


République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Akli Mohand Oulhadj de Bouira

Faculté des Sciences et des Sciences Appliquées

Département d'Informatique

Mémoire de Master

en Informatique

Spécialité : *ISIL et GSI*

Théme

Applications de la technologie blockchain

Encadré par

— Mme Z. MAHFOUD

Réalisé par

— Mlle Sabrina DELLYS

— Mlle Sofia BENBOUABDELLAH

2019/2020

Remerciements

Au début de ce travail, nous remercions dieu de nous avoir accordé le courage, la volanté et la patience pour parvenir à achever ce modeste travail.

Par la suite, nous voudrions exprimer notre profonde gratitude à notre promotrice, Z. MAHFOUD, qui nous a fait l'honneur de diriger ce travail, pour ses conseils et ses orientations.

Sans oublier les membres du jury d'avoir accepté d'examiner et d'évaluer notre travail. Nous remercions également les enseignants qui ont participé à notre progrès pendant ces 5 ans.

Enfin, nous adressons nos remerciement à toutes les personnes qui, de près où de loin, nous ont soutenus tout au long de notre parcours.

Merci

Dédicaces

Je dédie ce modeste travail :

A toute ma famille et mes proches, Notamment mes parents, qui m'ont Comblé de leur soutien et m'ont voué un amour inconditionnel,

A mes sœurs :Taous, Ouerdia, Samira

A mon frère : L'hacen

A toutes les personnes qui ont attendu l'achèvement de ce mémoire et qui ont prié dieu pour plus de réussite.

Sabrina.

Dédicaces

Je dédie ce modeste travail :

A toute ma famille et mes proches, Notamment mes parents, qui m'ont Comblé de leur soutien et m'ont voué un amour inconditionnel,

A ma sœur :Melissa

A mon frère : Hakim

A mes amis : Amine ,kahina

A toutes les personnes qui ont attendu l'achèvement de ce mémoire et qui ont prié dieu pour plus de réussite.

Sofia.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

DDoS	Distributed Denial Of Service attack
SARS-CoV-2	Syndrome respiratoire aigu sévère-Coronavirus de la même famille que SARS-CoV
OMS	Organisation Mondial de la Santé
API	Application Programming Interface
IA	Intelligence Artificielle
UML	Unified Modeling Language
UP	Unified Process
P2P	Peer To Peer
BTC	Bitcoin
ETH	Ethereum
DAO	Organisations Autonomes Democratiques
EVM	Machine Virtuelle Ethereum
PHP	Hypertext Preprocessor
HTML	Hyper Text Markup Language
PIN	Personal Identification Number
QR	Quick Reponce

Introduction générale

L'application de technologie de blockchain a apparu en novembre 2008 avec la publication de la première monnaie électronique Bitcoin. Cette technologie de registre distribué aide à rendre plus sûres et plus transparents les données et permet aux internautes de réaliser des transactions sécurisées de pair à pair et de se passer de tiers de confiance pour garantir l'intégrité de ces transactions.

Actuellement , la blockchain ne cessent pas d'attirer l'attention à différents niveaux (gouvernements, entreprises, etc.) son exploitation dans divers applications en dehors de son domaine classique de la monnaie électronique.

Dans notre projet de fin d'étude, nous cherchons à explorer la technologie de blockchain en réalisant un état de l'art sur le thème et en présentant un exemple réel son utilisation.

Dans ce contexte, nous avons développé une application de vote en ligne qui est un exemple classique d'utilisation des blockchains en dehors de monnaies électroniques. Nous avons aussi proposé une solution qui concerne la pandémie Covid-19, l'objective est de permettre aux étudiants universitaires de suivre des études en présentiel et en évitant d'être contaminé ou de propager le virus.

Le mémoire est organisé de la façon suivant : le premier chapitre présente en détaille les concepts fondamentaux de la technologie blockchain.Le deuxième chapitre aborde quelques plateformes de développement et applications de la blockchain. Le troisième chapitre est dédié à la présentation de système de vote en ligne. Le quatrième chapitre est destiné à la modélisation du système de vote en ligne. Le cinquième chapitre introduit la phase de réalisation du système de vote en ligne en spécifiant les outils, les langages

et l'environnement de développement.Le sixième chapitre est dédié à la présentation de la nouvelle pandémie "Covid-19". le septième chapitre est destiné à la modélisation du système de Covid-19. Le mémoire est clôturé par une conclusion générale.

Chapitre 1

Concept de base de la technologie blockchain

1.1 Introduction

En 2020 pas une semaine ne s'écoule sans que l'on entende parler de la blockchain dans les medias ! Il est vrai que le mot « blockchain » est sur toutes les lèvres mais pourtant peu de gens comprennent vraiment l'enjeu de cette technologie et comment elle peut être utilisée pour effectuer des transactions financières, transférer des informations de manière fiable, vérifiée et sécurisée [1].

1.2 Définition

Nous présentons ci-dessous quelques définitions qui permettent de mieux comprendre ce qu'est la blockchain selon plusieurs points de vue [2] :

Simpliste : la blockchain est considérée comme un grand livre de compte ouvert et accessible à tous en écriture et en lecture et qui est partagé sur un grand nombre d'ordinateurs.

Basique : la blockchain s'agit d'un logiciel qui stocke et transfère des données via internet, de façon transparente et sécurisée, et sans organe central de contrôle.

Littéral : une blockchain désigne une chaine de blocs dans lesquels sont stockés les informations de toute nature.

Généraliste : une blockchain est une technologie qui permet d'effectuer des transactions, grâce à un mécanisme de consensus collectif couplé avec l'utilisation d'un grand livre de compte public, décentralisé et partagé, établit la confiance, la responsabilité et la transparence tout en rationalisant les processus d'affaires..

Technique : une blockchain est une nouvelle technologie de base de données. Cette base de données transactionnelle distribuée est comparable à un registre dans lequel chaque nouvelle transaction est écrite à la suite des autres, sans avoir la possibilité de la modification ou la suppression. Ce registre est actif, chronologique, distribué, vérifiable et protégé contre la falsification par un système de confiance répartie entre les membres ou participants (nœuds).

Pour résumer : la blockchain est une base de données transactionnelle distribuée, elle permet de stockager et transmettre les informations via Internet, de façon transparente, sécurisée et autonome, tout cela sans organe central de contrôle [2].

1.3 Les origines de blockchain

En 1991, les chercheurs Stuart Haber et W. Scott Stornetta ont proposé une solution calculable pour horodater les documents numériques afin qu'ils ne soient pas manipulables. C'etait ça L'idée de la technologie blockchain.Leur système a utilisé une blockchain cryptée et sécurisée pour stocker les documents horodatés ,après en 1992, le protocole "arbres Merkle" a pu rendre le système plus efficace , en rassemblant plusieurs documents dans un bloc Cependant, cette technologie n'a pas été utilisée et le brevet a expiré en 2004 [3].

Fin 2008, un livre blanc sur l'introduction d'un système de paiement électronique peer-to-peer décentralisé appelé Bitcoin a été envoyé à une liste de diffusion cryptographique par une personne ou un groupe sous le pseudonyme Satoshi Nakamoto [3].

Bitcoin a été créé le 3 janvier 2009 après que le premier bloc de Bitcoin a été extrait par Satoshi Nakamoto et contenait une récompense de 50 Bitcoins. Le premier destinataire de Bitcoin était Hal Finney. Il a reçu 10 bitcoins de Satoshi Nakamoto lors de la première transaction bitcoin au monde le 12 janvier 2009 [3].

En 2013, Vitalik Buterin, programmeur et co-fondateur de Bitcoin Magazine, a déclaré que Bitcoin avait besoin d'un langage de script pour développer des applications décentralisées. Puisque Vitalik n'a pas pu parvenir à un accord dans la communauté, il a commencé à développer une nouvelle plate-forme informatique distribuée basée sur la blockchain, ethereum, qui avait une fonctionnalité de script appelée contrats intelligents [3].

1.4 Grands principes de la blockchain

Les principes sur lesquels est fondée la blockchain sont les suivants [2] :

- La blockchain est une base de données, qui est répartie entre tous les nœuds ;
- La décentralisation et la désintermédiation : il n'existe aucune autorité central pour contrôler la blockchain donc il n'y a pas de tiers de confiance ;
- Le consensus : le fruit d'un consensus distribué c'est d'effectuer une transaction ;
- L'immutabilité : Une fois qu'une transaction est enregistrée sur la blockchain et que la blockchain a été mise à jour, cette transaction ne peut pas être modifiée ;
- La confiance partagée et la transparence : la blockchain assure la sécurité et la transparence des données.

Les blockchains les plus connues et utilisées dans le monde sont : Bitcoin et Ethereum, mais la blockchain ne se limite pas à celles-ci car il existe d'autres types [2].

La technologie blockchain change les règles du jeu : moins de centralisation, moins d'autorité et plus de partage[2].

1.5 Types de blockchain

Il existe 3 types de blockchain [4] :

Les blockchains publiques : Les blockchains accessibles au public sont appelées blockchain publique. Ces blockchains n'ont aucune restriction sur le participatif et le validateur. Le principal avantage de ce type de blockchain est le caractère incontrôlable de la blockchain ce qui signifie que personne n'aura un contrôle total sur le réseau. Par conséquent, il garantit que les données sont sécurisées et contribue à l'immuabilité des

enregistrements. Tous les nœuds connectés à cette blockchain publique auront une autorité égale et, par conséquent, cette blockchain publique sera entièrement distribuée.

Les blockchains privées : Ces blockchain nécessitent que les participants soient invités avant de pouvoir faire partie de la blockchain. Ici, toutes les transactions ne sont visibles que par les personnes qui font partie de l'écosystème blockchain. Ces types de blockchains sont centralisés et bien mieux contrôlés que les blockchains publiques. Les blockchains privées ont généralement un administrateur réseau qui peut s'occuper des autorisations des utilisateurs au cas où un utilisateur particulier aurait besoin d'une autorité supplémentaire en déplacement. Ceux-ci sont généralement utilisés dans les organisations privées pour stocker des informations sensibles sur l'organisation.

Les consortiums : Ces blockchains sont divisées en deux types différents, où certains nœuds sont privés, tandis que les autres nœuds sont publics. En conséquence, certains des nœuds seront autorisés à participer aux transactions. Les autres nœuds contrôle le processus de consensus. blockchain hybride permet à tous les nœuds d' accéder à la blockchain, tandis que le niveau d'informations auquel il est possible d'accéder sera basé sur le nœud accédant à ces données particulières. Dans cette blockchain, il existe généralement deux types d'utilisateurs. L'un est l'utilisateur qui a tous les contrôles sur la blockchain et décide du niveau de sécurité pour un utilisateur particulier, tandis que les autres sont ceux qui accèdent simplement à la blockchain.

1.6 Acteurs de blockchain

Une blockchain est une infrastructure réseau où la conception, le développement, le déploiement, la gestion et le support centrés sur le réseau s'appliquent. Il est donc essentiel de comprendre les différents acteurs et leurs rôles qui interagissent avec le réseau blockchain[5, 6, 7] :

Un architecte blockchain : est la personne ou le groupe qui a conçu la blockchain. Pour qu'une solution blockchain soit fonctionnelle, elle doit d'abord exister.

Les opérateurs de la chaîne de blocs : Ils se soucient principalement de la sécurité du réseau blockchain et ne se soucient pas des contrats intelligents et des codes d'interface

utilisateur.Leurs roles est de définir le réseau d'entreprise, contrôler l'accès et surveiller le réseau d'entreprise.

Le développeur blockchain : Les développeurs peuvent implémenter des applications qui accèdent à la blockchain et créer des contrats intelligents à exécuter sur la blockchain.

Le régulateur blockchain : Le régulateur s'intéresse à la manière dont les données doivent être stockées et traitées.

L'utilisateur final : C'est le consommateur des services construits autour de la blockchain.

Le stockage de données : La blockchain fournit un stockage distribué immuable avec un contrôle d'intégrité intégré. Pour permettre la vérification de l'intégrité de grandes quantités de données, il est courant de stocker les données hors chaîne et de stocker un hachage des données en chaîne. Cela garantit que les données ne sont pas modifiées tout en protégeant la blockchain contre le gonflement.

Le traitement des données : Il s'agit d'un système externe utilisé pour un traitement supplémentaire. Lorsque les contrats intelligents s'exécutent sur la blockchain, ce la signifie que chaque membre du réseau homologue doit exécuter le code pour rester synchronisé avec l'état actuel du réseau.

1.7 Écosystème blockchain

L'écosystème de blockchain (Figure 1.1) comporte plusieurs couches [8] :

Les blockchains

Les blockchains ressemblent à des livres de comptes qui enregistrent les utilisateurs et les transactions d'un service donné : par exemple, les détails des transactions de la monnaie Bitcoin sont enregistrés sur la blockchain Bitcoin.

La couche technologique

Ces entreprises permettent de traiter les informations contenues dans une blockchain pour les rendre actionnables par des services tiers.

Blockchain-as-a-Service

Il s'agit d'applications utilisées directement par l'utilisateur final.

Les utilisateurs

Il s'agit des associations, acteurs privés, Les structures étatiques et même des particuliers qui bénéficient de services blockchain.

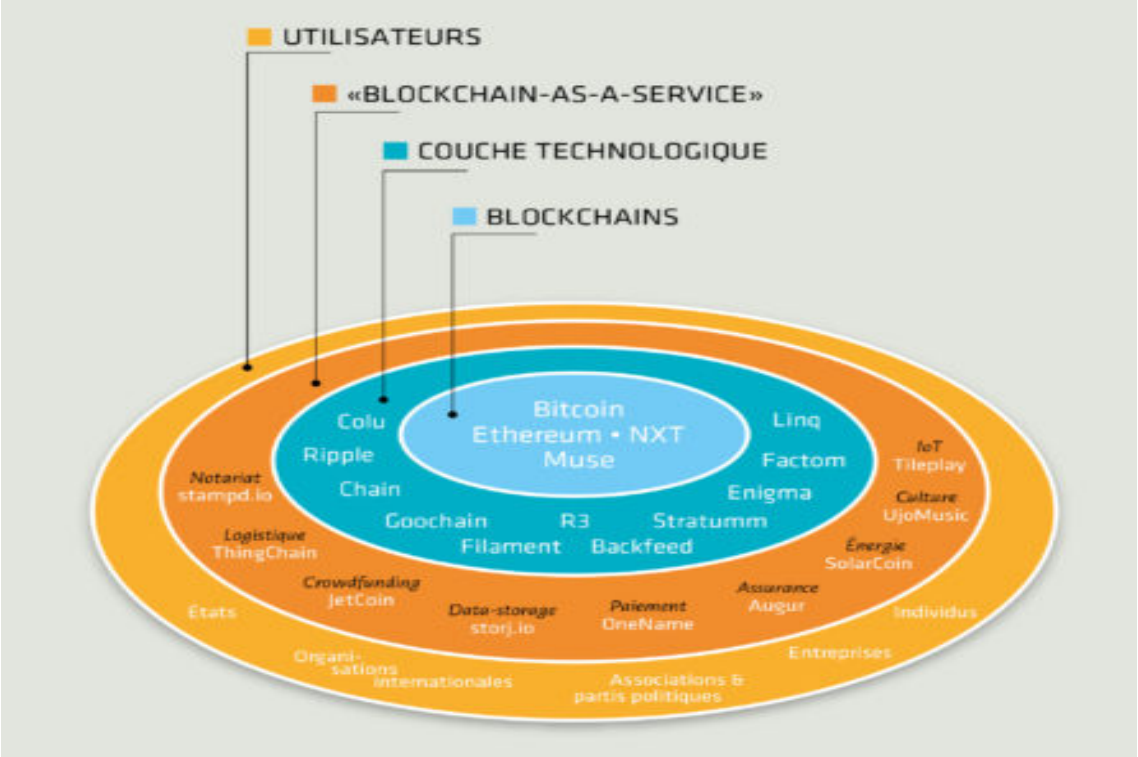

FIGURE 1.1 – Écosystème de blockchain.

1.8 Fonctionnement du blockchain bitcoin

La transparence de ce système repose sur le fait que tous les échanges effectués entre les utilisateurs depuis la création de la chaîne y sont inscrits [9].

Au moment que les utilisateurs de réseau effectuent des transactions, ces transactions seront regroupées en bloc, Chaque bloc est validé par les nœuds du réseau ou "mineurs" selon des techniques qui dépendent du type de blockchain[9].

Les "mineurs" sont des particuliers qui permettent de vérifier la validité des transactions bloc par bloc. Ils sont rémunérés pour mettre à disposition la puissance de calcul de leurs processeurs [9].

Le fonctionnement d'une transaction peut schématiquement être décrit en 5 étapes [9] :

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

La Figure 1.2 permet de visualiser le fonctionnement de la blockchain [10].

Au niveau de l'étape 3 du schéma, on a besoin de puissance de calcul afin de vérifier si le bloc est valide ou non. Pour cela, on utilise la puissance des ordinateurs connectés sur le réseau afin de valider les transactions contenues dans le bloc. Ensuite, on ajoute ce bloc à la base de données publique déjà existante. À ce moment se pose la question de comment être sûr qu'il ne s'agit pas d'une transaction frauduleuse ? Pour pallier à ce problème, on utilise un système de « Preuve de travail » aussi appelé « Proof of work », qui réside dans le principe de la résolution d'un problème mathématique reposant sur un principe de cryptographie. La première machine à obtenir la solution à ce problème, propose son bloc au réseau afin de le vérifier et de valider le bloc. Si une majorité de gens approuve ce bloc, il est alors ajouté à la blockchain. Si ce n'est pas le cas, le block est alors rejeté [10].

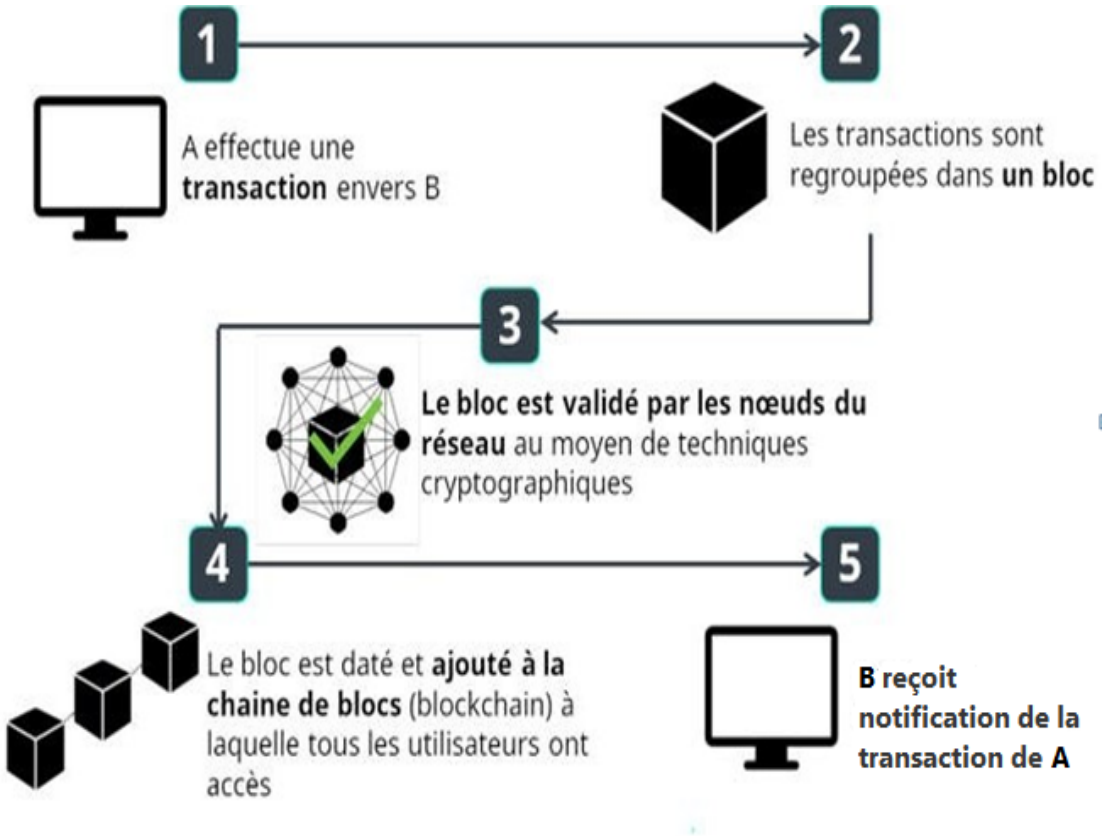

FIGURE 1.2 – Fonctionnement du la blockchain.

1.9 Système blockchain

Tout appareil connecté à la blockchain peut être classé comme un nœud et les exemples incluent : les serveurs, les ordinateurs, les ordinateurs portables, les téléphones mobiles...ect. Lorsqu'un nœud se connecte au réseau pour la première fois, il télécharge une copie complète de la base de données blockchain(Figure 1.3 [11]) sur son ordinateur ou son serveur[8].

Le réseau de nœuds permet de gérer la base de données blockchain. Les nœuds sont considérés comme des entrées pour de nouvelles données, ainsi que la validation et la propagation de nouvelles données qui ont été soumises à la blockchain[8].

Dans un système de blockchain, il existe des règles (protocole) pré convenues pour la validité technique et commerciale des données à écrire, et des règles pour déterminer comment un consensus est atteint [8].

Lorsque le bloc est validé il sera après ajouté d'une manière qui ressemble à une chaîne, d'où le nom blockchain. Les nœuds stockent ensuite ces nouveaux blocs sur la base de

données blockchain locale sur leur ordinateur ou serveur [8].

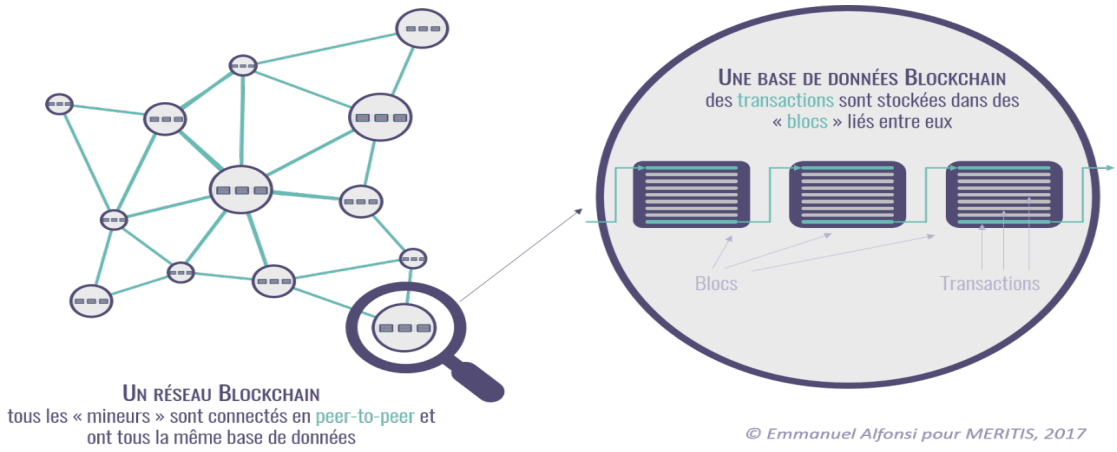

FIGURE 1.3 – Base de données blockchain.

1.10 Composition d'une blockchain

La blockchain est une chaîne de blocs (Figure 1.4) et chaque bloc contient les éléments suivants [12] :

— Un index.

— Un hash servant à identifier le bloc.

— Le hash du bloc précédent.

— Un timestamp.

— Un ensemble de transactions.

Le premier bloc d'une blockchain est appelé le "Genesis Block" [12].

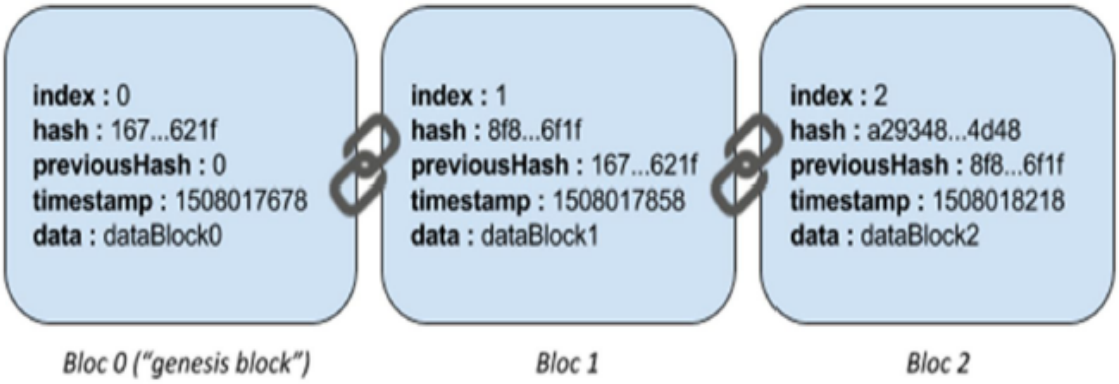

FIGURE 1.4 – Composante de bloc.

1.11 Smart contracts

Les smart contracts permettent de cartographier la logique contractuelle à l'aide d'algorithmes informatiques . Ce sont des contrats programmables qui sont définis par le code du programme et peuvent ensuite être automatiquement exécutés et appliqués sur les blockchains. À certains moments, les smart contracts vérifient automatiquement les conditions préalablement définies. Ainsi, vous déterminez automatiquement si, par exemple, une transaction est effectuée ou annulée [13].

Les smart contracts permettent d'appliquer directement les contrats. L'objectif est de réduire les coûts de transaction et d'augmenter la sécurité des contrats. Seul le code programmé d' un smart contract a un effet contractuel. Les smart contracts représentent une règle de contrôle ou de gestion dans le protocole technique. Par exemple, dans une voiture louée par un smart contract, le moteur ne peut démarrer que lorsque le paiement du leasing a été reçu. Une requête de la blockchain suffirait pour cela [13].

Les smart contracts garantissent un degré élevé d'indépendance, car les parties impliquées dans un accord n'ont pas à s'appuyer sur un intermédiaire. Cela réduit également les dangers potentiels de manipulation par des tiers, car l'exécution est gérée automatiquement par les mécanismes de la blockchain et non par une ou plusieurs entités qui pourraient commettre des erreurs ou être biaisées. Les smart contracts permettent également d'augmenter la vitesse d'exécution car le code logiciel est utilisé pour automatiser les tâches. De cette manière, les processus métier peuvent être simplifiés, ce qui minimise les erreurs humaines, les interfaces ou les perturbations des supports [13].

1.12 Avantages et inconvénients de la blockchain

La blockchain comme toutes autres technologies a des avantages ainsi des inconvénients et c'est ce que nous allons voir dans cette section.

1.12.1 Avantages

Parmi les avantages de blockchain on site [14,15] :

— **Des transactions sans intermédiaire :** La blockchain permet des transactions directes entre les participants sans l'intervention d'un tiers. Ces intermédiaires tels

que les banques ou les notaires ne sont plus nécessaires.

— **Stabilité :** Les blocs confirmés sont très difficiles à annuler, donc une fois les données enregistrées sur la blockchain, il est extrêmement difficile de les supprimer ou de les modifier. Cela fait de la blockchain une excellente technologie pour stocker des enregistrements financiers ou d'autres données nécessitant une piste d'audit, car chaque changement est suivi et enregistré en permanence dans un grand livre distribué et public.

— **La sécurité :** Comme cette technologie dispose de divers mécanismes de vérification des données, l'altération des informations contenues dans les blockchains devient pratiquement impossible. Pour commencer, chaque fois que vous souhaitez modifier des données dans un bloc, vous devez modifier tous les blocs de cette chaîne .

1.12.2 Inconvénients

Parmi les inconvénients du blockchain on trouve [15,16] :

— **Difficulté de mise en œuvre :** La blockchain étant quelque chose de révolutionnaire, l'un de ses inconvénients est sa difficulté à mettre en œuvre . Comme il s'agit d'une technologie disruptive, il faut du temps pour établir tous les protocoles essentiels à son bon fonctionnement . Les entreprises peuvent donc mettre des années à adopter et à fonctionner uniquement avec ce système.

— **Chômage :** Comme cette technologie vise à éliminer l'intermédiaire dans les transactions , l'une des conséquences possibles sera la perte définitive de celui-ci. Autrement dit, si cette technologie se développe et si elle doit être de plus en plus mise en œuvre, il n'y aura pas besoin d'intermédiaire. Et cela peut signifier son éradication totale (ou presque).

— **Anonymat :** Nous allons utiliser l'exemple des crypto-monnaies . Comme il s'agit d'un réseau ouvert, lorsqu'un utilisateur effectue une transaction, l'autre personne pourra voir le journal de ses activités. Imaginez faire un transfert à un parent. Cela peut voir toutes les données liées à vos crypto-monnaies. C'est à dire tout. De votre montant actuel, en passant par le montant que vous avez déjà dépensé et même la façon dont vous le dépensez. Et pas seulement les transactions passées, mais aussi les futures. Donc, si beaucoup de gens ne montrent leur relevé bancaire à personne

, pourquoi le feraient-ils avec cette technologie ?

— **Espace de rangement :** Les registres blockchain peuvent devenir très volumineux avec le temps. La blockchain Bitcoin nécessite actuellement environ 200 Go d'espace de stockage. La croissance actuelle de la taille de la blockchain semble dépasser celle des disques durs, et le réseau risque de perdre des nœuds si le grand livre devient trop volumineux pour être téléchargé et stocké par des particuliers.

— **Clés privées :** Blockchain utilise la cryptographie à clé publique (ou cryptographie asymétrique) pour donner aux utilisateurs le contrôle de leurs unités de crypto-monnaie (ou de toute autre donnée de la blockchain). Chaque compte (ou adresse) blockchain a deux clés correspondantes : une clé publique (qui peut être partagée) et une clé privée (qui doit rester secrète). Les utilisateurs ont besoin de leur clé privée pour accéder à leur argent, ce qui signifie qu'ils agissent comme leur propre banque. Si un utilisateur perd sa clé privée, l'argent est effectivement perdu et il ne peut rien y faire.

1.13 Risques et menaces

Attaque 51% : est une attaque potentielle contre Bitcoin (ou tout autre réseau blockchain) dans laquelle une seule entité ou organisation est capable de contrôler la majeure partie du taux de hachage, ce qui peut potentiellement entraîner une perturbation du réseau. En d'autres termes, l'attaquant à 51% disposerait d'une puissance minière suffisante pour exclure délibérément des transactions ou modifier leur ordre [17].

Les attaques "Man-in-the-middle-attack" : l'attaquant crée deux clés secrètes. Ensuite, il utilise la première clé pour démarrer la communication avec le premier côté. La réponse reçue de premier côté sera décryptée facilement par l'intrus, car il connaît la clé. L'intrus crypte à nouveau le message, cette fois avec la deuxième touche. Le message chiffré est ensuite renvoyé au deuxième côté. Puis, après avoir reçu la réponse du deuxième côté, il déchiffre le message, le lit, il le crypte par la première clé et renvoie au premier côté. De cette façon, toute la communication passe par l'attaquant. Il peut recevoir beaucoup d'informations sur l'ensemble du système et même réussir à usurper l'identité de personnes autorisées et accéder à l'accès aux données cachées [18].

La figure 1.5 ci-dessus montre le schéma général de l'attaque Man-in-the-middle-attack

[19] :

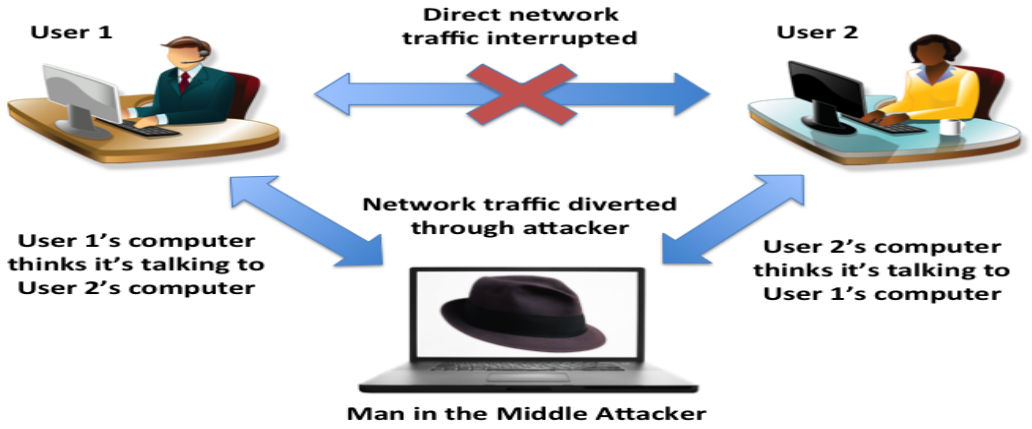

FIGURE 1.5 – Schéma de l'attaque Man-in-the-middle-attack.

Les attaques "SYN-Flood" : sont des attaques de protocol, L'attaquant envoie un flot de paquets de données malveillants vers un système cible. L'intention est de surcharger la cible et de la priver ainsi d'une utilisation légitime [18].

L'attaques "Sybil" : : est une tentative de manipuler un réseau P2P en créant plusieurs fausses identités. Pour l'observateur, ces différentes identités ressemblent à des utilisateurs réguliers, mais dans les coulisses, une seule entité contrôle toutes ces fausses entités à la fois. Ce type d'attaque est important à prendre en compte en particulier lorsque vous pensez au vote en ligne. Un autre domaine dans lequel nous assistons aux attaques Sybil est celui des réseaux sociaux où les faux comptes peuvent influencer le débat public [18].

Une autre utilisation possible des attaques Sybil est de censurer certains participants. Un certain nombre de nœuds Sybil peuvent entourer votre nœud et l'empêcher de se connecter à d'autres nœuds honnêtes sur le réseau. De cette façon, on pourrait essayer de vous empêcher d'envoyer ou de recevoir des informations sur le réseau [18].

Les attaques "Éclipse" : sont un moyen d'attaquer un réseau décentralisé à travers lequel un attaquant cherche à isoler et à attaquer un ou plusieurs utilisateurs spécifiques, plutôt que d'attaquer l'ensemble du réseau [18].

1.14 Conclusion

Au cours de ce chapitre, nous avons défini en détail la blockchain, ses grands principes, son fonctionnement, son utilité, ainsi que quelques avantages et inconvénients.

Dans le chapitre suivant, nous allons présenter des plateformes et applications de cette technologie.

Chapitre 2

Applications de la technologie blockchain

2.1 Introduction

La blockchain est une technologie qui ne cesse pas de s'agrandir. Elle est aujourd'hui proposée en vue d'améliorer divers secteurs.

Dans ce chapitre, nous allons aborder les domaines d'application de la blockchain ainsi que les plateformes de cette technologie et quelques applications décentralisées.

2.2 Domaines d'application de blockchain

Voici quelques domaines d'application de la technologie blockchain [20, 21, 22, 23, 24, 25] :

Vote : la blockchain promet un vote sécurisé et inviolable dont le résultat, transparent et fiable, est auditable par tous , même si les résultats de votes sont publiquement affichés sur la blockchain l'identité des personnes votant ne peut pas être connue grâce au système de clé publique/clé privée.L'identité est ainsi protégée, et les questions liées à une élection frauduleuse sont écartées. On peut trouver par exemple dans ce secteur la plate-forme start-up Follow My Vote.

Santé : les données médicales sont souvent stockées numériquement. Les rassembler et les rendre disponibles à tout moment est peut-être le plus grand potentiel de la blockchain. Dans certaines circonstances, la technologie peut sauver des vies. Cela peut être expliqué

de manière éclatante par trois exemples : un registre de dons d'organes, le rappel de médicaments contrefaits et des projets de recherche médicale.

Par le passé, les listes d'attente pour les dons d'organes ont été falsifiées à plusieurs reprises. En conséquence, la volonté de la population de donner un organe diminue. La blockchain pourrait empêcher la manipulation à l'avenir.

Avec l'aide de la technologie blockchain, la qualité des produits pharmaceutiques pourrait également être mieux contrôlée, puisque toute la chaîne de production, de la fabrication aux fluctuations de température et tout le parcours de transport jusqu'à la livraison aux pharmacies, pourrait être surveillée et stockée dans la blockchain. Le résultat : si la chaîne du froid n'est pas respectée, le médicament ne sera pas livré. Quoi qu'il en soit, les sociétés pharmaceutiques pourraient attribuer un code QR à chaque médicament que les patients peuvent scanner pour vérifier qu'il est authentique. Falsifier cela ne serait pas impossible, mais cela coûterait beaucoup plus cher qu'auparavant.

Les projets de recherche pourraient également bénéficier grandement de la technologie de la blockchain : d'une part, ils pourraient partager la puissance de calcul et travailler plus étroitement ensemble, et d'autre part, les patients pourraient rendre leurs données de la blockchain disponibles pour des études au moyen d'une déclaration de consentement.

Cela prendra du temps parce que la technologie blockchain en est encore au tout début. Les concepts fondamentaux ne peuvent être testés dans la pratique que lorsque les hôpitaux, les cabinets médicaux et autres organisations médicales ont mis en place l'infrastructure nécessaire. Mais c'est aussi son plus grand avantage : aujourd'hui, la nouvelle technologie peut être entièrement conçue pour le bénéfice du patient .

La figure 2.1 [26], ci-dessous, résume et représente les applications de la blockchain dans le domaine de la santé.

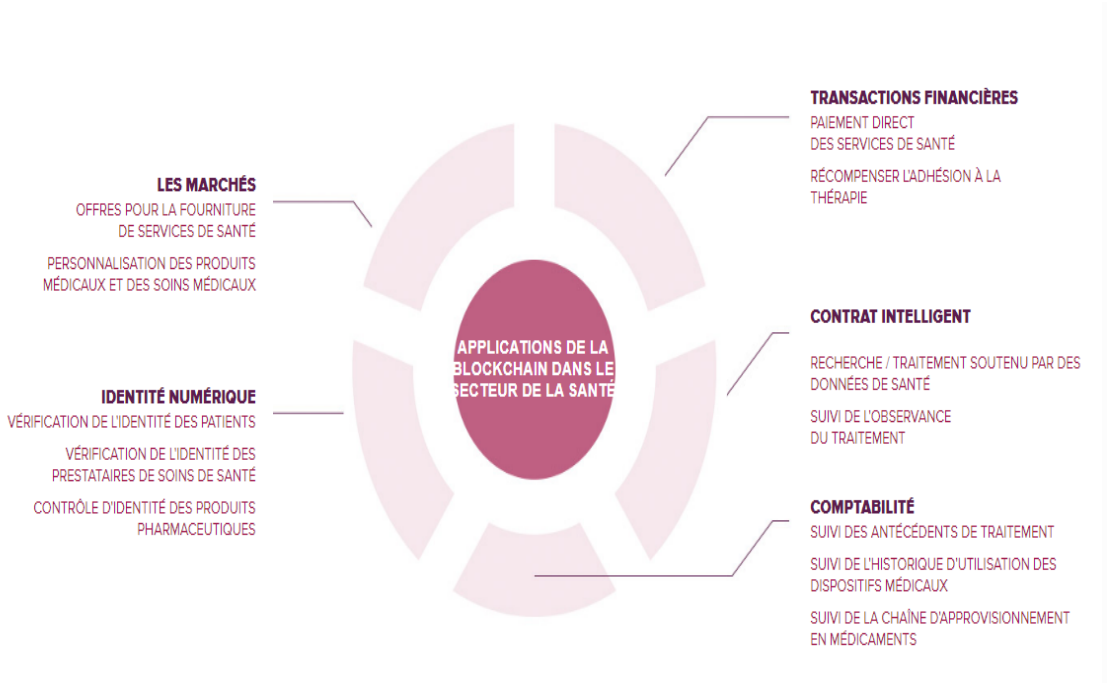

FIGURE 2.1 – Applications de la blockchain dans la santé.

Arts : La blockchain pourra être source de simplification pour l'industrie musicale son but est de garantir une meilleure traçabilité des œuvres, une transparence dans la gestion des droits d'auteur et la répartition des droits de paiements sans passer par des intermédiaires tel que Spotify ou Deezer. C'est ce que propose Voise une plateforme de streaming musical décentralisée.

Banque : Les banques agissent souvent en tant qu'intermédiaires au sein de l'économie mondiale, gérant et coordonnant le système financier grâce à leur comptabilité interne. Comme cela n'est pas visible publiquement, cela force la confiance dans les banques et leur infrastructure souvent obsolète.

La technologie blockchain a le potentiel de perturber non seulement le marché mondial des changes, mais le secteur bancaire dans son ensemble en désactivant ces intermédiaires et en les remplaçant par un système fiable, illimité et transparent, facilement accessible à tous.

La blockchain a permis d'effectuer des transactions plus rapides et moins chères, d'améliorer l'accès au capital, de créer plus de sécurité des données, d' appliquer des accords de confiance grâce à des contrats intelligents et de rendre la conformité plus fluide.

Les assurances : Les blockchains ont le potentiel de révolutionner le monde de l'assurance. Leurs potentiel technologique permet de cartographier de nouveaux business models totalement numériques, transparents et sécurisés pour des interactions rapides entre de nombreux acteurs. Avec les blockchains, les assureurs peuvent simplifier et accélérer la tarification et la fourniture de services, déterminer l'authenticité des biens et des documents, et suivre l'historique des activités frauduleuses d'une personne.

Commerce : La blockchain peut améliorer les processus de nombreuses façons. Par exemple, le suivi des marchandises dès le début de la chaîne d'approvisionnement jusqu'aux points de vente et de service, via cette technologie, nous pouvons prendre les mesures nécessaires en cas de problèmes dans la chaîne.

Énergie : Surtout dans le marché complexe de l'énergie, de grands progrès ont pu être réalisés grâce à la transparence et à la traçabilité de la technologie blockchain. Cela faciliterait le chargement des systèmes solaires privés, le suivi de l'énergie, la gestion des actifs et la délivrance de certificats d'origine. Cette bonne réglementation et ce suivi transparent devraient avoir une grande influence sur la réussite du changement, en particulier dans la transition énergétique. Un autre exemple serait celui des voitures électriques, où l'énergie peut être attribuée à chaque voiture individuellement, quel que soit l'endroit où elle fait le plein dans le réseau, par exemple, et faciliter ainsi la facturation.

La gestion des identités : La vérification de l'identité d'une personne est un défi dans certains domaines d'activité. Cependant, avec l'aide de la technologie blockchain, les identités des personnes peuvent être identifiées de manière plus sûre et plus rapide qu'auparavant. Ceci est basé sur des bases de données étendues qui permettent l'identification et la vérification. En particulier, les documents d'identification existants - permis de conduire, passeports et cartes d'identité - pourraient ainsi être mis en œuvre numériquement en toute sécurité. La perte de données serait également évitée puisque les données sont stockées de manière décentralisée.

Jeux : De nombreux jeux basés sur la technologie de la blockchain existent et peuvent se retrouver sur internet. Les jeux qu'on peut généralement trouver sont des jeux de hasard, comme le lancer de dés, ou des jeux de casino. Ces jeux basés sur la blockchain

permettent aux joueurs d'avoir une propriété permanente et un contrôle total sur leurs actifs en jeu.

2.3 Diverses applications décentralisées de la technologie blockchain

Nous présentons ci-dessous une liste non exhaustive des diverses applications de la technologie blockchain [20] :

Bitcoin : Bitcoin est la première crypto-monnaie distribuée bien connue et largement utilisée, exploite un réseau peer-to-peer sans autorité centrale ni banques, et a introduit la technologie et la plate-forme blockchain dans le monde. La gestion des transactions et l'émission de pièces sont réalisées collectivement par le réseau blockchain.

Coinbase : Coinbase a été lancé en 2012 c'est un portefeuille pour les devises numériques, cette plate-forme d'échange de cryptomonnaies permettant d'acheter, de vendre et de stocker des Bitcoin (BTC), des Ethereum(ETH). Le siège de La société est située à San Francisco en Californie.

Storj : La plate-forme Storj offre un stockage cloud basé sur la blockchain avec un système Chiffrement de bout en bout, Contrairement aux offres cloud classiques, les données ne sont pas stockées de manière centralisée sur les serveurs de Storj, mais distribué de manière centralisée sur les ordinateurs des membres du réseau.

Lorsque des transactions sont effectuées avec Storj pour payer l'espace de données, elles sont ajoutées à la chaîne en tant que bloc. Une fois ajoutés, ils ne peuvent pas être supprimés, ce qui rend la transaction complètement sécurisée. Les transactions sont également visibles pour les autres. Cette vulnérabilité garantit que tous les paiements sont légitimes.

Provenance : Provenance est une plate-forme basée sur la blockchain pour rendre la chaîne de produits plus visible pour le client.

Les entreprises utilisent la plate-forme pour permettre à leurs produits et leurs chaînes d'approvisionnement d'êtres présent d'une manière plus transparente et traçable.

MultiChain : MultiChain est une plate-forme blockchain pour créer et déployer des réseaux blockchain autorisés ou privés. En tant que fourchette de la blockchain Bitcoin, MultiChain se concentre sur la fourniture de fonctionnalités telles que l'intégration de la gestion des autorisations des utilisateurs et l'amélioration des fonctions du registre de données.

2.4 Plateformes de blockchain

Nous présentons ci-dessous une liste des plateformes de la technologie blockchain [27] :

Ethereum : La plate-forme de blockchain Ethereum a créé beaucoup de buzz sur le marché et c'est également l'une des meilleures plates-formes de blockchain à utiliser en 2019. Ethereum est une plateforme de blockchain open source connue pour exécuter des contrats intelligents sur le réseau blockchain personnalisé.

C'est également la meilleure plate-forme pour les développeurs pour créer des applications décentralisées et des organisations autonomes démocratiques (DAO).

Principales caractéristiques d'Ethereum :

— Ouvert au public,
— Système basé sur la preuve de travail,
— Fortement suivi dans Github,
— Application à plusieurs langages comme C ++ et python.

Fabric Hyperledger : C'est l'une des plates-formes blockchain les plus récemment développées. Le monde a découvert l'hyperledger en 2016. La Linux Foundation l'a fait. Son objectif est de stimuler l'utilisation des technologies blockchain dans différents secteurs.

Principales caractéristiques de Fabric Hyperledger :

— privé,
— 180+ entreprises collaboratrices,
— Séquence : Production prête pour les entreprises,
— Langages pris en charge : Python.

OpenChain : C'est une plate-forme open source populaire. Cette plate-forme est particulièrement utile pour les entreprises qui recherchent la gestion d'actifs numériques.

Principales caractéristiques d'OpenChian :

— Réseau privé,

— Langue prise en charge : JavaScript.

EOS : EOS est un réseau open-source lancé l'année 2018 par une société privée Block.one.Il est basé sur le concept de technologie décentralisée qui offre à un utilisateur final la capacité d'effectuer diverses tâches sur la plate-forme EOS. Il élimine également le besoin de frais pour ses utilisateurs, ce qui signifie qu'un utilisateur n'a rien à payer pour profiter des avantages d'une dApp basée sur EOS.

Principales caractéristiques d'EOS :

— Ouvert au public,

— Langages pris en charge : C ++.

Stellar : Stellar est un réseau de grand livre distribué basé sur la technologie blockchain et offre une solution de paiement transfrontalier rapide et rentable aux entreprises et aux particuliers. Avec la plateforme de blockchain Stellar, il est possible pour les développeurs de créer des portefeuilles mobiles et des outils bancaires intelligents comme la sphère de paiement en ligne Paypal.

Principales caractéristiques de Stellar :

— Type de réseau : public et privé,

— Langues prises en charge : Javascript, Java.

Neo : La plate-forme Neo est un réseau open source qui utilise des contrats intelligents blockchain pour gérer les actifs numériques. Neo a été fondée en 2014 et disponible sur GitHub en juin 2015.

La plate-forme Neo blockchain vous aide à payer des frais de transaction pour exécuter votre application sur le réseau Neo. cette plate-forme prend en charge diverses formes d'actifs numériques et vous pouvez également utiliser des certificats numériques pour créer en toute sécurité votre application sur le réseau Neo.

Principales caractéristiques de Neo :

— Ouvert au public,

— Langages pris en charge : C #, Java et Python.

2.5 Machine virtuelle « Ethereum »

EVM (ou machine virtuelle Ethereum) est l'environnement d'exécution de code d'octet des contrats intelligents Ethereum. Chaque nœud du réseau exécute EVM. Tous les nœuds exécutent toutes les transactions qui pointent vers des contrats intelligents à l'aide d'EVM, de sorte que chaque nœud effectue les mêmes calculs et stocke les mêmes valeurs. Les transactions qui ne transfèrent que de l'éther nécessitent également un calcul, c'est-à-dire pour savoir si l'adresse a un solde ou non et déduire le solde en conséquence [28].

Chaque nœud exécute les transactions et stocke l'état final pour diverses raisons. Par exemple, s'il existe un contrat intelligent qui stocke les noms et les détails de tous les participants à une fête, chaque fois qu'une nouvelle personne est ajoutée, une nouvelle transaction est diffusée sur le réseau. Pour que n'importe quel nœud du réseau affiche les détails de toutes les personnes participant à la fête, il leur suffit de lire l'état final du contrat [28].

2.6 Conclusion

La technologie blockchain pourrait être appliquée à différentes applications sur la conjonction de trois concepts : le fonctionnement grâce à un réseau pair à pair, des données publiques et anonymes ainsi qu'un fonctionnement décentralisé et sécurisé.

Au cours de ce chapitre, on a parlé sur les domaines d'application de la blockchain et les diverses plateformes existantes ainsi que quelques applications décentralisées .

Chapitre 3

Vote en ligne

3.1 Introduction

Ce chapitre fait le point sur les différents modes de vote électronique après avoir rappelé et expliqué les caractéristiques fondamentales des élections démocratiques [29].

3.2 Vote démocratique

La démocratie est un système politique dans lequel le pouvoir appartient au peuple. Le peuple y exerce sa souveraineté à travers des représentants intervenus, choisis et nommés. Les nominations sont faites lors d'élections qui doivent adhérer à plusieurs principes de base pour être considérées comme démocratiques et universelles [30].

Ces caractéristiques essentielles que doivent respecter les élections démocratiques sont les suivantes [30] :

— Transparence : chaque électeur a le droit et la capacité effective de contrôler toutes les étapes des élections,

— Unicité : un vote par électeur,

— Confidentialité : chaque électeur peut choisir en secret,

— Anonymat : Une carte d'électeur ne peut pas être liée à l'électeur qui l'a choisie,

— Sincérité : les résultats des élections représentent fidèlement la volonté des électeurs.

Pour voter, les citoyens doivent s'inscrire sur des listes électorales selon leurs lieux de résidence, et les candidats sont enregistrés sur des listes de vote. Le jour du vote, ils doivent se présenter au bureau de vote dans lequel ils sont inscrits. La procédure à suivre

pour un tel vote est représenté dans trois (03) étapes essentielles [31] :

— Avant l'ouverture des bureaux de vote, les cartes des candidats sont déposées sur une table appelée "table de décharge". Le responsable du bureau de vote indique officiellement les heurs d'ouverture et de clôture des bureaux de vote.

— Pendant le scrutin, les électeurs, à leur arrivés, présentent leur carte électorale et une pièce d'identité pour vérifier s'ils ont été inscrits sur le registre électoral.
Après cela, Ils prennent une enveloppe électorale et les différents bulletins de vote, se rendent dans un isoloir pour introduire le bulletin du candidat ou de la liste de leur choix dans l'enveloppe (permet d'assurer le secret du vote), puis se rendent à la table où se trouve l'urne. Ils présentent à nouveau leur carte électorale et leur pièce d'identité et lorsque leur nom est appelé, ils glissent leur enveloppe dans l'urne. Puis ils signent à côté de leur nom sur la liste prévue à cet effet. La carte électorale est tamponnée par un assistant avec un timbre portant date du scrutin.

— Après la fermeture des bureaux de vote, le bureau signe la liste des bulletins de vote et commence le dépouillement. Une fois tous les bulletins comptés, le secrétaire rédige le procès-verbal. Le président du bureau de vote annonce les résultats et les affiche dans la salle de vote.

3.3 Système de vote électronique

Nous pouvons définir un système de vote traditionnel par quatre propriétés [32] :

— identification au bureau de vote,

— prendre les bulletins de vote et une enveloppe dans la salle de vote,

— se rendre dans l'isoloir pour le dépôt du bulletin de vote dans l'enveloppe puis mettre l'enveloppe dans l'urne transparente,

— comptage manuel.

Lorsque nous impliquons une numérisation des données sur une des quatre opérations, le système de vote pourrait être considérer électronique. La numérisation implique l'utilisation des machines électroniques équipées de logiciels [32].

Il existe de multiples formes du vote électronique : vote par boîtier, par internet, machine à voter, stylo numérique, dépouillement automatisé, etc [33].

3.4 Systèmes de vote en ligne

Le vote en ligne est la forme de vote électronique la plus numérisée, mais elle peut impliquer des méthodes technologiques très différentes [32].

Le système de vote en ligne remplace la méthode de vote existante et aide les électeurs à utiliser des ordinateurs et des terminaux de communication mobiles pour exprimer leurs opinions et choisir des représentants dans l'environnement Web et mobile à tout moment et en tout lieu [29].

Il permet également de tenir divers bulletins de vote efficacement et en toute sécurité afin que les intentions des gens peut se refléter correctement dans la sélection des membres du conseil, la révision des statuts l'incorporation et la prise de décisions sur les ordres du jour. Les droits fondamentaux des électeurs sont garantis tout au long du processus de vote, comme la méthode électorale conventionnelle [29].

3.4.1 Corée du sud

La Commission électorale nationale gère le système de vote en ligne K-Voter (Figure 3.1 [34]) depuis octobre 2013, et le K-Vote est utilisé non seulement pour élire les représentants des communautés comme les écoles, les appartements, les villages et les coopératives, mais aussi de rassembler des avis sur certains ordres du jour et prendre des décisions politiques. En outre, la commission soutient le système de vote en ligne pour l'élection des représentants des milieux politiques partis politiques et nomination des candidats à la présidence. Le vote en ligne offre la commodité de voter quel que soit l'heure et le lieu, et a un gros avantage, à savoir la réduction des coûts. Mais néanmoins, il n'est pas encore largement utilisé en Corée [29].

FIGURE 3.1 – Système de vote en ligne national K-Voting.

3.4.2 Estonie

L'Estonie est parmi les quelque 40 pays du monde qui pratiquent le vote électronique et qui pratique le vote par Internet le plus avancé. L'Estonie est un petit pays de 1,34 million d'habitants. En conséquence, l'Estonie peut gérer et mener les politiques gouvernementales plus facilement que les autres pays [29].

L'Estonie a le vote électronique depuis 2005 et en 2007 a été le premier pays au monde à permettre le vote en ligne. Lors des élections législatives de 2015, 30,5% de tous les votes ont été enregistrés. Les bases de ce système sont les cartes d'identité nationale que tous les citoyens estoniens reçoivent. Ces cartes contiennent des fichiers cryptés qui identifier le propriétaire et lui permettre d'effectuer un certain nombre d'activités en ligne y compris les services bancaires en ligne, la signature numérique des documents, accéder à leurs informations sur les bases de données gouvernementales et le vote électronique [35].

Pour voter (Figure 3.2 [34]), l'électeur doit entrer sa carte dans un lecteur de carte, puis accéder au site web de vote sur l'ordinateur connecté. Ils saisissent ensuite leur code PIN et un contrôle est effectué pour voir s'ils ont le droit de voter. Une fois confirmés, ils peuvent voter/modifier leur vote jusqu'à quatre jours avant le jour du scrutin. L'électeur peut également utiliser un téléphone portable pour s'identifier et voter s'ils n'ont pas de lecteur de carte pour leur ordinateur, cependant, ce processus nécessite une carte SIM spécialisée pour le téléphone. [35].

Lorsqu'un électeur soumet son vote, le vote est transmis via le serveur d'organisation de vote accessible au public au serveur de stockage des votes où il est crypté et stocké jusqu'à la fin de la période de vote. Ensuite, le vote a nettoyé toutes les informations d'identification et l'a déplacé par disque sur le serveur de décompte des votes non connecté à tous les réseaux. Le serveur décode et calcule les votes, puis affiche les résultats. Chaque étape de ce processus est enregistrée et vérifiée [35].

Lors de l'élection locale de 2013, les chercheurs ont observé et étudié le processus de vote électronique et a mis en évidence un certain nombre de risques potentiels pour la sécurité du système. Un de ces risques est la possibilité de logiciels malveillants sur la machine côté client qui surveille l'utilisateur en train de voter, puis plus tard changer leur vote à un autre candidat. Un autre risque possible est qu'un attaquant infect directement les serveurs par le biais de logiciels malveillants placés sur les DVD utilisés pour configurer les serveurs et transférer les votes. Cependant, ce rapport a également fait l'objet de critiques de la part de l'Autorité estonienne des systèmes d'information [35].

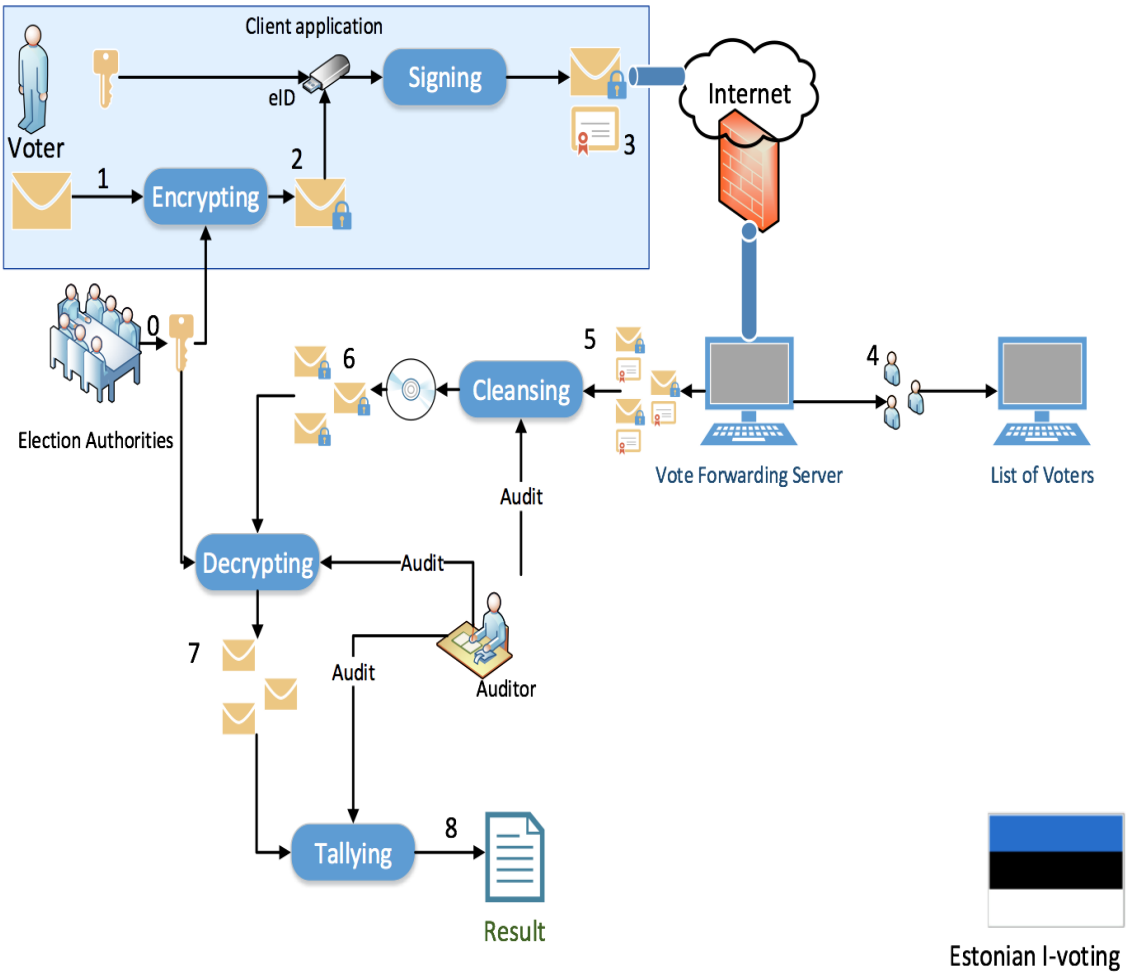

FIGURE 3.2 – Système de vote numérique estonien.

3.4.3 Suisse

Depuis 2004, deux systèmes de vote en ligne sont disponibles en Suisse jusqu'en 2019 :

— Le système postal fédéral

— Le système de vote dans les cantons.

Aucun incident n'a été détecté sur le site, mais lors des contrôles de sécurité 2018 du système postal, des failles ont été découvertes. De plus, au niveau fédéral, les partis sont contre le vote via Internet. Cependant, les consultations organisées par le Conseil fédéral en 2019 montrent que 19 des 26 cantons y étaient favorables. En d'autres termes, la grande majorité de la population le soutient, tandis que la classe politique, qui ne représente qu'une petite minorité de la population, s'y oppose. Concrètement, les deux systèmes sont suspendus depuis au moins quatre ans [32].

3.4.4 France

Les Français vivant à l'étranger ont la possibilité de voter en ligne comme alternative au vote traditionnel. Le Sénat français note dans son rapport sur le vote électronique que « le législateur doit nécessairement prendre en compte le fait que les conditions concrètes de vote pour un électeur français à l'étranger et sur le territoire national sont indéniablement différentes. Si la proximité entre l'électeur et le bureau de vote est assurée en France grâce au maillage des bureaux de vote, le réseau de ces bureaux à l'étranger, qui épouse celui de l'administration consulaire, ne peut en aucun cas se prévaloir de la même intensité. Il existe même un coût financier pour l'électeur expatrié qui souhaite exercer son droit de vote. Dans certains cas, l'impossibilité matérielle ou liée à des considérations géopolitiques est manifeste » [32].

3.5 Faille technique de vote en ligne

3.5.1 Confidentialité

Puisque il est possible de voter depuis n'importe quel ordinateur, il est difficile de garantir la confidentialité. Il faut s'assurer qu'il n'y a pas de vol d'identité, l'électeur étant seul devant l'ordinateur et n'étant exposé à aucune pression [30].

3.5.2 Anonymat

Il est difficile d'assurer l'anonymat car chaque bulletin de vote est envoyé avec un identifiant d'électeur et ces informations arrivent ensemble sur le premier serveur de vote [30].

3.5.3 Transparence

La transparence directe ne peut pas être mise en œuvre efficacement car les bulletins de vote ne sont pas importants, ce qui signifie que les citoyens ne pourront pas participer au suivi pendant le vote, assister au dépouillement public ou même y participer. Les bulletins de vote et le registre sont remplacés par un appareil qui imite ces objets. Ainsi le processus de vote est transféré du monde réel, dont l'expérience est accessible à la

majorité des citoyens, à un monde virtuel où les observations faites directement à travers nos perceptions ne s'appliquent pas. Dans le monde réel, il est impossible de changer ce qui est écrit sur le bulletin scellé dans une enveloppe scellée, dans le monde virtuel ce processus est faisable et même facile, il peut impliquer un grand nombre de votes, se dérouler en un instant et rester caché lors de tests ou d'expériences. Alors que dans le monde réel le vide de l'urne peut être vérifié visuellement et même au toucher, il semble peu probable de prétendre à la vérification qu'une «urne électronique» est vide en se fiant uniquement à l'affichage produit par ordinateur. Encore, l '«urne électronique» n'est en fait qu'une mémoire électronique, et la mémoire électronique n'est jamais vide, elle est toujours pleine de bits d'une valeur de 0 ou 1. Les électeurs n'ont donc aucun moyen de surveiller directement les procédures de vote et d'évaluer leur succès. Non seulement les auditeurs, les délégués des partis et les membres des bureaux de vote n'ont pas un meilleur accès au fonctionnement intime de l'application, mais ils doivent se contenter de processus de surveillance censés refléter le fonctionnement de l'ordinateur, mais peuvent également donner une vue déformée [30].

3.5.4 Confiance

La publication de logiciels souhaitables pour augmenter la sécurité du vote n'augmente pas la transparence de la procédure parce qu'il est nécessaire de démontrer que le logiciel utilisé est complètement identique à ce qui a été publié et qu'il ne souffre d'aucune interférence d'autres programmes. Cependant, dans tous les cas, le serveur utilise un système d'exploitation, il s'agit probablement d'un compilateur ou d'un interpréteur de code qui devrait pareillement être vérifié. Cette approche devient gigantesque et donc peu pratique. La surveillance de la mise en œuvre du vote est laissée à des tiers, ce qui mine la confiance des électeurs. Le contrôle des experts supprime l'élément «démocratique» du contrôle des processus électoraux et le remplace par le côté «technocratique». Mais il peut permettre aux citoyens de les informer d'éventuels dysfonctionnements ou irrégularités techniques. Mais là aussi, seuls les experts contrôlent ce qu'ils veulent, ou ce qu'ils peuvent faire [30].

3.6 Avantages du vote électronique

Avec la technologie que nous avons à portée de main, il est possible de créer un système de vote pour tout un pays. Le vote électronique présente de nombreux avantages qui rendent le vote plus facile que jamais. Parmi les avantages du vote on ligne on cite [37, 38] :

- Simplifier le processus électoral et le rendre accessible aux électeurs. Vous pouvez exercer votre droit de vote depuis n'importe quel ordinateur connecté à Internet ou depuis n'importe quel téléphone fonctionnel. Ces méthodes créent de nombreux points d'accès supplémentaires pour le vote.
- Grâce à une borne Internet, il est possible de voter à tout moment.
- L'Internet et le téléphone sont deux moyens particulièrement pratiques pour encourager la participation de jeunes qui sont plus technophiles.
- assurerait une plus grande confidentialité aux personnes handicapées. En votant électroniquement sans l'aide d'autrui. Cela maintient l'anonymat et encourage les personnes handicapées et les personnes âgées à se faire entendre.
- L'amélioration de l'accès et la création d'opportunités de vote supplémentaires peuvent avoir un impact positif sur le taux de participation.
- Résultats électoraux plus rapides et plus fiables. Ces méthodes de vote accéléreront le processus de comptage formel et sont plus fiables que les machines à compter.
- Tous les systèmes de vote en ligne sont susceptibles d'être moins chers que la méthode de vote traditionnelle, qui nécessite l'installation de bureaux de vote dotés de personnel.
- Tous les systèmes de vote en ligne ou par téléphone ont le potentiel d'améliorer la qualité globale des bulletins de vote en réduisant ou en éliminant le nombre d'erreurs de vote et il est possible d'afficher des renseignements supplémentaires sur les candidats et leurs positions en vue du vote.
- L'infrastructure peut être utilisée à chaque élection, ce sera donc un achat unique.
- Les résultats sont disponibles presque instantanément car les votes sont comptés pendant le vote, mais en utilisant les méthodes traditionnelles, les votes doivent être collectés et comptés dans les bureaux de vote. Ce processus prend beaucoup de temps et retarde le résultat final.

3.7 Problème de système de vote en ligne

Le vote en ligne offre aux électeurs la possibilité de voter sans aucune restriction dans le temps et place, et réduit les coûts. Malgré ces avantages, il n'est pas encore largement utilisé en Corée. Le vote en ligne passe par les processus suivants [29] :

— l'inscription des électeurs après identification,

— affichage des agendas,

— vote,

— affichage du résultat du vote.

Pour que les gens fassent confiance à la méthode de vote, la méthode doit être plus sûre et correcte. Et cela il faut prouver que les résultats du vote ont correctement reflété les intentions des électeurs. les problèmes suivants peuvent survenir lors du vote en ligne. Pour commencer, dans le processus d'identification, des problèmes se produisent lors de l'authentification non en face à face pour voir si l'électeur est inscrit électeur. Il existe d'autres problèmes, tels que la falsification et l'altération des résultats de vote cyber-attaques pendant le vote et arrêt du système en raison d'une panne de courant ou désastres naturels. Il peut également y avoir un problème avec la garantie du secret du vote détails aux électeurs. Si le vote se déroule dans un environnement en ligne dans lequel les informations peuvent être divulguées, les informations personnelles d'autrui peuvent être volées et utilisées pour vote par procuration et vote répété, et il peut y avoir un problème de sécurité en ce qui concerne garantir le secret du vote. Enfin, les résultats du vote peuvent être fabriqués, et s'il y a méfiance à l'égard de la sécurité, la confiance dans les résultats du vote ne peut pas non plus être garantie [29].

3.8 Inconvénients du vote électronique

Pour l'instant, les arguments en faveur du vote électronique semblent solides. Cependant, le vote électronique présente des inconvénients qui doivent être pris en compte. Parmi ces inconvénients [37, 38] :

— Menaces et attaques de virus informatiques organisées par des pirates informatiques.

— Les électeurs doivent être identifiés avec un type d'identification. Mais le problème

avec l'utilisation de ces méthodes de vérification est que si quelqu'un obtient une grande quantité de ces informations d'identification par le biais de violations de données, il peut émettre des milliers de votes frauduleux.

— Les dépenses initiales sont beaucoup plus importantes que le vote papier.

— Pannes de courant ou problèmes de connexion Internet, en plus de l'arrêt ou des dysfonctionnements du serveur.

— Problèmes de fraude : lorsque quelqu'un vote au nom de quelqu'un d'autre sans obtenir l'autorisation,

— Problèmes de coercition : lorsque l'électeur subit des pressions de la part d'autres personnes qui le font voter autrement qu'il l'aurait normalement fait.

— Il faut investir beaucoup de temps et d'argent pour s'assurer que le public est conscient de l'existence du vote électronique et comprend comment l'utiliser.

— Piratage électoral : Il existe toujours un risque que quelqu'un modifie illégalement les résultats des élections. Un seul agent nocif peut altérer des millions de sons électroniques qui ne seront pas détectés.

3.9 Problématique

Le vote doit respecter cinq (5) caractéristiques essentielles : la transparence, l'unicité, la confidentialité, l'anonymat et la sincérité.

Mais ni la transparence ni la sincérité n'est garanti dans le vote traditionnel vu que ces processus demandent des intermédiaires qui peuvent fausser le résultat.

En plus, le vote en ligne ou électronique, malgré qu'il facilite les procédures du vote, minime la consommation du temps et des ressources, mais ni la confidentialité ni l'anonymat ni la sincérité est garanti, parce que :

— Ils peuvent observer la procédure pendant son déroulement.

— Le scrutin laisse une trace permettant de lier chaque électeur à son bulletin.

— Le système de vote est centralisé dans un serveur contrôlé par un intermédiaire donc les données peuvent être modifiées. Enfin, les applications web du vote ont le problème de saturation des serveurs lors la phase du vote.

Comment donc éviter les problèmes cités ci-dessus ?

3.10 Solution proposée

Notre solution consiste à proposer un système de vote en ligne basé sur la technique de blockchain. La blockchain est un moyen efficace, sécurisé et transparent, pour gérer le vote.

Nous attendons de ce système d' :

— Assurer la transparence : les électeurs peuvent eux-mêmes contrôler toutes les étapes d'un scrutin (compter les votes et assurer qu'aucun vote n'avait été supprimé, manipulé ou modifié).

— Assurer l'unicité : chaque électeur peut effectuer un et un seul vote.

— Assurer la confidentialité : la procédure du vote n'est pas suivie lors du son déroulement donc l'électeur peut effectuer son choix en secret.

— Assurer l'anonymat des électeurs : il est impossible de relier un bulletin à l'électeur qui l'a choisi.

— Assurer la sécurité contre d'éventuelles tentatives de fraudes à tous les niveaux.

3.11 Conclusion

Dans ce chapitre, nous avons exposé le vote en ligne, ces avantages, ces inconvénients ainsi les failles techniques.

Chapitre 4

Conception et modélisation du système Vote en ligne

4.1 Introduction

Ce chapitre est consacré aux étapes fondamentales de conception et de modélisation du système de vote en ligne on se basant sur la technologie de blockchains.

Nous avons opté pour le Processus Unifié (UP) comme méthode de conception, et l'Unified Modeling Language (UML) comme langage de modélisation.

4.2 Processus unifié(UP)

Le processus unifié est un processus de développement logiciel itératif et incrémental, construit sur l'UML, centré sur l'architecture et piloté par les cas d'utilisation, il semble être la solution idéale pour remédier à l'éternel problème des développeurs [80].

Comme l'illustre la figure 4.1 [80], la démarche UP se résume dans les étapes suivantes [81] :

- **Spécification :** sert à définir les différents besoins du système :
  - **Fonctionnelles :** du point de vue utilisateur.
  - **Non fonctionnels :** du point de vue technique.
- **Analyse :** permet la compréhension des besoins et des exigences du client.
- **Conception :** permet d'acquérir une compréhension approfondie et déterminer la manière de résoudre le problème posé.

— **Implémentation :** consiste à construire un programme en utilisant un langage de programmation donnée.

— **Tests :** permet de vérifier que le système implémente bien les fonctionnalités attendues.

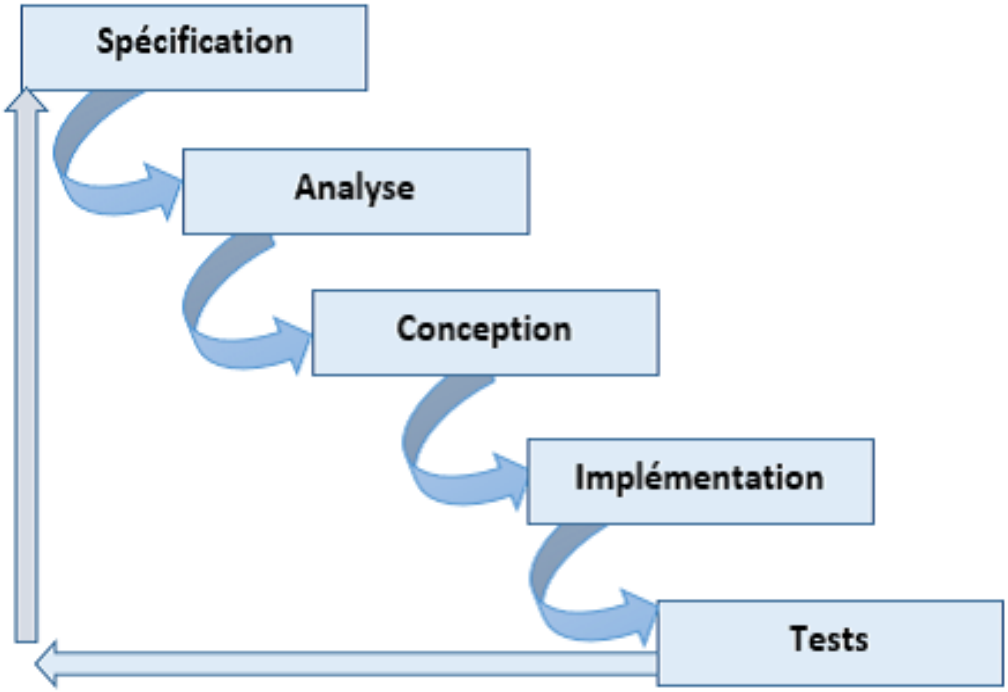

FIGURE 4.1 – Processus UP.

4.3 Unified Modeling Language (UML)

UML est un langage de modélisation graphique et textuel destiné à comprendre et décrire des besoins, spécifier et documenter des systèmes, concevoir des solutions et communiquer des points de vue [82]. UML comporte treize diagrammes. Pour la modélisation de notre système, nous utilisons les trois diagrammes fondamentaux suivants :

— Diagramme de cas d'utilisation (en anglais Use Cases) sert à exprimer le comportement du système en termes d'actions et de réactions, selon le point de vue de chaque utilisateur. Il définit les limites du système et ses relations avec son environnement [83].

— Diagramme de séquences, ces diagrammes sont la représentation graphique des interactions entre les acteurs et le système selon un ordre chronologique dans la

formulation UML [84].

— Diagramme de classe, une représentation graphique de ce que sera l'implémentation du système. Il apporte une vue statique du système grâce à la représentation des classes et des relations entre ces dernières [85].

4.4 Identification des besoins

Besoins fonctionnels, le système doit offrir les fonctionnalités suivantes :

— Lancement du vote.

— Authentification des électeurs et d'administrateur.

— Ajout des électeurs.

— Ajout des candidats.

— Vote.

— Affichage des résultats.

Besoins non fonctionnels, a part les besoins fondamentaux, notre système doit répondre aux critères suivants :

— **Traçabilité :** Les données sont enregistrées d'une manière sécurisée, dans le temps et sceller dans un registre décentralisé et infalsifiable. Les données sont ainsi certifiées et non répudiables.

— **Sécurité :** La blockchain assure un stockage des informations d'une manière non modifiable et toutes ces informations pourraient se retrouver de façon chronologique dans un registre sécurisé et aisément consultable.

— **Performances :** Un logiciel doit être avant tout performant c'est à-dire à travers ces fonctionnaliés, répond aux exigences des utilisateurs d'une manière optimale.

— **Utilisabilité :** Le système doit offrir à l'utilisateur une interface simple et facile à utiliser.

— **Scalabilité :** L'utilisateur doit pouvoir augmenter ses capacités de traitement, de stockage, de transmission et de réseaux selon ses besoins.

4.5 Diagramme des cas d'utilisation

4.5.1 Identification des acteurs du système

Dans le cas de notre système, nous avons identifié principalement deux acteurs (Administrateur, Electeur) et Pour chacun des deux acteurs cités, notre application doit donc offrir un ensemble de fonctionnalités :

Administrateur

— S'authentifier,

— Ajouter les électeurs,

— Ajouter les candidats,

— Lancer le vote,

— Consulter les résultats de vote.

Electeur

— S'authentifier (obtenir un compte),

— Accéder au système pour voter,

— Consulter les résultats de vote.

4.5.2 Pourquoi deux systèmes ?

Voir que la sécurité dans les systèmes de vote en line est un critère important, et pour permettre un vote équitable juste pour les citoyens qui appartiennent au pays concerné par le vote. Nous avons proposé de gérer les comptes des électeurs en utilisant les comptes MetaMask. Cette méthode permet à la fois de se connecter à la blockchain et de confirmer l'inscription des électeurs.

L'absence de stockage des données lors de la réalisation de l'application blockchain nous a poussé à utiliser la base de données traditionnelle.

Suite cette proposition, Notre système de vote est reparti en deux sous-systèmes. Le premier sous-système concerne le processus de vote lui-même et le deuxième sous-système pour la récupération des comptes MetaMask.

— Diagramme de cas d'utilisation général :

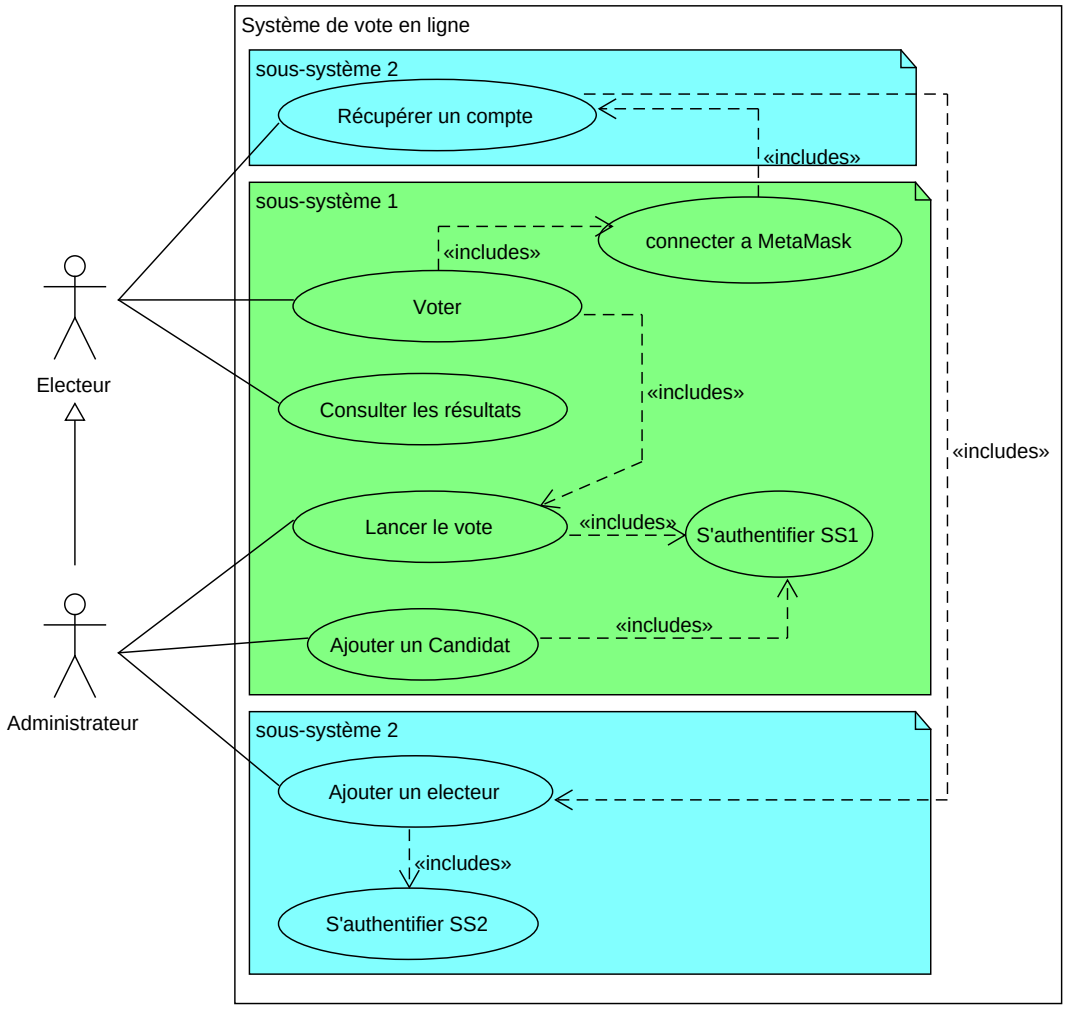

FIGURE 4.2 – Diagramme cas d'utilisation général.

4.5.3 Description textuelle

Dans le but de mieux comprendre notre système et les interactions avec les utilisateurs, dans le tableau (4.1) ci-dessous nous allons détailler les scenarios des cas d'utilisation.

CU1 :S'authentifier SS1
Résumé : Ce CU permet à l'acteur de se connecter au sous-système1.
Acteurs : Administrateur.
Précondition : l'Administrateur posséde un profil.
Post-Condition : l'Administrateur s'authentifier.
DESCRIPTION DU SCENARIO NOMINAL 01 : Le système invite l'acteur à entrer son identifiant et son mot de passe.

02 : L'acteur saisit le l'identifiant et le mot de passe et valide. 03 : Le système vérifie les paramètres. 04 : Le système ouvre la page principale de l'administrateur.
DESCRIPTION DU SCENARIO ALTERNATIF L'identifiant ou le mot de passe est incorrect : 01 : Le système informe l'acteur que les données saisies sont erronées et le scénario reprend.

CU2 :S'authentifier SS2
Résumé : Ce CU permet à l'acteur de se connecter au sous-système2.
Acteurs : Administrateur.
Précondition : l'Administrateur possède un compte MetaMask.
Post-Condition : l'Administrateur s'authentifier.
DESCRIPTION DU SCENARIO NOMINAL 01 : Le système invite l'acteur à entrer Nom, Prenom et le numéro de la carte de vote. 02 : L'acteur saisit le son Nom, Prénom, le numéro de sa carte de vote et valide. 03 : Le système vérifie les paramètres. 04 : Le système ouvre la page principale de l'administrateur.
DESCRIPTION DU SCENARIO ALTERNATIF Nom ou Prénom et le numéro de carte de vote est incorrect : 01 : Le système informe l'acteur que les données saisies sont erronées et le scénario reprend.

CU3 : Ajouter electeur (sous-système2)
Résumé : Ce CU permet à l'acteur d'ajouter un électeur dans le sous-système2.
Acteurs : Administrateur.
Précondition : l'Administrateur est authentifié.
Post-Condition : l'Administrateur ajoute un électeur.
DESCRIPTION DU SCENARIO NOMINAL 01 : Le système invite l'acteur à entrer id, Nom, Prenom, le numéro de

la carte de vote, compte et la clé. 02 : L'acteur saisit id, Nom, Prenom, le numéro de la carte de vote, compte, la clé et valide. 03 : Le système vérifie les paramètres. 04 : Le système ajoute l'électeur a la base de données et ouvre une page à l'administrateur qui permet d'ajouter un autre électeur.
DESCRIPTION DU SCENARIO ALTERNATIF Nom ou le numéro de carte de vote existe déjà : 01 : Le système informe l'acteur que les données saisies sont erronées et le scénario reprend.
CU4 : Récupérer un compte
Résumé : Ce CU permet à l'acteur de récupérer son compte MetaMask.
Acteurs : Electeur.
Précondition : /
Post-Condition : L'électeur récupére son compte.
DESCRIPTION DU SCENARIO NOMINAL 01 : Le système invite l'acteur à entrer Nom, Prénom et le numéro de la carte de vote. 02 : L'acteur saisit le son Nom, Prénom, le numéro de sa carte de vote et valide. 03 : Le système vèrifie les paramètres. 04 : Le système ouvre la page principale des informations d'électeur dans laquelle il récupère son compte.
DESCRIPTION DU SCENARIO ALTERNATIF Nom ou Prénom et le numéro de carte de vote est incorrect : 01 : Le système informe l'acteur que les données saisies sont erronées et le scénario reprend.
CU5 : Lancer le vote
Résumé : Ce CU permet à l'acteur de lancer le vote.
Acteurs : Administrateur.

Précondition : l'Administrateur authentifié.
Post-Condition : l'Administrateur lance le vote.
DESCRIPTION DU SCENARIO NOMINAL 01 : Le système invite l'acteur à entrer la date et l'heur de fin de vote. 02 : L'acteur saisit la date et l'heur. 03 : Le système calcule la différence entre les la date entrer et la date du jour de lancement de vote. 04 : Le système ouvre la page compte à rebours de l'administrateur.
DESCRIPTION DU SCENARIO ALTERNATIF Si la différence entre les deux dates est égale ou inférieur à zéro : 01 : Le système affiche un message fin votepour l'acteur .

CU6 : voter
Résumé : Ce CU permet à l'acteur de voter.
Acteurs : Electeur.
Précondition : l'électeur posséde un compte et le vote est lancé.
Post-Condition : l'Electeur vote.
DESCRIPTION DU SCENARIO NOMINAL 01 : Le système invite l'acteur à sélectionner un candidat et de valider le choix. 02 : L'acteur sélectionne le candidat et valide. 03 : Le système vérifie les paramètres. 04 : Le système ouvre la page des résultats.
DESCRIPTION DU SCENARIO ALTERNATIF L'électeur a déjà voté ou n'a pas un compte ou le vote n'est pas encore lancé : 01 : Le système affiche la page des résultats.

CU7 : consulter les résultats
Résumé : Ce CU permet à l'acteur de consulter les résultats de vote.
Acteurs : Administrateur, Electeur.

Précondition : /
Post-Condition : /
DESCRIPTION DU SCENARIO NOMINAL /
DESCRIPTION DU SCENARIO ALTERNATIF /
CU8 : Ajouter Candidat
Résumé : Ce CU permet à l'acteur d'ajouter un Candidat dans le sous-système1.
Acteurs : Administrateur.
Précondition : l'Administrateur est authentifié.
Post-Condition : l'Administrateur ajoute un candidat.
DESCRIPTION DU SCENARIO NOMINAL 01 : Le système invite l'acteur à entrer id, Nom, Prenom, le numéro de la carte de vote, compte et la clé. 02 : L'acteur saisit id, Nom, Prenom, le numéro de la carte de vote, compte, la clé et valide. 03 : Le système vérifie les paramètres. 04 : Le système ajoute le candidat a la base de données et ouvre une page qui permet à l'administrateur d'ajouter un autre candidat.
DESCRIPTION DU SCENARIO ALTERNATIF Nom ou le numéro de carte de vote existe déjà : 01 : Le système informe l'acteur que les données saisies sont erronées et le scénario reprend.

TABLE 4.1 – Scénario des cas d'utilisation.

4.6 Diagrammes de séquences

4.6.1 Diagramme de séquence « Authentification »

Le diagramme de séquence « Authentification» présente le séquencement des interactions entre l'Administrateur et le système (sous-système 1 afin d'ajouter un candidat ou pour lancer le vote ou bien de s'authentifier au sous-système 2 afin d'ajouter les électeurs).

Dans ce diagramme loop(1, 3) indique qu'il y aura une répétition d'affichage de la page authentification jusqu'à la validation des données où après trois (3) essayes non effectues.

L'opérateur alt indique la structure conditionnelle if. Cette condition va permettre d'accéder à la page souhaiter et d'afficher un message de succès si (et seulement si) les données entrés sont valide, sinon le système affiche un message d'erreur.

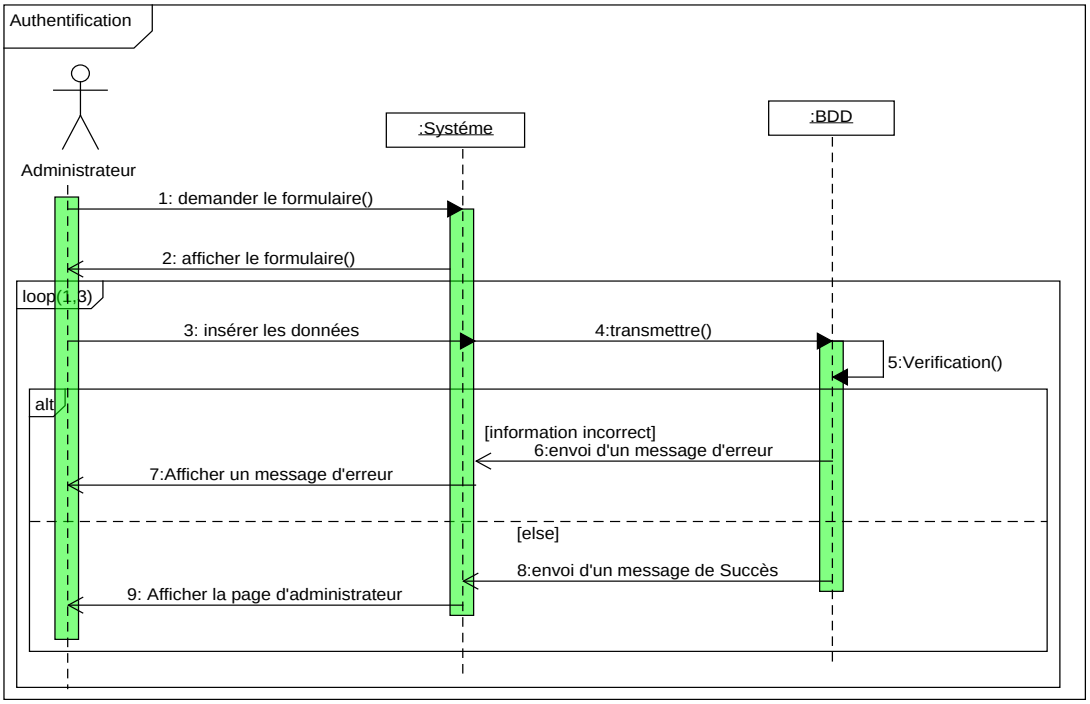

FIGURE 4.3 – Diagramme de séquence « Authentification ».

4.6.2 Diagramme de séquence « Ajouter »

Le diagramme de séquence « Ajouter » présente le séquencement des interactions entre Administrateur et le système.

Un Administrateur peut ajouter un électeur ou un candidat par le remplissage du formulaire (formulaire d'ajout d'un candidat ou bien celui d'ajout d'un électeur). La validation de l'ajout nécessite la vérification des champs saisis.

L'operateur alt indique la structure conditionnelle if. Cette condition va permettre d'ajouter et d'afficher un message de succès si (et seulement si) les données entrés sont valide, sinon le système affiche un message d'erreur.

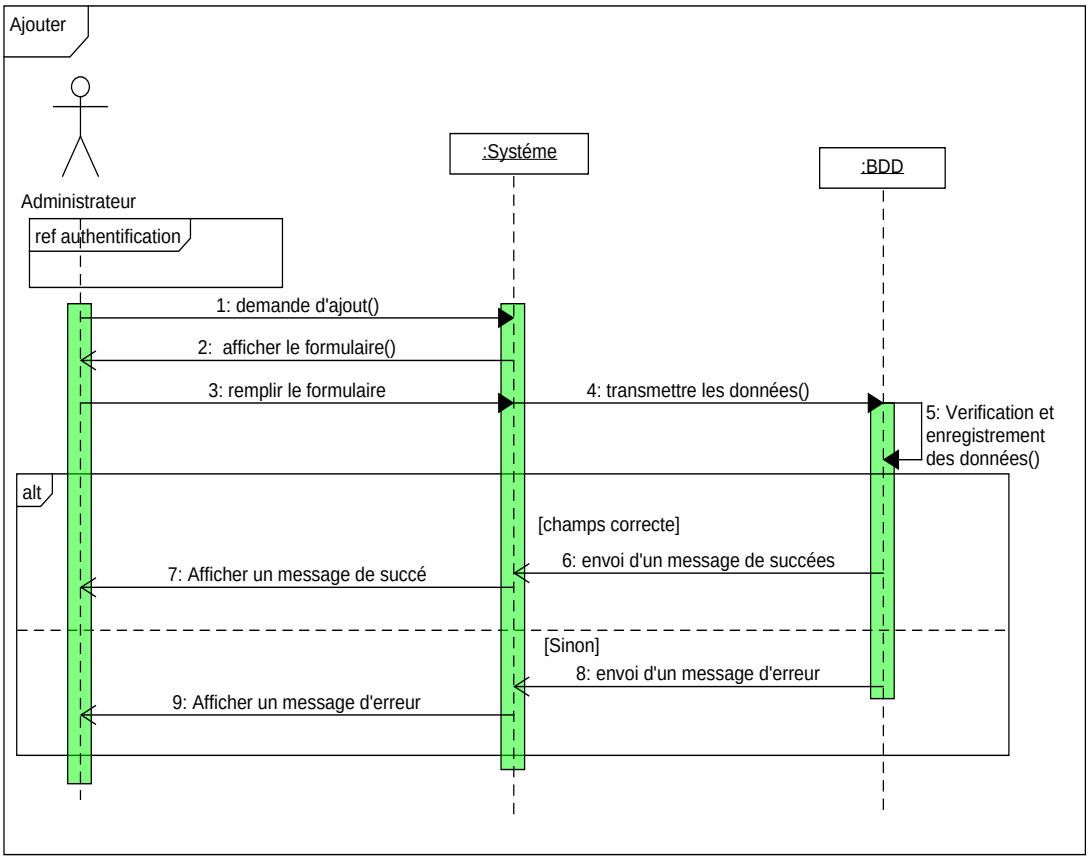

FIGURE 4.4 – Diagramme de séquences « Ajouter ».

4.6.3 Diagramme de séquence « Obtenir compte »

Le diagramme de séquence «Récupérer le compte» présente le séquencement des interactions entre un électeur et le sous-système2 afin de s'inscrire et de récupérer le compte et sa clé.

L'operateur alt indique la structure conditionnelle if. Cette condition permet d'afficher la page contenue les informations d'un électeur si (et seulement si) les données sont correctes, sinon le système affiche un message d'erreur.

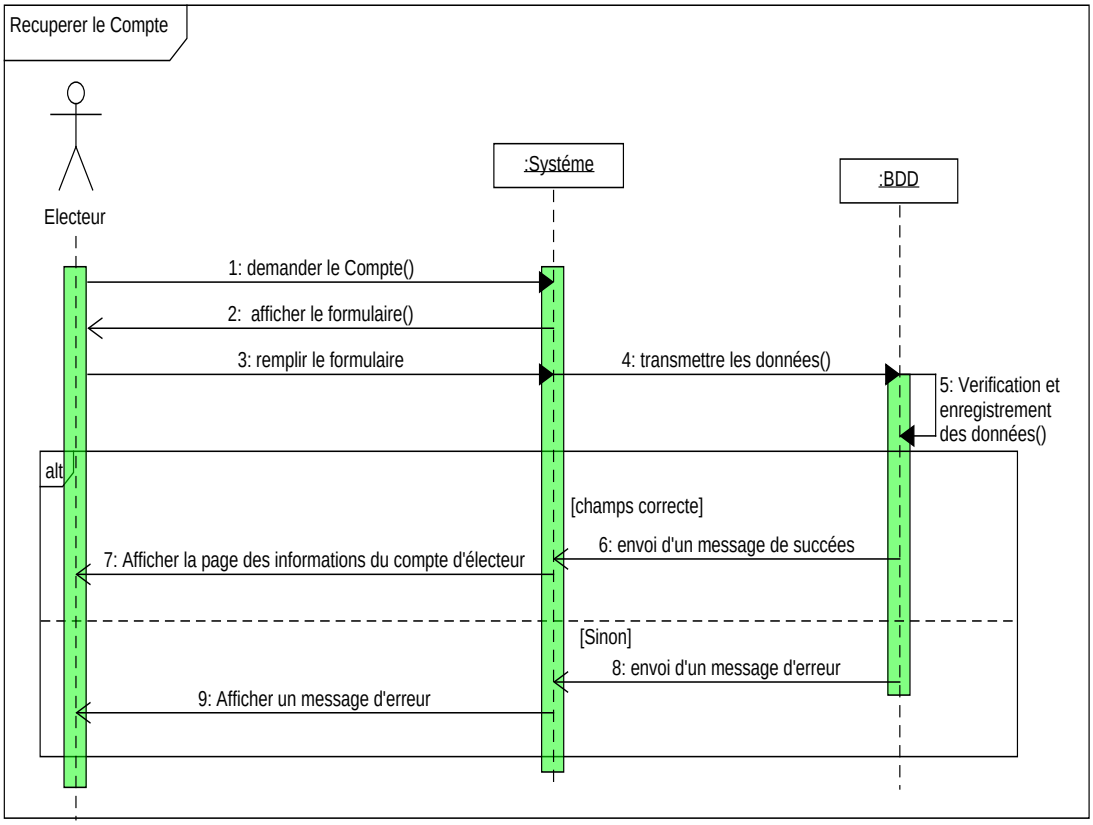

FIGURE 4.5 – Diagramme de séquence « Récupérer le compte ».

4.6.4 Diagramme de séquence « Lancer le vote »

Le diagramme de séquence "Lancer le vote" présente le séquencement des interactions entre Administrateur, Electeur et le sous-système1. L'operateur alt indique la structure conditionnelle if. Cette condition va permettre d'afficher la page compte à rebours pour l'Administrateur et la page de vote pour l'électeur si (et seulement si) la différence entre les deux dates est supérieur à 0, sinon le système affiche un message fin de vote pour l'Administrateur et la page des résultats pour l'électeur.

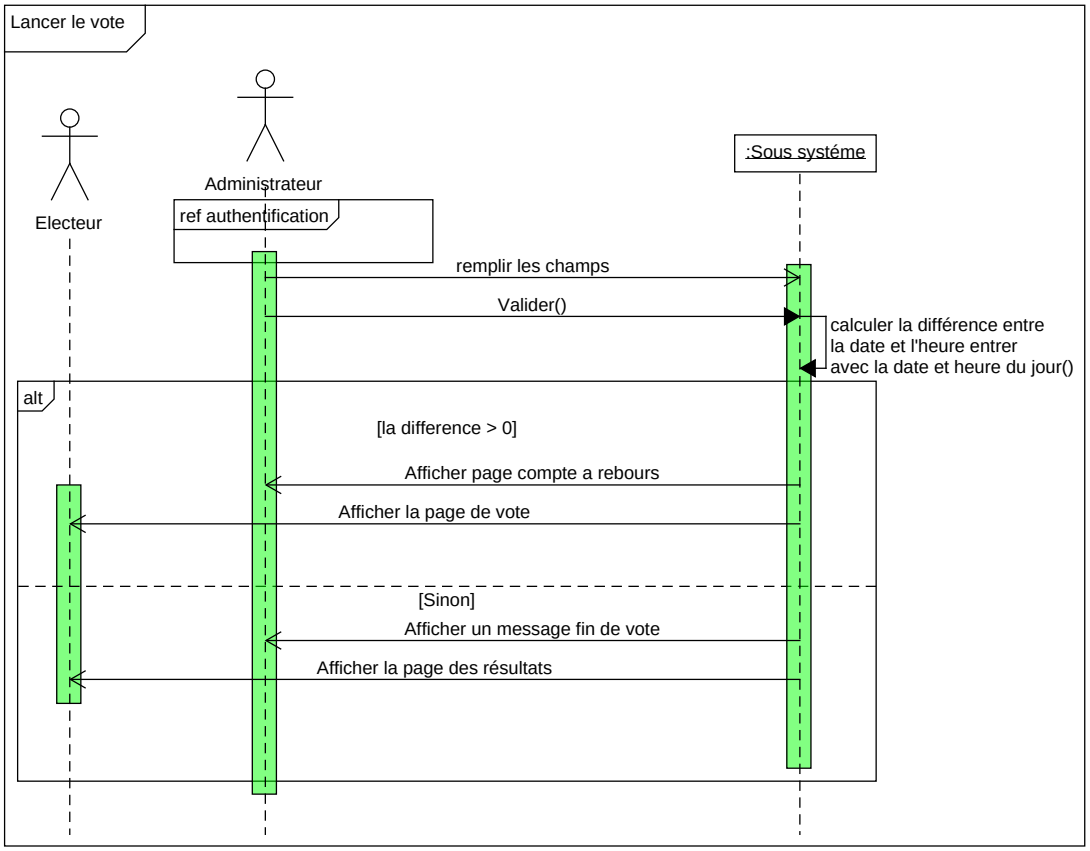

FIGURE 4.6 – Diagramme de séquence « Lancer le vote ».

4.6.5 Diagramme de séquence « Voter »

Le diagramme de séquence « Voter » présente le séquencement des interactions entre Electeur et le sous-système1.

L'operateur alt indique la structure conditionnelle if. Cette condition va permettre d'afficher la page de vote dans laquelle l'électeur sélectionne un candidat et confirme la transaction dans une fenêtre MetaMask affiché par le système si seulement si le vote est lancer, l'électeur n'a pas déjà voté et le compte est valide, sinon le système affiche la page des résultats.

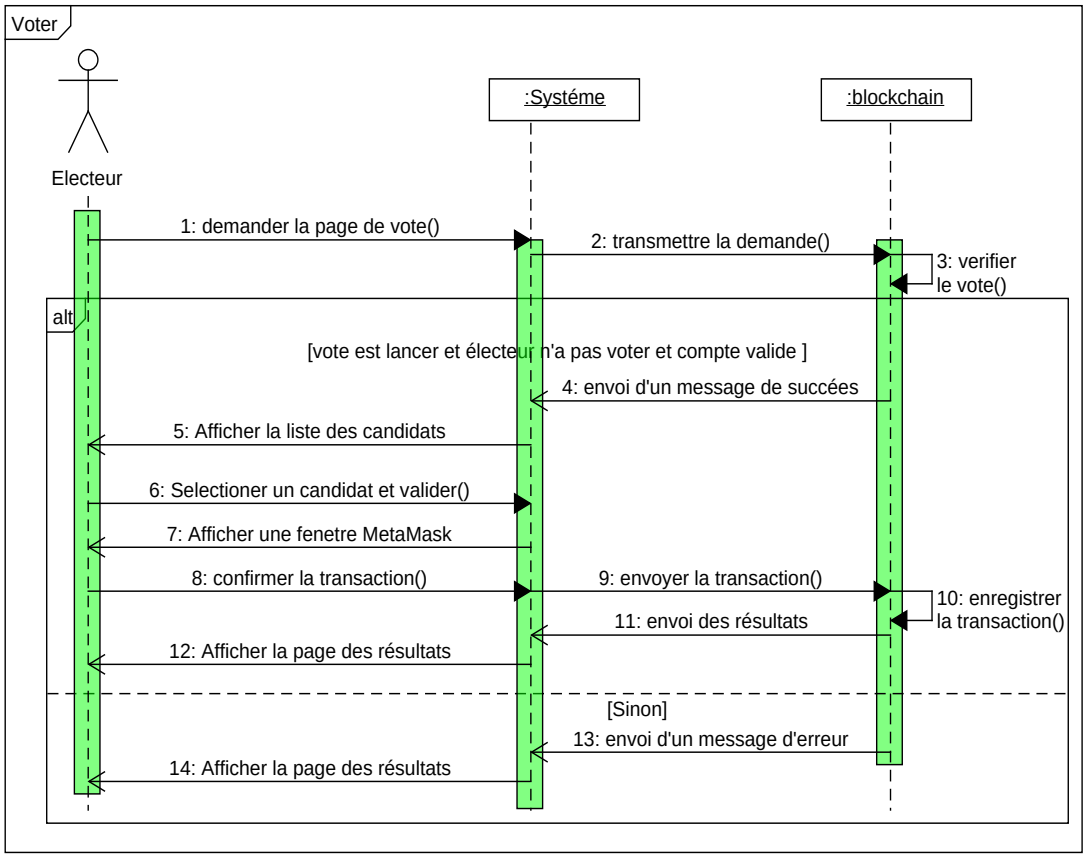

FIGURE 4.7 – Diagramme de séquence « Voter ».

4.7 Diagramme des classes

4.7.1 Dictionnaire des données

Le figure ci-dessous (figure 4.8) représente la liste des attributs composants toutes les classes formants notre système ainsi que leurs descriptions, leurs types et leurs tailles.

N°	Attribut	Description	Type	Taille
1	Id	Identifiant d'une personne (électeur ou administrateur ou candidat).	Entier	255
2	Nom	Le nom d'une personne (électeur ou administrateur ou candidat).	Chaine de caractères	50
3	Prenom	Le prénom d'une personne (électeur ou administrateur ou candidat).	Chaine de caractères	50
4	NumeroCarteVote	Numéro de carte de vote d'un électeur ou d'un administrateur.	Entier	100
5	Compte	Compte d'une personne (électeur ou administrateur ou candidat).	Chaine de caractères	50
6	Clé	Clé du compte d'une personne (électeur ou administrateur ou candidat).	Chaine de caractères	50
7	Identifiant	Identifiant d'un administrateur.	Chaine de caractères	50
8	MotDePasse	Mot de passe de l'administrateur.	Chaine de caractères	8
9	nbrVote	Nombre d'électeur qui ont voté sur un candidat.	Entier	N
10	idVote	Identifiant du vote	Entier	255
11	Date	La date ou la session du vote.	Date	
12	Type	Présidentielle ou législative ou locale.	Chaine de caractères	50

FIGURE 4.8 – Dictionnaire de données.

4.7.2 Représentation des classes

La figure ci-dessous (figure 4.9) représente les classes ainsi leurs méthodes et leurs attributs.

N°	Nom Classe	Liste des attributs	Méthodes
01	Administrateur	Id Nom Prenom NumeroCarteVote Compte Clé Identifiant MotDePasse	LancerVote() ConsulterResultat() AjouterElecteur() AjouterCandidat() Voter()
02	Candidat	Id Nom Prenom Compte Clé nbrVote()	ConsulterResultat() Voter()
03	Electeur	Id Nom Prenom NumeroCarteVote Compte Clé	Voter() ConsulterResultat()
04	Vote	idVote Date Type	/
05	Personne	Id Nom Prenom Compte Clé	ConsulterResultat() Voter()

FIGURE 4.9 – Représentation des classes.

4.7.3 Représentation des associations

— **Ajouter :** entre Candidat et Electeur (Figure 4.10).

Association	Cardinalité	Désignation
Voter	1 0..*	Un électeur vote sur un et un seul candidat Un candidat a été voté zéro ou plusieurs fois par des électeurs

FIGURE 4.10 – Représentation des associations

— Diagramme des classes :

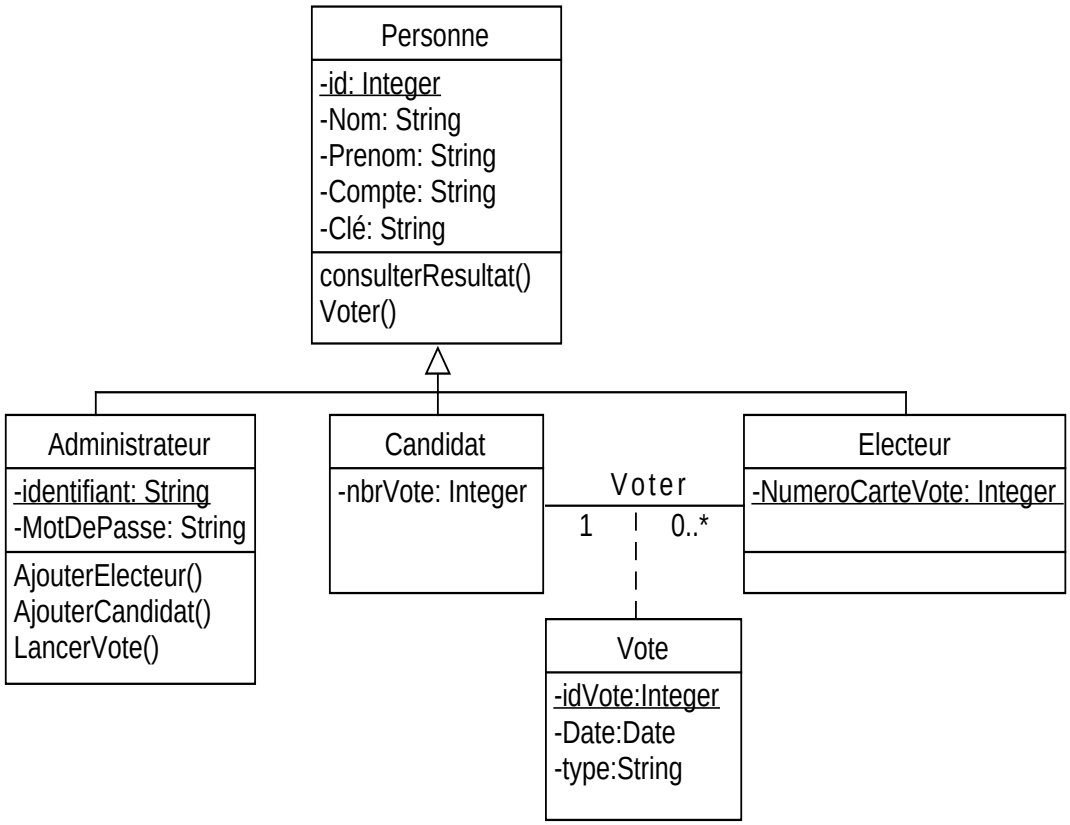

FIGURE 4.11 – Diagramme des classes général.

4.8 Conclusion

Au cours de ce chapitre, nous avons montré le principe de fonctionnement et les relations qui existent entre les différents acteurs et leurs interactions avec le système.et nous avons pu concevoir une application pour le vote en s'adaptant sur les diagrammes du formalisme UML à savoir le diagramme de cas d'utilisation, le diagramme de séquence et le diagramme de classe.

Dans le chapitre suivant nous allons présenter les outils de développement ainsi les interfaces réalisées.

Chapitre 5

Réalisation de l'application vote en ligne

5.1 Introduction

Après avoir élaboré la conception de notre application, nous exposons la phase de réalisation. En premier lieu, nous spécifierons Les outils, les langages et les techniques utilisés dans les deux parties de notre application après nous décrivons quelques interfaces des deux parties implémentées en utilisant quelques scenarios d'utilisation.

5.2 Outils de développement et langages utilisés

Les outils utilisés pour la réalisation de la première partie de notre application concernant la récupération des comptes de portefeuille Metamask :

XAMPP : Un logiciel open source développé par Apache Friends . Le progiciel XAMPP contient des distributions Apache pour le serveur Apache, MariaDB, PHP et Perl. Et c'est essentiellement localhost ou un serveur local. Ce serveur local fonctionne sur votre propre ordinateur de bureau ou portable. L'utilisation de XAMPP consiste à tester les clients ou votre site Web avant de le télécharger sur le serveur Web distant. Ce logiciel serveur XAMPP vous offre l'environnement approprié pour tester les projets MYSQL, PHP, Apache et Perl sur l'ordinateur local [86].

Sublime text 3 : est un éditeur de texte (beta) qui peut servir pour coder en quelques langages que ce soit du moment qu'on enregistre le fichier sous le bon format[87].

Les outils utilisés pour la réalisation de la deuxième partie concernant le vote :

Ganache : permet de créer une blockchain Ethereum pour que vous puissiez exécuter des tests, exécuter des commandes et inspecter l'état tout en contrôlant le fonctionnement de la chaîne. Il vous donne la possibilité d'effectuer toutes les actions que vous feriez sur la chaîne principale sans le coût . De nombreux développeurs l'utilisent pour tester leurs contrats intelligents pendant le développement. Il fournit des outils pratiques tels que des contrôles d'exploration avancés et un explorateur de blocs intégré [88].

Grace à ganache nous pouvons avoir 10 comptes Ethereum avec une balance de 100 ether (du faux ether) pour chaque compte et même il nous permet d'examiner tout ce qui ce passe dans cette blockchain c'est pourquoi que nous l'avons choisi.

Remarque : Pour installer ganache il faut avoir

1. un processeur de 64 bits.
2. système d'exploitation Windows 10 .

Metamask est un portefeuille de crypto qui peut être utilisé sur les navigateurs Chrome, Firefox. C'est aussi une extension de navigateur. Il fonctionne comme un pont entre les navigateurs normaux et la blockchain Ethereum.il est Accessible à tous, son but premier est de rendre le développement d'applications décentralisées plus simple [89].

Truffle est un Framework permettant aux développeurs de lancer un projet de contrat intelligent en un clic et vous fournit une structure de projet, des fichiers et des répertoires qui facilitent le déploiement et les tests [90].

Nous avons choisi truffle parcequ'il est puissant et il nous facilite l'interaction avec notre smart contract.

Remarque : Il est nécessaire d'installer NodeJS sur la machine, puis Truffle par la commande suivante : **npm install -g truffle**.

Node.js : Un environnement d'exécution côté serveur open source basé sur le moteur JavaScript V8 de Chrome. Il peut être utilisé pour créer différents types d'applications telles que les applications Web, les applications de chat en temps réel... [91].

Remarque : Pour développer des smart contracts ,nous devons configurer notre environnement par l'installation de Node Package Manager(NPM), fourni avec Node.js.

Remix : Un outil open source puissant qui vous aide à rédiger des contrats Solidity directement depuis le navigateur. Écrit en JavaScript, Remix prend en charge à la fois l'utilisation dans le navigateur et localement[92].

Nous avons choisi Remix car [93] :

- Il est très pratique et très pertinent pour apprendre à coder sur Solidity
- On y accéde juste par navigateur et il n'y a rien à installer
- On dispose automatiquement des dernières versions de Solidity
- Il permet de compiler et d'exécuter les smart contracts instantanément, dans toutes sortes de blockchains, c'est à dire qu'on peut déployer dans la vrai blockchain Ethereum un smart contract directement depuis Remix, mais il peut aussi se connecter à une blockchain locale comme Ganache. Il est donc trés souple et flexible.

Bootstrap : Bootstrap est un framework front-end open source avec lequel vous pouvez créer des sites Web. Le framework a été lancé à 2012 par un concepteur et développeur sur Twitter. Il contient des modèles de conception (typographie, formulaires, boutons, tableaux, etc.) basés sur CSS et HTML. Bootstrap est très souvent utilisé dans la conception de sites Web qui ont un design Web réactif afin de pouvoir afficher des pages Web sur l'ordinateur, la tablette et le smartphone [94].

JavaScript : Un langage informatique utilisé sur les pages web. Ce langage est considéré comme un langage côté client, en d'autres mots c'est votre ordinateur qui va recevoir le code et qui devra l'exécuter. C'est en opposition à d'autres langages qui sont activé côté serveur comme les scripts PHP. L'exécution du code est effectuée par votre navigateur internet tel que Firefox ou Internet Explorer[95].

Web3.js : Il s'agit d'une collection de bibliothèques qui vous permettent de développer des clients qui interagissent avec l'ethereum blockchain et effectuer des actions comme envoyer Ether d'un compte à un autre, lire et écrire des données à partir de contrats intelligents, créer des contrats intelligents, et bien plus encore [96].

Remarque : Pour installer Web3.js taper la commande suivante : **npm install web3**.

Solidity : Langage de programmation orienté objet, il a été développé par les principaux contributeurs de la plateforme Ethereum. Il est utilisé pour concevoir et mettre en œuvre des contrats intelligents au sein de la plate-forme virtuelle Ethereum et de plusieurs autres plates-formes blockchain [97].

Solidity est de type statique, prend en charge l'héritage, les bibliothèques et les types complexes définis par l'utilisateur, entre autres fonctionnalités [97].

PHP : PHP signifie Hypertext Preprocessor ,C'est un langage de script open source, côté serveur il est utilisé pour la création ded pages Web dynamique, Il peut être intégré facilement au HTML [98].

5.3 Arborescence de l'application

La figure 5.1 ci-dessous, représente une arborescence de l'application vote en ligne.

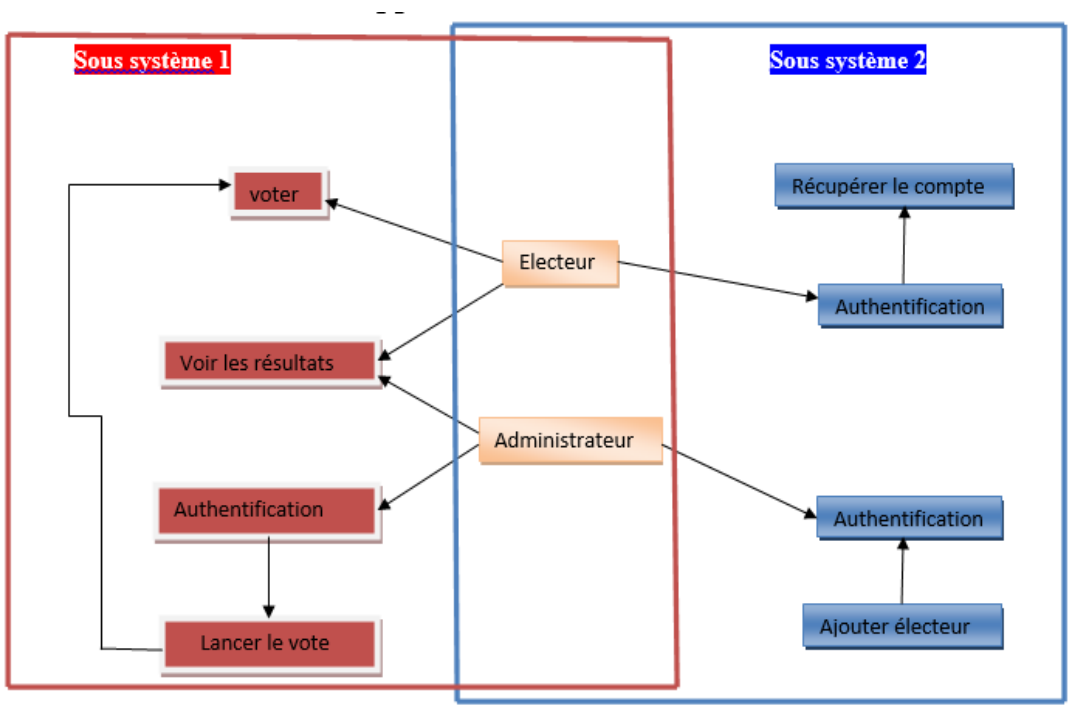

FIGURE 5.1 – Arborescence de l'application vote en ligne.

5.4 Configuration d'environnement

Nous allons d'abord créer un répertoire qui va contenir les fichiers de notre projet comme ceci :

$ mkdir election

$ cd election

Maintenant que nous sommes dans notre dossier, nous voulons être rapidement opérationnels avec un projet de truffes déjà existant. Donc, dans le dossier élection, exécutez la commande ci-dessous

$ truffle unbox pet-shop

Après que les dépendances sont installées, examinons la structure de répertoire de projet que nous venons de créer (Figure 5.2).

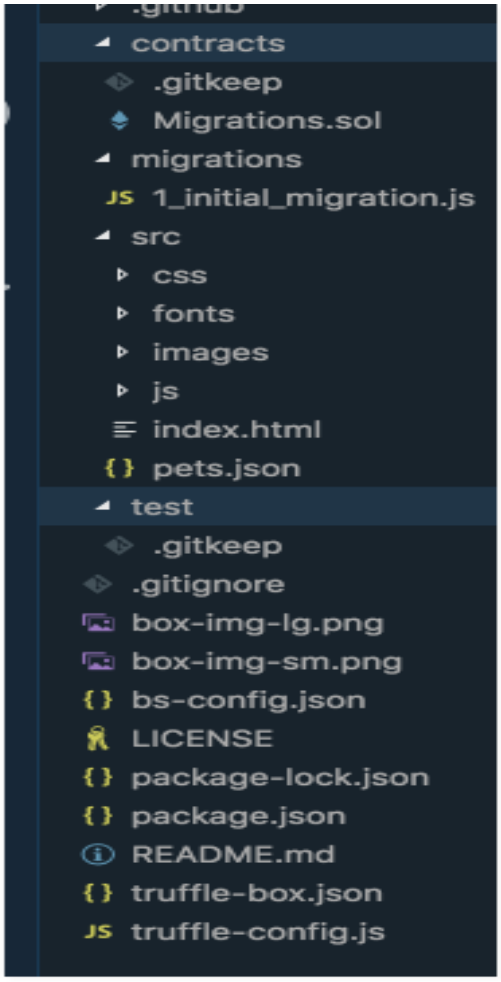

FIGURE 5.2 – Structure de répertoire election.

Répertoire des contrats : c'est ici que nous conserverons tous nos contrats intelligents. Vous pouvez déjà voir que nous avons un contrat de migration à l'intérieur qui gère nos migrations vers la blockchain.

Répertoire des migrations : c'est là que vivent tous les fichiers de migration. Chaque fois que nous déployons des contrats intelligents sur la blockchain, nous mettons à jour l'état de la blockchain et avons donc besoin d'une migration.

Répertoire node_modules : c'est le répertoire de toutes nos dépendances Node.

Répertoire src : c'est ici que nous développerons notre application côté client.

Répertoire de test : c'est ici que nous allons écrire nos tests pour nos contrats intelligents.

Fichier truffle-config.js : il s'agit du fichier de configuration principal de notre projet Truffle.

Fichier truffle-box.json : ce fichier contient des commandes pouvant être utilisées dans le projet.

5.5 Présentation des interfaces de développement

Dans ce qui suit nous avons choisi d'illustrer quelques interfaces de notre application :

5.5.1 Présentation des interfaces pour la récupération des comptes

Interface principale pour la récupération des comptes

La figure 5.3 représente l'interface principal de notre plateforme dédie aux utilisateurs. Elle offre la possibilité d'accéder aux différents espaces.

Figure 5.3.1 : interface principale.

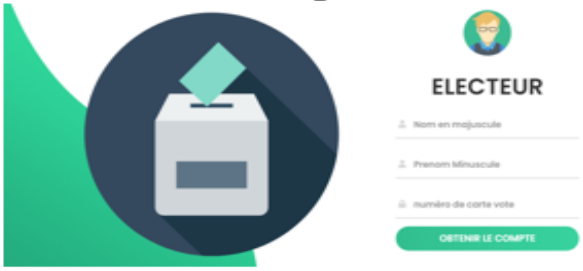

Figure 5.3.2 : espace électeur

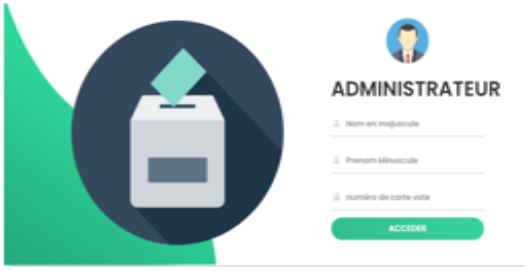

Figure 5.3.3 : espace administrateur.

FIGURE 5.3 – Interface principale pour la récupération des comptes.

Espace d'électeur

Avant toute action, l'électeur doit passer par l'étape d'authentification qui consiste à saisir ses informations (Figure 5.4.1), pour qu'il puisse récupérer son compte Metamask (Figure 5.4.2).

Figure 5.4.1 : authentification d'électeur.

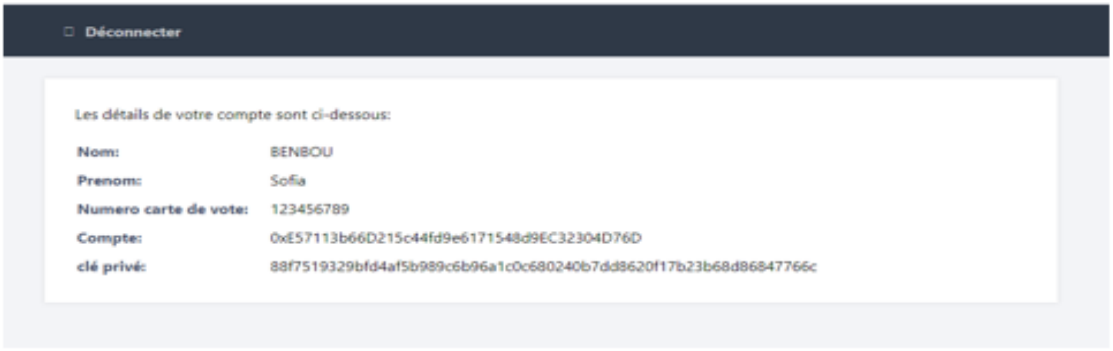

Figure 5.4.2 : récupération du compte.

FIGURE 5.4 – Espace électeur.

Espace administrateur

Après avoir passé par l'étape d'authentification (Figure 5.5.1), l'administrateur a la possibilité d'ajouter un électeur (Figure 5.5.2), donc s'il a rempli les informations pour ajouter l'électeur , il peut passer soit vers la (Figure 5.5.3)qui indique que l'enregistrement est fait avec succès ,soit vers la (Figure 5.5.4)pour indiquer que l'électeur n'est pas ajouté .

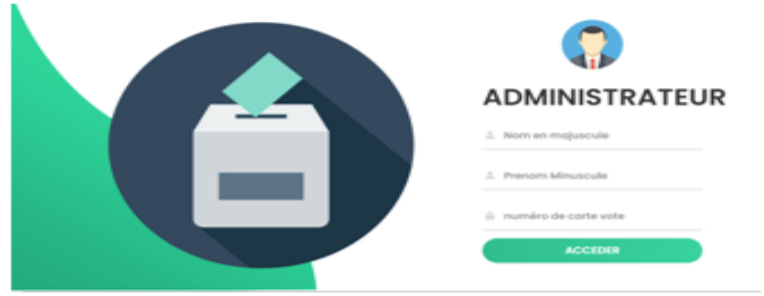

Figure 5.5.1 : authentification d'administrateur.

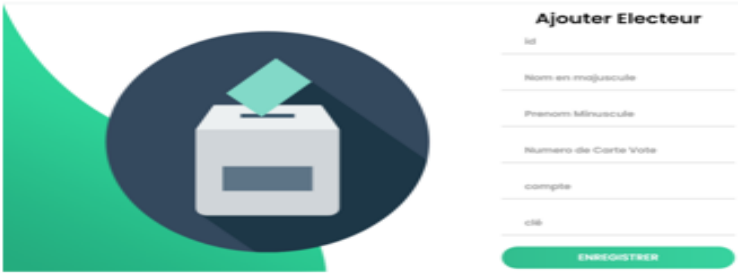

Figure 5.5.2 : ajouter un électeur.

Figure 5.5.3 :l'ajout est fait avec succès.

Figure 5.5.4 :l'ajout n'est pas fait Succès.

FIGURE 5.5 – Espace administrateur.

5.5.2 Présentation des interfaces pour le vote

Interface Connexion à la blockchain

L'électeur doit se connecter à la blockchain en utilisant l'extension «MetaMask» (figure 5.6.1) puis importer le compte (figure 5.6.2) qui a été récupérer de site précédant.

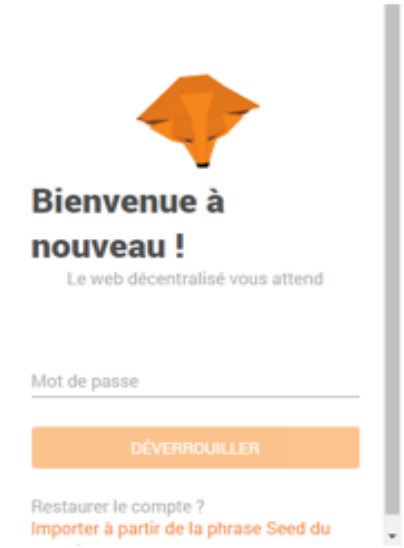

Figure 5.6.1 : connecter à MetaMask.

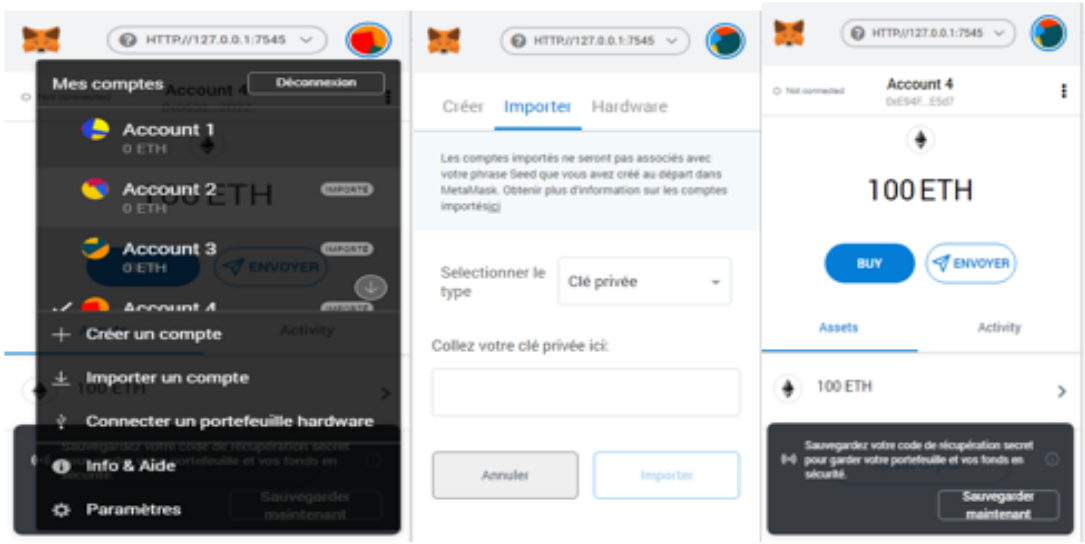

Figure 5.6.2 : importer le compte.

FIGURE 5.6 – Connexion à la blockchain

Interface principale de vote

La figure 5.7 représente l'interface principal de notre plateforme de vote dédie aux utilisateurs. Elle lui offre la possibilité d'accéder aux différents espaces.

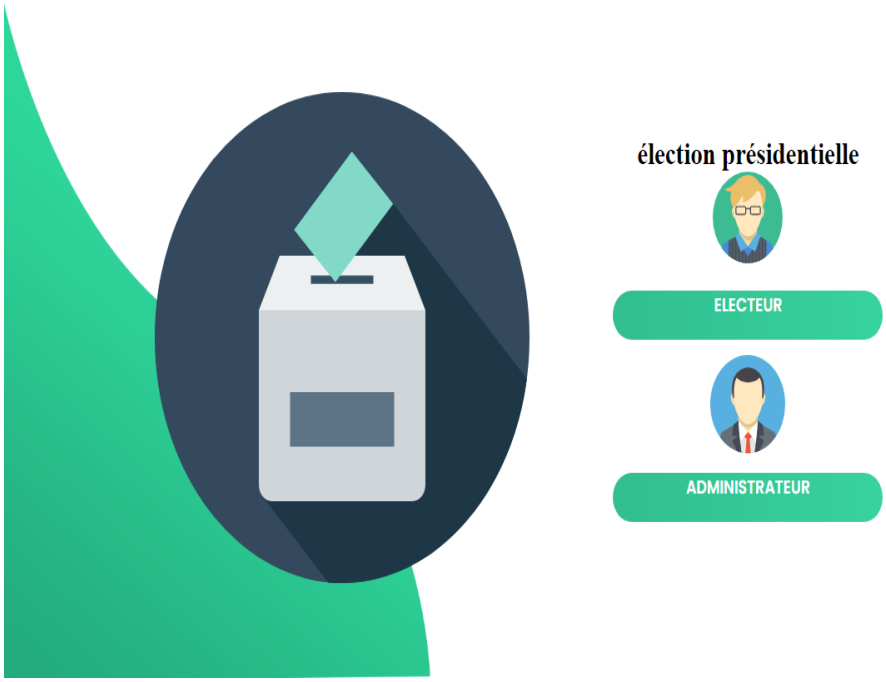

FIGURE 5.7 – Interface principale de vote.

Espace administrateur

La figure 5.8 montre que l'administrateur doit passer par l'étape d'authentification qui consiste à saisir ces informations (Figure 5.8.1), pour qu'il puisse soit lancer le vote ou voir les résultats (Figure 5.8.2).

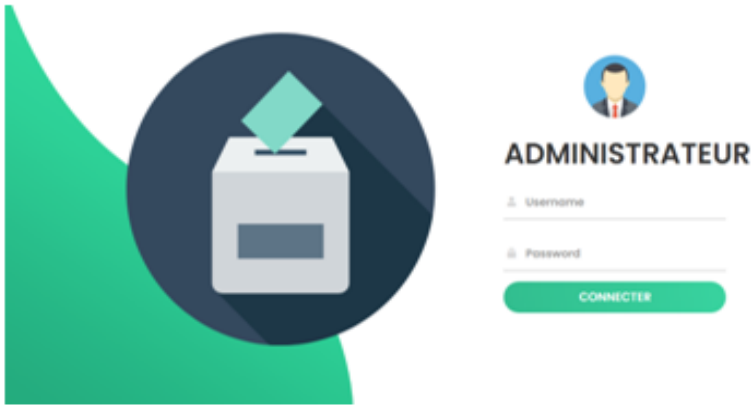

Figure 5.8.1 : authentification d'administrateur.

Figure 5.8.2 : les fonctionnalités de l'administrateur.

FIGURE 5.8 – Espace administrateur.

Espace électeur

Lorsque l'électeur accède à son espace le système va vérifier si le compte Metamask est autorisé pour voter (Figure 5.9.1).

Si le compte est autorisé l'électeur va recevoir une listes des candidats et après avoir choisi le candidat en cliquant sur le bouton du vote, une transaction est initialisée vers la fonction vote de notre smart contract (Figure 5.9.2).

Après que l'électeur a voté le bouton est caché et sa voix est affichée, il peut voir le total des voix pour chaque candidat (Figure 5.9.3).

Figure 5.9.1 : vérification de compte Metamask.

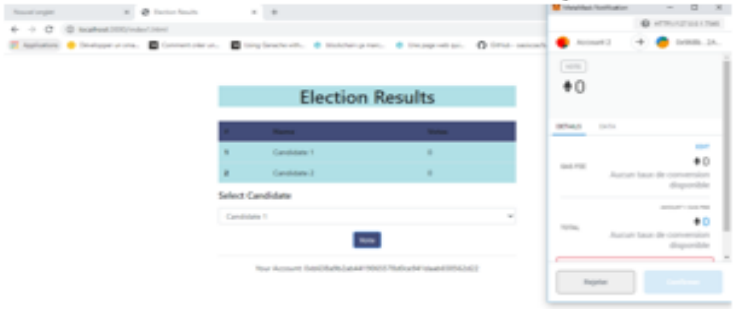

Figure 5.9.2 : voter pour un candidat.

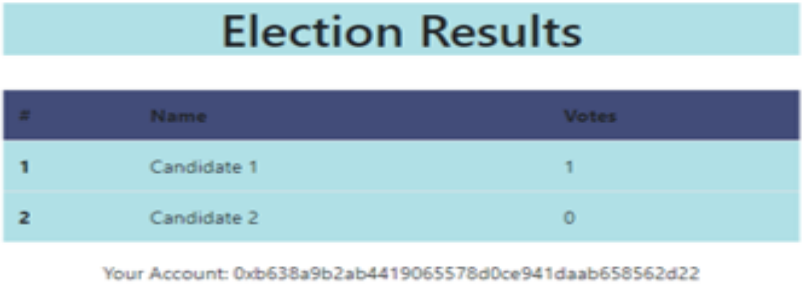

Figure 5.9.3 : voir les résultats.

FIGURE 5.9 – Espace électeur.

Transactions (Ganache)

Chaque vote est sous forme de transaction, chaque transaction est écrite dans la blockchain de façon permanente et immutable, voici à quoi ressemble les transactions du déroulement précédent (Figure 5.10) :

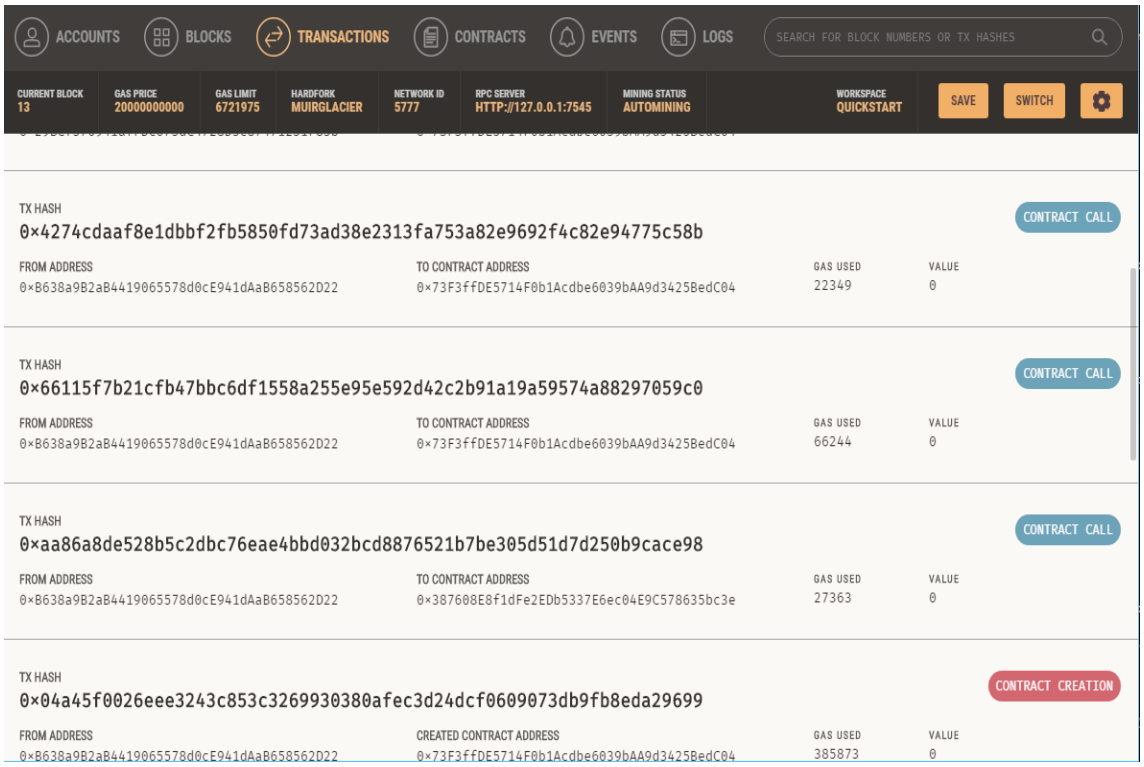

FIGURE 5.10 – Transactions (Ganache).

5.6 Comparaison des solutions de vote

La solution du Rajat Biswas avait juste limité le nombre de vote pour une seule fois, par contre La solution Dappuniversity dispose d'une interface interactive simple mais sans identification des citoyens et même les candidats n'ont pas le droit de voter [99, 100].

Après avoir vu les fonctionnalités des solutions précédentes, nous avons mis en place un système avec une interface conviviale, qui a une fonction d'identification des citoyens, et qui permet même au candidats de voter.

Le tableau ci-dessus (tableau 5.1) représente une comparaison entre les solutions décentralisées de vote électronique existant sur Github et le système que nous avons développé :

Fonctionnalité	**Notre solution**	**La solution du Dappuniversity**	**La solution du Rajat Biswas**
Interface d'interaction	Oui	Oui	Non
Identification des citoyens	Oui	Non	Non
Limiter le nombre de vote à 1	Oui	Oui	Oui
Gestion du temps	Oui	Non	Non
Un candidat est un électeur et peut voter	Oui	Non	Non

TABLE 5.1 – Comparaison des solutions de vote.

5.7 Conclusion

Dans ce chapitre, nous avons présenté le côté implémentation de notre projet en spécifiant les outils, les langages et l'environnement de développement ainsi que les interfaces les plus significatives de notre application à travers un ensemble des captures d'écran.

Chapitre 6

Covid-19

6.1 Introduction

Depuis décembre 2019 le monde est secoué par la pandémie du Covid-19 connue sous le nom Coronavirus. Ce nouveau virus se propage à travers le monde on posant beaucoup de dégâts. C'est quoi Covid-19 ? Comment se transmet-il ? Quels sont les symptômes ? Comment se protéger ? Y a-t-il un traitement ? Comment intervient le domaine informatique dans ce problème sanitaire ? Ce sont les questions auxquelles le présent chapitre répond.

6.2 Définition

La maladie à coronavirus 2019, abrégée en Covid-19 (abréviation de COronaVIrus Disease 2019), est une maladie infectieuse émergente de type zoonose virale, causée par le coronavirus SRAS-CoV-2 (Figure 6.1 [39]), responsable de la propagation d'une pandémie qui a commencé en décembre 2019 à Wuhan, capitale de la province du Hubei, Chine centrale [40].

Il est à noter que le Covid-19 peut être «Maladie X», le nom donné par l'Organisation mondiale de la santé en 2018 à une maladie susceptible de provoquer un danger international. En fait, au cours des premiers mois de 2020, le Covid-19, décrit par l'Organisation mondiale de la santé comme une pandémie, s'est propagé à l'échelle mondiale, affectant gravement des pays comme l'Italie, complètement isolés en mars [40].

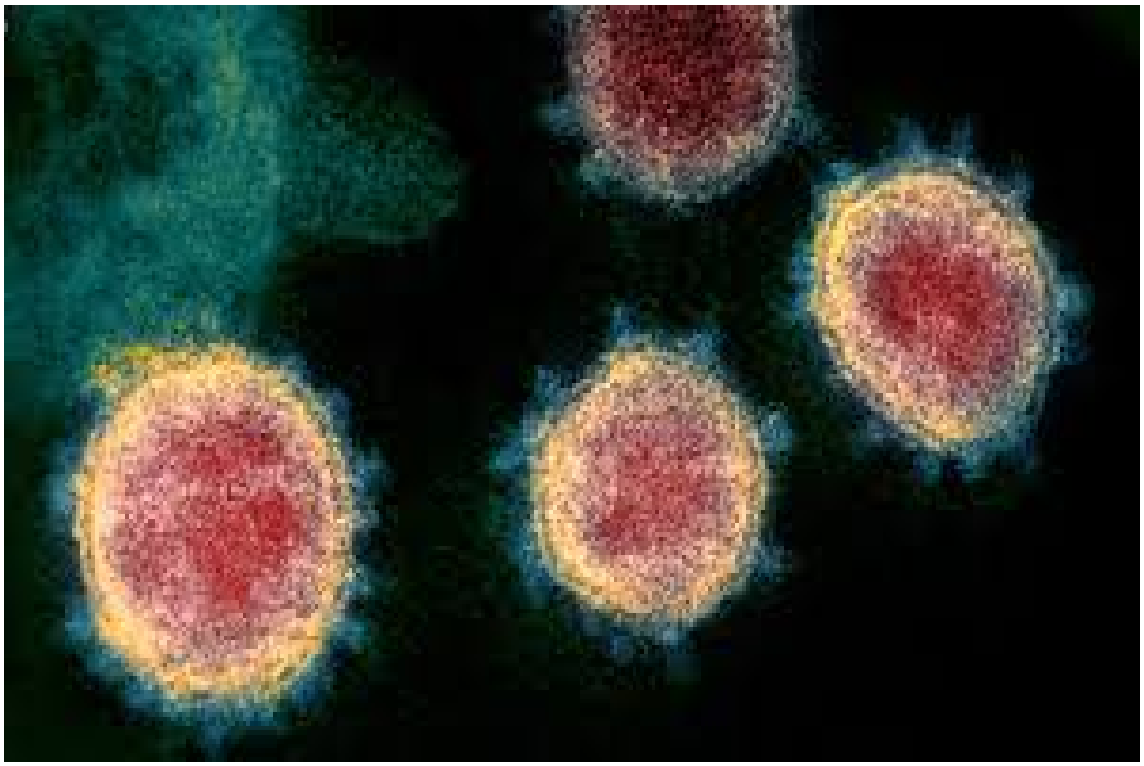

FIGURE 6.1 – Forme microscopique de Covid-19.

6.3 Transmission

La maladie peut être transmise d'une personne à l'autre par des gouttelettes respiratoires expulsées du nez ou de la bouche lors de la toux ou des éternuements. Ces gouttes peuvent être trouvées sur des objets ou des surfaces autour d'une personne infectée, y compris pendant plusieurs heures [41].

Une étude montre que le coronavirus peut résister jusqu'à [42] :

— 3 jours sur du plastique,

— 2 jours sur de l'acier inoxydable,

— 24 heures sur du carton,

— 4 heures sur du cuivre,

— 3 heures après sa projection hors du corps de son hôte dans l'air.

Cependant, ces chiffres doivent être pris avec prudence, car ils dépendent fortement de la quantité pulvérisée [42].

Vous pouvez alors être infecté par le coronavirus si vous touchez ces objets ou surfaces, puis touchez vos yeux, votre nez ou votre bouche. Vous pouvez également attraper le virus corona en inhalant des gouttelettes d'une personne malade qui vient de tousser ou d'éternuer [41].

Mais il n'a pas encore été prouvé que la contamination peut se produire à travers des objets car il est difficile de distinguer comment une personne malade a été infectée. Par conséquent, les contacts personnels antérieurs génèrent la majorité des transmissions du Coronavirus [42].

6.4 Symptômes

Les signes courants d'infection sont [43, 44, 45] :

— la fièvre,
— la toux,
— le nez qui coule,
— une fatigue intense,
— des douleurs musculaires inhabituelles,
— une sensation d'oppression ou d'essoufflement,
— des difficultés respiratoires.

Dans les cas plus graves, l'infection peut provoquer :

— une pneumonie,
— un syndrome respiratoire aigu sévère,
— une insuffisance rénale,
— la mort dans les pire cas.

La maladie reste bénigne dans 80% des cas et les chercheurs estiment le taux global de mortalité due au virus à environ 3,2%. Certains patients contractent également le virus sans symptômes : ils sont porteurs du virus mais sans symptômes [43, 46].

6.5 Traitement

Pour le moment, aucun traitement spécifique n'a été identifié, mais des chercheurs du monde entier ont uni leurs forces dans cette course au traitement et plusieurs essais cliniques ont commencé. Les stratégies sont principalement de deux formes [47] :

— Passer les tests virologiques (RT-PCR) ou les tests sérologiques pour identifier les personnes malades avec covid-19.

— Utilisation de médicaments sur le marché qui ont fait leurs preuves contre d'autres virus (VIH, Ebola, etc.).

La chloroquine est l'un des médicaments les plus prometteurs discutés à ce moment de la pandémie. Ce médicament antipaludique, connu depuis très longtemps, sera une méthode de recherche prometteuse dans la lutte contre Covid-19. Cependant, l'efficacité de la chloroquine, qui a été développée par les équipes du professeur français Didier Raoult, pour traiter les individus infectés par Covid-19 est au cœur de la polémique mondiale. Malgré les avertissements de l'Organisation mondiale de la santé, de nombreux pays, dont l'Algérie, ont choisi d'utiliser la chloroquine comme traitement contre le virus Corona [48, 49].

La controverse sur l'utilisation de la chloroquine pour traiter le coronavirus n'a pas diminué. Le professeur Raoult a continué à préconiser l'utilisation de ce traitement, et en a profité pour dénoncer les critiques de son protocole. L'Agence européenne des médicaments (EMA), pour sa part, a mis en garde contre les effets secondaires potentiels associés à la prise de chloroquine, et jusqu'à présent aucune étude n'a prouvé les effets bénéfiques du médicament. Le communiqué de presse en ligne de l'EMA déclare : «Des études récentes ont rapporté des problèmes de rythme cardiaque graves, voire mortels, avec la chloroquine et l'hydroxychloroquine, en particulier à fortes doses ou avec l'azithromycine. [50].

Des problèmes de foie, de reins et de cellules nerveuses peuvent également survenir. Et l'Agence européenne des médicaments n'est pas la seule à remettre en question l'efficacité de l'hydroxychloroquine dans le traitement du virus Corona. Une première étude américaine, portant sur 368 patients admis dans les hôpitaux publics pour vétérans américains, a montré que le taux de mortalité était de 11% dans le groupe témoin contre

28% dans le groupe hydroxychloroquine seule et 22% dans le groupe hydroxychloroquine-azithromycine. En conséquence, la mortalité augmente avec l'utilisation du traitement [50].

D'autres chercheurs tentent également de repositionner les médicaments déjà en place, pour voir s'ils peuvent agir contre Covid-19 [48].

Quant aux vaccins, les chercheurs se sont également lancés dans une course effrénée. Plus de cinquante projets de recherche ont été mis en place dans le monde [48].

6.6 Prévention

Jusqu'à présent, il n'y a pas de vaccin, encore moins de traitement complet, contre le coronavirus. Pour éviter de propager des virus, vous devez suivre ces petites étapes (Figure 6.2 [45]) qui offrent une excellente protection [43, 44, 45, 51] :

- Lavez-vous fréquemment les mains avec de l'eau et du savon pendant au moins 20 secondes, surtout après être allé aux toilettes, avant de manger et après s'être mouché, tousser ou éternuer. Un gel aqueux à base d'alcool peut également être utilisé.
- Évitez de vous toucher les yeux, le nez et la bouche avec des mains non lavées, car ce sont les canaux les plus susceptibles de contracter le virus.
- N'oubliez pas de vous couvrir la bouche et le nez lorsque vous toussez ou éternuez (le pli du coude peut être utilisé). Vous devez immédiatement jeter le mouchoir dans une litière fermée et vous laver les mains pour éviter la propagation de virus et autres agents pathogènes.
- Éviter autant que possible tout contact étroit avec des personnes malades. Une distance de plus d'un mètre peut être une bonne caractéristique.
- Se saluer sans se serrer la main plutôt que de s'embrasser.
- Ne pas prêter les objets de la vie quotidienne tels sa brosse à dents, ses couverts, son téléphone, ...
- Nettoyez et désinfectez les objets et les surfaces fréquemment touchés.
- Restez à la maison du travail ou de l'école jusqu'à ce que vous soyez exempt de fièvre, de signes de fièvre et de tout autre symptôme pendant au moins 24 heures et

sans utiliser de médicaments contre la fièvre ou d'autres médicaments modifiant les symptômes et portez un masque chirurgical jetable en présence d'autres personnes.

— Consultez un médecin si vous avez des raisons de croire que vous avez été exposé au coronavirus ou à la grippe. Appelez votre professionnel de la santé avant de visiter un établissement de santé.

— Utilisation de la politique de capture et d'isolement des cas suspects.

— Le confinement.

— Augmentation de la demande dans les secteurs des soins.

— La diminution des voyages.

FIGURE 6.2 – Gestes à suivre pour se protéger.

6.6.1 Confinement

La recherche des contacts et l'isolement des cas sont une intervention courante pour contrôler les épidémies de maladies infectieuses et ont été utilisées pour la maladie à coronavirus 2019. Cela peut être efficace mais peut nécessiter des efforts de santé publique et une coopération importants pour y parvenir. Contrôle efficace de toutes les communications [52].

Le confinement et L'isolement partiel reste le meilleur moyen de limiter la propagation du Covid-19 car il réduit le nombre de contacts et donc le nombre de personnes contaminées. Le confinement n'a pas vraiment sa raison d'être. Par contre, dans les villes où le virus circule, le confinement s'impose pour pouvoir rompre la chaîne de transmission [53].

6.6.2 Maladies chroniques et Covid19

Les études réalisées jusqu'à maintenant montrent qu'une forte proportion des patients atteints de la Covid-19 sont affectés par une condition de santé précaire. À Wuhan en Chine, par exemple, une étude a révélé que chez les patients atteints des formes plus sévères de la maladie et qui ont été admis aux soins intensifs, 58% souffraient d'hypertension, 25% de maladies cardiovasculaires et 22% de diabète de type 2. La contribution de ces maladies chroniques préexistantes à la sévérité de la Covid-19 est particulièrement frappante en Italie, un des pays les plus durement touchés par le coronavirus : une analyse récente révèle que 99% des personnes décédées de cette maladie présentaient au moins un problème de santé chronique, les plus fréquentes étant l'hypertension (76%), le diabète de type 2 (36%), les maladies coronariennes (33%), la fibrillation auriculaire (25%) ou le cancer (20%) [54].

La comparaison des taux de mortalité de la Covid-19 illustre bien l'énorme influence des maladies chroniques sur la sévérité de la maladie, avec des augmentations de 5 à 10 fois comparativement aux personnes qui ne présentent pas de pathologies préexistantes [54].

Taux de mortalité de la Covid-19 (%) [54] :

— Aucune : 0,9

— Cancer : 5,6

— Hypertension : 6,0

— Maladie respiratoire : 6,3

— Diabète de type 2 : 7,3

— Maladie cardiovasculaire : 10,5

6.6.3 Evolution de la pandémie dans le monde et en Algérie

Selon le graphe (Figure 6.3), La pandémie de coronavirus Covid-19 a fait jusqu'à vendredi 16/10/2020 au moins 1 096 252 morts (0.015% de la population) dans le monde depuis son apparition en décembre en Chine. Plus de 38 826 134 cas positifs (0.413 de la population) ont été recensé. Le nombre des guérisons a été arrivé à 26 798 435 ce qui représente 0.354 de la population [55].

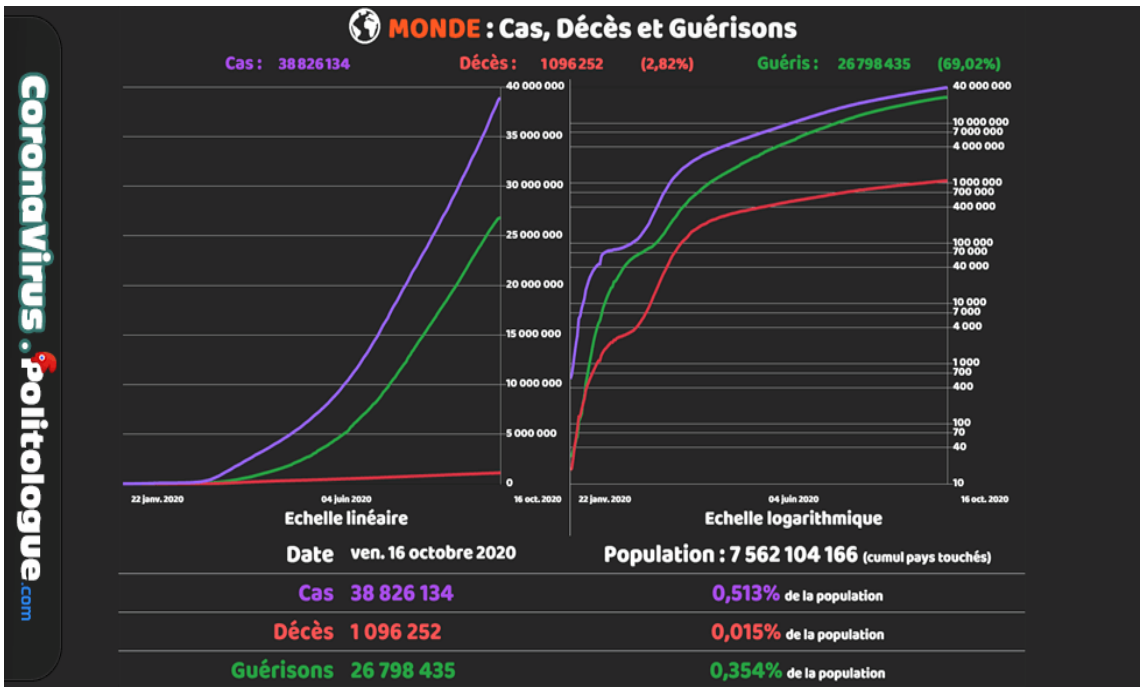

FIGURE 6.3 – Graphe cas, décès et guérisons de Covid-19 dans le monde.

L'Algérie a enregistré selon le graphe (Figure 6.4), le 16/10/2020, 1 841 nouveaux cas confirmés de coronavirus (Covid-19), celui des décès à 53 777 (Figure 6.5) [56].

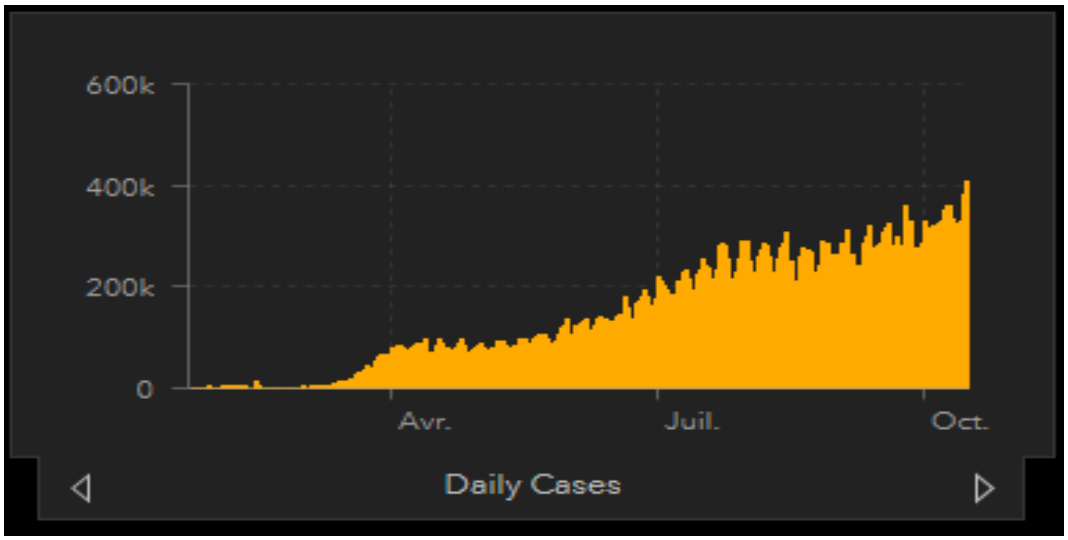

FIGURE 6.4 – Graphe de nombre des cas contaminé par Covid-19 par jour en Algérie.

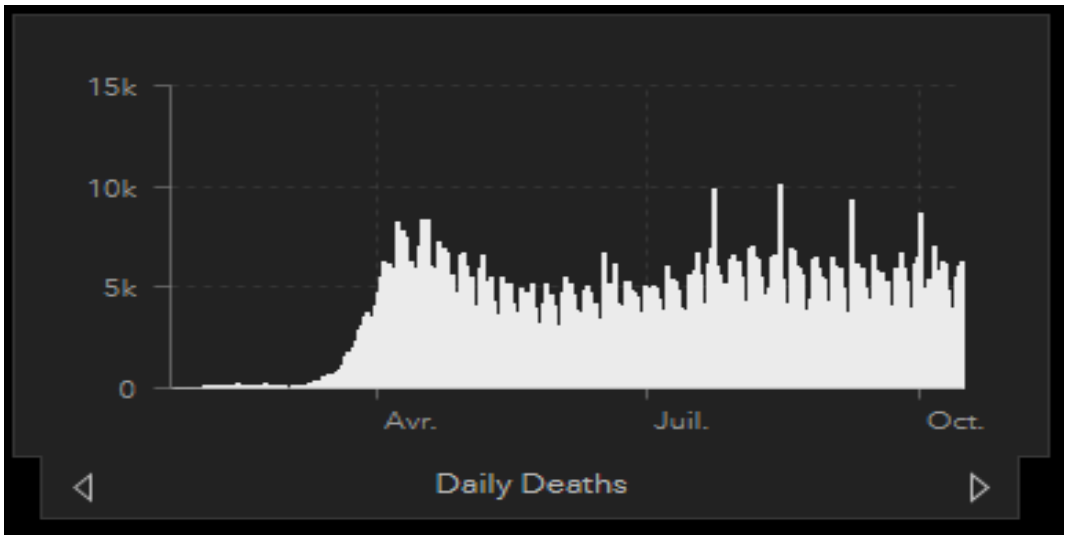

FIGURE 6.5 – Graphe de nombre des décédé par Covid-19 par jour en Algérie.

6.7 Covid-19 et le domaine informatique

L'Organisation nationale de la santé a adopté le confinement comme solution pour freiner la propagation du virus, mais de nombreuses personnes sont stressées. Et c'est là que le domaine informatique joue un rôle dans ce problème de santé, offrant des sites et des applications de détection et de prévention et même des applications pour réduire au maximum les déplacements vers les lieux publics.

6.7.1 L'application Coronavirus Algérie

Une application officielle pour lutter contre le virus Corona en Algérie [Figure 6.6], vous pouvez l'installer depuis Play Store pour rester informé de l'évolution de la maladie, envoyer des alertes aux structures de santé à proximité si vous développez des symptômes de la maladie, et recevoir des notifications si quelqu'un autour de vous est porteur du virus [57].

FIGURE 6.6 – L'application 'coronavirus Algérie' sur Google Play Store

6.7.2 Site covid-19.sante.gov.dz

Le ministère de la Santé, de la Population et de la Réforme hospitalière, en coordination avec le ministère des Postes et des Télécommunications, a lancé un site Web [Figure 6.7] qui vise à sensibiliser aux dangers du Coronavirus (Covid-19). Disponible en arabe et en français. Ce site contient plusieurs sections auxquelles il est possible de se référer [58].

FIGURE 6.7 – Page principale de site covid-19.sante.gov.dz

6.7.3 Site maladiecoronavirus.fr

Le site maladiecoronavirus.fr [Figure 6.8] référencé par le ministère de la Santé permet à toute personne soupçonnée d'être infectée de passer un "test" anonyme et gratuit : 24 questions sur leurs symptômes (fièvre, toux, inconfort respiratoire, douleurs musculaires ...) mais Toujours dans ses antécédents médicaux, son âge [59].

Grâce à un algorithme développé et mis à jour avec les dernières connaissances scientifiques disponibles, en collaboration avec les professionnels de santé et l'Institut Pasteur, le site vous conseille soit de rester confiné à votre domicile, de consulter votre médecin ou de vous rendre immédiatement au 15 [59].

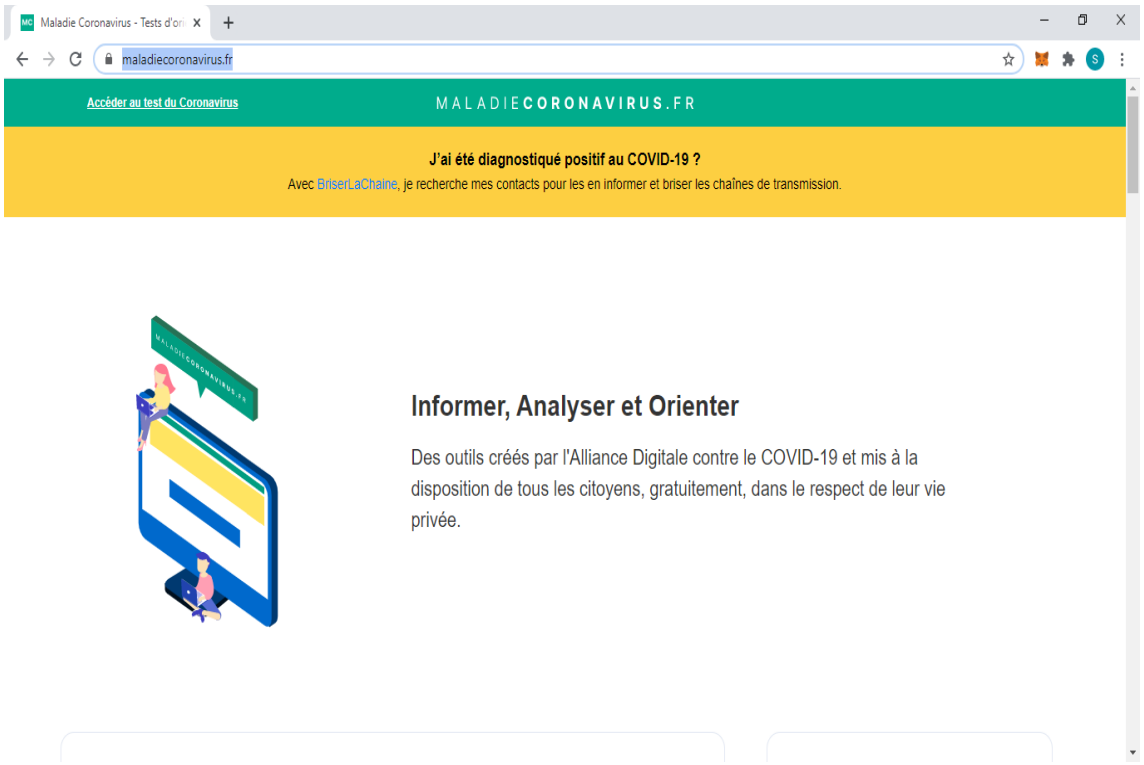

FIGURE 6.8 – Page principale de site maladiecoronavirus.fr

6.7.4 Logiciels de visioconférence

Rien ne peut remplacer un chat ou une réunion physique, mais à un moment où de nombreuses personnes sont confinées et doivent travailler à distance, la visioconférence est la forme de communication la plus proche possible. Vous pouvez utiliser un logiciel de visioconférence gratuit pour cela [60].

Le meilleur logiciel de visioconférence gratuit pour la communication à domicile, par exemple les versions gratuites de Hangouts et U Meeting ou Skype [60].

6.7.5 Télé-enseignement

Le télé-enseignement est une solution pour que la plupart des établissements d'enseignement puissent continuer leurs activités.

L'université de Bouira, comme tant d'autres, ont mis en place un système de formation à distance malgré les contraintes y afférentes. Ce site [Figure 6.9] permet aux étudiants de consulter et télécharger les cours les séries de TD et TP, ainsi de remettre leurs travailles qui seront récupérer par les enseignants [61].

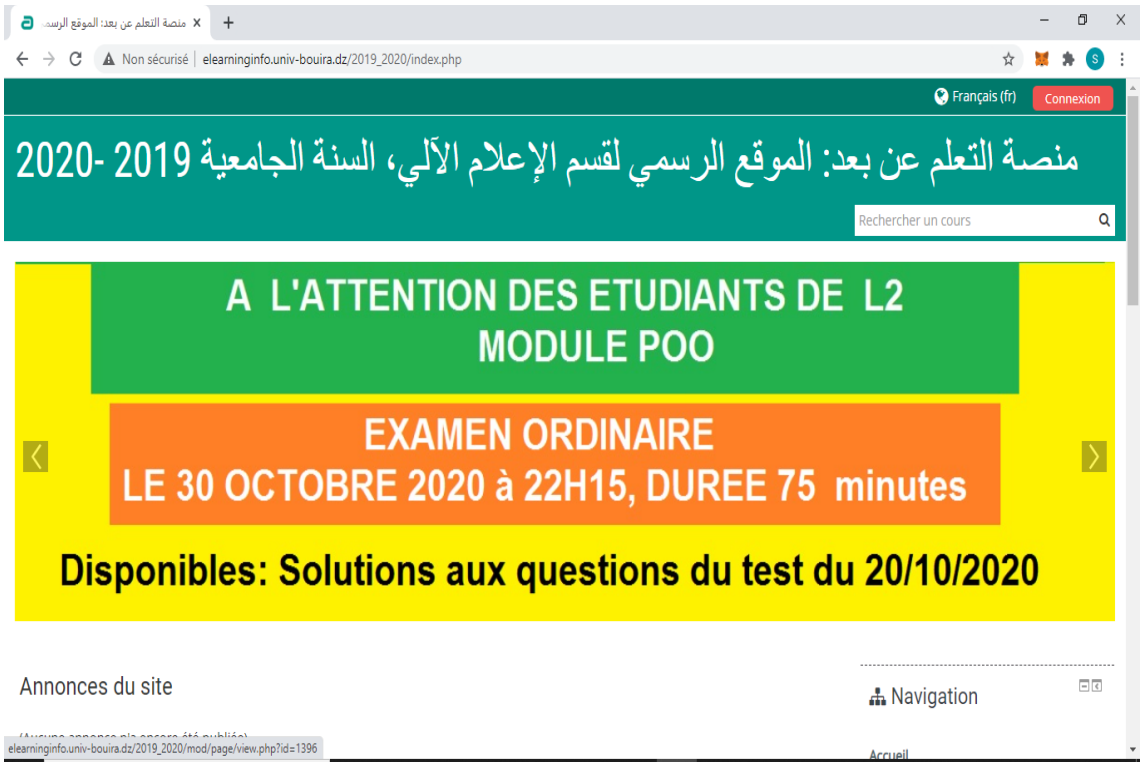

FIGURE 6.9 – Page d'accueil de site elearninginfo.univ-bouira.dz .

6.7.6 Consultation médicale en ligne

La téléconsultation, c'est mettre le patient en contact avec un professionnel de santé, afin de faire place à un véritable conseil médical sans aucune restriction de déplacement. La session se déroule différemment selon la plateforme utilisée : par visioconférence, appel, ou simplement par messagerie instantanée. Comme pour toute consultation classique, le professionnel de santé procède à un examen médical sur les informations fournies par le patient. Le principal avantage de la consultation à distance est qu'il n'y a aucune restriction sur les déplacements. Par conséquent, il fournit du temps réel, ce qui vous évitera de parcourir des kilomètres et de passer de longues heures dans la salle d'attente [62].

Parmi les plateformes utilisées en Algérie pour la téléconsultation on cite la page web Home consulte (https ://www.facebook.com/CanbbHomeConsult/ ?modal=admin_todo_tour) [Figure 6.10] dans laquelle ils publient des vidéos pour la sensibilisation ainsi la possibilité de les contacter par message afin de contacter des professionnels de santé.

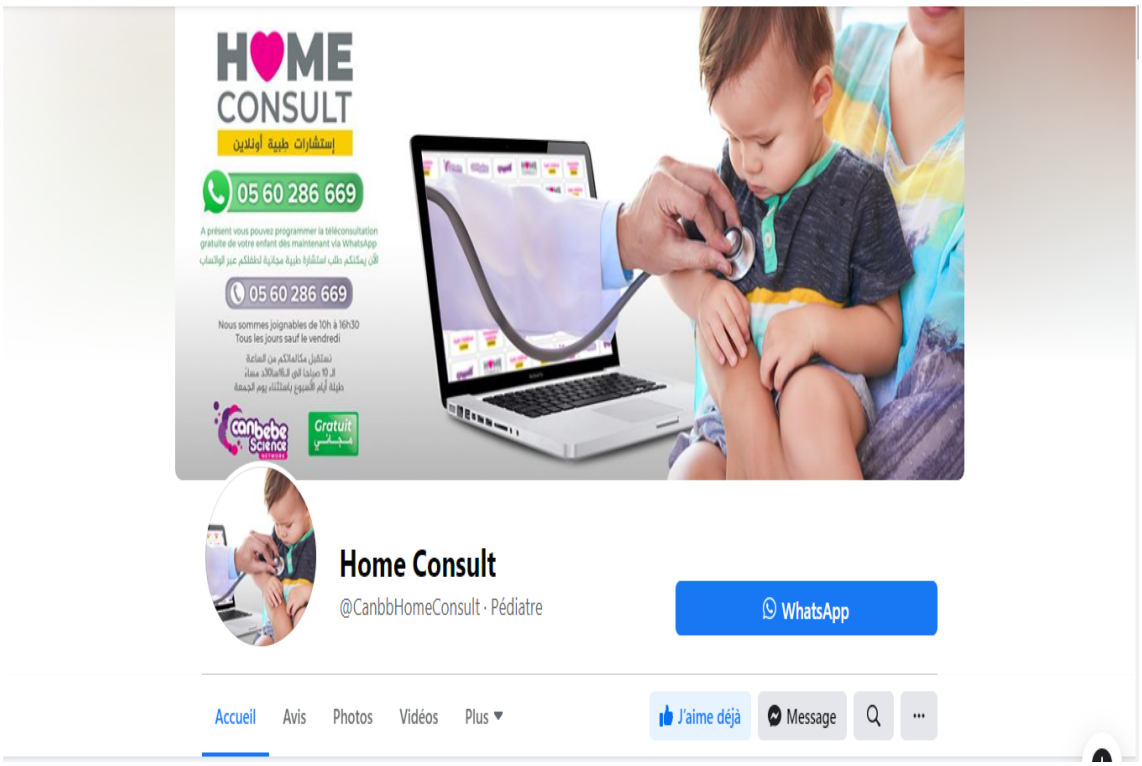

FIGURE 6.10 – Page d'accueil de la page facebook Home consult.

6.8 Travaux de recherches liés à la pandémie de Covid-19 utilisant blockchain

6.8.1 Passeports médicaux numériques de Covid-19 et les certificats d'immunité

Le concept du passeport de santé numérique défini en [63] décrit d'un document immuable qui est authentifié par le ministère de la santé et le ministère des affaires étrangères pour un usage international. Le contrat intelligent du patient contient le hachage des dossiers de vaccination et d'immunisation ainsi que les antécédents médicaux et de voyage d'un individu. Dans le cadre des informations personnelles utilisées dans cette structure, la divulgation des informations est déléguée au propriétaire de l'information.

Les certificats d'immunité : sont prévus pour vérifier qu'une personne a déjà été infectée par Covid-19, a développé les anticorps pertinents et n'est donc pas une menace pour (ne peut pas infecter) d'autres personnes. Par conséquent, ils peuvent être exemptés de restrictions physiques et sociales car ils sont immunisés contre la désinfection[63].

Ce travail permit de retrouver et de suivre les patients pour leurs examens médicaux ainsi que leurs antécédents de voyage. Il a pour but de réduire le stress des employeurs, des services gouvernementaux, des services sociaux et universitaires ainsi que des systèmes de transport dans les pays de l'Union Européenne.

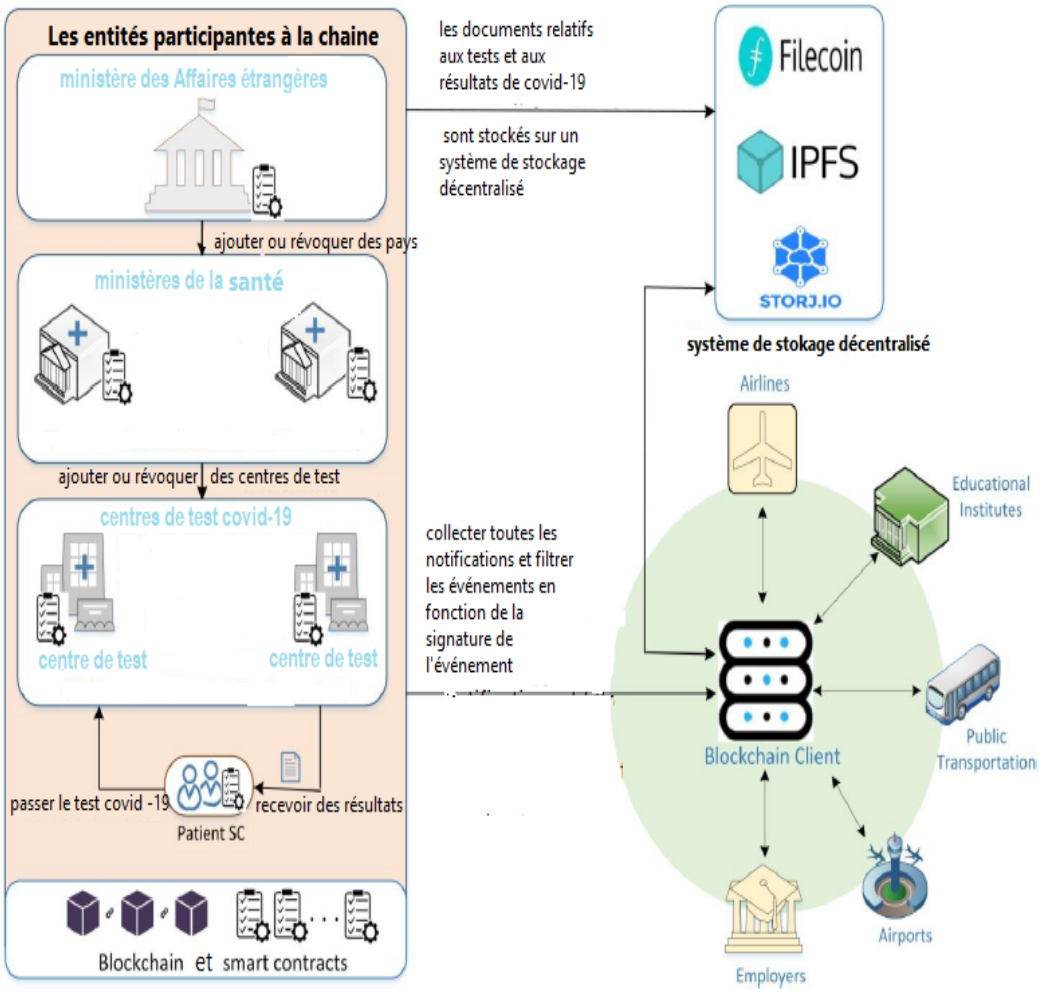

FIGURE 6.11 – Schéma du système complet des passeports médicaux et les certificats d'immunité.

La figure 6.11 [63] présente les entités participant à la chaîne avec différents contrats intelligents, le stockage distribué, les clients de la blockchain et les parties prenantes intéressées. Il existe quatre principaux types de contrats intelligents utilisés dans ce travail : le contrat intelligent du ministère des affaires étrangères, le contrat intelligent du ministère de la santé, le contrat intelligent du centre d'essai Covid-19 et le contrat intelligent du patient.

Le ministère de la santé et le ministère des affaires étrangères sont des parties im-

portantes dans ce travail. Ils représentent les autorités qui veillent à ce que les tests soient légitimes et que les résultats soient tous réels. Chaque centre de dépistage Covid-19 doit être affilié à un ministère de la santé qui est lui-même affilié au ministère des affaires étrangères. Le ministère de la santé peut ajouter des centres de test Covid-19 qui répondent à ses exigences et peut également révoquer un ou plusieurs centres de test Covid-19 précédemment ajoutés. Tout cela se fait en utilisant les événements immuables et les journaux de transactions dans le réseau de la chaîne de blocage.

En outre, un ministère des affaires étrangères peut ajouter des ministères de la santé et les révoquer en fonction de leurs exigences et de leurs règlements. Le ministère des affaires étrangères joue un rôle important dans l'atténuation de la propagation des maladies à travers les frontières et les différents territoires. Il n'affilie que les ministères de la santé qui respectent ses règles et règlements. Cela se fait également par le biais d'événements qui sont communiqués aux entités participantes et aux publics intéressés. Les centres de test Covid-19 affiliés peuvent alors effectuer des tests pour les personnes testées et les patients enregistrés. Les informations biométriques de chaque individu sont associées à leur adresse Ethereum unique sur la chaîne pour préserver la confidentialité.

6.8.2 Test Covid-19 anonyme utilisant le système Epios

De nombreux cas de discrimination sociale, d'abus et de harcèlement sont signalés dans le monde entier pendant la pandémie de Covid-19. Les personnes souffrant des symptômes de Covid-19 sont ciblées pour provoquer la pandémie et sa propagation. Pour éviter une telle discrimination sociale, les hôpitaux ou les laboratoires doivent préserver l'intimité des personnes infectées par Covid-19. Epios [64,65] vise à exploiter la plate-forme blockchain Telos pour faciliter le dépistage anonyme des personnes souffrant de Covid-19. Il permet aux utilisateurs de se connecter de manière transparente avec les laboratoires qui fournissent et traitent les kits de test PCR. Epios assure que le paiement ne peut pas être effectué directement aux laboratoires de traitement des tests. Il exige plutôt que les fournisseurs de kits de test fournissent aux utilisateurs un coupon pour chaque kit de test. En outre, elle protège le coupon par un procédé cryptographique pour aider les laboratoires à vérifier les paiements sans avoir à retracer les kits de test PCR achetés individuellement. En outre, Epios vise à mettre en œuvre une application mobile qui sera utilisée pour acquérir et soumettre les kits de test aux fournisseurs de tests de manière anonyme. Le

projet vise également à partager les données relatives à Covid-19, telles que les résultats individuels de Covid-19 et les statistiques sur les épidémies, avec les chercheurs, le gouvernement et les autorités, tout en garantissant que les références d'une personne ne sont pas divulguées.

6.8.3 Gestion de la fausse infodémie à l'aide de la plateforme MiPasa

L'épidémie de Covid-19 a mis en évidence le besoin urgent d'un système fiable, rapide, transparent et préservant la vie privée, qui devrait résoudre les problèmes liés aux systèmes ad hoc, cloisonnés et non extensibles existants pour lutter contre la pandémie de Covid-19. La vérifiabilité des données liées à Covid-19 peut avoir un impact profond sur la prise de décision dans plusieurs secteurs d'activité à travers le monde. MiPasa [66,67,68] est une plateforme centrée sur une blockchain qui intègre, traite et partage les informations relatives à la propagation du virus Covid-19 provenant de multiples sources vérifiables telles que l'OMS avec les organisations et autorités sanitaires enregistrées. Elle aide les autorités ou les gouvernements à identifier les erreurs humaines et les fausses déclarations, permettant ainsi aux scientifiques et aux responsables de la santé publique de trouver des solutions pour limiter la propagation du virus. MiPasa peut aider les organismes publics à identifier les porteurs du Covid-19 et les points chauds d'infection de manière privée, sécurisée et rapide. De par sa conception, MiPasa est un système entièrement privé qui est mis en œuvre au sommet de la structure de l'hyperlivre. Grâce à des interfaces web, les particuliers et les représentants de la santé publique peuvent utiliser MiPasa pour télécharger la localisation des personnes infectées. En réponse, il le valide en utilisant les données fournies par l'OMS pour s'assurer que les nouvelles données correspondent à l'original. Dans l'étape suivante, les nouvelles données vérifiées sont partagées avec les autorités publiques et les institutions de santé désignées par les pays.

6.8.4 Prévention de la propagation des virus grâce à la plateforme VIRI

La recherche numérique des contacts vise à limiter la propagation des virus infectieux transmis par voie aérienne tels que le Covid-19. Le VIRI [69,70] est basé sur la techno-

logie de la blockchain ,en proposant une plateforme universelle à l'échelle mondiale pour les utilisateurs. Le développement d'une plateforme inter-entités utilisant le VIRI pour suivre la propagation du virus dans différents pays peut permettre d'identifier l'apparition du Covid-19 à différents endroits. La plateforme de VIRI garantit la préservation de la confidentialité des données des utilisateurs. Elle avertit les individus lorsqu'ils ont été en contact étroit avec une personne infectée en suivant l'identité d'utilisateur générée de manière aléatoire. Par la suite, l'individu peut être alerté sur des maladies infectieuses en fonction du niveau de risque. Par exemple, après avoir croisé le chemin de personnes infectées, VIRI peut faire passer le statut d'un individu de "cas clair" à "cas d'infection potentielle". Grâce à des API ouvertes, la plateforme VIRI peut être intégrée de manière transparente aux solutions d'entreprise existantes. VIRI garantit que l'utilisateur a un contrôle total sur ses données et que celles-ci sont stockées localement sur son appareil. Les données stockées en chaîne sont anonymes (pour la préservation de la vie privée) et peuvent aider l'apprentissage machine et les outils d'IA à prévoir la pandémie mondiale de Covid-19.

6.8.5 Assurance de la confidentialité des données à l'aide de l'application WIShelter

WIShelter [72,73,74] est basé sur l'application WiseID qui est la plate-forme d'identité numérique de Wisekey pour fournir des services de sécurité à ses utilisateurs. Wisekey a utilisé la technologie blockchain et des outils basés sur l'IA pour développer des écosystèmes d'identité numérique à grande échelle. WIShelter est une application basée sur un téléphone intelligent qui stocke les données de santé des individus sur le registre distribué de manière fiable et sûre. Les enregistrements des données de santé comprennent de nombreux spécimens médicaux essentiels tels que les allergies, la pression sanguine et de nombreux autres détails pharmaceutiques. WIShelter a pour but de faciliter le téléchargement des certificats numériques indiquant les résultats du test Covid-19 sur la plateforme de la chaîne de contrôle . Grâce à WIShelter, les résultats du test Covid-19 téléchargés par une personne peuvent être consultés et vérifiés par des fonctionnaires gouvernementaux autorisés à délivrer des permis de voyage à la personne qui souhaite voyager. Toutefois, le fait de négliger la confidentialité des données des utilisateurs (par exemple, les résultats du test Covid-19) peut entraîner divers problèmes liés à la maltraitance et à

la discrimination à l'égard des personnes infectées. Pour faire face à une telle situation, WIShelter garantit que les données des utilisateurs ne peuvent pas être partagées avec d'autres sans leur consentement. Le formulaire de consentement peut être dûment signé par le propriétaire des données et les utilisateurs, et il pourrait être stocker de manière transparente sur la chaîne de blocage à des fins de responsabilité et d'auditabilité. De plus, pour sécuriser les dossiers médicaux et la communication des données, WIShelter crypte les données des utilisateurs. Le cryptage des données garantit également la préservation de la confidentialité des données. WIShelter est flexible et peut aider les autorités à vérifier la conformité avec les politiques de séjour à domicile conçues par les autorités pour les patients infectés par le Covid-19.

6.8.6 Soins de santé à distance à l'aide des systèmes Medicalchain et HealPoint

Medicalchain [75] est une plateforme basée sur Ethereum et Hyperledger Fabric,a été utiliser pour mettre en place des services à distance liés à la consultation entre patients et médecins et aux applications du marché. Elle garantit la sécurité et la confidentialité du transfert des données de santé lors des consultations entre patients et médecins. Grâce à des applications de marché, Medicalchain permet au propriétaire des données de santé (le patient) de partager en privé les données avec des tiers (les chercheurs) sur la base d'un formulaire de consentement convenu. Une autre plateforme appelée HealPoint [76] permet aux patients d'obtenir le deuxième avis d'un médecin à distance sur la santé d'un patient. HealPont peut également recommander les médecins les plus appropriés à un patient sur la base de plusieurs facteurs tels que le lieu, l'expérience et le conflit d'intérêts.

6.8.7 Auto identité souveraine à l'aide des systèmes Covid et E-Rezept

La plateforme E-Rezept [77,78,79] est un système de soins de santé à distance qui repose sur le principe d' auto identité souveraine. Elle permet aux patients de commander des médicaments à distance en présentant leurs identifiants uniques comme preuve . Par rapport à Medicalchain et HealPoint , E-Rezept est flexible et peut être facilement intégré aux systèmes de santé existants. COV-ID est une start-up basée sur la blockchain, il

récompense les citoyens respectueux de la loi de manière responsable et transparente . Le programme de passe d'accès qui a été intégré à WeChat en Chine a utilisé une blockcahin pour enregistrer de manière immuable les informations cryptées relatives aux citoyens locaux sur le registre distribué. Les données stockées sur le registre ont été par la suite utilisées par les autorités et les gouvernements pour établir une carte des antécédents de voyage du patient infecté par le Covid-19. La cartographie de l'historique des voyages des patients infectés a été utilisée pour identifier les points chauds de l'infection.

6.9 Problématique

Depuis l'apparition de la pandémie de Covid-19, plusieurs gouvernements ont appliqué des mesures strictes du confinement. Le confinement a consisté à maintenir les personnes à domicile afin de réduire la propagation de la maladie. Cette politique de lutte contre la pandémie a conduit au freinage de toutes sortes d'activités économiques, commerciales, sociales et éducatives. Ici on Algérie, des mesures de confinement ont été appliqués dans tous les secteurs depuis le début de la pandémie. Et ainsi, les études présentielles aux universités ont été suspendu pour une longue période (du Mars à Septembre 2020). Les études en ligne ont permis d'avancer l'enseignement universitaire durant cette période. Mais elles ne sont pas complètement appropriées dans quelques domaines, notamment où les travaux pratiques nécessitent que l'étudiant manipule un matériel au niveau du laboratoire. La tentative du retour à la vie normale accompagné par la reprise études universitaires en septembre 2020 a conduit à élever le nombre des cas contaminés par Covid-19 [58].

Dans cette partie, nous cherchons à proposer une solution pour permettre aux étudiants universitaires de suivre des études en présentiel et en évitant d'être contaminé ou de propager le virus.

6.10 Solution proposée

Notre solution consiste à utiliser les blockchains en conjonction avec les passeports d'immunité pour permettre aux étudiants qui ne présente pas des risques d'être contaminé ou de contaminer d'autres personnes de suivre des études en présentiel à l'université.

Le principe de la proposition (Figure 6.12) est de créer une blockchain globale pour

enregistrer les personnes qui ont un passeport immunitaire, c-à-d les personnes qui ont une immunité contre Covid-19. Cela concerne des personnes qui ont été touché par le virus et ont une immunité pour une période. Et des personnes qui ont été vaccinées. L'utilisation de la blockchain permet d'enregistrer d'une façon immutable et sécurisée les données concernant les personnes immunisées. A chaque fois qu'un étudiant est ajouté à la blockchain globale, l'étudiant est ajouté automatiquement à la blockchain Etudiants, construisant ainsi une blockchain spécifique destinée aux différents services de l'université. Des smart contracts sont lancés régulièrement afin d'archiver les personnes qui ont perdu son immunité, réduisant ainsi la taille des deux blockchains. La réduction de la taille de la afin de réduire le temps d'exécution des requêtes.

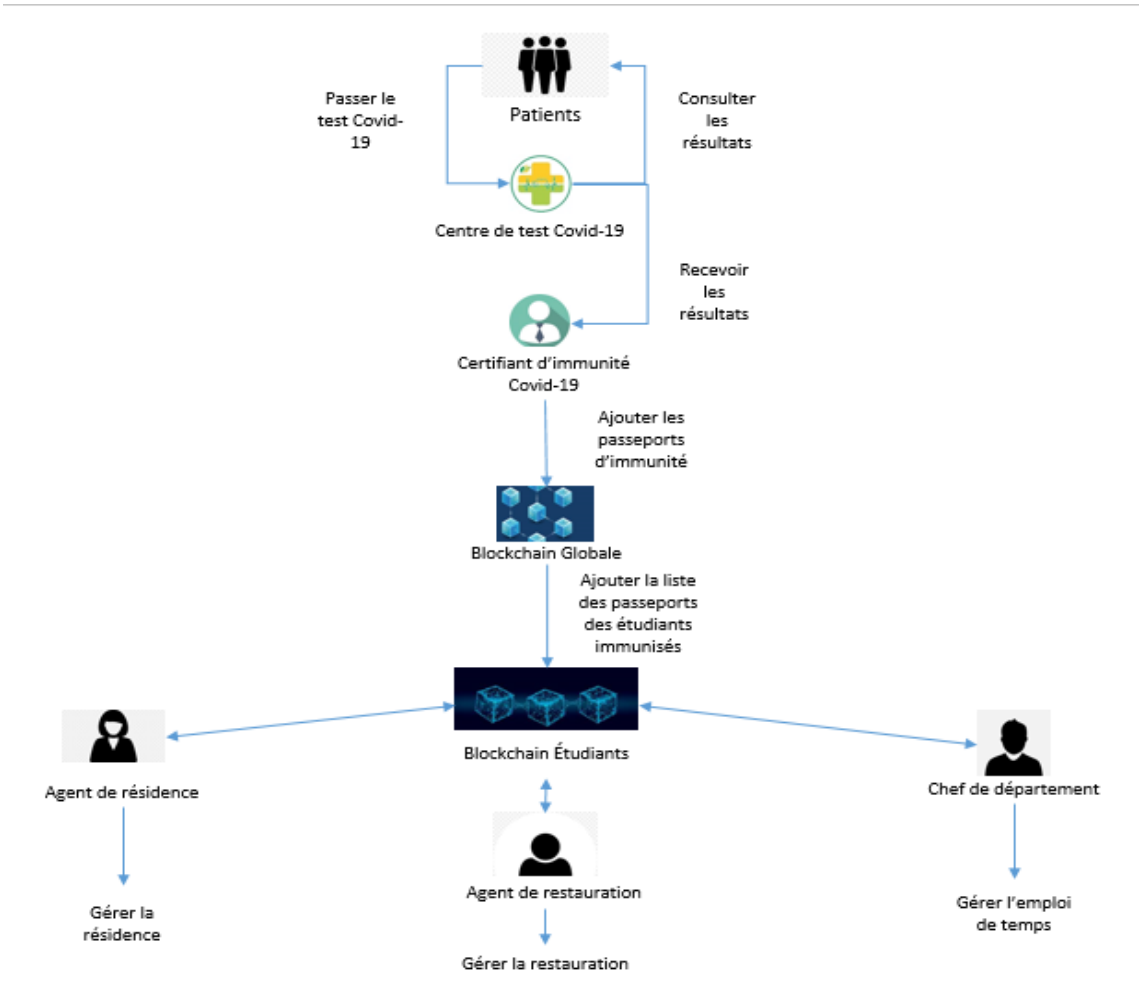

FIGURE 6.12 – Schéma du système de la solution Covid-19.

La solution proposée permet à :

— Une personne de posséder un passeport d'immunité après avoir passé le test Covid-19 dans un centre de test et avoir des résultats positives concernant l'immunité

contre Covid-19. Et aussi après être vaccinée.

- Un certifiant d'immunité Covid-19 :
  - de recevoir les résultats des patients immunisés ensuite créer des passeports d'immunité dans une blockchain globale et lorsque le patient est de type étudiant, il sera encore ajouter dans une blockchain des étudiants d'une façon automatique.
  - de consulter la liste des passeports d'immunité.
- L'université d'accéder à la blockchain étudiants et de consulter les passeports d'immunité de leurs étudiants.
- Un chef de département de gérer l'emploi du temps et les examens pour ces étudiants immunisés après avoir accéder à la blockchain étudiants.
- Un agents de résidence d'accéder à la blockchain étudiants dans le but de gérer la résidence pour les étudiants immunisés.
- Un agents de restauration de gérer la restauration pour les étudiants immunisés après avoir accéder à la blockchain étudiants.

La liste des passeports d'immunité est enregistré sous forme de block afin de pouvoir mesurer et permettre aux personnes qui ne présentent pas de risques de retrouver leurs vies quotidiennes.

6.11 Conclusion

Au cours de ce chapitre, nous avons parlé de la pandémie du Covid-19, ses symptômes, comment elle se transmit, comment se protéger et quelques sites et applications permettant la détection, la prévention et autres informations. nous avons terminé ce chapitre par une problématique et une solution proposée.

Chapitre 7

Conception et modélisation du système Covid-19

7.1 Introduction

Ce chapitre est consacré aux étapes fondamentales de conception et de modélisation du système d'ajout des passeports d'immunité Covid-19 ,on se basant sur la technologie de blockchains.

Nous avons opté pour le Processus Unifié (UP) comme méthode de conception, et l'Unified Modeling Language (UML) comme langage de modélisation.

7.2 Identification des besoins

Besoins fonctionnels : le système doit offrir les fonctionnalités suivantes :

— Créer les passeports d'immunité pour les personnes immunisées.

— Consulter la liste des passeports d'immunité.

— Consulter les passeports d'immunité des étudiants.

— Gérer l'emploi du temps et les examens pour les étudiants immunisés.

— Gérer la résidence pour les étudiants immunisés.

— Gérer la restauration pour les étudiants immunisés.

Besoins non fonctionnels : à part les besoins fondamentaux, notre système doit répondre aux critères suivants :

Sécurité : La blockchain assure un stockage des informations d'une manière non modifiable et toutes ces informations pourraient se retrouver de façon chronologique dans un registre sécurisé et aisément consultable.

Performances : Un logiciel doit être avant tout performant c'est-a-dire répond aux exigences des utilisateurs d'une manière optimale.

Utilisabilité : Le système doit offrir à l'utilisateur une interface simple et facile à utiliser.

Scalabilité : L'utilisateur doit pouvoir augmenter ses capacités de traitement, de stockage, de transmission et de réseaux selon ses besoins.

Traçabilité : Les données sont enregistrées d'une manière sécurisée, dans le temps et stockées dans un registre décentralisé et infalsiable. Les données sont ainsi certifiées et non répudiables.

7.3 Diagramme des cas d'utilisation

7.3.1 Identification des acteurs du système

Dans le cas de notre système, nous avons identifié principalement cinq acteurs (certifiant d'immunité Covid-19, université, chef de département, agent de résidence ,agent de restauration) et Pour chacun des cinq acteurs cités, notre application doit donc offrir un ensemble de fonctionnalités :

Certifiant d'immunité Covid-19 :

— Créer les passeports d'immunité pour les personnes immunisées.

— Consulter la liste des passeports d'immunité.

Université :

— Consulter les passeports d'immunité des étudiants.

Chef de département :

— Gérer l'emploi du temps et les examens pour les étudiants immunisés.

— Consulter les passeports d'immunité des étudiants.

Agent de résidence :

— Gérer la résidence pour les étudiants immunisés.

— Consulter les passeports d'immunité des étudiants.

Agent de restauration :

— Gérer la restauration pour les étudiants immunisés.

— Consulter les passeports d'immunité des étudiants.

Diagramme de cas d'utilisation :

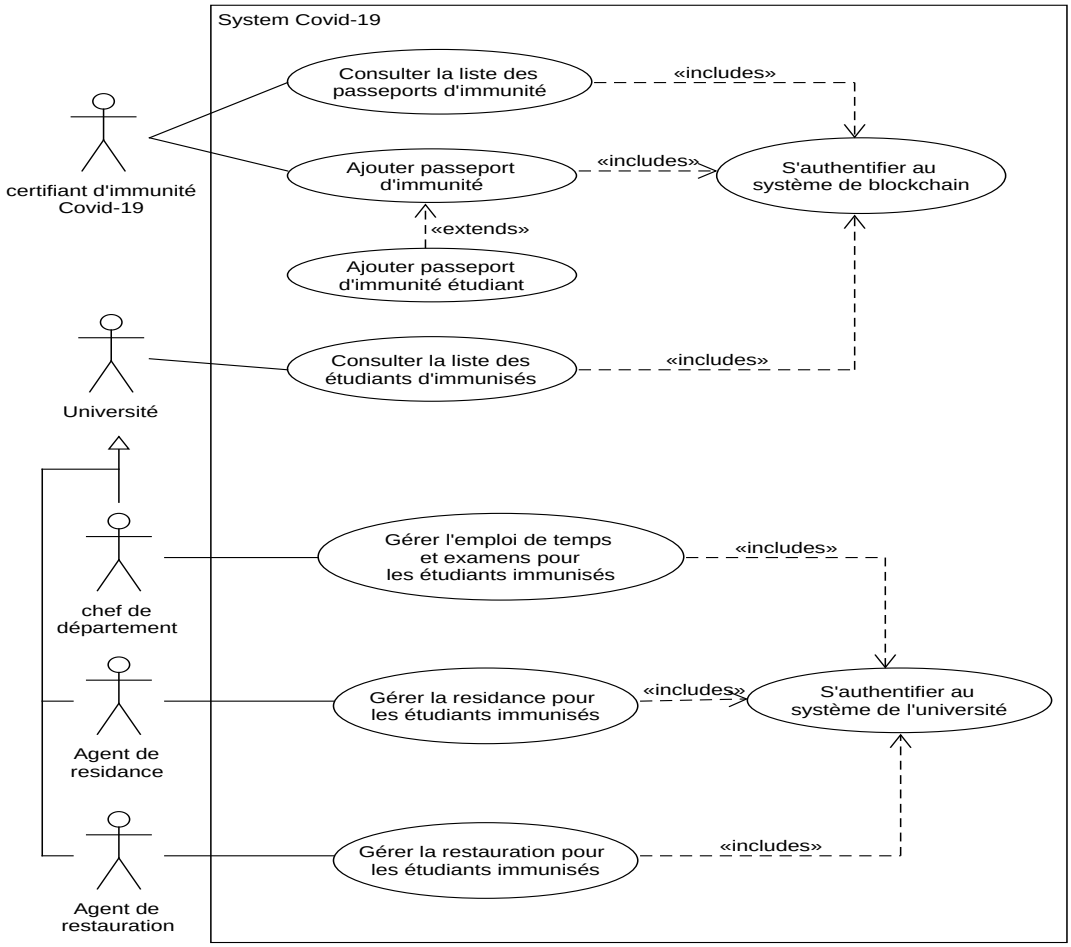

FIGURE 7.1 – Diagramme de cas d'utilisation général.

7.4 Diagrammes de séquences

7.4.1 Diagramme de séquence « Authentification »

Le diagramme de séquence Authentification présente le séquencement des interactions entre le certifiant d'immunité covid -19 et le système. Dans ce diagramme loop(1, 3) indique qu'il y aura une répétition d'affichage de la page authentification jusqu'à la validation des données où après trois (3) essayes non effectue.

L'operateur alt indique la structure conditionnelle if. Cette condition va permettre

d'acc´eder a la page souhaitée et d'afficher un message de succès si (et seulement si) les données entrées sont valide, sinon le système affiche un message d'erreur.

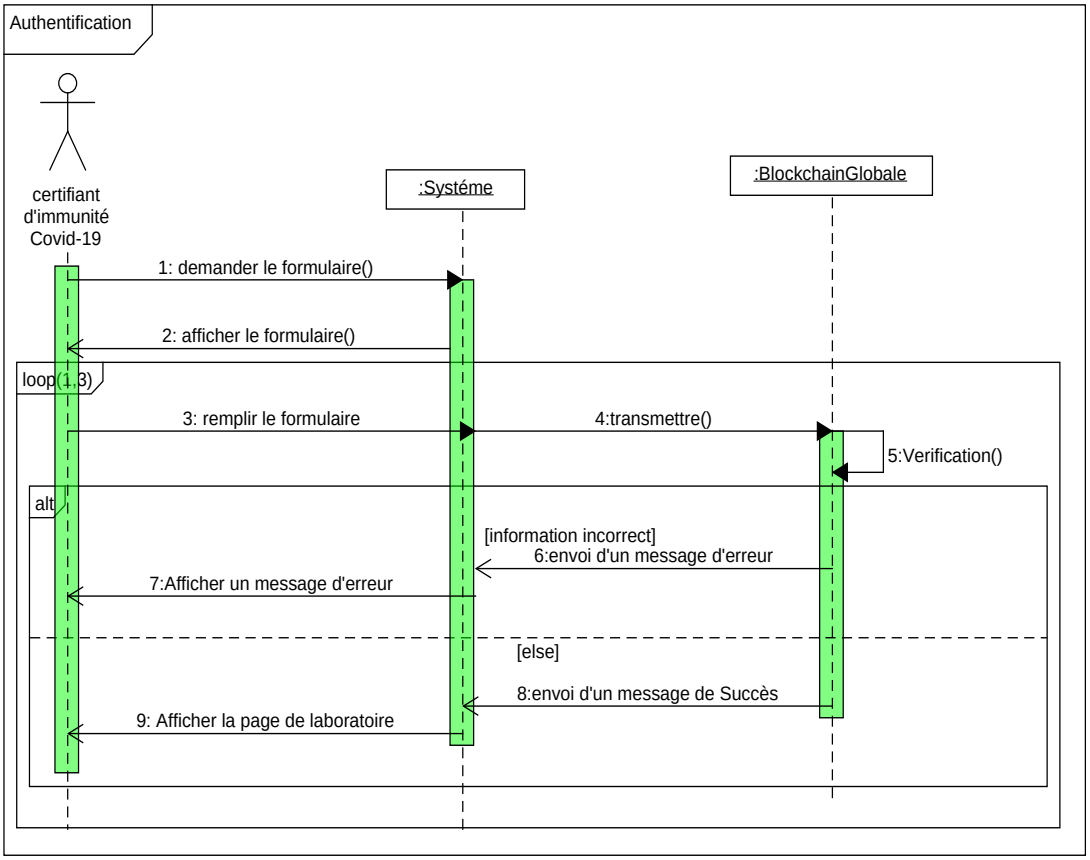

FIGURE 7.2 – Diagramme de séquence « Authentification ».

7.4.2 Diagramme de séquence « Ajouter passeport »

Le diagramme de séquence Ajouter présente le séquencement des interactions entre le certifiant d'immunité Covid-19 et le système.

Le certifiant d'immunité Covid-19 peut ajouter les passeportd pour les personnes immunisées par le remplissage du formulaire La validation de l'ajout nécessite la vérification des champs saisis.

Si la personne immunisée est un étudiant donc il sera ajouté à la blockchain globale et même à la blockchain étudiants pour faciliter la recherche des universités de leurs étudiants immunisés

L'operateur alt indique la structure conditionnelle if. Cette condition va permettre d'ajouter et d'afficher un message de succés si (et seulement si) les données entrer sont

valide, sinon le système affiche un message d'erreur.

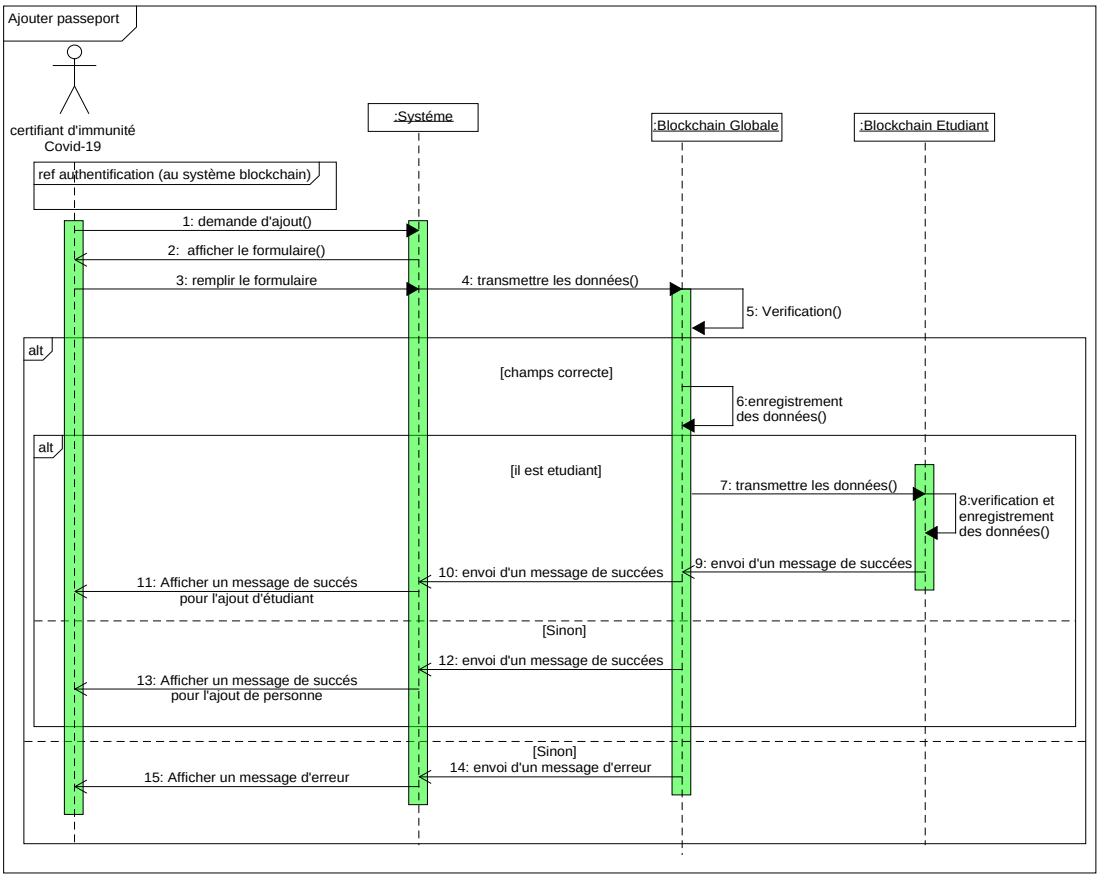

FIGURE 7.3 – Diagramme de séquence « Ajouter passeport ».

7.4.3 Diagramme de séquence « Consulter la liste des passeports d'immunité »

Le diagramme de séquence consulter présente le séquencement des interactions entre certifiant d'immunité covid -19 et le système. Le certifiant d'immunité covid -19 peut consulter la liste des passeports des personnes immunisées.

L'operateur alt indique la structure conditionnelle if. Cette condition va permettre d'afficher la liste des passeports d'immunités si (et seulement si) la liste n'est pas vide , sinon le système affiche un message indique que la liste est vide .

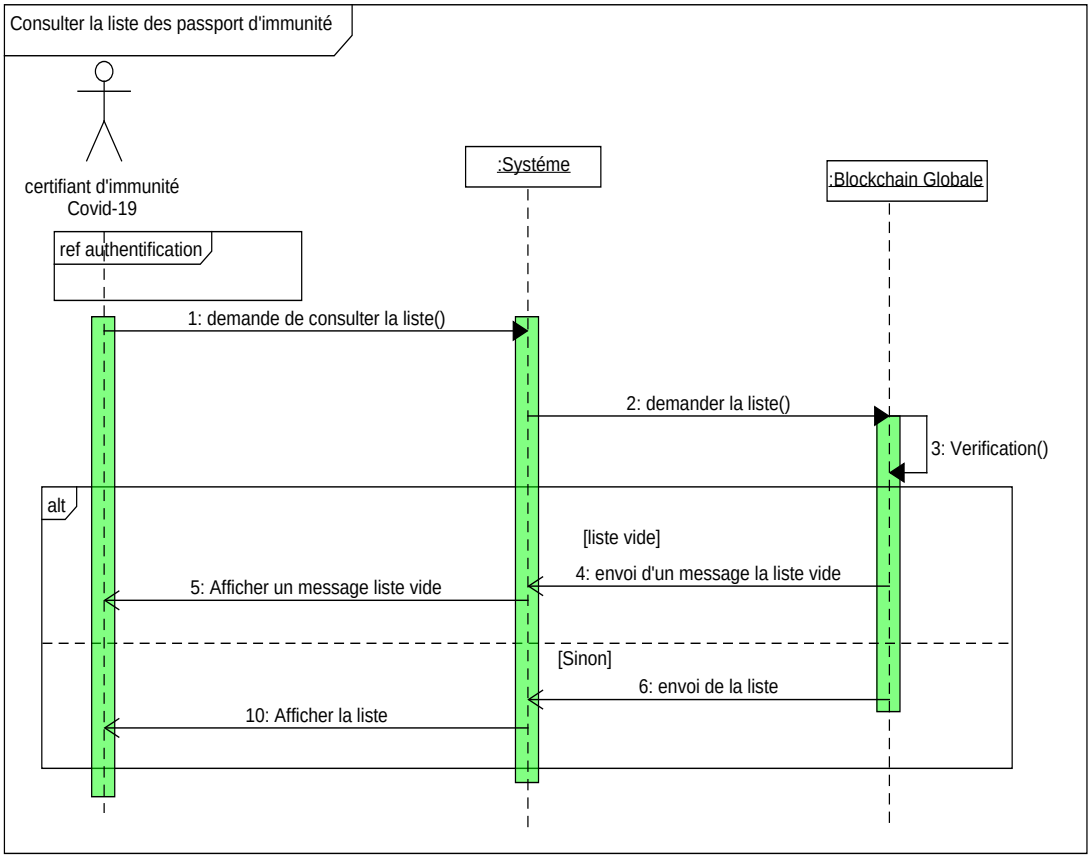

FIGURE 7.4 – Diagramme de séquence « Consulter la liste des passeports d'immunité »

7.4.4 Diagramme de séquence « Consulter la liste des passeports des étudiants immunités »

Le diagramme de séquence consulter présente le séquencement des interactions entre université et le système.

L'université peut consulter la liste des passeports des étudiants immunisés.

L'operateur alt indique la structure conditionnelle if. Cette condition va permettre d'afficher la liste des passeports d'immunités si (et seulement si) la liste n'est pas vide , sinon le système affiche un message indique que la liste est vide .

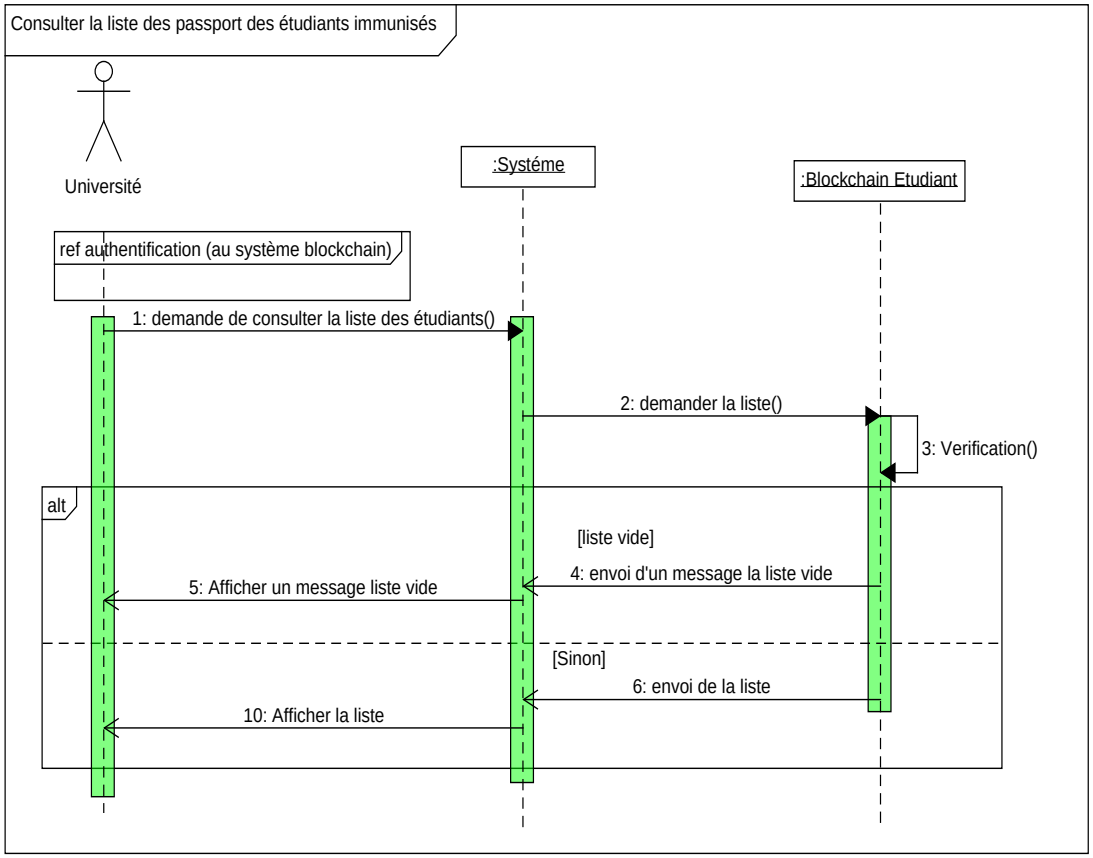

FIGURE 7.5 – Diagramme de séquence « Consulter la liste des passeports des étudiants immunités »

7.4.5 Diagramme de séquence « Gérer l'emploi du temps »

Le diagramme de séquence Gérer l'emploi du temps présente le séquencement des interactions entre chef de département et le système.

Chef de département peut Gérer l'emploi du temps pour les étudiants immunisés.

L'operateur alt indique la structure conditionnelle if. Cette condition va permettre au chef de département de gérer un emploi du temps si (et seulement si) le nombre des étudiants immunisés supérieur à 30 dans son département, sinon le système affiche un message indique que le nombre des étudiants immunisés insuffisant pour créer un emploi.

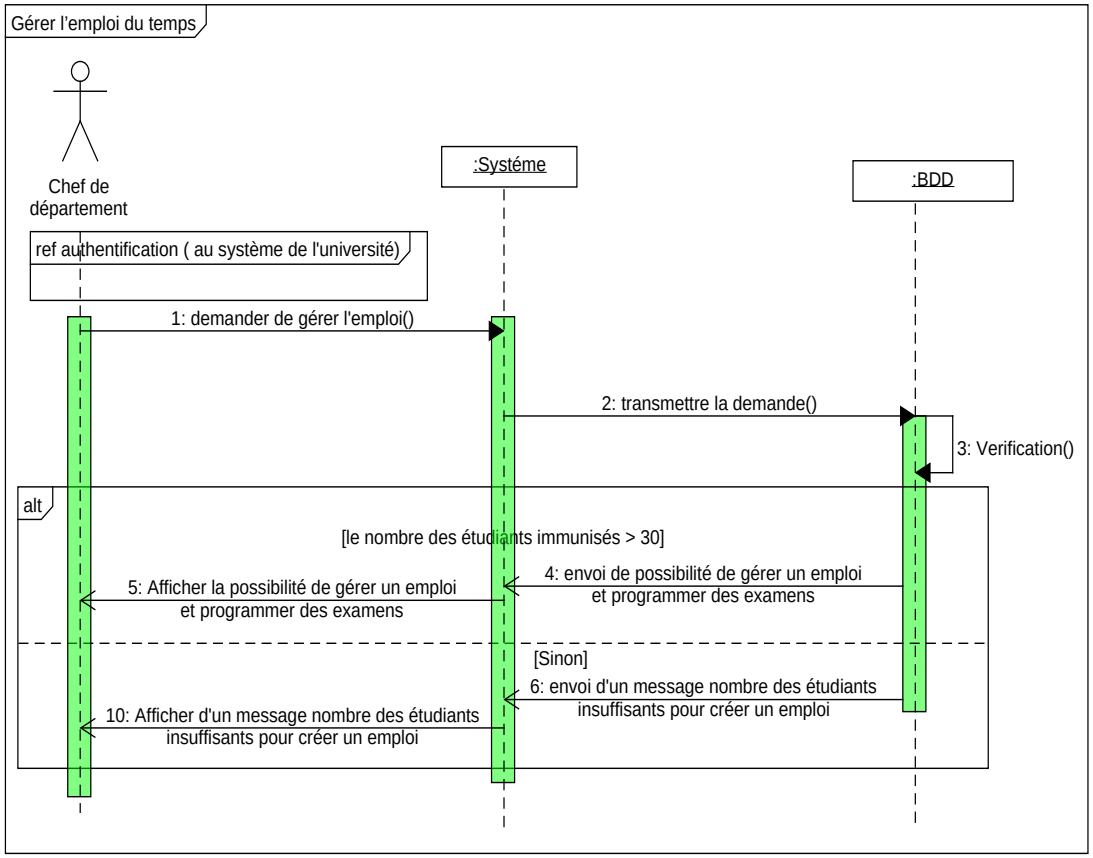

FIGURE 7.6 – Diagramme de séquence « Gérer l'emploi du temps »

Remarque : le même principe pour la création de diagramme de séquence pour gérer la résidence des étudiants immunisés et gérer la restauration.

7.5 Diagramme des classes

7.5.1 Dictionnaire des données

La figure ci-dessous (Figure 7.7) représente la liste des attributs composants toutes les classes formant notre système ainsi que leurs descriptions, leurs types et leurs tailles.

N°	Attribut	Description	Type	Taille
1	Id	Identifiant d'un certifiant d'immunité covid-19, passeport d'immunité, université, chef de département, agent de résidence, agent de restauration	Entier	255
2	Nom	Le nom d'un certifiant d'immunité covid-19 ou le nom de la Personne immunisée	Chaine de caractère	50
3	Prenom	Le prénom d'une Personne immunisée	Chaine de caractère	50
4	Code	Mot de passe de certifiant d'immunité covid-19	Chaine de caractère	10
5	Période	une date d'expiration d'immunité	date	
6	Université	Le nom de l'université de l'étudiant immunisé	Chaine de caractère	50
7	Spécialité	La spécialité de l'étudiant immunisé	Chaine de caractère	50
8	Nom de département	Nom de département où travaille le chef de département	Chaine de caractère	50
9	Nom de résidence	Nom de résidence où travaille l'agent de résidence	Nom de résidence	50
10	Code de restauration	Code de restauration où travaille l'agent de restauration	Chaine de caractère	50
11	MotDePasse	Mot de passe de la Personne immunisée qui possède un passeport d'immunité ou mot de passe d'université, chef de département, agent de résidence, agent de restauration	Chaine de caractère	15
12	MatEtudiant	Le matricule de l'étudiant immunisé	Chaine de caractères	25

FIGURE 7.7 – Dictionnaire des données

7.5.2 Représentation des classes

La figure ci-dessous (Figure 7.8) représente les classes ainsi leurs méthodes et leurs attributs.

N°	Nom Classe	Liste des attributs	Méthodes
01	Certifiant d'immunité covid-19	Id Nom code	-Créer les passeports d'immunité pour les personnes immunisées () -Consulter les listes des passeports d'immunité ()
02	Passeport d'immunité	id Nom Prenom Période Mot de passe	
3	Passeport d'immunité d'étudiant	id Nom Prenom Période Mot de passe MatEtudiant Université Spécialité	
4	Université	Id Mot de passe	-Consulter la liste des passeports d'immunité des étudiants ()
5	Chef de département	Id Mot de passe Nom de département	-Consulter la liste des passeports d'immunité des étudiants () -Gérer l'emploi du temps et des examens pour les étudiants immunisés ()
6	Agent de résidence	Id Mot de passe Nom de résidence	-Consulter la liste des passeports d'immunité des étudiants () -Gérer résidence ()
7	Agent de restauration	Id Mot de passe Code de restauration	-Consulter la liste des passeports d'immunité des étudiants ()

FIGURE 7.8 – Représentation des classes

7.5.3 Représentation des associations

Ajouter : entre le certifiant d'immunité Covid-19 et le passeport d'immunité.

Avoir : entre université et passeport d'immunité d'étudiant.

Association	cardinalité	Désignation
Ajouter	1 0..*	Le passeport est ajouté par un seul certifiant d'immunité covid-19. certifiant d'immunité covid-19 peut ajouter zéro ou plusieurs Personnes immunisées
Avoir	1 0..*	Le passeport d'immunité de l'étudiant se trouve dans une seule université. Université a zéro ou plusieurs passeports d'immunité d'étudiant

FIGURE 7.9 – Représentation des associations

Diagramme des classes :

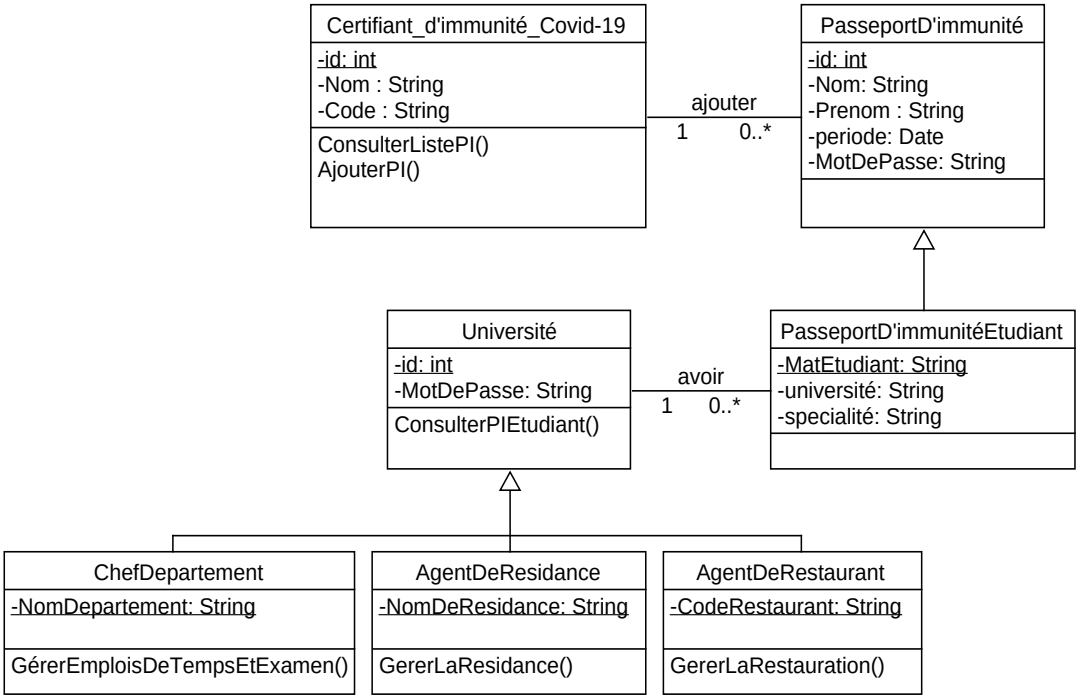

FIGURE 7.10 – Diagramme des classes.

7.6 Conclusion

Au cours de ce chapitre, nous avons montré le principe de fonctionnement et les relations qui existent entre les différents acteurs et leurs interactions avec le système.et nous avons pu concevoir une application pour l'ajout des passeports d'immunité Covid-19 en s'adaptant sur les diagrammes du formalisme UML à savoir le diagramme de cas d'utilisation, le diagramme de séquence et le diagramme de classe.

Conclusion générale

La blockchain a dépassé largement son application classique de monnie électronique sans autorité centrale. Cette technologie a apporté des nouveaux concepts qui assure l'immutabilité et renforce la sécurité. Ces caractéristiques rendent la technologie de blockchain appropriée pour plusieurs domaines, tels que : les systèmes de vote et la santé.

Dans ce mémoire, nous avons exploré la blockchain et proposé des solutions basées sur cette technologie. Nos propositions concernent une application pour le vote électronique et une solution pour lutter contre le virus Covid-19.

Pour réaliser notre application de vote en ligne basée sur la blockchain. Nous avons élaboré une conception et une modélisation basée sur l'UP et L'UML. Nous avons commencé par une étude préliminaire pour d'identifier les différents acteurs qui interagissent avec le système et de procéder à l'analyse des besoins en spécifiant les besoins fonctionnels et non fonctionnels. Après, nous avons décrit le système utilisant à travers les diagrammes de cas d'utilisation, de séquence et de classe. L'implémentation a nécessité de manipuler des outils spécifiques à savoir la plateforme Ethereum basé sur les smart contract. L'application développé a permet de garantir les besoins essentielles d'un vote démocratique.

Notre solution concernant Covid-19, consiste à utiliser les blockchains en conjonction avec les passeports d'immunité pour permettre aux étudiants qui ne présente pas des risques d'être contaminé ou de contaminer d'autres personnes de suivre des études en présentiel à l'université. Nous avons modélisé la solution proposée utilisant des diagrammes UML.

Ce projet nous a été très bénéfique, car il nous a permis d'enrichir nos connaissances concernant la blockchain sur les deux plans : théorique et pratique. Il nous a aussi permis de découvrir et d'acquérir de nouvelles connaissances en matière de programmation et de

développement dans le domaine des applications décentralisées.

La technologie blockchain est encore très complexe à appréhender et le développement d'un système décentralisé nécessite énormément du temps, de ressources, de recherches et aussi de grands efforts de programmation.

A cause de ces contraintes ainsi que des circonstances exceptionnelles suite aux conséquences de la pandémie Covid-19, nous n'avons pas pu réaliser l'application des passeports d'immunités Covid-19 même certains points n'ont pas été pris en compte dans la partie réalisation de l'application de vote en ligne.

bibliographie

[1] : https ://www.cryptolia.fr/universite/introduction-block chain/, consulté le 20/03/2020

[2] : « blockchain la revolution de la confiance », laurent leloup, paris, eyrolles, 2017

[3] : https ://academy.binance.com/fr/articles/history-of- blockchain, consulté le 11/10/2020

[4] : «blockchain» amritha jayanti, bogdan belei 2020.

[5] : «hands-on blockchain with hyperledger»,nitin gaur, luc desrosiers, petr novotny, venkatraman ramakrishna, anthony o'dowd, salman a. baset ,juin 2018

[6] : «oracle blockchain quick start guide», vivek acharya, anand eswararao yerrapati, nimesh prakash, septembre 2019

[7] :https ://www.researchgate.net/publication/335174496_chapitre_ iii_etat_de_l'art_de_la_blockchain consulté le 12/05/2020

[8] : « comprendre la blockchain » richard caetano stratumn, ceo livre blanc sous licence creative commons '' uchange." 2017

[9] : https ://www.gralon.net/articles/internet-et-webmaster/ logiciel/article-c-est-quoi– la-blockchain–10468.htm, consulté le 11/05/2020

[10] : https ://www.supinfo.com/articles/single/4368-blockchain, consulté le 11/05/2020

[11] : https ://meritis.fr/finance/blockchain-revolution-ou-epip henomene/, consulté le 29/09/2020

[12] : «la blockchain decryptee» l'observatoire netexplo ,paris ,mai 2016

[13] :« situacion economia digital» jorge sicilia serrano ,juillet 2015

[14] :«blockchain blueprint for a new economy» melanie swan, fevrier 2015.

[15] :«beginning blockchain» bikramaditya singhal, gautam dhameja, priyansu sekhar panda ,2018.

[16] :«learning bitcoin» richard caetano, november 2015.

[17] : «glossaire blockchain» matthieu quiniou et christophe debonneuil ,paris,avril 2019

[18] : «les risques des blockchains», laurent dehouck etaudrey thomas, juin 2010

[19] :http ://web.cs.ucla.edu/classes/winter13/cs111/scribe/17b/ consulté le 26/10/2020

[20] : «die blockchain – technologie-feld und wirtschaftliche anwendungsbereiche» johannes scherk b.sc., mag. gerlinde pöchha cker-tröscher, mai 2017

[21] : « principes cles d'une application blockchain» godebarge ferreol,rossat romain, em lyon business school , decembre 2016.

[22] : «music on the blockchain» marcus o'dair,2016

[23] :«la blockchain, une revolution pour la finance ?» leonard beth et annika cayrol 2017

[24] :« der blockchain-nebel lichtet sich auch für die assekuranz» christian richter , andre schlieker 2017

[25] : https ://www.industrie-techno.com/article/ces-5-secteurs-que-va-revolutionner-la-blockchain.53233, consulté le 26/10/2020

[26] : https ://www.reply.com/de/content/healthcare, consulté le 26/10/2020

[27] : https ://www.leewayhertz.com/blockchain-platforms-for-top-blockchain-companies/, consulté le 26/10/2020

[28] : «building blockchain projects» narayan prusty,2017

[29] : chantal enguehard «vote par internet : failles techniques et recul democratique », jus politicum, n° 2 [http ://juspoliticum. com/article/vote-par-internet-failles-techniques-et-recul-dem ocratique-74.html] consulté le 19/06/2020.

[30] :https ://www.vie-publique.fr/fiches/23984-comment-se-dero ulent-les-operations-de-vote, consulté le 26/10/2020

[31] : https ://democratiedirecte.net/vote-par-internet, consulté le 20/06/2020

[32] : https ://journals.openedition.org/terminal/4190#tocto1n4, consulté le 20/06/2020.

[33] : le journal "international journal of control and automationvol. 10", no. 12 (2017), pp.121-130 http//dx.doi.org/10.14257/ijca. 2017.10.12.11

[34] : http ://www.kvoting.go.kr/necvote/intro.html, consulté le 25/10/2020

[35] : « vote numerique avec l'utilisation de la technologie blockchain », team plymouth pioneers - universite de plymouth, andrew barnes, christopher brake et thomas perry

[36] : «dutch e-vote opportunities» r. verbij. memoire de maitrise, universite de twente,

2014 « https ://courses.cs.ut.ee/2015/inf sec/fall/main/e-voting », consulté le 20/06/2020

[37] : https ://www.dz-techs.com/fr/how-electronic-voting-works consulté le 20/06/2020

[38] :https ://elections.ca/content.aspx ?section=res&dir=rec/ tech/ivote/comp&document=benefit
consulté le 13/10/2020

[39] : https ://www.news-medical.net/news/20200305/138/french.aspx, consulté le 20/10/2020.

[40] : https ://dicocitations.lemonde.fr/dico-mot-definition/186774/covid_19.php, consulté le 20/10/2020

[41] :https ://www.rtbf.be/info/societe/detail_comment-le-coronaviruse-se-transmet-il ?id=10444399, consulté le 20/10/2020

[42] :https ://www.science-et-vie.com/corps-et-sante/la-resistance-du-coronavirus-sur-les-objets-ce-qu-il-faut-retenir-55012, consulté le 20/10/2020

[43] : https ://www.lumni.fr/article/coronavirus-definition-transmission-et-symptomes #containertype=folder&containerslug=coronavirus, consulté le 20/10/2020

[44] : https ://coronavirus.dc.gov/page/what-covid-19, consulté le 20/10/2020

[45] :https ://www.lavoixdunord.fr/714573/article/2020-02-24/coronavirus-ce-qu-il-faut-savoir-pour-ne-pas-etre-infecte-par-le-covid-19, consulté le 20/10/2020

[46] : lettre de recherche (transmission présumée de porteuse asymptomatique de covid-19) téléchargé depuis : https ://jamanetwork.com/ le 28/04/2020

[47] :https ://www.topsante.com/medecine/maladies-infectieuses/zoonoses/traitement-du-coronavirus-quels-sont-les essais-les-plus-prometteurs-636010, consulté le 16/04/2020

[48] : https ://www.elwatan.com/edition/actualite/traitement-et-vaccins-contre-le-covid-19, consulté le 16/04/2020

[49] : le journal de antimicrobial chemotherapy article (covid-19 : a recommendation to examine the effect of hydroxychloroquine in preventing infection and progression)

[50] : https ://www.linternaute.com/actualite/guide-vie-quotidienne/2489467-chloroquine-et-coronavirus-de-nouvelles-alertes-inquietantes/, consulté le 20/10/2020

[51] : document (preventing a covid-19 pandemic) http ://www.bmj.com/ publié pour la première fois en tant que 10.1136 / bmj.m810 le 28 février 2020.

[52] :document (feasibility of controlling covid-19 outbreaks by isolation of cases and contacts)

[53] :https ://www.msn.com/fr-xl/northafrica/other/covid-19-le-confinement-reste-le-meilleur-moyen-de-freiner-la-propagation/ar-bb12ed80, consulté le 26/10/2020

[54] :https ://w/ww.journaldemontreal.com/2020/04/05/les-maladies-chroniques-et-la-/covid-19, consulté le 20/10/2020

[55] : https ://coronavirus.politologue.com/, consulté le 20/10/2020

[56] : https ://gisanddata.maps.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6, consulté le 20/10/2020

[57] :https ://play.google.com/store/apps/details ?id=com.covid19_algeria&hl=en_us

[58] :http ://covid19.sante.gov.dz/, consulté le 26/10/2020

[59] : https ://www.estrepublicain.fr/france-monde/2020/03/21/coronavirus-un-site-web-pour-s-autodiagnostiquer-et-etre-oriente, consulté le 26/10/2020

[60] :https ://www.lemonde.fr/pixels/article/2020/03/17/les-meilleurs-logiciels-de- visioconference-gratuits-pour-communiquer-depuis-la-maison_6033387_4408996.html, consulté le 26/10/2020

[61] : http ://elearninginfo.univ-bouira.dz/2019_2020/, consulté le 26/10/2020

[62] :https ://www.teleconsultations.fr/foire-aux-questions-sur-la-consultation-en-ligne.html, consulté le 26/10/2020

[63] :≪blockchain-based solution for covid-19 digital medical passports and immunity certificates≫ haya r. hasan, khaled salah, raja jayaraman, junaid arshad, ibrar yaqoob, mohammed omar, samer ellahham ,2020

[64] :≪anonymous epidemic disease testing≫,white paper 2020, douglas horn, syed mahdi hosseini, sergey illin, rami james, kevin quaintance, suvi rinkinen

[65] :https ://www.enterprisetimes.co.uk/, consulté le 15/10/2020

[66] :https ://gcn.com/articles/2020/04/06/mipasa-blockchain-covid-tracking.aspx, consulté le 26/10/2020

[67] :https ://mipasa.org/blog/mipasa-an-open-data-platform-to-support-covid-19-response/, consulté le 26/10/2020

[68] :https ://www.himss.org/news/blockchain-coronavirus-emerging-technologies, consulté le 26/10/2020

[69] :https ://www.viri.io/, consulté le 26/10/2020

[70] :https ://techcrunch.com, consulté le 15/10/2020

[72] :https ://www.wisekey.com/press/, consulté le 26/10/2020

[73] :https ://www.wisekey.com/products-services/digital-identity-pki/trust-services/managed-pki-services/, consulté le 26/10/2020

[74] :https ://www.newsbreak.com/news/, consulté le 15/10/2020

[75] :« medicalchain», white paper 2018, medicalchain sa, march

[76] : «healpoint», white paper, laboratory information systems, los angeles, 2018.

[77] :https ://medium.com/spherity/spherity-contributes-to-wirvsvirus-hackathon-for-corona-virus-solutions-3c59b1557fdf, consulté le 26/10/2020

[78] :https ://appinventiv.com/blog/blockchain-adoption-amidst-coronavirus/, consulté le 26/10/2020

[79] :http ://www.news.cn/, consulté le 15/10/2020

[80] : jacobson, g. booch, j. rumbaugh. the unified software development process. eyrolles, 2000.

[81] : https ://www.dappuniversity.com/articles/web3-js-intro, consulté le 15/07/2020

[82] : «uml2 modeliser une application web», pascal roques, 4°edition 2007

[83] : jacques lonchamp, genie logiciel sixieme partie la modelisation objet uml, cours, cnam cra nancy. 2003.

[84] : josef gabay, david gabay .uml 2 analyse et conception .dunod .paris :2008.

[85] : https ://www.supinfo.com/articles/single/2594-bases-uml, consulté le 11/07/2020.

[86] : http ://dictionnaire.sensagent.leparisien.fr/xampp/fr-fr/, consulté le 26/10/2020

[87] : https ://www.supinfo.com/articles/single/1114-sublime-text-3, consulté le 12/07/2020

[88] : https ://www.trufflesuite.com/docs/ganache/overview, consulté le 26/10/2020

[89] : https ://fr.bitdegree.org/tutos/metamask/, consulté le 14/07/2020

[90] : https ://golden.com/wiki/truffle_framework, consulté le 14/07/2020

[91] : https ://www.tutorialsteacher.com/nodejs/what-is-nodejs, consulté le 14/07/2020

[92] : https ://remix-ide.readthedocs.io/en/latest/, consulté le 15/07/2020

[93] : https ://www.une-blockchain.fr/tutorial-developpement-solidity-remix/, consulté lee 26/10/2020

[94] : https ://agency-inside.com/2016/06/definition-webmarketing-bootstrap/, consulté le 26/10/2020

[95] : http ://glossaire.infowebmaster.fr/javascript/, consulté le 15/07/2020

[96] : https ://www.dappuniversity.com/articles/web3-js-intro, consulté le 15/07/2020

[97] : https ://solidity.readthedocs.io/en/v0.6.11/, consulté le 16/07/2020

[98] :https ://www.php.net/manual/fr/intro-whatis.php, consulté le 16/07/2020

[99] : https ://github.com/dappuniversity/election, consulté le 26/10/2020

[100] : https ://git hub.com/rajatdiptabiswas/ethereum-dapp-vote, consulté le 26/10/2020

Code source du système vote en ligne

.1 Fichier « Election.sol »

Les deux figure (Figure 11 et Figure 12) représente le code source du smart contract « Election.sol ».

```
pragma solidity ^0.5.16;

contract Election {
  // Model a Candidate
  struct Candidate {
    uint id;
    string name;
    uint voteCount;
  }

  // Store & Fetch Candidate
  mapping(uint => Candidate) public candidates;

  // Store Candidates Count
  uint public candidatesCount;

  // Store accounts that have voted
  mapping(address => bool) public voters;

  // Voted event
  event votedEvent (uint indexed _candidateId);

  // Constructor
  constructor () public {
    addCandidate("Candidate 1");
    addCandidate("Candidate 2");

  }

  // Add Candidate
  function addCandidate (string memory _name) private {
    candidatesCount++;
    candidates[candidatesCount] = Candidate(candidatesCount, _name, 0);
  }
```

FIGURE 11 – Smart contract du vote (partie 01).

```
  // Vote for Candidate
  function vote (uint _candidateId) public {
    // require that they have not voted before
    require(!voters[msg.sender]);

    // require a valid candidate
    require(_candidateId > 0 && _candidateId <= candidatesCount);

    // record that voter has voted
    voters[msg.sender] = true;

    // update candidate vote count
    candidates[_candidateId].voteCount++;

    // trigger voted event
    emit votedEvent(_candidateId);
  }
}
```

FIGURE 12 – Smart contract du vote (partie 02).

.2 Fichier « App.js »

Le code contient plusieurs sections, voici quelques détails sur chacune d'elles :

InitWeb3 : C'est la fonction ou on configure Web3 pour permettre à notre application côté client de communiquer avec la blockchain.

```
App = {
  web3Provider: null,
  contracts: {},
  account: '0x0',
  hasVoted: false,

  init: function() {
    return App.initWeb3();
  },

  initWeb3: function() {
    // TODO: refactor conditional
    if (typeof web3 !== 'undefined') {
      // Si une instance web3 est déjà fournie par Meta Mask.
      App.web3Provider = web3.currentProvider;
      web3 = new Web3(web3.currentProvider);
    } else {
      //Spécifie l'instance par défaut si aucune instance web3 n'est fournie.
      App.web3Provider = new Web3.providers.HttpProvider('http://localhost:7545');
      web3 = new Web3(App.web3Provider);
    }
    return App.initContract();
  },
```

FIGURE 13 – Fonction Web3.

InitContract : On récupère l'instance déployée du contrat intelligent à l'intérieur de cette fonction et on y attribue des valeurs qui nous permettront d'interagir avec elle.

```
initContract: function() {
  $.getJSON("Election.json", function(election) {
    // Instantier un nouveau  contract truffle de l'artefact
    App.contracts.Election = TruffleContract(election);
    // Connectez le fournisseur pour interagir avec le contrat
    App.contracts.Election.setProvider(App.web3Provider);

    App.listenForEvents();

    return App.render();
  });
},
```

FIGURE 14 – Fonction InitContract.

Fonction castVote : Lorsqu'on appelle la fonction de vote à partir de notre smart contract, on passe cet ID et on fournit au compte courant les métadonnées "from" de la fonction.

```
  castVote: function() {
    var candidateId = $('#candidatesSelect').val();
    App.contracts.Election.deployed().then(function(instance) {
      return instance.vote(candidateId, { from: App.account });
    }).then(function(result) {
      // Wait for votes to update
      $("#content").hide();

      $("#loader").show();
    }).catch(function(err) {
      console.error(err);
    });
  }
};
```

FIGURE 15 – Fonction CastVote.

Résumé

La blockchain a dépassé largement son application classique de monnie électronique sans autorité centrale. Cette technologie a apporté des nouveaux concepts qui assure l'immutabilité et renforce la sécurité. Ces caractéristiques rendent la technologie de blockchain appropriée pour plusieurs domaines, tels que : les systèmes de vote et la santé.

Dans ce mémoire,nous avons étudié le système blockchain ,les smart contrat ainsi que la plateforme Ethereum. Nous avons abordé la problématique de vote et le Covid-19 qui ont besoin de confiance et de transparence des données ,nous avons proposé des solutions basées sur cette technologie. Nos propositions concernent une application pour le vote électronique et une solution pour permettre de suivre les études universitaires durant la pandémie de Covid-19 sans risque

Pour la conception et la modélisation nous avons utilisée l'UP et UML alors que la réalisation est faite sous la plateforme de développement Ethereum basé sur les smart contracts.

Mots clés : blockchain, vote en ligne, santé, Covid-19, smart contract, Ethereum.

Abstract

Blockchain has gone well beyond its classic application of cryptocurrency without a central authority. This technology has introduced new concepts that ensure immutability and enhance security. These characteristics make the technology of blockchain suitable for several areas, such as : voting systems and healthcare.

In this thesis ,we studied the blockchain system , the smart contract and the Ethereum platform. We tackled the issue of voting and covid-19 which need confidence end transparency of data and proposed solutions based on this technology. Our proposals concern an application for electronic voting and a solution to allow university studies to be followed during the Covid-19 pandemic without risk.

For the design and the modelization we used UP and UML while for the development we used the Ethereum platform based on smart contracts.

Key words : blockchain, online voting, health, Covid-19, smart contract, Ethereum.