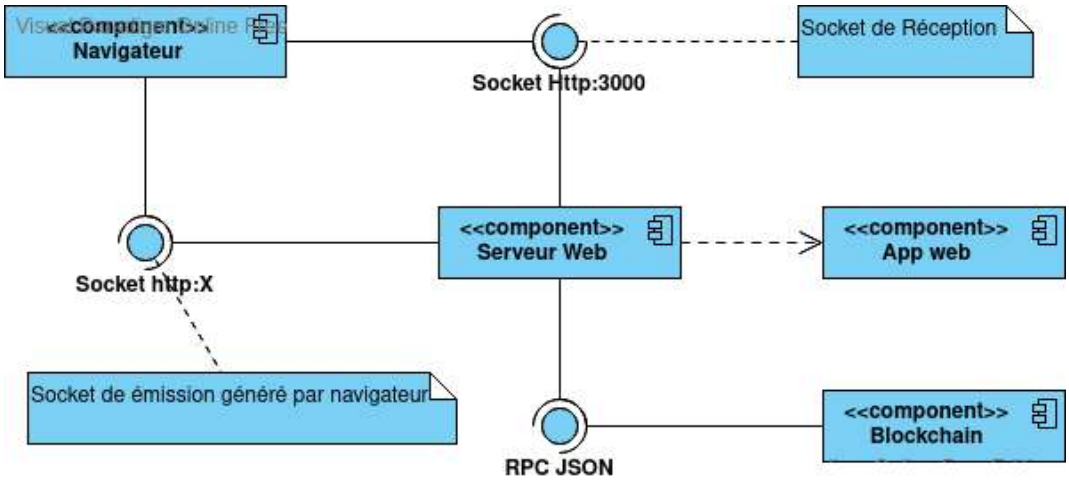

Figure III.9 : Cinématique des processus fonctionnels.

2. Acheter une bande de fréquence

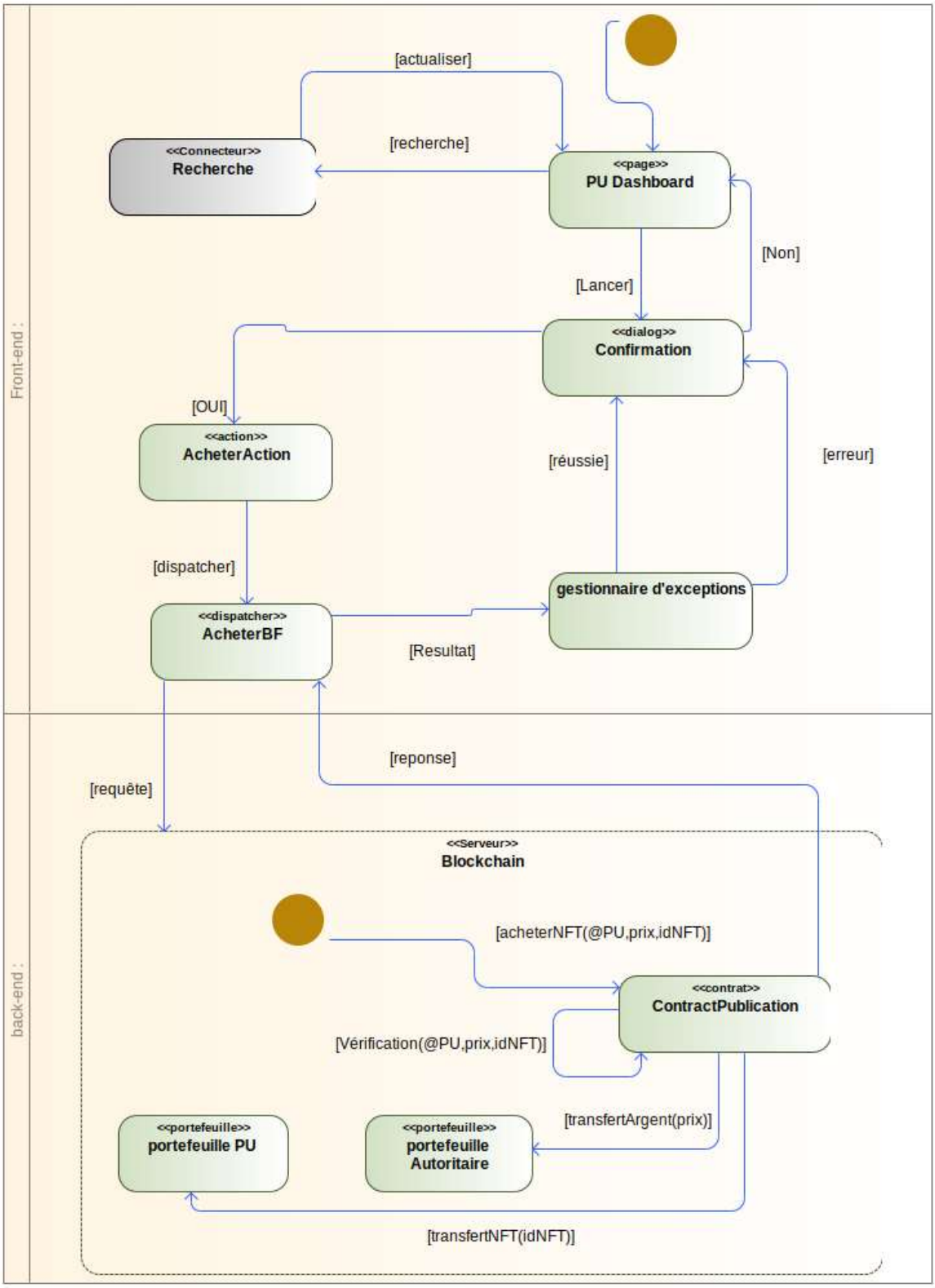

Figure III.10 : Cinématique d'Acheter une BF.

3. Renouveler une bande de fréquence

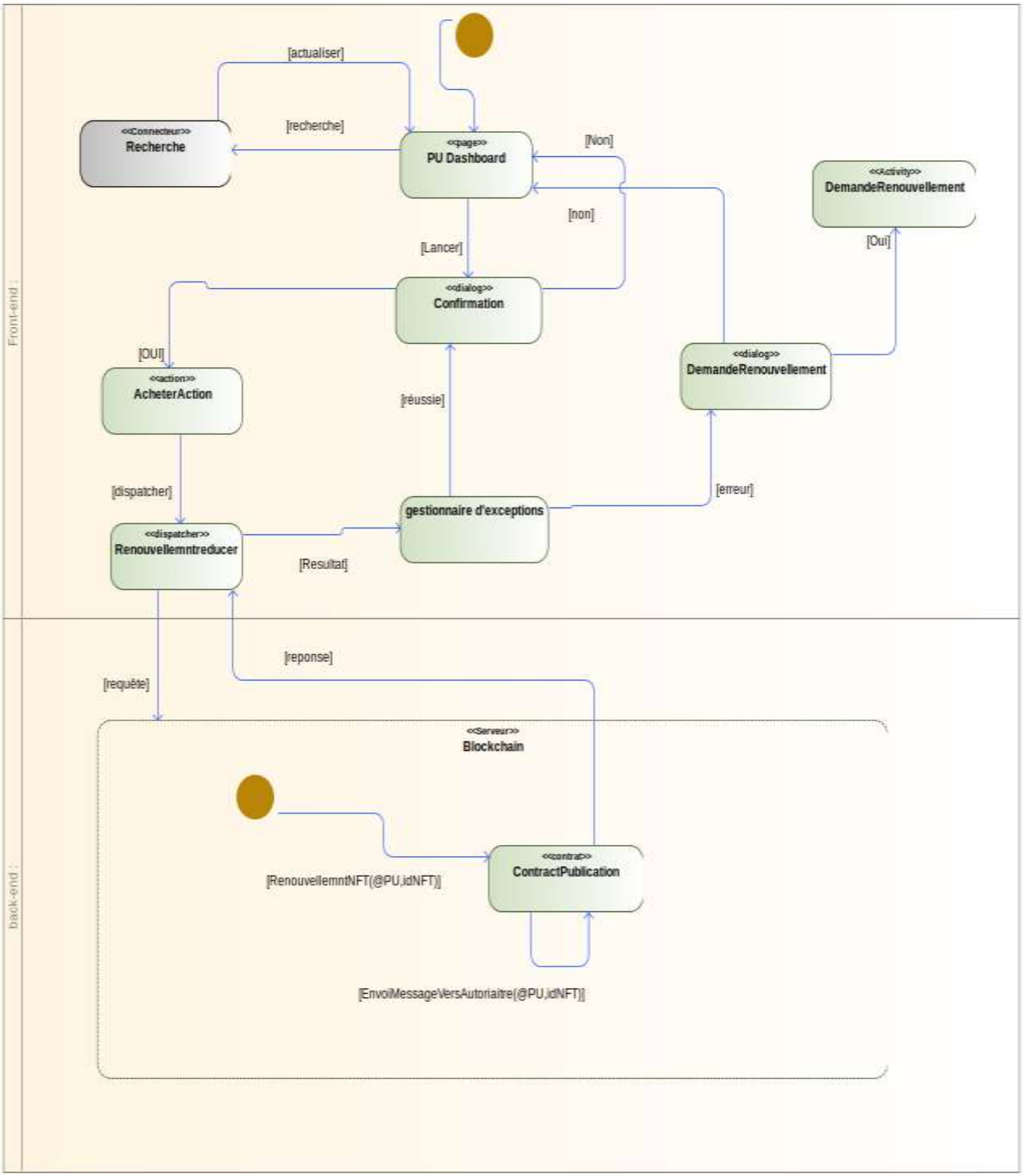

Figure III.11 : Cinématique de renouveler un BF.

4. Cinématique de navigation

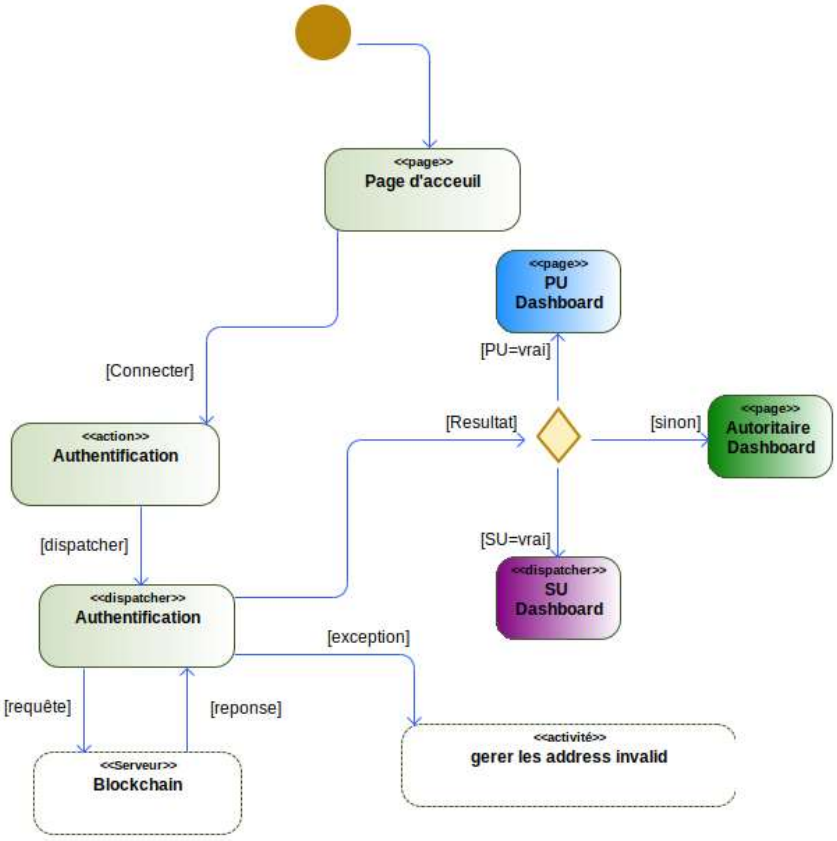

Figure III.12 : Cinématique de navigation.

III.6.1.5 Implémentation

L'implémentation de l'application « Solidromo » comprend une application front-end et application back-end .

Visual Studio Code

Visual Studio ou bien VS Code est un IDE qui combine la simplicité d'un éditeur de code source avec de puissants outils de développement, comme la complétion et le débogage de code IntelliSense [59].

Nous avons utilisé VS Code car il offre plein d'extensions comme ES7 React/Redux ,Solidity,Github Helpers qui facilitent le développement des applications web .

III.6.1.5.1 Front-end

1. Architecture FLUX

Flux est une architecture que Facebook utilise pour créer des applications Web côté client. Il complète les composants de vue composable de React en utilisant un

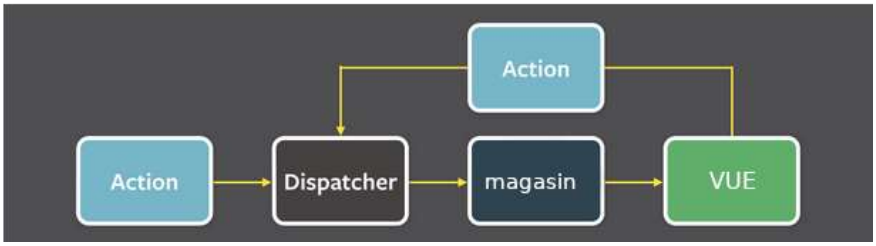

Figure III.13 : Système Flux.

flux de données unidirectionnel. Il s'agit plus d'un modèle que d'un cadre formel, et vous pouvez commencer à utiliser Flux immédiatement sans beaucoup de nouveau code.

Au début, l'utilisation d'un flux de données unidirectionnel est un grand problème pour les développeurs parce qu'avec cette architecture, ils ne peuvent pas manipuler les évènements asynchronisés comme par exemple l'accès aux base de données ou bien utilisation d'une API, dans notre cas accès à la Blockchain doit être avec des fonctions asynchronisées.

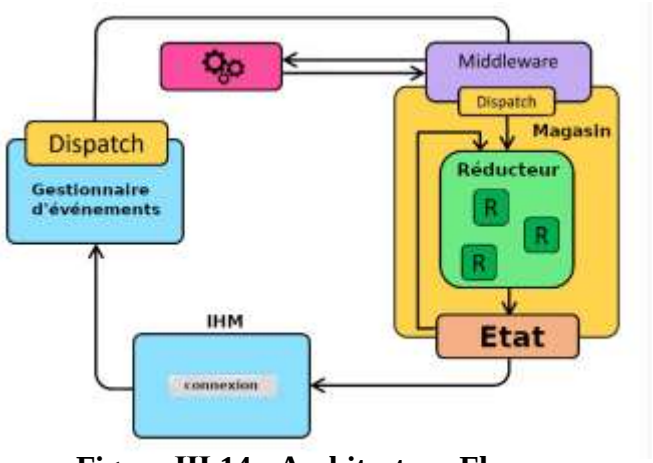

Figure III.14 : Architecture Flux.

Pour résoudre le problème, on doit utiliser un middleware entre les actions et les dispatchers et assurer que le middleware va déclencher les dispatchers.

2. React

Nous avons implémenté l'application front-end avec **React**, qui est une bibliothèque de développement des interfaces web basée sur JavaScript et typeScript développée par Facebook et une communauté de développeurs open source l'exécutent. Bien que React soit une bibliothèque plutôt qu'un langage, il est largement utilisé dans le développement Web. La bibliothèque est apparue pour la première fois en Mai 2013 et est maintenant l'une des bibliothèques frontales les plus couramment utilisées pour le développement Web [60].

3. Redux

Redux bibliothèque pour optimiser et rendre l'application plus performante, Redux est une bibliothèque JavaScript open source pour une gestion centralisée des états des composants React et implémenter l'architecture FLUX.

Redux crée par Dan Abramov and Andrew Clark en 2015 [61], cette librairie change complètement la logique et architecture des applications React et facilite l'échange des états entre les différents composants de React , avant l'apparition de Redux, il était difficile de réaliser quelques comportements dans le React comme par exemple le fait de passer des attributs à des compostants qui ne sont pas dans le même arbre. Mais avec la gestion centralisée des états, on peut facilement implémenter ce genre de problèmes.

Redux fournit des middlewares prédéfinis comme Redux-logger qui est un middleware pour journalisation des évènements.

III.6.1.5.2 Présentation de l'application

1) Page d'accueil

Tous les utilisateurs voient cette page qui contient plein d'informations comme (la réponse de quelques questions, formulaire de contact...), basé sur un modelé appelé « FlexStart » qui utilise le Framework Bootstrap .

Figure III.15 : Capture de page d'accueil.

2) Tableau de bord de l'autoritaire

Cette page contient toutes les fonctionnalités dont l'autoritaire a besoin, on a une barre d'outils avec plusieurs options comme le montre la figure ci-dessous :

- **Un panneau de recherche** (1) : l'autoritaire peut personnaliser la table des données.
- **Un bouton** pour rendre quelques colonnes invisibles (2).
- **Un panneau de filtration** (3) : l'autoritaire peut facilement trouver la bande concernée.
- **Un bouton** pour créer une bande fréquence (4).

L'autoritaire a une barre de notifications qui va afficher tous les payements et les demandes des utilisateurs primaires.

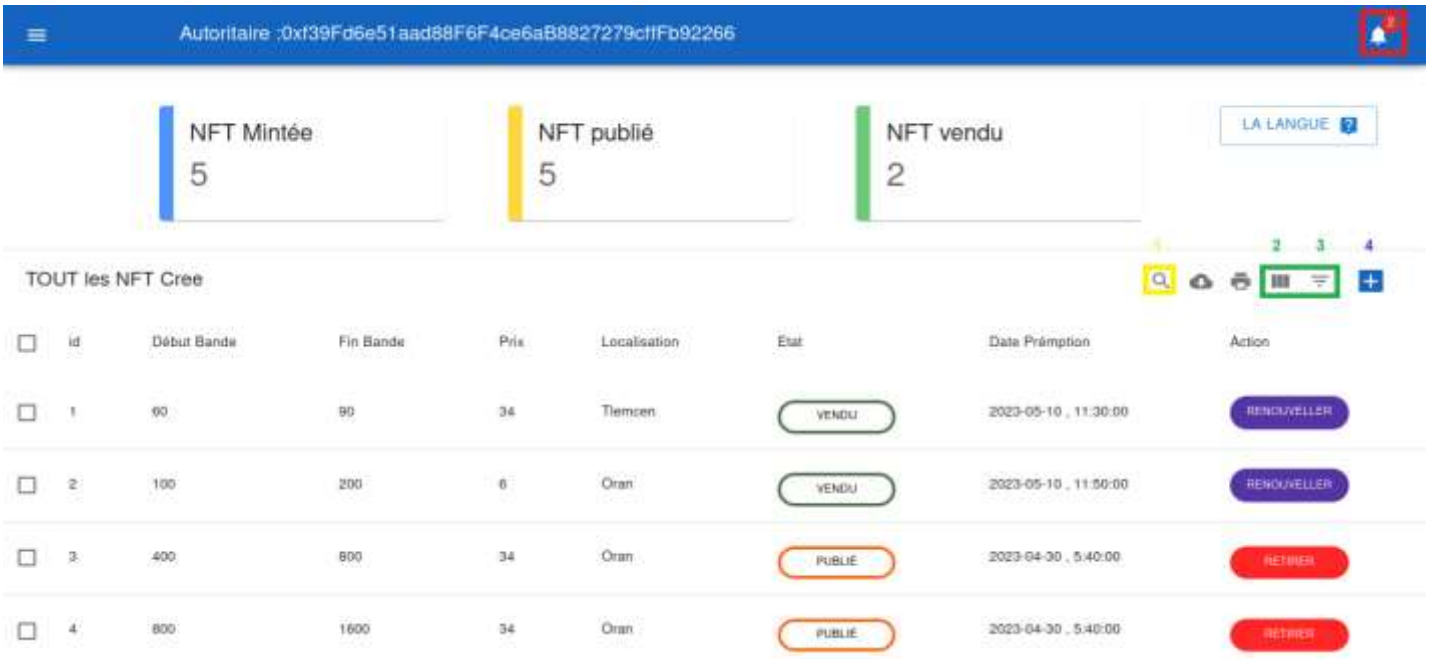

Figure III.16 : page Autoritaire.

3) Tableau de bord de l'utilisateur Primaire

Cette page contient toutes les fonctionnalités dont l'utilisateur primaire a besoin.

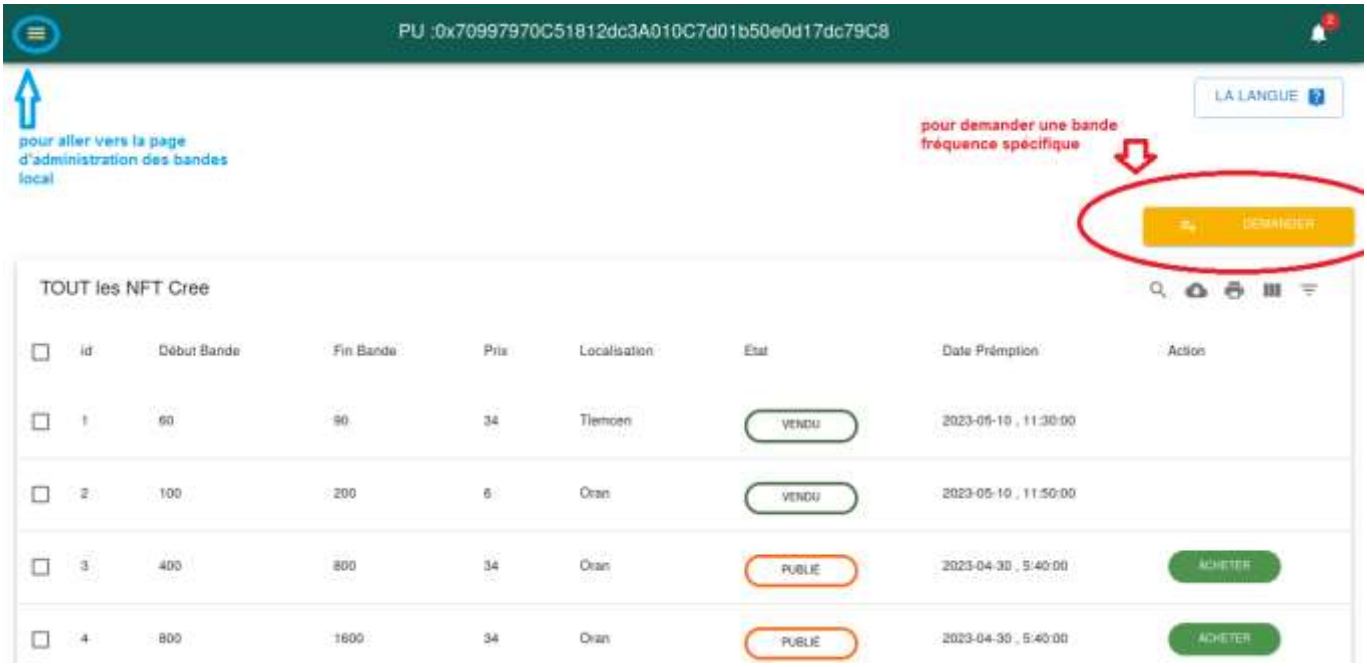

Figure III.17 : page utilisateur primaire.

4) Page d'administration des bandes de fréquence locales du PU

Cette page contient toutes les fonctionnalités dont l'utilisateur primaire a besoin pour créer des bandes de fréquence locales et les publier aux utilisateurs secondaires afin de les utiliser.

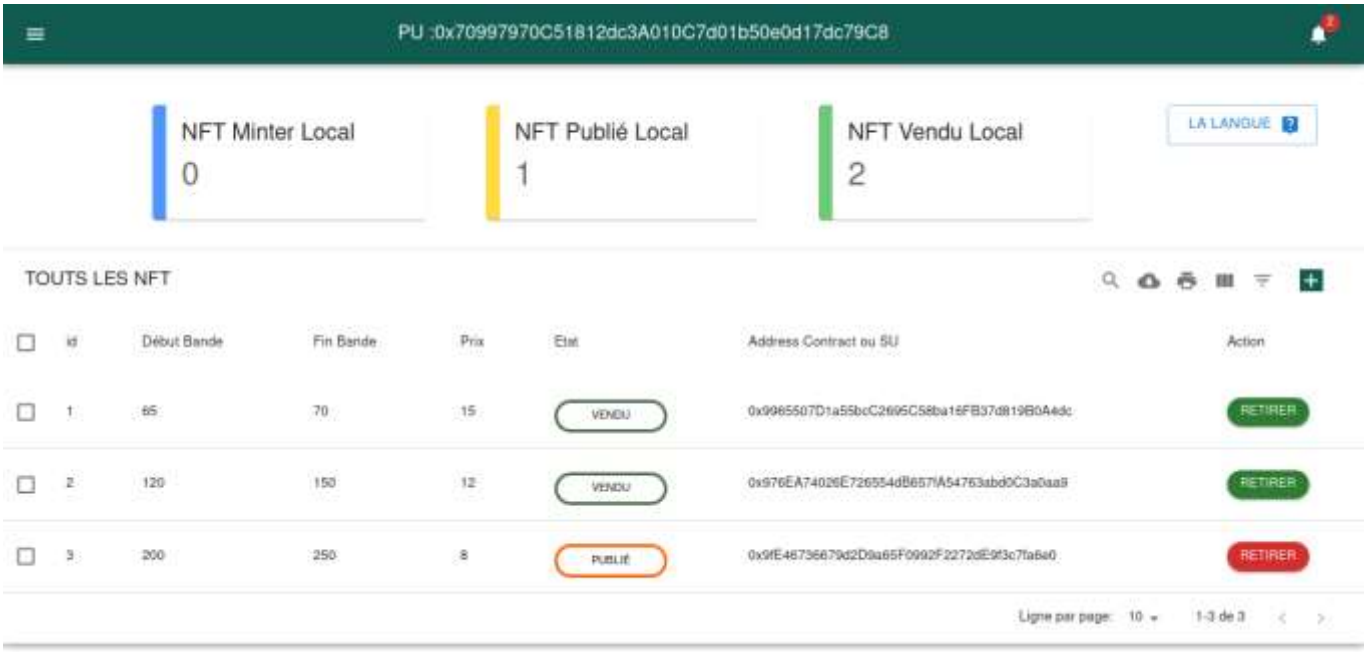

Figure III.18 : page utilisateur primaire (page d'administration BF).

5) Tableau de bord de l'utilisateur secondaire

Dans cette page, l'utilisateur secondaire peut facilement cibler la bande fréquence grâce aux panneaux des filtres et barres de recherche et l'acheter.

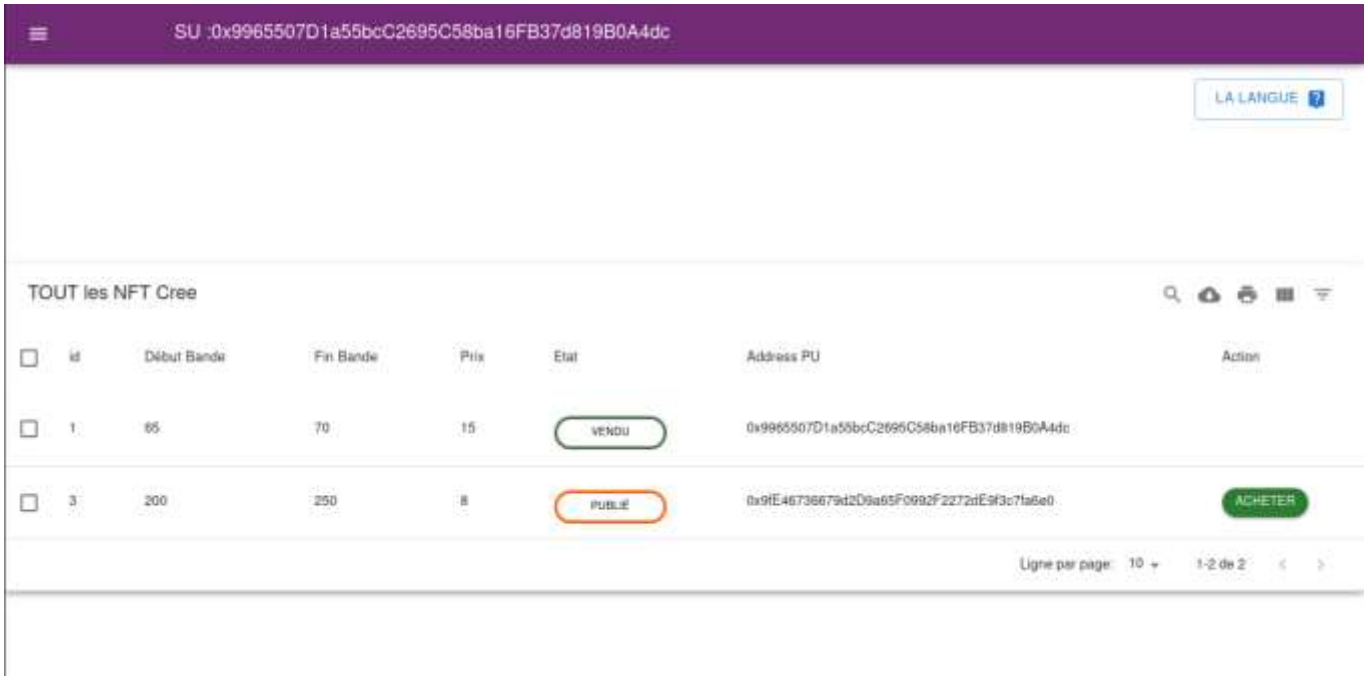

Figure III.19 : page utilisateur secondaire.

i. Back-end (Blockchain)

1. Blockchain

Nous avons implémenté une blockchain Ethereum privée grâce à la bibliothèque « Hardhat » et extension Metamask pour déployer des contrats intelligents sans avoir besoin de la vraie crypto-monnaie, ainsi que pour contrôler les paramètres expérimentaux (comme frais d'essence en anglais « gas fees » et nombre des blocks …).

ii. Hardhat

Hardhat est un environnement de développement pour compiler, déployer, tester et déboguer votre logiciel Ethereum. Il aide les développeurs à gérer et à automatiser les tâches récurrentes inhérentes au processus de création de contrats intelligents et d'application décentralisée, ainsi qu'à introduire facilement plus de fonctionnalités autour de ce flux de travail. Cela signifie compiler, exécuter et tester des contrats intelligents au cœur même.

Hardhat est intégré à un réseau Hardhat, un réseau Ethereum local conçu pour le développement. Sa fonctionnalité se concentre sur le débogage de Solidity, avec des traces de pile, console.log () et des messages d'erreur explicites lorsque les transactions échouent [63].

Hardhat possède des extensions qui sont développées par les développeurs des applications comme « Hardhat-gas-reporter » qui permet de créer des rapports détaillés sur la consumation de gas des opérations effectuées dans la blokchain.

iii. Metamask

MetaMask est une extension de navigateur conçue pour faciliter l'accès à l'écosystème Dapp d'Ethereum. Il sert également de portefeuille pour contenir les jetons ERC-20 permettant aux utilisateurs d'accéder aux services construits sur le réseau via le portefeuille [62].

MetaMask joue un rôle important dans les systèmes Dapp parce que contient des informations comme clé privée de l'utilisateur qui va interroger avec l'application pour les signatures numériques et l'authentification.

iv. Les contacts intelligents

L'implémentation du contrat intelligent a été faite en langage Solidity qui est le langage de programmation pour coder les contrats intelligents sur la blockchain Ethereum. L'une des principales raisons pour lesquelles nous avons choisi la blockchain Ethereum était d'implémenter une solution de preuve de concept. Cette fonctionnalité est la possibilité d'écrire des contrats intelligents contenant des

termes contractuels en utilisant le langage de Solidity. Les contrats intelligents éliminent le besoin d'un tiers de confiance pour coordonner les transactions entre les utilisateurs primaires et secondaires par un morceau de code auto-exécutable codé et déployé dans le réseau blockchain.

Nous avons décidé utilise trois contrat intelligent d'un cote pour minimise la consommation gaz et pour l'autre cote pour sécuriser nous avons base sur un contrat joue le rôle d'une banque pour évite la fraude, la tromperie entre les utilisateurs.

2. Contract PUNFT_Global

Nous avons programmé le contrat intelligent « PUNFT_Global » qui hérite du standard ERC721 (le standard des jetons non fongible (NFT) afin de souligner les comportements d'un jeton numérique. Ce qui suit décrit ces caractéristiques et comportements.

Le jeton sera non fongible et avec une métadonnée suivante :

1. **SBF :** c'est le début de bande de Fréquence.
2. **EBF :** c'est la fin de bande de Fréquence.
3. **Price :** le prix de cette bande.

```
struct metadata {
    uint SBF;
    uint EBF;
    uint   price;
```

Figure III.20 : Structure metadata.

Le contrat va utiliser les structures de type clé, valeur comme (**HashMap** dans java) suivant :

StatusNFT : représenter l'état d'un jeton soit : vendu, expiré, publié.

isRenewal : pour le jeton qui sont déjà renouvelé.

WhoMintNft : utilisé une fois pour garder l'adresse autoritaire.

La Algorithme **purchaseToken()** permettre de teste si Autoritaire est le propriétaire de cette bande de fréquence et test si PU a l'argent pour acheter cette NFT .Ensuite, retirer L'argent de PU est envoyé à l'autoritaire, modifier la propriété de cette NFT de l'autoritaire a PU et afficher la notification de paiement dans l'autoritaire.

Msg.sender => Adresse d'utilisateur qui exécute cette fonction

Msg.value =>la valeur envoyée dans ce ça c'est l'argent de Msg.sender.

Algorithme 1 : Algorithme de paiement

```
1: procedure purchaseToken (uint256 _tokenId)
2:       if (msg.sender == Autoritaireaddress and msg.sender == propriétaire NFT and
msg.sender == addressDeContrat)
3:            Afficher (“Address problem,you’re the owner of this NFT”)
4:     else if (msg.value < prix NFT)
5:           Afficher (“Amount is less then price of this nfts”)
6:     else
7 :         address tokenSeller = le créateur de cette NFT
8 :         Transfère la propriété NFT de propriétaire à la personne qui acheté NFT.
9 :         Modifier le statut de NFT à vendu.
10 :        Envoyé l’argent a le créateur de NFT
11 :        Ajouter cette transaction à le tableau de notification.
12 :        Incrémente le tableau de notification par 1.
13 :   end if
14 :   end if
15: end procedure
```

Figure III.21 : Algorithme purchaseToken.

3. Contrat PUBNFT_PU

Nous avons programmé ce contrat intelligent qui hérite une interface « IERC721Receiver » pour rendre ce contrat Récepteur de notre jeton, et ce contrat et accessible par tous les utilisateurs primaires pour voir quels sont les jetons disponibles que l’autoritaire offre et peut acheter avec la fonction « PurchaseToken ».

4. Contrat PUNFT_ALL_PU

L’utilisateur primaire peut avec ce contrat jouer le rôle de « PUNFT_Global » et PUBNFT_PU en même temps mais seulement pour les jetons locaux générés par les utilisateurs primaires, ce contrat est accessible par les utilisateurs primaires et secondaires parce que les utilisateurs secondaires peuvent voir avec ce contrat quels sont les jetons disponibles pour les utiliser .

b. Résultats obtenus

a) Evaluation de consommation de gaz des contrats

Pour tester la consommation gaz des contrats, on a fait deux tests :

1- **Un contrat pour tous les PU** : il y a trois contrats déployés au lancement d’application (PUNFT_Global pour autoritaire créer les jetons Global, PUBNFT_PU intermédiaire entre PU et autoritaire pour faire les changements d’argent et des jetons, PUBNFT_ALL_PU pour PU créer les jetons de bandes de fréquence locaux et faire les changements d’argent et de jeton avec SU).

2- **Un contrat par PU** : il y a deux contrats déployés au lancement d'application (PUNFT_Global, PUBNFT_PU) et le troisième contrat déployé pour chaque bande de fréquence (jeton) acheté par PU.

Test \ Contrat	PUNFT_Global	PUBNFT_PU	PUBNFT_ALL_PU
TEST 1	0.0174 ETH	0.00913 ETH	0.0197 ETH
TEST 2	0.030 ETH	0.00913 ETH	0.015 ETH * nombre jeton Acheté par PU

Tableau III.1 : Comparaison de consommation gaz des contrats entre deux tests.

A noter sur la figure III.19 que la consommation de gaz de test 1 est mieux que test 2 surtout dans contrat PUNFT_Global, PUBNFT_ALL_PU. Dans la contrat global le test 2 est élevé à cause de stocke les adresses des contrats de chaque NFT acheté par PU pour n'est pas déployé contrat deux fois pour le même NFT, pour la deuxième contrat nous avons déployé ce dernier pour chaque NFT acheté par PU dans test 2 contrairement pour test 1 ont déployé le contrat une seule fois, mais par rapport au PUBNFT_PU la consommation de gaz était la même pour les deux tests.

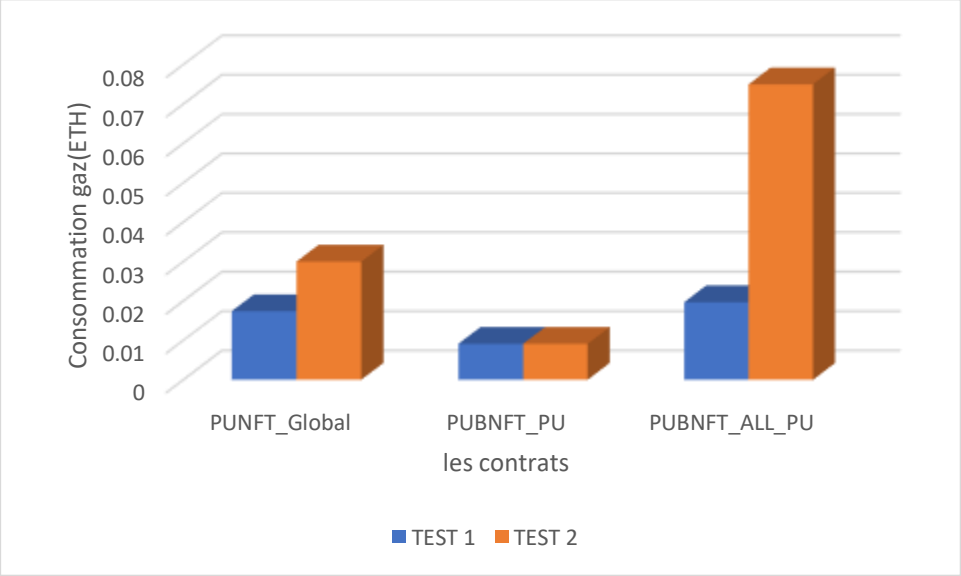

Figure III.22 : Histogramme de comparaison de consommation gaz des contrats entre de test.

b) Consommation de gaz côté Autoritaire

Le tableau suivant représente la consommation de gaz en moyenne de 10 tests de chaque méthode utilisée dans le côté Autoritaire, le résultat obtenu est les tests précèdent sont les mêmes à cause de la même structure utilisé pour stocker dans métadonnées, la même implémentation des méthodes.

La méthode	La consommation de gaz (ETH)
Création de jeton(_mint())	0.00094
Publication de jeton(publieband())	0.00025
Suppression de jeton (BurnNFT())	0.00015
Renouvèlement de jeton (RnewNFT())	0.00036
Réponse aux demandes de PU (setNotifyReponce())	0.00059
Retirer de jeton (RevokeNFTFrom())	0.00022

Tableau III.2 : Consommation gaz des méthodes d'Autoritaire.

c) Consommation de gas côté PU

Le tableau suivant représente la consommation de gaz moyenne de 10 essais pour chaque méthode utilisée côté PU . A noter que la différence entre les deux tests dans la deuxième méthode dans Test 2 est plus importante que dans Test 1, car elle doit tester si le contrat a été déployé avant, si le cas il récupère l'adresse de contrat contrairement aux Test 1 l'adresse est prédéfinit, mais les autres méthodes ayant la même consommation car la même méthode et la même implémentation.

La consommation de gas / La méthode	Test 1 (ETH)	Test 2 (ETH)
Acheté un jeton(purchaseToken())	0.00074	0.00074
Création d'un jeton local(_mint())	0.001	0.00126
Publication d'un jeton local (publieband ())	0.00024	0.00024
Retirer d'un jeton local (recupererband ())	0.00015	0.00015
Demander renouvèlement de jeton	0.0003	0.0003
Demander d'un jeton (setNotifyOautoDelande())	0.00059	0.00059

Tableau III.3 : Consommation gaz des méthodes de PU.

d) Consommation gas côté SU

Le tableau ci-dessous présente la consommation moyenne de gaz de 10 tests pour chaque mode d'achat des NFT locaux. Les deux tests qui apparaissent au début ont le même résultat car ils utilisent la même méthode et la même implémentation.

La méthode	La consommation de gas (ETH)
Acheté un jeton(purchaseToken())	0.00064

Tableau III.4 : Consommation gaz des méthodes de SU.

e) Consommation gas totale

Le tableau suivant représente la consommation de gaz de la création du jeton par Autoritaire jusqu'à son obtention par le SU.

Nombre Foix / TEST	1	5	10	15	20
Test 1	0,049 ETH	0.245 ETH	0,49 ETH	0.73 ETH	0.98 ETH
Test 2	0,058 ETH	0.3 ETH	0.6 ETH	0.9 ETH	1.2 ETH

Tableau III.5 : Comparaison de consommation gaz totale entre deux tests avec modification de nombre de test.

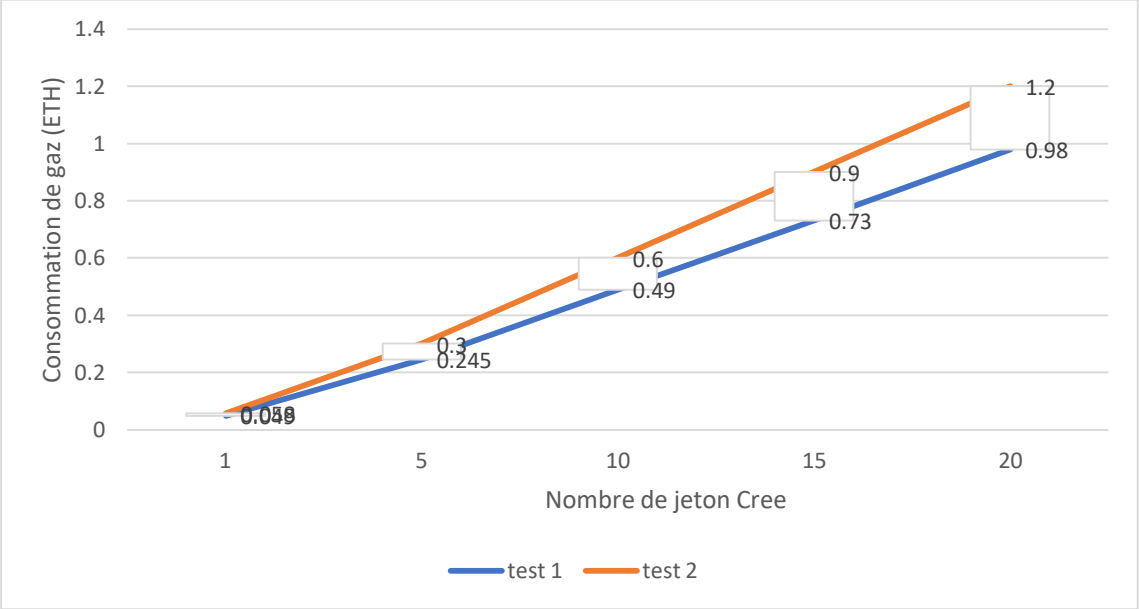

Figure III.23 : Impact du Nombre de jeton crée sur la consommation de gaz totale.

Dans le graphe précédant on remarque que la consommation gaz ont parallèle avec le nombre de jeton crée pour les deux tests, mais le test 2 est plus élevé car il déploie le contrat a chaque sous band fréquence publie.

c. Analyse de Sécurité

Comme nous avons dit dans le premier chapitre, la philosophie « ouverte » du paradigme de la radio cognitive est de rendre le RRC vulnérable à pleins d'attaques comme l'attaque PUE.

Notre application Solidromo prend en considération ce type d'attaques et fournit des solutions efficaces pour les attaques qui touchent la disponibilité des services et authentifications.

i. Solution pour l'attaque Emulation de l'utilisateur Primaire

Après l'analyse de cette attaque , il s'est avéré que dans la radio cognitive aucune méthode ne permet d'identifier ou bien authentifier n'importe quel utilisateur donc dans l'application Solidromo tous les utilisateurs ont deux clés uniques, une Clé public et une Clé privée qui sont stockées dans le portefeuille, toutes les transactions faites dans la blockchain seront signées par la clé privée, et à un moment donnée n'importe quel utilisateur peut consulter les transactions dans la blockchain pour vérifier que cet utilisateur est un utilisateur légitime ou malveillant.

ii. Solution pour l'attaque DDOS

L'Objectif de cette attaque est de rendre les services indisponibles ; dans notre système Solidromo, les services sont des services installés dans la blockchain qui est complètement distribuée et les contrats sont disponibles dans tous les nœuds, et même pour réaliser cette attaque, l'attaquant doit consommer beaucoup de gas, dans notre application Solidromo, on a fixé la consommation de gas par block pout résoudre ce problème.

iii. Solution pour l'attaque Falsification de données de détection de spectre

Cette attaque est liée beaucoup plus à la phase « détections de spectre », la plateforme Solidromo et grâce à la qualité de chiffrement fournit par la blockchain, les données sont stockées dans la blockchain et sont claires pour tout le monde dans le système et même la récupération des données via les contrats intelligents qui ont les droits pour vérifier et refuser les données erronées.

d. Conclusion

Nous avons présenté dans ce chapitre le fonctionnement de notre application et l'utilisation de la blockchain qui s'assure que tous les utilisateurs sont honnêtes par leur clé privée. Ensuite, nous avons proposé l'utilisation de la notion de NFT (ERC721) pour sécuriser la communication entre les PU et SU dans le réseau de radio cognitive.

Nous avons enfin présenté trois interfaces dans cette application pour éliminer un peu le problème de limite de bande de fréquence, la première interface de l'autoritaire pour créer, publier, retirer, supprimer et renouveler des bandes de fréquence. Ensuite la deuxième interface pour les PU pour acheter des bandes de fréquence, demander des bandes de fréquence spéciales et aussi une sous-interface pour créer, publier et retirer des bandes de fréquence locales. Enfin la troisième interface pour les SU dans le but est d'acheter des bandes de fréquence locales.

Conclusion Générale

La radio cognitive est une technologie d'accès sans fil émergente, où l'utilisateur peut détecter intelligemment le canal de communication utilisé ou non utilisé. Chaque utilisateur secondaire a le droit d'utiliser les bandes de fréquence libres qui ne sont pas utilisées par l'utilisateur primaire qui est le propriétaire de cette bande. Les utilisateurs secondaires doivent libérer la bande après avoir terminé ou une fois l'utilisateur primaire la redemande.

Le concept de la radio cognitive est une interaction entre les technologies sans fil et intelligence artificielle, elle joue un rôle particulier dans la liaison entre capacité de détection, d'apprentissage, de raisonnement et de sécurité.

Notre travail est consacré au concept de sécurité dans la radio cognitive, nous avons utilisé la blockchain dans un premier temps pour assurer que tout utilisateur existant dans le réseau est honnête. Ensuite, dans le but de sécuriser l'accès dynamique au spectre, nous avons proposé de protéger les utilisateurs contre l'attaque PUE et nous avons utilisé pour cela les jetons non fongibles NFT (ERC721). Ce dernier fonctionne afin de renforcer la sécurité des communications entre les différents utilisateurs. Le SU doit choisir le PU qui a un NFT obtenu par l'autoritaire afin de vérifier si le jeton est valide ou non, si valide le SU demande l'utilisation de cette bande en envoyant l'argent au PU qui lui-même doit créer un nouveau NFT et le donner au SU. Si le SU termine son utilisation de la bande de fréquence, le jeton doit être supprimé par le PU qui l'a créé.

Ensuite, nous avons développé une application qui va permettre à chaque utilisateur de s'authentifier avant d'accéder pour permettre de sécuriser l'accès dynamique au spectre. Notre application est facilitée d'utilisation, elle permet aux utilisateurs d'acheter des bandes, créer des sous bandes et allouer les sous bandes et aussi sécuriser la communication entre les différents utilisateurs.

Pour conclure, ce travail est instructif pour nous car il nous permet de découvrir une nouvelle technologie innovante, puis nous a permis également de se confronter à plusieurs contraintes à la fois : contraintes de temps, expérience et contraintes techniques.

Ce projet nous a permis de travailler dans deux thématiques : d'un côté les réseaux et la sécurité avec l'utilisation de la RC et la blockchain et d'un autre coté nous avons l'ingénierie logiciel qui nous a permis de développer une application web complète.

Il serait même intéressant de penser à tester cette application web avec plusieurs utilisateurs où chacun a son propre metamask et une machine séparée reliée avec un réseau local ou internet et comparer le passage à l'échelle et le temps de réponse de ce site.

RÉFÉRENCES BIBLIOGRAPHIQUES

[1] AMRAOUI, Asma, BENMAMMAR, Badr, KRIEF, Francine, *et al.* Intelligent wireless communication system using cognitive radio. *International Journal of Distributed and Parallel Systems*, 2012, vol. 3, no 2.

[2] MITOLA, Joseph et MAGUIRE, Gerald Q. Cognitive radio: making software radios more personal. *IEEE personal communications*, 1999, vol. 6, no 4, p. 13-18.

[3] AMRAOUI, Asma. *Vers une architecture Multi-agents pour la Radio Cognitive opportuniste*. 2015. Thèse de doctorat. Université de Tlemcen-Abou Bekr Belkaid.

[4] VISHNEVSKIY, Vladimir M. et KOZYREV, Dmitry V. (ed.). *Distributed Computer and Communication Networks: 21st International Conference, DCCN 2018, Moscow, Russia, September 17–21, 2018, Proceedings*. Springer, 2018.Livre.

[5] BENMAMMAR, Badr et AMRAOUI, Asma. *R'eseaux de radio cognitive*: *Allocation des ressources radio et acces dynamique au spectre. arXiv preprint arXiv:1407.2705*, 2014.

[6] BENMAMMAR, Badr. *Présentation de la radio cognitive*. 2012,Cour En Ligne. Available: https://cel.archives-ouvertes.fr/cel-00680189v1.

[7] BEN DHAOU, Ahmed. *Allocation dynamique des bandes spectrales dans les réseaux sans-fil à radio cognitive*. 2011. Thèse de doctorat. Université du Québec à Montréal.

[8] ELANGOVAN, K. et SUBASHINI, S. Particle bee optimized convolution neural network for managing security using cross-layer design in cognitive radio network. *Journal of Ambient Intelligence and Humanized Computing*, 2018, p. 1-9.

[9] CEPHELI, Özge et KURT, Güneş Karabulut. Physical layer security in cognitive radio networks: A beamforming approach. In : *2013 First International Black Sea Conference on Communications and Networking (BlackSeaCom)*. IEEE, 2013. p. 233-237.

[10] CHEN, Ruiliang et PARK, Jung-Min. Ensuring trustworthy spectrum sensing in cognitive radio networks. In : *2006 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks*. IEEE, 2006. p. 110-119.

[11] CLANCY, T. Charles et GOERGEN, Nathan. Security in cognitive radio networks: Threats and mitigation. In : *2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008)*. IEEE, 2008. p. 1-8.

[12] BHUNIA, Suman, SENGUPTA, Shamik, et VÁZQUEZ-ABAD, Felisa. Cr-honeynet: A learning & decoy based sustenance mechanism against jamming attack in crn. In : *2014 IEEE Military Communications Conference*. IEEE, 2014. p. 1173-1180.

[13] KHASAWNEH, Mahmoud et AGARWAL, Anjali. A survey on security in Cognitive Radio

networks. In : *2014 6th International Conference on Computer Science and Information Technology (CSIT)*. IEEE, 2014. p. 64-70.

[14] BIAN, Kaigui et PARK, Jung-Min. MAC-layer misbehaviors in multi-hop cognitive radio networks. In : *2006 US-Korea Conference on Science, Technology, and Entrepreneurship (UKC2006)*. 2006. p. 228-248.

[15] HLAVACEK, Deanna et CHANG, J. Morris. *A layered approach to cognitive radio network security: A survey*. *Computer Networks*, 2014, vol. 75, p. 414-436.

[16] HERNANDEZ-SERRANO, Juan, LEÓN, Olga, et SORIANO, Miguel. Modeling the lion attack in cognitive radio networks. *EURASIP Journal on Wireless Communications and Networking*, 2011, vol. 2011, p. 1-10.

[17] AKYILDIZ, Ian F., LEE, Won-Yeol, et CHOWDHURY, Kaushik R. CRAHNs: Cognitive radio ad hoc networks.*AD hoc networks*, 2009, vol. 7, no 5, p. 810-836.

[18] IREDALE, G. History of Blockchain Technology: A Detailed Guide. 03 11 2020. [En ligne]. Available: https://101blockchains.com/history-of-blockchain-timeline/. [Accès le 2022 02 16].

[19] MARRAST, Philippe. 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)*.Séminaire IFERISS-IMH | 12 Octobre 2018 | Toulouse.

[20] ZHENG, Zibin, XIE, Shaoan, DAI, Hongning, *et al.* An overview of blockchain technology: Architecture, consensus, and future trends. In : *2017 IEEE international congress on big data (BigData congress)*. Ieee, 2017. p. 557-564.

[21] ZABAT, Anis, *et al. Combinaison de blockchain et biométrie pour la gestion des identités*. 2020. Thèse de doctorat. University of Jijel.

[22] PIGNEL, Marion et STOKKINK, Denis. *LA TECHNOLOGIE BLOCKCHAIN Une opportunité pour l'économie sociale?*. 2018.(Mémoire de Master, 2018).

[23] VILLANI, M. Cédric et LONGUET, M. Gérard. *Les enjeux technologiques des blockchains (chaînes de blocs)*. tech. rep, 2018,Livre.

[24] PLISSON, Claire Fénéron. La blockchain, un bouleversement économique, juridique voire sociétal. *I2D-Information, donnees documents*, 2017, vol. 54, no 3, p. 20-22.Livre.

[25] ADAM, Ibrahim Osman et ALHASSAN, Muftawu Dzang. Bridging the global digital divide through digital inclusion: the role of ICT access and ICT use. *Transforming Government: People, Process and Policy*, 2021, vol. 15, no 4, p. 580-596.

[26] Ripple, *RippleNet*, 2013. [En ligne]. Available: https://ripple.com/. [Accès le 2022 02 16].

[27] MOHAMMED, Alaa Hamid, ABDULATEEF, Alaa Amjed, et ABDULATEEF, Ihsan Amjad.

Hyperledger, ethereum and blockchain technology: A short overview. In : *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*. IEEE, 2021. p. 1-6.

[28] DUMAS, Jean-Guillaume et LAFOURCADE, Pascal. 4. Les crypto-monnaies, une réalité virtuelle?. 2020.

[29] K.S.A,Qu'est-ce que la blockchain?,[Enligne]. Available: https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/. [Accès le 18 2 2022].

[30] VUJIČIĆ, Dejan, JAGODIĆ, Dijana, et RANĐIĆ, Siniša. Blockchain technology, bitcoin, and Ethereum: A brief overview. In : *2018 17th international symposium infoteh-jahorina (infoteh)*. IEEE, 2018. p. 1-6.

[31] CHAN, Wren et OLMSTED, Aspen. Ethereum transaction graph analysis. In : *2017 12th international conference for internet technology and secured transactions (ICITST)*. IEEE, 2017. p. 498-500.

[32] KHANNA, Ashish, RANI, Poonam, SHEIKH, Tariq Hussain, *et al.* Blockchain-based security enhancement and spectrum sensing in cognitive radio network. *Wireless Personal Communications*, 2021, p. 1-23.

[33] How blockchain technology could help to manage UK telephone numbers?, 09 10 2018. [En ligne]. Available: https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/blockchain-technology-uk-telephone-numbers. [Accès le 21 02 2022].

[34] EGGERTON, J. FCC's Rosenworcel Talks Up 6G. *Future Publ. Ltd., Bath, UK, Sep*, 2018, [En ligne]. Available: https://www.nexttv.com/news/fccs-rosenworcel-talks-up-6g. [Accès le 21 02 2022].

[35] YRJÖLÄ, Seppo. Analysis of blockchain use cases in the citizens broadband radio service spectrum sharing concept. In : *International Conference on Cognitive Radio Oriented Wireless Networks*. Springer, Cham, 2017. p. 128-139.

[36] BEN-MOSBAH, Azza. *Privacy-preserving spectrum sharing*. 2017. Thèse de doctorat. Institut National des Télécommunications.

[37] WEISS, Martin BH, WERBACH, Kevin, SICKER, Douglas C., *et al.* On the application of blockchains to spectrum management. *IEEE Transactions on Cognitive Communications and Networking*, 2019, vol. 5, no 2, p. 193-205.

[38] BAYHAN, Suzan, ZUBOW, Anatolij, et WOLISZ, Adam. Spass: Spectrum sensing as a service via smart contracts. In : *2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*. IEEE, 2018. p. 1-10.

[39] Sidi Aissa, Ikram & Keddar, Souria. *Proposition D'un Système À Base De Blockchain Pour La Gestion Des Opérations Sur Les Véhicules Au Niveau National*.. 2018. Université Abou Bekr Belkaid - Tlemcen, Mémoire de Master.

[40] JI, Chu et ZHU, Qi. Smart contract-based secure cooperative spectrum sensing algorithm.

International Journal of Distributed Sensor Networks, 2021, vol. 17, no 12.

[41] SAMARATI, P. et DE, S. S. De Capitani di Vimercati. Access control: Policies, models, and mechanisms. *In R. Focardi and R. Gorrieri, editors, Foundations of Security Analysis and Design, LNCS 2171. Springcr-Verlag*, 2001.

[42] FERRAIOLO, David F., SANDHU, Ravi, GAVRILA, Serban, *et al.* Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security (TISSEC)*, 2001, vol. 4, no 3, p. 224-274.

[43] HU, Vincent C., FERRAIOLO, David, KUHN, Rick, *et al.* Guide to attribute based access control (abac) definition and considerations (draft). *NIST special publication*, 2013, vol. 800, no 162, p. 1-54.

[44] FINK, Torsten, KOCH, Manuel, et OANCEA, Cristian. Specification and enforcement of access control in heterogeneous distributed applications. In : *International Conference on Web Services*. Springer, Berlin, Heidelberg, 2003. p. 88-100.

[45] THOMAS, Roshan K. et SANDHU, Ravi S. Task-based authorization controls (TBAC): A family of models for active and enterprise-oriented authorization management. In : *Database security XI*. Springer, Boston, MA, 1998. p. 166-181.

[46] THOMAS, Roshan K. Team-based access control (TMAC) a primitive for applying role-based access controls in collaborative environments. In : *Proceedings of the second ACM workshop on Role-based access control*. 1997. p. 13-19.

[47] A KALAM, Anas Abou El, BAIDA, R. El, BALBIANI, Philippe, *et al.* Organization based access control. In : *Proceedings POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks*. IEEE, 2003. p. 120-131.

[48] CRANE, Stephen, HOMESCU, Andrei, LARSEN, Per, *et al. The Continuing Arms Race: Code-Reuse Attacks and Defenses*. MIT Lincoln Laboratory Lexington United States, 2018.

[49] DENNIS, Jack B. et VAN HORN, Earl C. Programming semantics for multiprogrammed computations. *Communications of the ACM*, 1966, vol. 9, no 3, p. 143-155.

[50] YAVATKAR, Raj, PENDARAKIS, Dimitrios, et GUERIN, Roch. Rfc2753: A framework for policy-based admission control. 2000.

[51] WESTERINEN, Andrea, SCHNIZLEIN, John, STRASSNER, John, *et al. Terminology for policy-based management*. 2001.

[52] DRAMÉ-MAIGNÉ, Sophie. *Blockchain and access control: towards a more secure Internet of Things*. 2019. Thèse de doctorat. Université Paris-Saclay (ComUE).

[53] AZARIA, Asaph, EKBLAW, Ariel, VIEIRA, Thiago, *et al.* Medrec: Using blockchain for medical data access and permission management. In : *2016 2nd international conference on open and big data (OBD)*. IEEE, 2016. p. 25-30.

[54] XIA, Q. I., SIFAH, Emmanuel Boateng, ASAMOAH, Kwame Omono, *et al.* MeDShare: Trust-

less medical data sharing among cloud service providers via blockchain. *IEEE access*, 2017, vol. 5, p. 14757-14767.

[55] CHEN, Lydia Y. et REISER, Hans. *Distributed Applications and Interoperable Systems*. Springer International Publishing, 2017,Livre.

[56] OUADDAH, Aafaf, ABOU ELKALAM, Anas, et AIT OUAHMAN, Abdellah. FairAccess: a new Blockchain-based access control framework for the Internet of Things. *Security and communication networks*, 2016, vol. 9, no 18, p. 5943-5964.

[57] CRUZ, Jason Paul, KAJI, Yuichi, et YANAI, Naoto. RBAC-SC: Role-based access control using smart contract. *Ieee Access*, 2018, vol. 6, p. 12240-12251.

[58] GUO, Hao, MEAMARI, Ehsan, et SHEN, Chien-Chung. Multi-authority attribute-based access control with smart contract. In : *Proceedings of the 2019 international conference on blockchain technology*. 2019. p. 6-11.

[59] Why did we build Visual Studio Code? , 3 5 2022. [En ligne]. Available: https://code.visualstudio.com/docs/editor/whyvscode.

[60] C. Deshpande, The Best Guide to Know What Is React , 30 1 2022. [En ligne]. Available: https://www.simplilearn.com/tutorials/reactjs-tutorial/what-is-reactjs. [Accès le 3 5 2022].

[61] D. A. a. A. Clark, «The History of React and Flux with Dan Abramov,» 06 11 2015. [En ligne]. Available: https://threedevsandamaybe.com/the-history-of-react-and-flux-with-dan-abramov/. [Accès le 3 5 2022].

[62] D. P. a. M. Hussey, What is MetaMask? How to Use the Top Ethereum Wallet, 3 5 2022. [En ligne]. Available: https://decrypt.co/resources/metamask. [Accès le 20 5 2022].

[63] V. Tran, «Ethereum development environment for professionals,» [En ligne]. Available: https://hardhat.org/getting-started. [Accès le 20 5 2022].

Resumé

La radio cognitive est une technologie pour résoudre le problème de la rareté du spectre causée par l'évolution et la multiplication des systèmes de communication sans fil. Dans notre travail, nous nous intéressons à la sécurisation des réseaux radio cognitive contre les attaques PUE (Primary User Emulation). Pour cela, nous avons utilisé la technologie de Blockchain pour assurer que tous les utilisateurs sont honnêtes et la notion de jeton non fongible (ERC721) pour sécuriser la communication entre les utilisateurs.

Mots-clés : Radio cognitive – Blockchain – Sécurité – jeton non fongible – Attaque PUE.

Abstract

Cognitive radio is a technology to solve the problem of spectrum scarcity due to the evolution and multiplication of wireless communication systems. In our work, we focus on securing cognitive radio networks against PUE (Primary User Emulation) attacks. For this purpose, we assign the Blockchain technology to ensure that all users are honest and the notion of non-fungible token (ERC721) to secure the communication between users.

Keywords: Cognitive radio - Blockchain - Security - non-fungible token – PUE attacks.

ملخص

الراديو المعرفي (الإدراكي) هو تقنية لحل مشكلة ندرة الطيف بسبب تطور وتكاثر أنظمة الاتصالات اللاسلكية. في هذه المذكرة نحن مهتمون بتأمين شبكة الراديو الإدراكي ضد هجوم محاكاة المستخدم الأساسي. لهذا قمنا بإدراج تقنية قاعدة البيانات الموزعة للتأكد من أن جميع المستخدمين أصليين وأضفنا أيضاً مفهوم الرمز غير القابل للاستبدال من أجل تأمين الاتصال بين المستخدمين.

الكلمات المفتاحية: الراديو المعرفي - قاعدة البيانات الموزعة – التأمين - الرمز غير القابل للاستبدال - محاكاة المستخدم الأساسي.