الجـــــــــــــــــــــمـهـوريـــــة الجـــــــــــــزائـريـة الديمـــــــقـراطيـة الـشـــــــــعبيـة

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التـــــــــــــــــــــــــــعـليـم العـــــــالي و البـــــــــحث العـــــلـمـــي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جـــــــــــــــامعة أبي بكـــر بـلـقـايد – تـلمســـــــــــــــان –

Université Aboubakr Belkaïd – Tlemcen –

Faculté de TECHNOLOGIE

MEMOIRE

Présenté pour l'obtention du **diplôme** de **MASTER**

En : Télécommunications

Spécialité : Réseaux et Télécommunications

Par: BOUCHAOUR Abdelhamid Nabil

BENYAHIA Anes Zakarya

Sujet

Le vote électronique basé sur la Blockchain

Soutenu publiquement, …/07/2021, devant le jury composé de :

Sidi mohammed Hadj irid	MCA	Univ. Tlemcen	Président
Mourad Hadjila	MCA	Univ. Tlemcen	Examinateur
Moussaoui Djilali	MCB	Univ. Tlemcen	Encadrant


بسم الله الرحمن الرحيم

Dédicaces

Tout d'abord, je rends grâce à Dieu le tout puissant de m'avoir donné la foi et la force de mener à terme ce modeste travail que je dédie particulièrement : A mon soutien moral et source de joie et de bonheur, celui qui s'est toujours sacrifié pour me voir réussir, mon père que Dieu lui prête longue vie, santé et joie. A la lumière de mes jours, la source de mes efforts, la flamme de mon cœur, ma vie, mon bonheur, ma mère que j'adore qui m'a conseillée, aidée et encouragée durant toute la période de préparation de ce mémoire. A ma sœur qui m'a été d'un grand soutien moral. Aux familles du plus grand au plus petit pour leurs encouragements.

A mes amies pour leur soutien et leur loyauté envers ma personne. A tous qui m'ont inculqué le savoir du primaire jusqu'à l'université.

Benyahia Anes Zakarya

Dédicaces

Tout d'abord, je rends grâce à Dieu le tout puissant de m'avoir donné la foi et la force de mener à terme ce modeste travail que je dédie particulièrement : A mon soutien moral et source de joie et de bonheur, celui qui s'est toujours sacrifié pour me voir réussir, mon père que Dieu lui prête longue vie, santé et joie. A la lumière de mes jours, la source de mes efforts, la flamme de mon cœur, ma vie, mon bonheur, ma mère que j'adore qui m'a conseillée, aidée et encouragée durant toute la période de préparation de ce mémoire. A mes frères et sœurs et qui m'ont été d'un grand soutien moral. Aux familles du plus grand au plus petit pour leurs encouragements.

A mes amies pour leur soutien et leur loyauté envers ma personne. A tous qui m'ont inculqué le savoir du primaire jusqu'à l'université.

Bouchaour Abdelhamid Nabil

Remerciement

Tout d'abord nous adressons nos plus sincères sentiments de reconnaissance et de remerciement envers ALLAH, le clément et le miséricordieux, lequel nous a accordé la force et le courage de mener à bien ce modeste travail.

Notre gratitude s'adresse à Monsieur Moussaoui Djilali Docteur à l'université de Tlemcen pour son encadrement, son orientation, ses conseils et la disponibilité qu'il nous a témoignée pour nous permettre de mener à bien ce travail. Ses conseils et son support moral nos énormément aidé à mener à terme ce travail.

Nos vifs remerciements à Messieurs Medjadji Mohammed Yacine et Medjadji Abdelmounaim, pour nous avoir codirigé, soutenu, encouragé et orienté tout au long de ce projet.

Nos vifs remerciements aux membres du jury d'avoir accepté d'examiner et d'évaluer notre travail. Un grand merci à tous les professeurs de Télécommunications qui ont participé à notre progrès pendant ces 5 ans.

Enfin, nos remerciements à tous nos amis, nos collègues qui nous ont soutenu et encouragé pour la réalisation de cet humble mémoire.

Résumé

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

Dans ce mémoire, nous avons étudié le système blockchain, les smart contracts ainsi que la plateforme Ethereum.

Nous avons abordé la problématique de vote qui exige confiance et transparence des données, nous avons proposé des solutions basées sur cette technologie. Nos propositions concernent une application pour le vote électronique

Pour la conception et la modélisation nous avons utilisé l'UP (Unified Process) et l'UML (Unified Modeling Language), quant à la réalisation elle a été faite sous la plateforme de développement Ethereum basée sur les smart contracts.

Mots clés : blockchain, bitcoin, vote en ligne, sécurité, réseau, 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 In this Master project, we studied the blockchain system, the smart contract and the Ethereum platform.

We tackled the issue of voting need confidence end transparency of data and proposed solutions based on this technology. Our proposals concern an application for electronic voting.

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, bitcoin, online voting, security, network, smart contract, Ethereum

ملخص

لقد ذهب blockchain إلى أبعد من تطبيقه الكلاسيكي للنقود الإلكترونية بدون سلطة مركزية. جلبت هذه التكنولوجيا مفاهيم جديدة تضمن ثباتها وتعزز الأمن. هذه الخصائص تجعل تقنية blockchain مناسبة لعدة مجالات، مثل: أنظمة التصويت

في هذا المشروع، درسنا نظام blockchain والعقود الذكية بالإضافة إلى منصة.Ethereum

تناولنا مسألة التصويت التي تحتاج إلى ثقة وشفافية في البيانات، واقترحنا حلولاً تعتمد على هذه التقنية. تتعلق مقترحاتنا بطلب للتصويت الإلكتروني

بالنسبة للتصميم والنمذجة، استخدمنا UP وUML أثناء التنفيذ في إطار منصة تطوير Ethereum على أساس العقود الذكية.

Table des matières

Liste des tables

Liste des figures

Introduction générale

La blockchain est un terme dans le domaine des technologies de l'information. il s'agit de Partager essentiellement la base de données et les informations qu'elle contient. Les caractéristiques du stockage sont «infalsifiables», «traçables», «ouvertes et Transparentes». Sur la base de ces caractéristiques, la technologie de La blockchain a jeté les bases solides de la "confiance " et mis en place un mécanisme de coopération Il est **fiable** et à **de larges perspectives d'application**.

Le 10 janvier 2019, le National Internet Information Office a publié le « Règlement sur la gestion des services d'information sur la blockchain ». Le 24 octobre 2019, lors de la dix-huitième étude collective du Bureau politique du Comité central, le secrétaire général Xi Jinping a souligné que "prendre la blockchain comme une percée importante dans l'innovation indépendante des technologies de base" "accélérer le développement de la technologie blockchain et l'innovation industrielle". La « blockchain » est entrée dans le champ de vision du public est devenue le centre d'intérêt de la société. La blockchain provient du Bitcoin de Satoshi Nakamoto. En tant que technologie, la blockchain est une solution technique qui ne repose pas sur des tiers et utilise ses propres nœuds décentralisés pour stocker, vérifier, transférer et communiquer les données du réseau. Par conséquent, c'était sous un angle de comptabilité financière, la technique blockchain est considérée comme un grand centre de facturation de réseau distribué. Tout le monde peut utiliser en même temps les normes techniques, ajouter leurs propres informations, étendre La blockchain et continuer de répondre aux besoins de saisie de données induites par divers besoins. Cette technologie, qui fait l'objet de notre travail, a été adaptée avec succès sur **l'étude et la conception d'un vote électronique.**

Le mémoire est organisé de la façon suivante : le premier chapitre détail les concepts fondamentaux de la technologie blockchain. Le deuxième chapitre est dédié à la présentation du système de vote en ligne. Le troisième chapitre est destiné a la modélisation et la réalisation du système de vote en ligne en spécifiant les outils, les langages et l'environnement de développement. Le mémoire est clôturé par une conclusion générale.

Chapitre 01

Concept de base de la technologie blockchain

1. Historique

La technologie sur laquelle se base les crypto-monnaies se nomme la Blockchain, ou chaîne de blocs en français. Elle permet à tous les acteurs d'un même réseau d'atteindre un consensus sans jamais remettre en cause la confiance, et donc les rôles, accordés à chacun d'entre eux.

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

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

En 2004, l'informaticien et activiste cryptographique Hal Finney (Harold Thomas Finney II), lance un système appelé PoW « Reusable Proof Of Work » pour « Preuve de travail réutilisable »).

Le système fonctionnait en recevant un jeton preuve du travail non échangeable et non fongible basé sur le système Hashcash, celui-ci créait en retour un jeton possédant une signature RSA qui pouvait ensuite être transféré de personne en personne.

Le PoW a résolu le problème de la double dépense en conservant un registre de la propriété des jetons, enregistré sur un serveur de confiance, conçu pour permettre à n'importe quel utilisateur à travers le monde de vérifier son exactitude et son intégrité en temps réel.

On peut considérer le PoW comme un premier prototype et une première étape dans l'histoire des crypto-monnaies.

2. Définition

Nous présentons ci-dessous quelques définitions qui permettent de mieux comprendre ce qu'est la blockchain selon plusieurs points de vue [1] :

2.1 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.

2.2 Basique

La blockchain est une sorte de logiciel capable de stocker et de transmettre des données de manière transparente et sécurisée sur Internet sans avoir besoin d'une agence de contrôle centrale.

2.3 Littéral

Une blockchain désigne une chaine de blocs qui stocke diverses informations de toute nature.

2.4 Généraliste

Une blockchain est une technologie qui permet d'effectuer des transactions, Grâce à l'adoption d'un mécanisme de consensus collectif et à l'utilisation de registres publics, décentralisés et partagés, des transactions peuvent être effectuées, simplifiant ainsi les processus d'affaires tout en instaurant la confiance, la responsabilité et la transparence.

2.5 Technique

La blockchain est une nouvelle technologie de base de données. Cette base de données de transactions distribuée est comparable à un grand livre, dans lequel chaque nouvelle transaction est écrite après d'autres transactions sans possibilité de modification ou de suppression. Grâce à un système de confiance réparti entre les membres ou les participants (nœuds), ce registre est actif, chronologiquement, distribuable, vérifiable et peut empêcher la falsification.

Pour résumer : La blockchain est une base de données de transactions distribuée, qui permet de stocker et de transmettre des informations via Internet de manière transparente, sûre et autonome, sans avoir besoin d'une agence de contrôle centrale. [1].

3. Pourquoi utiliser la technologie Blockchain

La deuxième question que les gens posent habituellement lorsqu'ils entendent parler de la blockchain est : pourquoi utiliser la blockchain ? Pourquoi utiliser un grand livre distribué ? Pourquoi ne pas utiliser une base de données régulière ou un système hérité comme système d'enregistrement dans ce monde déjà numérique ? Dans cette partie, nous examinons ce qu'est réellement une blockchain, ce qu'elle peut faire et, surtout, pourquoi utiliser la blockchain ?

3.1 La Blockchain et le registre distribué

Juste au cas où vous auriez besoin d'un petit rattrapage, les gens parlent souvent de « blockchain » au singulier, comme s'il n'en était qu'un. En réalité, ils devraient parler de la technologie de la chaîne de blocs également connue sous le nom de technologie de registre distribué ou DLT ou des chaînes de blocs au pluriel, car il en existe de nombreuses différentes, y compris les chaînes de blocs publiques (sans autorisation) et privées (avec autorisation)

La blockchain est un moyen simple mais ingénieux de transmettre des informations de A à B de manière entièrement automatisée et sûr. Une partie à une transaction lance le processus en créant un bloc. Ce bloc est vérifié par des milliers, voire des millions d'ordinateurs répartis sur le Net. Chaque bloc de la chaîne est chronologiquement connecté aux blocs précédents et synchronisé avec les nœuds du réseau, créant non seulement un enregistrement unique, mais la falsification d'un seul block signifierait la falsification de la chaîne de block entière ce qui rend très difficile la falsification.

4. Architecture technique de la blockchain

Cette partie se concentre sur l'analyse du cadre technique de la technologie Blockchain.

Après l'avoir parcouru et démontré son intérêt pour les nouveaux cas d'utilisation émergents, cette section présentera les éléments constitutifs de la technologie. Avant de résumer les technologies et les outils, nous présenterons des produits à différentes étapes de la blockchain. Sur la figure 1-1, il est essentiellement divisé en 9 dimensions. Ensuite, nous analyserons en détail le contenu spécifique de chaque module. [4].

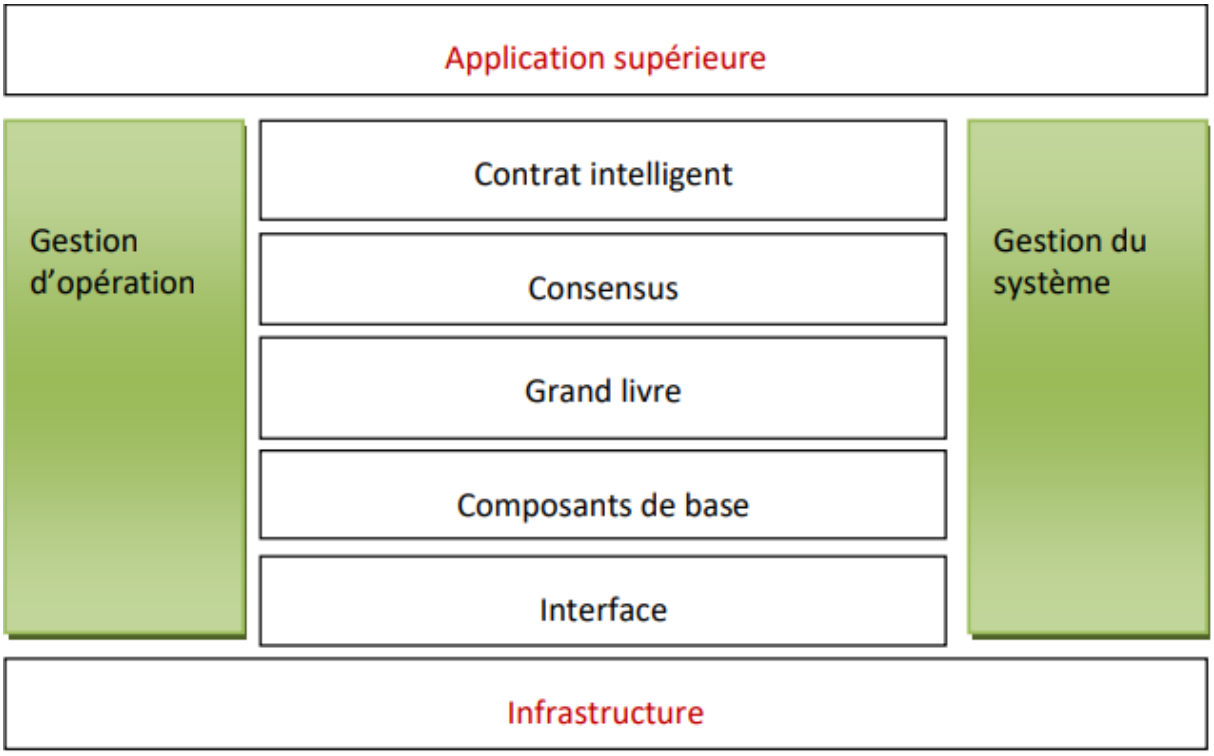

Figure 1-1 – Architecture technique de la technologie blockchain

4.1 Infrastructure

La couche infrastructure fournit des systèmes d'exploitation et des installations matérielles, y compris des serveurs physiques, des hôtes cloud, etc… Il peut être divisé en trois zones pour le fonctionnement normal du système blockchain :

- Ressources informatiques (CPU, GPU, ASIC, etc.).
- Ressources de stockage (disque dur).
- Cette partie des ressources du réseau (bande passante) n'est pas très différente des autres systèmes. Elle n'est rien de plus qu'orientée vers le calcul, certaines orientées vers le stockage et d'autres fortement dépendantes du réseau [5].

4.2 Les composants de base

La couche de composant de base réalise l'enregistrement, la vérification et la diffusion des informations dans le système blockchain. La blockchain est un système distribué, ce qui signifie que tous les blocs signés sont répliqués sur tous les nœuds du réseau. Comme tout le monde, vous pouvez utiliser un ordinateur pour faire des nœuds au besoin. Pour ce faire, vous devez télécharger tous les blocs qui ont été signés jusqu'à présent. Pour Bitcoin, cela a dépassé 180 Go.

Lorsqu'un nœud parvient à signer un nouveau bloc en premier, il sera ajouté à la blockchain de tous les autres nœuds du réseau afin qu'il dispose toujours de la dernière blockchain n'importe où sur le réseau. Il existe un grand nombre de nœuds dans le monde, et ils ont tous une copie complète de la blockchain.

4.2.1 Découverte du réseau

Le système blockchain est composé de nombreux nœuds connectés via le réseau, en particulier dans le système de chaîne publique, le nombre de nœuds est généralement très important. Chaque nœud doit découvrir le nœud voisin via le protocole de découverte de réseau et établir un lien avec le nœud voisin.

4.2.2 émetteur-récepteur de données

Une fois que le nœud est connecté au nœud voisin avec le protocole de communication réseau, le module émetteur-récepteur de données termine l'échange de données avec d'autres nœuds. La diffusion des transactions, le consensus des messages et la synchronisation des données sont tous effectués par ce module.

4.2.3 Les algorithmes de cryptage

sont utilisés pour assurer l'intégrité de la blockchain, l'identité des participants, l'authenticité des transactions et la confidentialité du contenu, y compris divers algorithmes de codage, algorithmes de hachage, algorithmes de signature, algorithmes de protection de la vie privée, etc..

4.2.4 Stockage de données

Les données du système de blockchain utilisent différents modes de stockage de données. Les modèles de stockage incluent des bases de données relationnelles (telles que MySQL 3) et des bases de données non relationnelles (telles que LevelDB4). Généralement, les données à sauvegarder comprennent des données publiques (par exemple : données de transaction, données d'état, etc.) et des données privées locales.

4.2.5 Notification de message

Le module de notification de message fournit des services de notification de message entre différents composants de la blockchain et entre différents nœuds.

Une fois la transaction réussie, le client doit généralement suivre, enregistrer et obtenir les résultats de l'exécution de la transaction pendant que la transaction est en cours d'exécution. Le module de notification de message peut compléter la génération, la distribution, le stockage et d'autres fonctions de messages pour répondre aux besoins du système blockchain.

4.3 Grand livre

La couche du grand livre est responsable du stockage. Tous les participants au réseau ont accès au grand livre distribué et à ses enregistrements de transactions immuables. Avec ce grand livre partagé, les transactions ne sont enregistrées qu'une seule fois. La couche du registre fusionne la signature de hachage du bloc précédent dans le bloc suivant pour former une structure de données blockchain. La couche du grand livre dispose de deux méthodes pour enregistrer les données basées sur les actifs et les données sur les comptes. Dans le modèle basé sur l'actif, l'actif est d'abord modélisé, puis la propriété de l'actif est enregistrée, c'est-à-dire que la propriété est un champ de l'actif. Dans le modèle basé sur le compte, le compte est établi en tant qu'objet d'actifs et de transactions, et les actifs sont les champs sous le compte.

Le grand livre possède les avantages suivants :

4.3.1 Modèle de données basé sur le compte

Facile à enregistrer et à interroger les informations associées

4.3.2 Modèle de données basé sur les actifs

Ce modèle possède une haute simultanéité afin d'obtenir des performances de traitement simultanées élevées et d'interroger les informations liées au compte dans le temps. Plusieurs plateformes de blockchain migrent vers deux modèles de données ce qui conduit au développement d’un modèle mixte.

4.4 Consensus

La couche de consensus est chargée de coordonner et d'assurer la cohérence des enregistrements de données de chaque nœud dans l'ensemble du réseau, c'est-à-dire que tous les nœuds sont en concurrence pour ajouter le bloc suivant à la blockchain, mais un seul d'entre eux sera sélectionné pour le faire (Seulement il paiera). Pour chaque nouveau bloc, cette sélection est aléatoire. Ce caractère aléatoire est très important pour la sécurité de la blockchain. Parce que personne ne sait quel mineur choisir. Il existe de nombreuses manières de réaliser cette sélection aléatoire de mineurs : il s'agit d'un mécanisme de consensus.

Le premier mécanisme de consensus est Proof of Work (POW) qui est généralement utilisé dans les blockchains publiques. Par conséquent, plus la puissance de calcul du mineur est élevée, plus la probabilité de sélection est élevée. La puissance de calcul étant chère, le coût d'acquisition de 51% de la puissance de calcul totale du réseau est très élevé Il s'agit d'un moyen de protéger la sécurité du réseau qui rend le coût d'une attaque disproportionné par rapport au bénéfice.

Le deuxième mécanisme de consensus est utilisé pour les blockchains privées où les nœuds appartiennent à la même entité, ou les blockchains semi-privées où les nœuds appartiennent à un Consortium de différents utilisateurs autorisés. Le second type ne nécessite pas un mécanisme de consensus coûteux comme POW, car les participants sont connus et font confiance dans une certaine mesure. Dans ce cas, le mécanisme de consensus utilisé est beaucoup plus simple que l'algorithme PBFT5 [6]

Ci-dessous, nous listons la comparaison de quelques algorithmes de consensus [7]

Mécanisme du consensus	**Description**	**Avantages**	**inconvénients**
POW	Dans une blockchain publique, les ordinateurs des mineurs sont mis à disposition pour résoudre un problème mathématique compliqué. Le 1erqui trouve une solution gagne la récompense du prochain bloc de la chaine	Simple à mettre en œuvre. Sécurisé. Faible. Consommation des ressources réseau.	Consomme trop de ressources informatiques. La probabilité de bifurcation est élevée. Le consensus prend plus de temps.
POS	Preuve d'enjeu. Les validateurs de transactions doivent mettre en gage la possession de crypto monnaie pour recevoir une récompense. Si un nœud est malveillant, il peut perdre sa mise en gage au profit des validateurs honnêtes	Moins de consommation de ressources.	La mise en œuvre est plus compliquée. Faille de sécurité. Pression de trafic réseau élevée.
BPFT	Consensus dont la liste des validateurs est connue au départ et peut tolérer jusqu'à 1/3 de nœuds compromis (déconnectés ou malveillants).	Consensus de groupe rapide et performant. Pas de fork ou de réorganisation de chaine	Chaine privée uniquement.
POA	Preuve d'autorité. Consensus dont la liste des validateurs est connu au départ et qui valide à tour de rôle un bloc. Ce type de consensus peut tolérer jusqu'à 49% de	Consensus de groupe rapide.	Chaine privée uniquement. Fork ou réorganisation de la chaine possible.

	nœuds malveillants ou déconnectés.		

Tableau 1-1 – Comparaison des mécanismes de consensus de la blockchain

4.5 Contrat intelligent

La couche de contrat intelligent est responsable de la mise en œuvre, de la compilation et du déploiement de la logique métier du système blockchain sous forme de code, de la finalisation du déclenchement des conditions et de l'exécution automatique des règles établies, et de la minimisation des interventions manuelles.

Les objets d'exploitation des contrats intelligents sont principalement des actifs numériques. Une fois les données confirmées, il est difficile de changer et la condition de déclenchement est forte, ce qui signifie que l'application de contrats intelligents a une valeur élevée et un risque élevé. Comment éviter les risques et exercer de la valeur est une difficulté dans l'application actuelle à grande échelle des contrats intelligents.

À l'heure actuelle, l'application des contrats intelligents en est encore à un stade relativement précoce et les contrats intelligents sont devenus la «zone la plus touchée» de la sécurité de la blockchain. Du point de vue du temps de sécurité causé par les vulnérabilités des contrats intelligents précédents, il existe de nombreuses vulnérabilités de sécurité dans le contrat portable, ce qui pose de grands défis à sa sécurité. [8].

À l'heure actuelle, il existe plusieurs idées pour améliorer la sécurité des contrats intelligents :

Le premier est la vérification formelle, qui utilise des preuves mathématiques rigoureuses pour s'assurer que la logique représentée par le code du contrat répond à l'intention. La loi est logiquement stricte, mais difficile, et oblige généralement une organisation professionnelle tierce à réaliser des audits.

Le second est le cryptage intelligent des contrats, Les tiers ne peuvent pas lire les contrats intelligents au format texte brut, ce qui réduit les attaques de contrats intelligents en raison de vulnérabilités de sécurité logique. Cette méthode est moins chère, mais pas open source.

Le troisième est de réglementer strictement le format grammatical de la langue contractuelle. Résumez d'excellents modèles de contrats intelligents, développer des modèles de contrats intelligents standards et standardiser la préparation de contrats intelligents avec certaines normes pour améliorer la qualité des contrats intelligents et améliorer la sécurité des contrats.

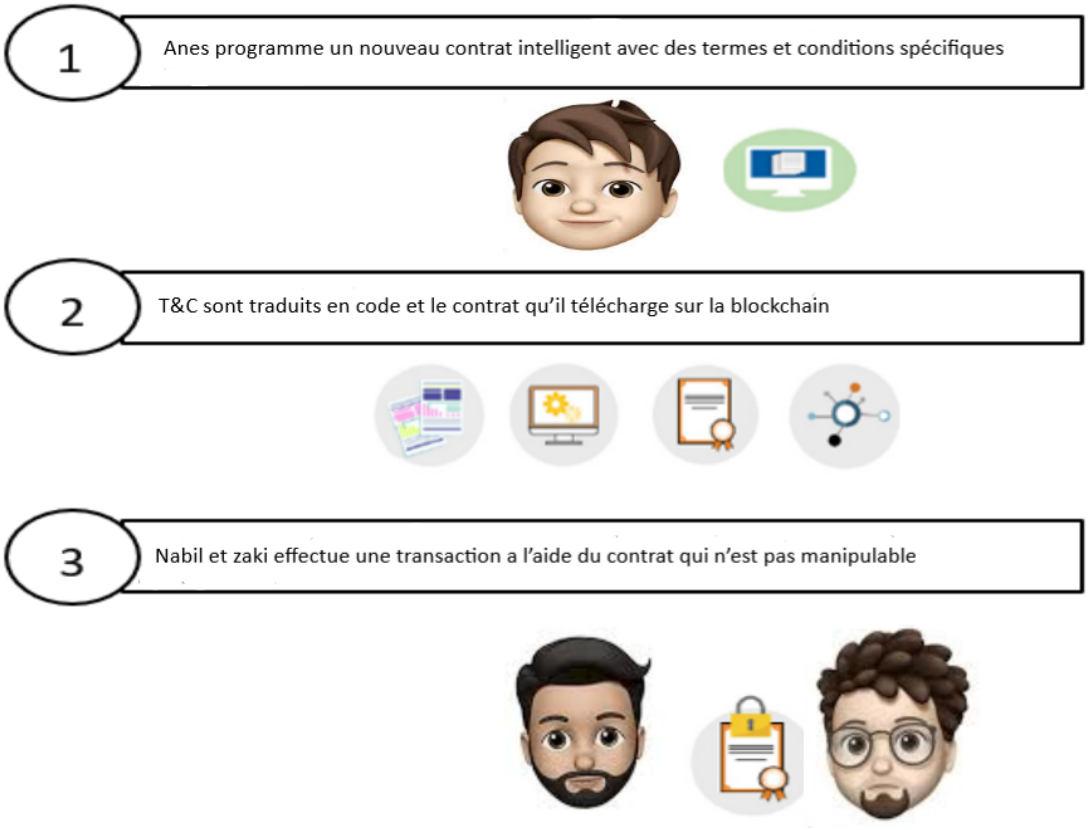

Figure 1-2 – Fonctionnement de contrat intelligent

4.6 Gestion de système

La couche de gestion du système est responsable de la gestion d'autres parties de l'architecture de la blockchain, comprenant principalement deux fonctions : la gestion des autorisations et la gestion des nœuds. La gestion des droits est un élément clé de la technologie blockchain, en particulier pour les chaînes d'autorisation qui ont plus d'exigences d'accès aux données.

4.7 Interface

La couche d'interface est principalement utilisée pour compléter l'encapsulation des modules fonctionnels et fournir une méthode d'appel simple pour la couche d'application.

4.8 Application

La couche application est la partie qui est finalement présentée à l'utilisateur. Sa fonction principale est d'appeler l'interface de la couche de contrat intelligent pour s'adapter à différents scénarios d'application blockchain et fournir aux utilisateurs différents services et applications.

4.9 Fonctionnement et maintenance

L'équipe de gestion de l'exploitation et de la maintenance est principalement responsable de l'exploitation et de la maintenance quotidienne du système blockchain, Y compris la journalisation, la surveillance, la gestion et l'expansion.

Dans une architecture unifiée, les plates-formes traditionnelles ont différents modules de stockage, modèles de données, structures de données, langages de programmation et environnements sandbox 6 en fonction de leurs propres besoins et emplacements.

5. Domaines d'application de blockchain

Voici quelques domaines d'application de la technologie blockchain [9, 10, 11, 12 ,13 ,14] :

5.1Vote

La blockchain promet un vote sécurisé et inviolable dont le résultat, transparent et fiable, est audit able 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.

5.2 Jeux

Il existe de nombreux jeux basés sur la technologie blockchain, et ils peuvent être trouvés sur Internet. Les jeux que l'on trouve généralement sont des jeux de hasard, tels que le craps ou les jeux de casino. Ces jeux basés sur la blockchain permettent aux joueurs d'avoir la propriété permanente et le contrôle complet de leurs actifs de jeu

5.3 La gestion des identités

Dans certains domaines de l'entreprise, la vérification de l'identité personnelle est un défi. Cependant, avec l'aide de la technologie blockchain, les identités des personnes peuvent être identifiées de manière plus sûre et plus rapide que jamais. Ceci est basé sur un grand nombre de bases de données qui permettent l'identification et la vérification. En particulier, les documents d'identité existants - permis de conduire, passeport et carte d'identité peuvent donc être mis en œuvre numériquement en toute sécurité. Étant donné que les données sont stockées de manière décentralisée, la perte de données peut également être évitée.

5.4 Energie

En particulier sur le marché complexe de l'énergie, en raison de la transparence et de la traçabilité de la technologie blockchain, des progrès considérables ont été réalisés. Cela facilitera la recharge des systèmes solaires privés, le suivi de l'énergie, la gestion des actifs et la délivrance des certificats

d'origine. Une bonne supervision et un suivi transparent devraient avoir un impact majeur sur le succès des changements, en particulier dans la conversion d'énergie. Autre exemple, les véhicules électriques par exemple, peu importe où vous faites le plein sur le réseau, l'énergie peut être allouée à chaque voiture séparément pour faciliter la facturation.

5.5 Commerce

La blockchain peut améliorer les processus de plusieurs manières. Par exemple, en utilisant cette technologie pour suivre les marchandises du début de la chaîne d'approvisionnement au point de vente et au service, nous pouvons prendre les mesures nécessaires lorsque des problèmes surviennent dans la chaîne.

5.6 Les assurances

La blockchain a le potentiel de révolutionner le secteur de l'assurance. Leur potentiel technique permet de dessiner de nouveaux modèles économiques entièrement numériques, transparents et sécurisés pour obtenir une interaction rapide entre de nombreux participants. Avec l'aide de la blockchain, les compagnies d'assurance peuvent simplifier et accélérer la tarification et la prestation de services, déterminer l'authenticité des biens et des documents et suivre l'historique des activités frauduleuses individuelles.

5.7 Banque

Les banques agissent généralement en tant qu'intermédiaires de l'économie mondiale, gérant et coordonnant le système financier par le biais de leurs comptes internes. Comme cela n'est pas visible publiquement, cela oblige les gens à faire confiance à la banque et à son infrastructure souvent obsolète.

La technologie blockchain peut non seulement perturber le marché mondial des changes, mais également perturber l'ensemble du secteur bancaire en désactivant ces intermédiaires et en les remplaçant par un système fiable, sans restriction, transparent et accessible à tous.

La blockchain rend les transactions plus rapides et moins chères, améliore l'accès aux fonds, crée plus de sécurité des données, applique les accords de confiance par le biais de contrats intelligents et rend la conformité plus fluide.

5.8 Arts

La blockchain peut simplifier l'industrie de la musique, et son objectif est d'assurer une meilleure traçabilité des œuvres, la transparence de la gestion des droits d'auteur et la distribution des droits de paiement sans passer par des intermédiaires tels que Spotify ou Deezer. Il s'agit de la plate-forme de diffusion de musique décentralisée fournie par Voise.

5.9 Santé

Les données médicales sont généralement stockées numériquement. Les mettre ensemble et prêts à être utilisés peut être le plus grand potentiel de la blockchain. Dans certains cas, la technologie peut sauver des vies. Cela peut s'expliquer visuellement à travers trois exemples : l'enregistrement des dons d'organes, le rappel de faux médicaments et les projets de recherche médicale.

Dans le passé, des listes d'attente pour les dons d'organes ont été forgées à plusieurs reprises. En conséquence, la volonté des gens de faire un don d'organes a diminué. La blockchain peut empêcher de futures manipulations.

Avec l'aide de la technologie blockchain, la qualité des médicaments peut également être mieux contrôlée, car l'ensemble de la chaîne de production de la fabrication aux fluctuations de température et l'ensemble du trajet de transport du transport à la pharmacie peuvent être surveillés et stockés dans la blockchain. Résultat : Si le principe de la chaîne du froid n'est pas respecté, le médicament ne sera pas délivré. Dans tous les cas, la société pharmaceutique peut attribuer un code QR à chaque médicament que les patients peuvent scanner pour vérifier qu'il est authentique. Il n'est pas impossible de faire semblant, mais cela coûtera plus cher qu'avant.

Les projets de recherche peuvent également bénéficier grandement de la technologie blockchain : d'une part, ils peuvent partager la puissance de calcul et collaborer plus étroitement, d'autre part, les patients peuvent utiliser leurs données blockchain pour la recherche via une déclaration de consentement. Cela prendra du temps, car la technologie blockchain en est encore à ses débuts. Le concept de base ne peut être testé dans la pratique que si l'infrastructure nécessaire a été mise en place dans les hôpitaux, les cabinets de médecins et autres organisations médicales. Mais c'est aussi son plus grand avantage : désormais, les nouvelles technologies peuvent être entièrement conçues au profit des patients.

La figure ci-dessous [15], résume et représente les applications de la blockchain dans le domaine de la santé.

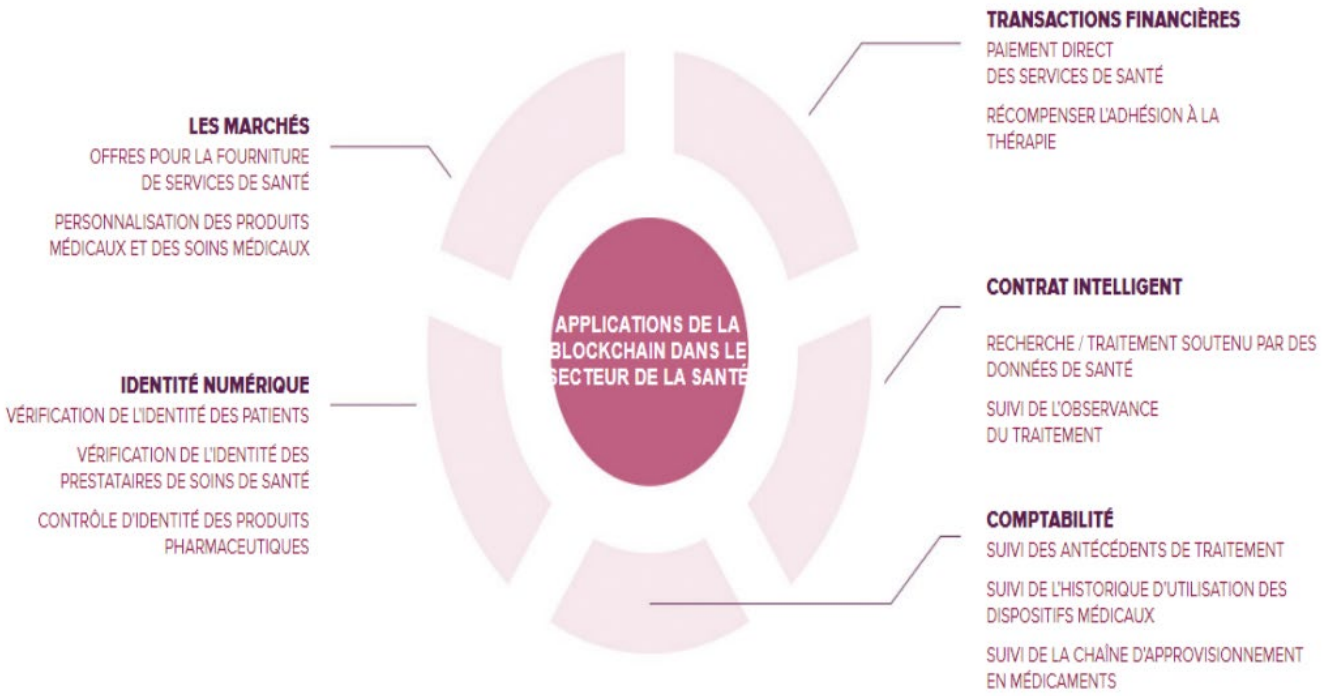

Figure 1-3 – Applications de la blockchain dans la santé

6. Comment fonctionne la Blockchain

Les tâches que nous effectuons sur les appareils numériques peuvent être divisées en deux catégories transactionnelles et non transactionnelles. Écrire des e-mails, regarder des vidéos et naviguer sur Internet sont pour la plupart des activités non transactionnelles, ce qui signifie que nous n'avons rien acheté ou vendu, ni signé d'accords contractuels. Cependant, nous effectuons de plus en plus de transactions en ligne, telles que la signature de contrats et l'achat d'articles ,Les transactions numériques sont plus rapides et plus pratiques, mais peuvent ne pas être sécurisées, ce qui permet aux cybercriminels de se connecter à nos comptes ou d'obtenir nos numéros de sécurité sociale et d'autres informations sensibles. La blockchain est conçue pour agir comme un compte public virtuel que tout le monde peut afficher et écrire avec une encre durable. Chaque bloc est un fichier et un nouveau bloc est créé toutes les 10 minutes, qui contient les enregistrements de toutes les transactions précédentes, répertoriées dans l'ordre et se terminant par une nouvelle transaction [16].

En termes techniques, la blockchain est une base de données distribuée basée sur des Merkle-Trees cryptés, c'est-à-dire qu'elle n'est ni créée, ni développée, et la base de données n'est pas non plus stockée dans l'unité centrale de traitement. Au lieu de cela, il existe une copie de chaque ordinateur ou «nœud» utilisé pour traiter et vérifier les transactions. Après avoir ajouté une nouvelle transaction, toutes les

copies seront modifiées en même temps. Si un nœud de réseau détecte une transaction non conforme aux règles du protocole, il sera expulsé immédiatement [17].

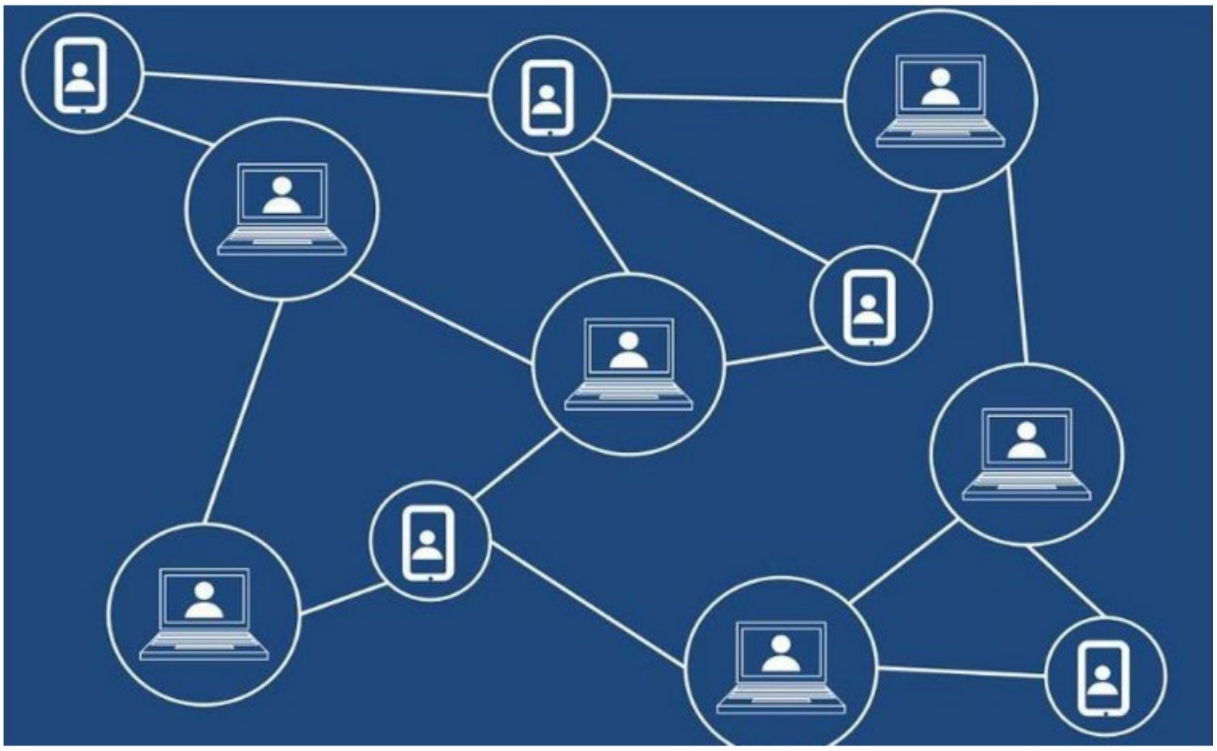

Figure 1-4 – Base de données de la blockchain

La blockchain la plus connue est le réseau Bitcoin. Lorsqu'une transaction est générée par un nœud, la transaction doit être transmise à d'autres nœuds pour vérification, puis confirmée par le mineur. L'opération ne peut pas être annulée. Ce processus implique le chiffrement des données de transaction via des signatures numériques et l'obtention d'une série de valeurs de hachage uniques représentant la transaction via une fonction de hachage, puis la diffusion des valeurs de hachage vers d'autres nœuds participants du réseau blockchain pour la vérification Bitcoin (voir figure ci-dessous). Chaque nœud effectue un calcul de preuve de travail (POW) pour déterminer qui peut vérifier les transactions.

Le nœud qui a obtenu le droit de vérification diffuse le bloc à tous les nœuds qui terminent le POW dès que possible, et diffuse son propre bloc à d'autres nœuds. A ce moment, d'autres nœuds confirmeront si la transaction contenue dans ce bloc est valide. Après avoir confirmé qu'ils n'ont pas été réutilisés et qu'ils ont une signature numérique valide, ils acceptent le blocage. À l'heure actuelle, le bloc est officiellement connecté à la blockchain [18].

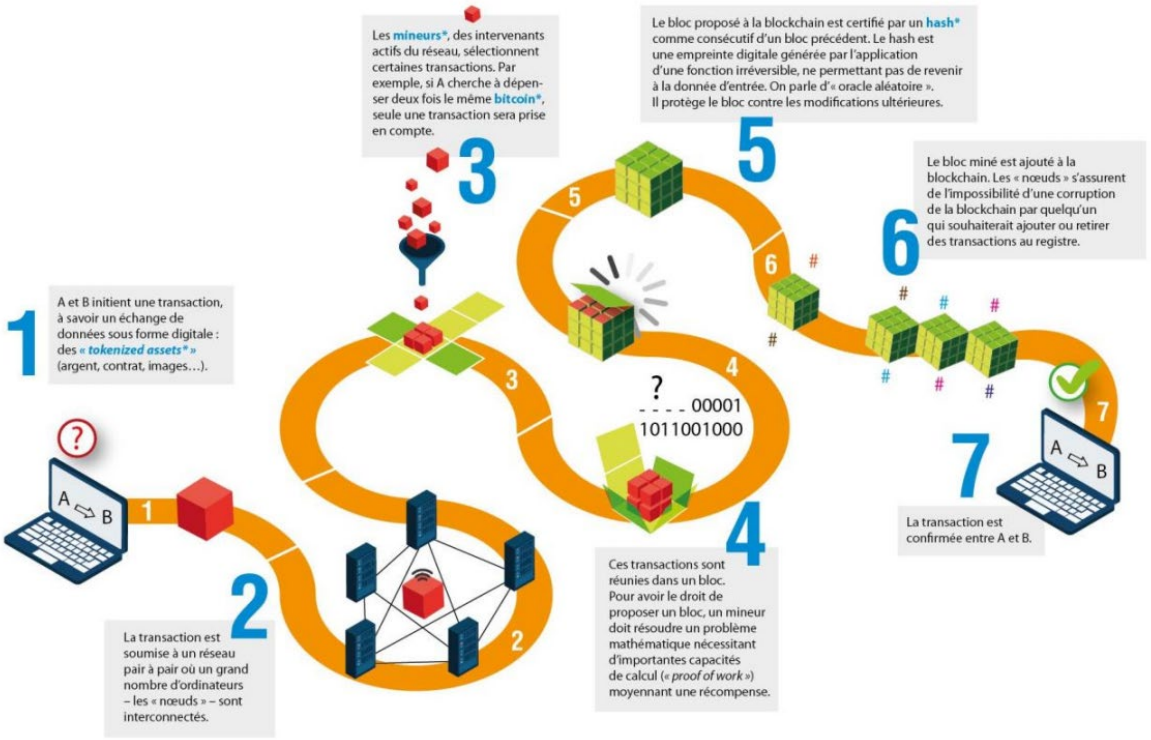

Figure 1-5 – Fonctionnement de la Blockchain

7. Blockchain vs Base de données normales

On dit que la blockchain est une sorte de base de données, donc « Quelle est la différence entre la blockchain et la base de données traditionnelle ? »

7.1 Centralisation vs Décentralisation système

Nous étudions la vraie raison du débat entre centralisation et décentralisation car la blockchain vise à être décentralisée. Cependant, les termes décentralisation et centralisation ne sont pas toujours clairs. La plupart des concepts et exemples de cette section sont donc inspirés des notes du fondateur de la blockchain Ethereum, M. Vilatik Buterin. Alors, qu'est-ce qu'un système distribué ? Un système distribué centralisé est un système, par exemple, un nœud maître est responsable de la décomposition des tâches ou des données et de la répartition de la charge entre les nœuds. En revanche, un système distribué décentralisé est un système sans "maître" [18]. La blockchain est donc un exemple, et nous en verrons de nombreux schémas plus loin dans ce chapitre.

7.1.1 Système centralisé

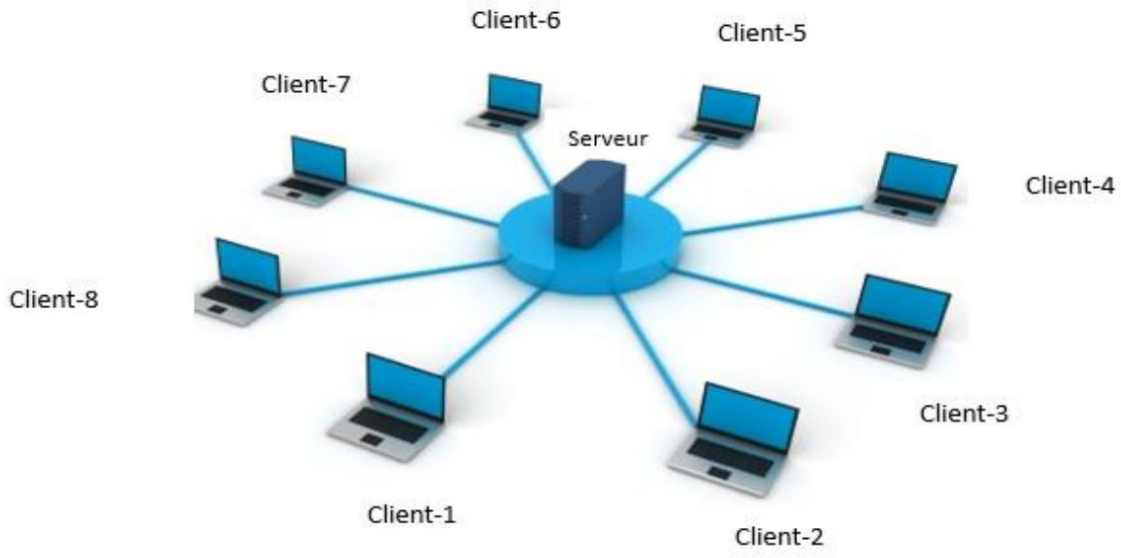

Figure 1-6 – Système centralisé

C'est un système de contrôle centralisé avec tous les droits de gestion, dans le cas de l'informatique c'est a priori serveur [19]. Comme le montre la figure ci-dessous, un système centralisé typique apparaîtra. Comme le montre la figure, tous les nœuds d'application sont hébergés sur un seul ordinateur et les utilisateurs peuvent se connecter directement à l'ordinateur central. Le principal problème d'un système centralisé est qu'il n'est pas facile à mettre à niveau. Le nombre de processeurs dans le système est limité et l'ensemble du système doit éventuellement être mis à niveau ou remplacé.

7.1.2 Système décentralisé

Comme son nom l'indique, ce système n'a pas de centre. L'idée du système de communication est que tous les nœuds peuvent faire partie d'un réseau sans autorité principale, et ces autorités peuvent communiquer entre elles [20].

Un système décentralisé typique peut apparaître comme illustré dans la figure ci-dessous :

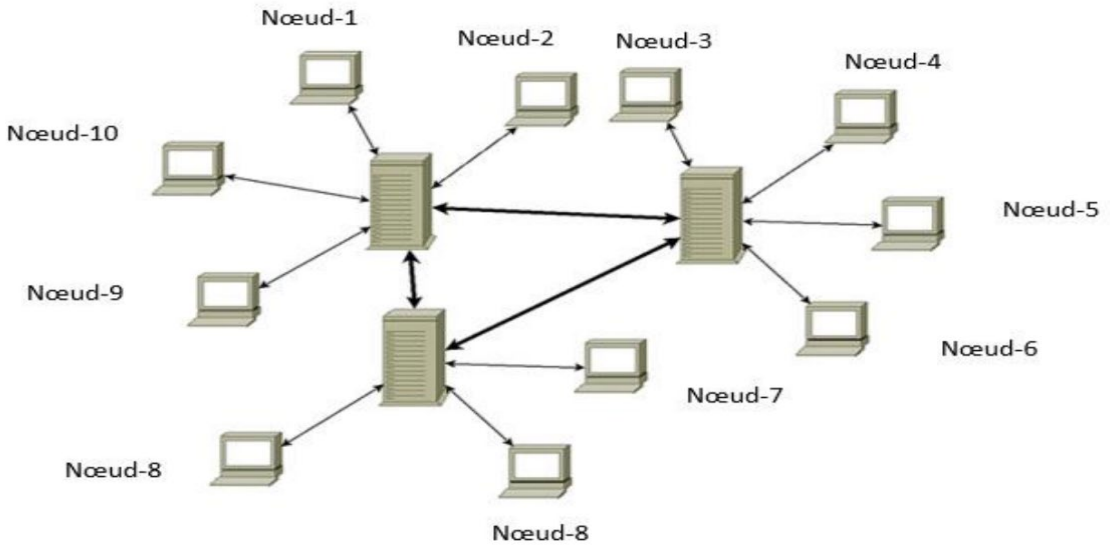

Figure 1-7 – Système décentralisé

Notez que les systèmes distribués peuvent également être décentralisés. Par exemple, la blockchain ! Cependant, contrairement aux systèmes distribués ordinaires, cette tâche n'est pas subdivisée en nœuds, car aucun maître n'effectuera cette tâche dans la blockchain. Pour les réseaux P2P ou « peer-to-peer », l'idée de cette architecture est de permettre au réseau de fonctionner normalement même si le réseau est coupé d'une partie de lui-même.

Le système peer-to-peer est illustré à la Figure I-8.

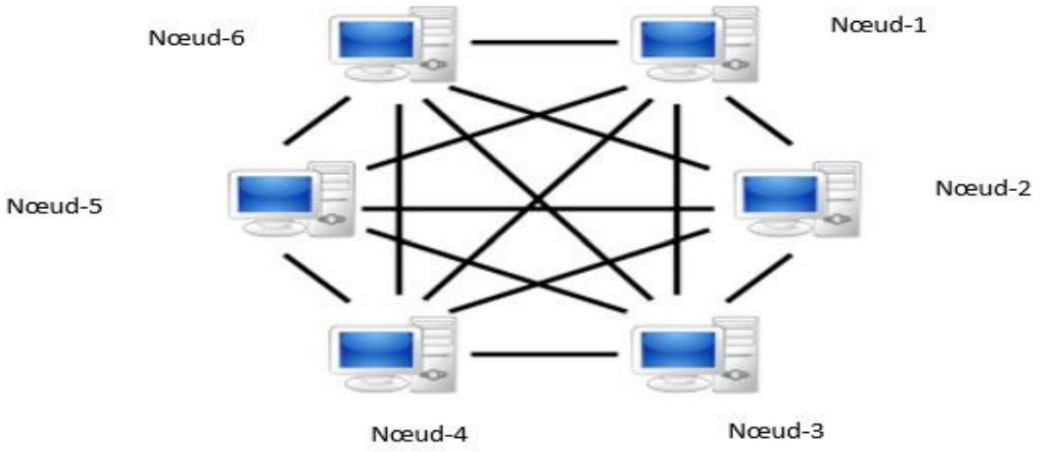

Figure 1-8 – Système décentralisé avec p2p architecture

La principale différence entre les systèmes «décentralisés» et «P2P complet» est l'emplacement des serveurs. Pour transformer un système distribué avec un serveur en un système P2P complet, vous placez un seul client sur le serveur, puis placez le serveur et le client sur la même machine. [21].

8. Grands principes de la blockchain

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

La Blockchain est une base de données, répartie entre tous les nœuds ;

La Décentralisation et désintermédiation : il n'y a pas d'autorité centrale pour contrôler la blockchain, il n'y a donc pas de tiers de confiance.

Consensus : Le résultat d'un consensus distribué est de réaliser une transaction

Infalsifiable : Une fois la transaction enregistrée sur la blockchain et la blockchain mise à jour, la transaction ne peut plus être modifiée.

Confiance et transparence partagées : la blockchain garantit la sécurité et la transparence des données.

Les blockchains les plus connues et les plus utilisées dans le monde sont : Bitcoin et Ethereum, mais en raison de l'existence d'autres types, les blockchains ne se limitent pas à ces derniers [2].

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

9. Types de blockchain

Vous ne pouvez pas devenir un investisseur ou un entrepreneur en crypto-monnaie sans vraiment comprendre les différences entre les types de blockchain et leurs implications. Alors, quelle est la différence entre une blockchain privée et une blockchain publique ? Et comment choisir l'une de ces options ? On dit que la blockchain est publique, ce qui signifie que n'importe qui peut être « ouvert » en tant que membre du réseau. La chaîne d'alliance est ouverte à des organisations spécifiques. De nos jours, l'industrie considère généralement que les chaînes d'alliance se situent entre les chaînes publiques et les chaînes privées, et appartiennent principalement à la catégorie des chaînes privées. Nous nous concentrerons sur les chaînes publiques et privées, car les chaînes de l'alliance peuvent être qualifiées de chaînes privées [23].

Il existe 3 types de blockchain :

9.1 Les blockchains publiques

Une blockchain accessible au public est appelée une blockchain publique. Ces blockchains n'ont aucune restriction sur la participation et les vérificateurs. Le principal avantage de ce type de blockchain est l'incontrôlabilité de la blockchain, ce qui signifie que personne ne peut contrôler totalement le réseau. Par conséquent, il assure la sécurité des données et contribue à l'immuabilité de

l'enregistrement. Tous les nœuds connectés à la blockchain publique auront les mêmes droits et, par conséquent, la blockchain publique sera entièrement distribuée.

9.1.1 Les caractéristiques de la blockchain publique

- Protéger les utilisateurs des développeurs.
- Faible barrière à l'accès.
- Toutes les données sont publiques par défaut.

9.2 Les blockchains privées

Ces blockchains nécessitent que les participants soient invités à faire partie de la blockchain. Ici, toutes les transactions ne sont visibles que par les personnes qui appartiennent à l'écosystème blockchain. Ces types de blockchains sont centralisés et bien meilleurs que les blockchains publiques. Les blockchains privées ont généralement des administrateurs réseau qui peuvent s'occuper des autorisations des utilisateurs au cas où un utilisateur spécifique aurait besoin d'autres autorisations à un certain endroit. Ceux-ci sont généralement utilisés dans les organisations privées pour stocker des informations sensibles sur l'organisation.

9.2.1 Les caractéristiques de la blockchain privée

- La vitesse de transaction est très rapide.
- Meilleure protection de la vie privée.
- Les coûts de transaction sont considérablement réduits voire nuls.
- Aide à protéger ses produits de base contre les dommages.

9.3 Les consortiums

Ces blockchains sont divisées en deux types différents, certains des nœuds sont privés, tandis que d'autres nœuds sont publics. Par conséquent, certains nœuds seront autorisés à participer à la transaction. D'autres nœuds contrôlent le processus de consensus. La blockchain hybride permet à tous les nœuds d'accéder à la blockchain, et le niveau d'informations accessible 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 droits de contrôle sur la blockchain et détermine le niveau de sécurité d'un utilisateur spécifique, tandis que les autres sont des utilisateurs qui accèdent simplement à la blockchain.[8]

10. 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.

10.1 Avantages

Parmi les avantages de blockchain on site [25,26] :

10.1.1 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.

10.1.2 Stabilité

Un blocage confirmé est difficile à annuler, donc une fois les données enregistrées sur la blockchain, il est 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 des pistes d'audit, car chaque changement sera suivi et enregistré en permanence dans les grands livres distribués et publics.

10.1.3 La sécurité

Étant donné que cette technologie dispose de divers mécanismes de vérification des données, il devient presque impossible de falsifier les informations contenues dans la blockchain. Tout d'abord, chaque fois que vous souhaitez modifier les données d'un bloc, vous devez modifier tous les blocs de la chaîne.

10.2 Inconvénients

Parmi les inconvénients du blockchain on trouve :

10.2.1 Difficulté de mise en œuvre

La blockchain est révolutionnaire, et l'une de ses lacunes est qu'elle est difficile à mettre en œuvre. Puisqu'il s'agit d'une technologie disruptive, il faut du temps pour établir tous les accords nécessaires à son fonctionnement normal. Par conséquent, il peut s'écouler des années avant que l'entreprise adopte et exploite le système.

10.2.2 Chômage

Puisque cette technologie vise à éliminer l'intermédiaire dans la transaction, l'une des conséquences possibles est sa perte permanente. En d'autres termes, si la technologie est fermée et doit être mise en œuvre de plus en plus, alors il n'y a pas besoin d'intermédiaire. Cela peut signifier son éradication totale (ou presque).

10.2.3 Anonymat

Nous utiliserons la crypto-monnaie comme exemple. Comme il s'agit d'un réseau ouvert, lorsqu'un utilisateur exécute une transaction, une autre personne pourra voir son journal d'activité. Imaginez le transfert aux parents. Cela peut voir toutes les données liées à votre crypto-monnaie. Cela signifie tout. De votre montant actuel au montant que vous avez déjà dépensé, et même à la façon dont vous le dépensez. Non seulement les transactions passées, mais aussi les contrats à terme. Donc, si beaucoup de gens ne montrent les traites bancaires à personne, pourquoi utiliser cette technologie ?

10.2.4 Espace de rangement

Au fil du temps, le grand livre de la blockchain deviendra très volumineux. La blockchain Bitcoin ne nécessite actuellement qu'environ 200 Go d'espace de stockage. La taille actuelle de la chaîne de blocs semble avoir augmenté au-delà des disques durs, et si le registre devient trop volumineux pour être téléchargé et stocké par des individus le réseau risque de perdre des nœuds

10.2.5 Clés privées

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

11. Plateformes de blockchain

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

11.1 Ethereum

La plate-forme blockchain Ethereum a fait beaucoup de bruit sur le marché, et c'est également l'une des meilleures plates-formes blockchain en 2019. Ethereum est une plate-forme blockchain open source, connue pour exécuter des contrats intelligents sur des réseaux blockchain personnalisés.

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 a plusieurs langages comme C ++ et python.

11.2 Fabric Hyperledger

C'est l'une des plateformes blockchain récemment développées. Le monde a découvert Hyperledger en 2016, et la Linux Foundation l'a également découvert. Son objectif est de stimuler l'utilisation de la technologie blockchain dans différents domaines.

Principales caractéristiques de Fabric Hyperledger :

- privé,
- 180+ entreprises collaboratrices,

- séquence : Production prête pour les entreprises,
- Langages pris en charge : Python.

11.3 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.

11.4 EOS

EOS est un réseau open source lancé en 2018 par la société privée Block.one.

Basé sur le concept de technologie décentralisée, il offre aux utilisateurs finaux la possibilité d'effectuer diverses tâches sur la plate-forme EOS. Il élimine également le besoin de frais d'utilisation, ce qui signifie que les utilisateurs peuvent profiter des avantages des applications basées sur EOS sans payer de frais.

Principales caractéristiques d'EOS :

- Ouvert au public,
- Langages pris en charge : C ++.

11.5 Stellar

Stellar est un réseau de grand livre distribué basé sur la technologie blockchain qui fournit des solutions de paiement transfrontalier rapides et économiques pour les entreprises et les particuliers. Avec l'aide de la plate-forme de blockchain Stellar, les développeurs peuvent créer des portefeuilles mobiles et des outils bancaires intelligents, tels que Paypal pour les paiements en ligne.

Principales caractéristiques de Stellar :

- Type de réseau : public et privé,
- Langues prises en charge : JavaScript, Java.

11.6 Neo

La plate-forme Neo est un réseau open source qui utilise des contrats intelligents blockchain pour gérer les actifs numériques. Neo a été fondé en 2014 et est devenu disponible sur GitHub en juin 2015. La plateforme Neo blockchain peut vous aider à payer des frais de transaction pour exécuter vos applications sur le réseau Neo. La plate-forme prend en charge diverses formes d'actifs numériques et vous pouvez également utiliser des certificats numériques pour créer en toute sécurité vos applications sur le réseau Neo.

Principales caractéristiques de Neo :

- Ouvert au public
- Langages pris en charge : C #, Java et Python.

11.7 Machine virtuelle Ethereum

EVM (ou Ethereum Virtual Machine) est l'environnement d'exécution de bytecode des contrats intelligents Ethereum. Chaque nœud du réseau exécute EVM. Tous les nœuds utilisent EVM pour exécuter toutes les transactions dirigées vers le contrat intelligent, de sorte que chaque nœud effectue le même calcul et stocke la même valeur. Une transaction qui ne transfère que de l'éther doit également être calculée, c'est-à-dire si l'adresse à un solde et le solde est déduit en conséquence. [28]

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

12. Diverses applications décentralisées de la technologie blockchain

Nous présentons ci-dessous une liste non exhaustive des diverses applications de la technologie blockchain [29] :

12.1 Bitcoin

Bitcoin est la première crypto-monnaie distribuée largement connue et largement utilisée. Il exploite un réseau peer-to-peer sans institution centrale ni banque, et introduit la technologie et les plates-formes blockchain dans le monde. La gestion des transactions et l'émission des pièces sont assurées conjointement par le réseau blockchain.

12.2 Coinbase

Coinbase a été lancé en tant que portefeuille de devises numériques en 2012, qui est une plate-forme d'échange de crypto-monnaie pour acheter, vendre et stocker Bitcoin (BTC) et Ethereum (ETH). La société a son siège à San Francisco, en Californie.

12.3 Storj

La plate-forme Storj fournit un stockage cloud basé sur la blockchain et un système de cryptage de bout en bout. Contrairement aux produits cloud traditionnels, les données ne sont pas stockées de manière centralisée sur les serveurs Storj, mais sont distribuées sur les ordinateurs des membres du réseau.

Lorsque vous utilisez Storj pour les transactions de paiement de l'espace de données, elles sont ajoutées à la chaîne sous forme de bloc. Une fois ajouté, il ne peut pas être supprimé, ce qui rend la transaction totalement sécurisée. D'autres personnes peuvent également voir la transaction. Cette vulnérabilité garantit que tous les paiements sont légitimes.

12.4 Provenance

Provenance est une plate-forme basée sur la blockchain qui rend la chaîne de produits plus visible pour les clients.

L'entreprise utilise la plate-forme pour présenter ses produits et sa chaîne d'approvisionnement de manière plus transparente et traçable.

12.5 MultiChain

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

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 entrainer 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 [30].

Les attaques "Man-in-the-middle-attack" : l'attaquant crée deux clés secrètes.
Ensuite, il utilise la première clé pour d´démarrer la communication avec le premier coté.
La réponse reçue de premier coté sera décryptée facilement par l'intrus, car il connait la clé. L'intrus crypte à nouveau le message, cette fois avec la deuxième touche. Le message chiffré est ensuite renvoyé au deuxième coté. Puis, après avoir reçu la réponse du deuxième coté, il déchiffre le message, le lit, il le crypte par la première clé et renvoie au premier coté.
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 [31].
La figure 1.9 ci-dessus montre le schéma général de l'attaque Man-in-the-middle-attack[32]

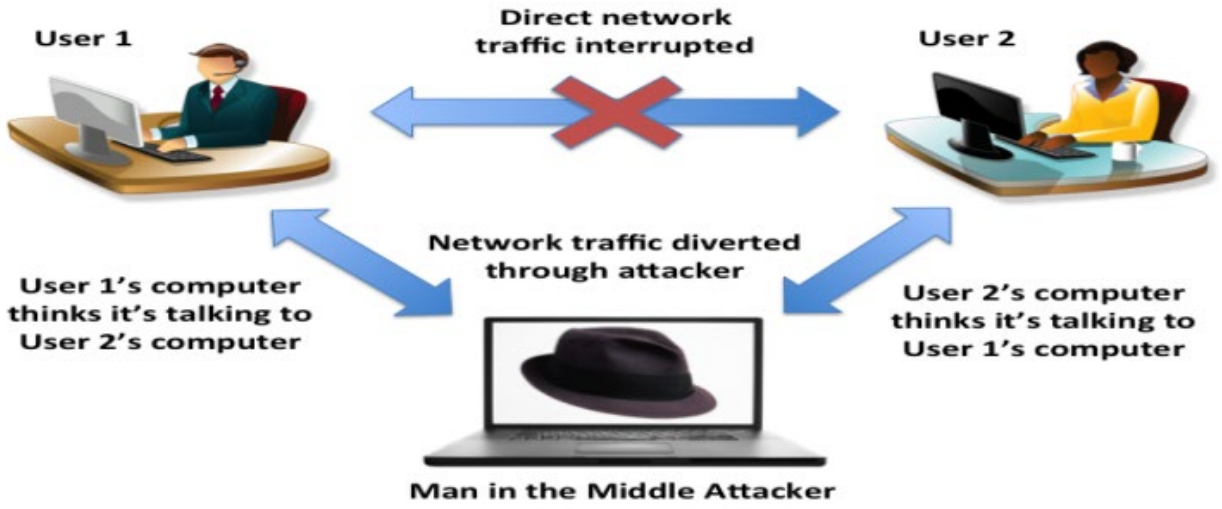

Figure 1-9 – Schema de l'attaque Man-in-the-middle-attack.

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 [31].

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 d´ébat public [31]. 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 [31].

Les attaques "Eclipse" : sont un moyen d'attaquer un réseau d´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 [31].

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 le vote en ligne.

Chapitre 02

Vote en ligne

1. Introduction

Le vote électronique est un système de vote automatique, notamment des scrutins, qui utilisent un système informatique. Ce terme général implique en fait plusieurs situations spécifiques. En fait, depuis le milieu des années 1990, on peut voir beaucoup de créativité dans les méthodes de vote. Par conséquent, deux tendances sont apparues, qui expliquent différemment l'informatisation du système électoral. Pour la première de ces tendances, le vote électronique signifie l'intégration via une urne électronique (également appelée machine à voter en droit français), permettant aux entreprises privées d'intervenir dans le système de vote. Le principal argument commercial utilisé pour promouvoir ces produits repose sur l'idée d'accélérer le processus de traitement des suffrages exprimés. Pour la seconde de ces tendances, l'informatisation du processus de vote rendra possible le vote à distance.

En France, les élections professionnelles s'effectuent de plus en plus par vote électronique, ce qui suscite des débats dans le monde de l'entreprise, en particulier dans les plus petites entreprises.

Cependant, le vote électronique est idéal pour les scrutins où le bulletin secret n'est pas requis comme certains votes de parlementaires.

2. Vote par internet

Le vote par Internet est similaire au vote par correspondance. Les électeurs peuvent commencer à partir de n'importe quel ordinateur connecté à Internet, que cet ordinateur soit à la maison, au travail, dans un lieu public ou dans un cybercafé. Vous devez vous connecter au site de vote officiel hébergé sur un ordinateur de bureau centralisé (serveur). Après la phase d'identification et d'authentification (à l'aide du nom d'utilisateur et du mot de passe généralement reçus à l'avance par courrier), les électeurs peuvent faire un choix. Après confirmation, ils vont recevoir une lettre de confirmation confirmant la réception de son vote (cette lettre de confirmation ne mentionne pas la signification du vote). L'échange d'informations s'effectue via Internet. L'ordinateur faisant office de serveur est chargé de sauvegarder la liste des signatures, des votes reçus collecter et de les compter à la fin de la période de vote.

3. Vote démocratique

La démocratie est un système politique dans lequel le pouvoir appartient au peuple. Le peuple y exerce sa souveraineté par des représentants intervenants, élus et nommés. Les candidatures doivent être proposées lors d'élections, et ces élections doivent suivre plusieurs principes de base pour être considérées comme démocratiques et universelles [33].

Ces caractéristiques fondamentales que les élections démocratiques doivent respecter sont les suivantes [33] :

• Transparence : chaque électeur a le droit et la capacité effective de contrôler toutes les étapes de l'élection,

• Unicité : une voix pour chaque électeur,

• Confidentialité : chaque électeur peut choisir en secret,

• Anonymat : la carte d'électeur ne peut pas être liée aux électeurs qui la choisissent,

• Sincérité : les résultats de l'élection représentent fidèlement les souhaits des électeurs. Pour voter, les citoyens doivent s'inscrire sur la liste électorale en fonction de leur lieu de résidence et les candidats et les candidats sont enregistrés sur des listes de vote.

Le jour du scrutin, ils doivent se présenter au bureau de vote enregistré.

La procédure de vote comprend trois étapes de base [34] :

Avant l'ouverture du bureau de vote, le responsable du bureau de vote doit indiquer formellement l'heure d'ouverture et de fermeture du bureau de vote avec les pouvoirs du candidat.

Pendant le processus de vote, l'électeur doit présenter la carte électorale et voter à l'arrivée. L'identité vérifie s'ils sont inscrits au registre électoral, puis ils prennent l'enveloppe électorale et les différents bulletins de vote, puis pénètrent dans le bureau de vote, et introduisent les candidats les bulletins de vote ou la liste de leurs choix dans l'enveloppe (pour assurer la confidentialité) ils sont ensuite rendus à la table où se trouvait l'urne. Ils montrent à nouveau leurs cartes électorales et leurs cartes d'identité. Lorsqu'ils sont appelés, ils glissent l'enveloppe dans l'urne.

• Ensuite, ils signent à côté de leur nom sur la liste prévue à cet effet. La carte électorale est tamponnée par un assistant et porte la date de l'élection.

Après la fermeture du bureau de vote, le bureau signe la liste des bulletins de vote et commence à compter les votes. Après avoir compté tous les votes, le secrétaire a rédigé le procès-verbal de la réunion. Le président du bureau de vote annonce le résultat et l'affiche dans la salle de vote.

4. Système de vote électronique

Le système de vote électronique est défini en quatre attributs [35] :

• 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

• Mettre l'enveloppe dans l'urne transparente

• Comptage manuel

Lorsque nous impliquons la numérisation des données dans l'une des quatre opérations, le système de vote peut être considéré comme électronique, la numérisation implique l'utilisation de machines électroniques équipées de logiciels [35].

Il existe de nombreuses formes de vote électronique : vote par box, vote via Internet, machines à voter, stylos numériques, comptage automatique, etc. [36].

5. Systèmes de vote en ligne

Le vote en ligne est la forme la plus numérique du vote électronique, mais elle peut impliquer des méthodes techniques très différentes [35].

Le système de vote en ligne remplace la méthode de vote existante et aide les électeurs à utiliser des ordinateurs et des appareils de communication mobiles pour exprimer leurs opinions et sélectionner des représentants à tout moment, n'importe où dans l'environnement réseau et mobile [32].

Il peut également organiser divers votes de manière efficace et sûre afin que les intentions des gens puissent être correctement reflétées 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 [32].

5.1Corée du sud :

La Commission électorale nationale gère le système de vote en ligne K-Voter (Figure 2.1 [37]) 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 [32].

Figure 2-1 – Système de vote en ligne national K-Voting.

5.2Estonie :

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 [32].

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 l´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 [38].

Pour voter (Figure 2.2 [37]), 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 confirmes, ils peuvent voter/modifier leur vote jusqu''a 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 n´nécessite une carte SIM spécialisée pour le téléphone. [38].

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 d´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 [38].

Lors de l'élection locale de 2013, les chercheurs ont observé et étudie 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 coté client qui surveille l'utilisateur en train de voter, puis plus tard changer leur vote a 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 [38].

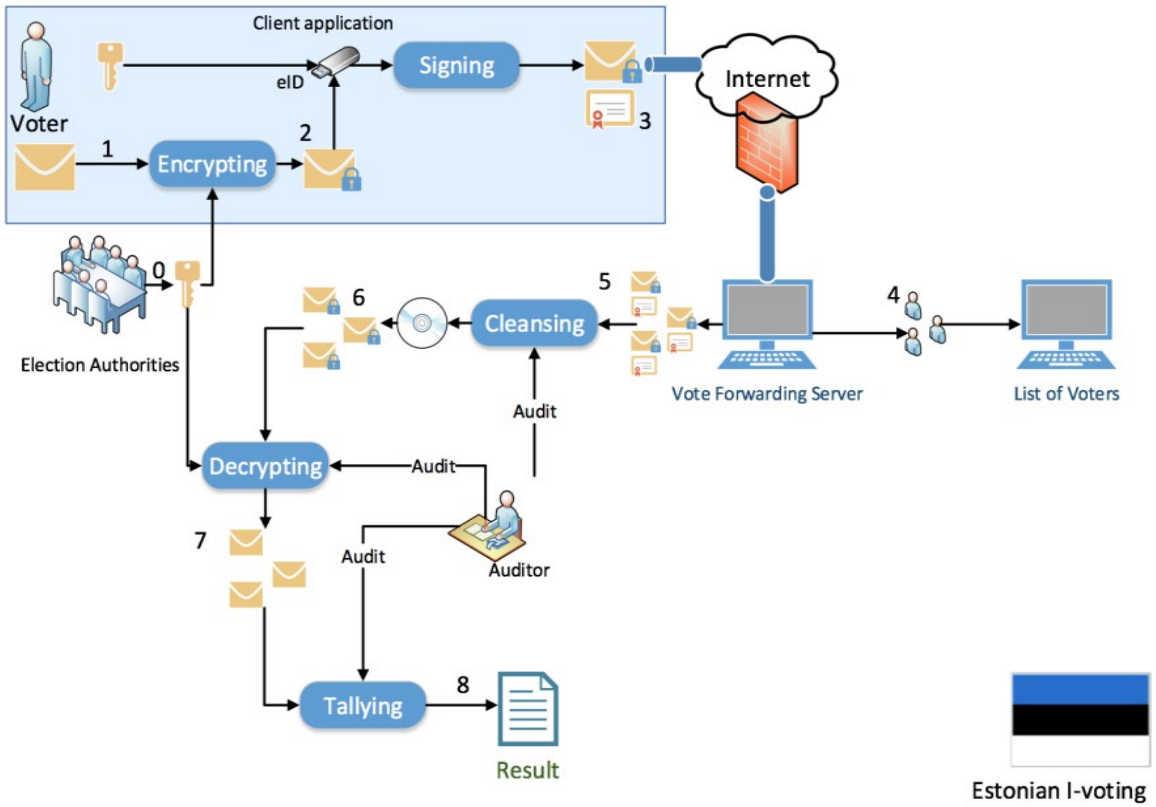

Figure 2-2 – Système de vote numérique estonien.

5.3 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 d´détecte sur le site, mais lors des contrôles de s´sécurité 2018 du système postal, des failles ont été d´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 [35]

5.4France :

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 l´législateur doit n´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 expatrie qui souhaite exercer son droit de vote. Dans certains cas, l'impossibilité matérielle ou liée à des considérations géopolitiques est manifeste [35].

6. Faille technique de vote en ligne

6.1Confidentialité

Le vote étant possible de n'importe quel ordinateur, il est difficile de garantir la confidentialité. Il faut s'assurer qu'il n'y a pas de vol, l'électeur est seul devant l'ordinateur et n'est pas sous pression. [33].

6.2Anonymat

Il est difficile d'assurer l'anonymat car chaque bulletin de vote est envoyé avec l'identifiant de l'électeur ces informations réunies sur le premier serveur de vote [33].

6.3Transparence

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, a 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 scelle 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 cache lors de tests ou d'expériences. Alors que dans le monde réel le vide de l'urne peut être vérifie visuellement et même au toucher, il semble peu probable de prétendre à la vérification qu'un vote électronique est vide en se fiant uniquement à l'affichage produit par ordinateur. Encore, le vote 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 [33].

6.4Confiance

On s'attend à ce que les versions de logiciels qui augmentent la sécurité du vote n'augmentent pas la transparence du programme, car il est nécessaire de prouver que le logiciel utilisé est exactement le même que le logiciel publié et ne subira pas de dommages. À partir d'autres programmes. Cependant, dans tous les cas, le serveur utilise un système d'exploitation, éventuellement un compilateur ou un interpréteur de code, et doit également être vérifié. Cette méthode devient énorme et donc peu pratique. La supervision de la mise en œuvre du vote a été laissée à un tiers, ce qui a sapé la confiance des électeurs. Le contrôle expert supprime l'élément « démocratique » du contrôle du processus électoral et remplace cet élément par l'aspect «technocratique». Cependant, il peut permettre aux citoyens de les signaler d'éventuelles défaillances ou irrégularités techniques. Mais encore une fois, seuls les experts contrôlent ce qu'ils veulent ou ce qu'ils peuvent faire [33].

7. Avantages du vote électronique

Grâce à notre technologie facilement accessible, un système de vote peut être créé pour tout un pays. Le vote électronique présente de nombreux avantages, ce qui rend le vote plus facile que jamais. Parmi les avantages du vote en ligne, on peut citer [39,40] :

Simplifiez le processus électoral et mettez-le à la disposition des électeurs. Vous pouvez exercer le droit de vote depuis n'importe quel ordinateur connecté à Internet ou n'importe quel téléphone disponible. 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 utiles pour encourager la participation de qui sont plus technophiles.

Offrir une plus grande confidentialité aux personnes handicapées

En votant électroniquement sans l'aide des autres, préservant ainsi l'anonymat et encourageant les personnes handicapées et les personnes âgées à se faire entendre. L'amélioration des droits d'accès et la création de plus d'opportunités de vote 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 peuvent être moins chers que les méthodes de vote traditionnelles, qui nécessitent 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 du vote en réduisant ou en éliminant le nombre d'erreurs de vote, et il est possible d'afficher plus d'informations sur les candidats et leurs positions de vote.

L'infrastructure peut être utilisée pour chaque élection, il s'agit donc d'un achat unique.

• Les résultats peuvent être obtenus presque immédiatement, car les votes peuvent être comptés pendant le processus de vote, mais avec la méthode traditionnelles les votes doivent être collecté et compter les votes dans les bureaux de vote. Ce processus prend beaucoup de temps et peut retarder le résultat final.

8. Problème de système du vote en ligne

Le vote en ligne permet aux électeurs de voter quels que soient l'heure et le lieu et réduit les coûts. Malgré ces avantages, il n'a pas été largement utilisé en Corée. Le vote en ligne passe par le processus suivant [32] :

• l'inscription des électeurs après identification,

• affichage des agendas,

•vote

• Afficher les résultats du vote.

Pour que les gens aient confiance dans la méthode de vote, la méthode doit être plus sûre et correcte, et il doit être prouvé que les résultats du vote reflètent correctement les intentions des électeurs. Les problèmes suivants peuvent survenir pendant le processus de vote en ligne : Premièrement, pendant le processus de vérification d'identité, lorsque la vérification d'identité personnelle n'est pas effectuée pour vérifier si l'électeur est inscrit électeur, il y aura des 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. Garantir la confidentialité des détails du vote par les électeurs peut également être problématique. Si le vote se déroule dans un environnement en ligne où des informations peuvent être divulguées, les informations personnelles d'autres personnes peuvent être volées et utilisées pour le vote par procuration et le vote répété, il peut donc y avoir des risques de sécurité en ce qui concerne garantir le secret du vote. Enfin, les résultats du vote peuvent être fabriqués, et s'il n'y a pas de et s'il y a méfiance à l´égard de la sécurité, la confiance dans les résultats du vote ne peut être garantie [29].

9. Inconvénients du vote électronique

Jusqu'à présent, les raisons du vote électronique semblent fortes. Cependant, le vote électronique présente des inconvénients dont il faut tenir compte. Parmi ces lacunes [39, 40] :

Menaces et attaques de virus informatiques organisées par des pirates.

Les électeurs doivent être identifiés avec un type d'identification. Cependant, le problème lié à l'utilisation de ces méthodes de vérification est que si quelqu'un obtient un grand nombre de ces informations d'identification via une violation de données, il peut émettre des milliers de votes frauduleux.

Le coût initial est beaucoup plus important que le vote par papier.

En plus de l'arrêt ou de la panne du serveur, il y aura des pannes de courant ou des problèmes de connexion Internet.

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 pour le faire voter autrement qu'il ne le ferait normalement.

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

Piratage des élections : il y a toujours le 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 détectes.

10.Problématique

Le vote doit respecter cinq (5) caractéristiques de base : la transparence, l'unicité, la confidentialité, l'anonymat et la sincérité. Mais le vote traditionnel ne peut garantir la transparence et la sincérité, car ces processus nécessitent des intermédiaires pour déformer les résultats. De plus, bien que le vote en ligne ou électronique puisse simplifier le processus de vote, il peut minimiser la consommation de temps et de ressources, mais il ne peut pas garantir la confidentialité, l'anonymat ou la sincérité, car :

Ils peuvent observer la procédure pendant son déroulement.

Les bulletins de vote laissent des traces, permettant à chaque électeur de se connecter à son bulletin de vote.

Le système de vote est centralisé dans un serveur contrôlé par un intermédiaire, donc les données peuvent être modifiées. Enfin, l'application de vote par Internet a le problème de la saturation des serveurs lors de la phase de vote. Alors, comment éviter les problèmes ci-dessus ?

11.Solution proposée

Notre solution est un système de vote en ligne basé sur la technologie blockchain. La blockchain est une méthode de gestion des votes efficace, sûre et transparente

Nous attendons de ce système d’assurer :

• la transparence : les électeurs peuvent contrôler toutes les étapes du vote par eux-mêmes (compter les votes et s'assurer qu'aucun vote n'est supprimé, manipulé ou modifié).

• l’unicité : chaque électeur ne peut exprimer qu'un seul vote

• la confidentialité : les procédures de vote ne seront pas lors du son d´déroulement, De ce fait l’électeur peut effectuer son choix en secret.

• l'anonymat des électeurs : il est impossible de relier les bulletins avec les électeurs qui l’ont choisi

• la sécurité et prévenir la fraude à tous les niveaux.

12.Conclusion

Dans ce chapitre, nous avons exposé le vote en ligne, tout d'abord on a présenté le vote par internet, le vote démocratique, le système du vote électronique et en ligne qui a été utilisé dans 4 pays (Corée du sud, Estonie, Suisse, France) ensuite on a abordé ces avantages, ces inconvénients et ces failles techniques, enfin nous avons proposés la solution du vote en ligne basé sur la technologie blockchain, Dans le chapitre suivant, nous allons présenter la Conception et la réalisation du système vote en ligne.

Chapitre 03

Conception et realisation du système vote en ligne

1. Introduction

Ce chapitre présente spécifiquement les étapes fondamentales de la conception, modélisation et la réalisation d'un système de vote en ligne basé sur la technologie blockchain.

Nous avons choisi Unified Process (PU) comme méthode de conception et Unified Modeling Language (UML) comme langage de modélisation.

2. Processus unifié(UP)

Le processus unifié est un processus de développement logiciel itératif et incrémental, construit sur UML, centré sur l'architecture, piloté par des cas d'utilisation, et semble être une solution idéale aux éternels problèmes des développeurs [43].

Comme le montre la figure 3.1 [44], le processus UP est résumée comme les étapes suivantes [44] :

- **Spécifications :** utilisées pour définir les différentes exigences du système :
- **Fonctionnalité :** Du point de vue de l'utilisateur.
- **Non fonctionnel :** D'un point de vue technique.
- **Analyse :** Permet de comprendre les besoins et les exigences des clients.
- **Conception :** Permet d'acquérir une compréhension approfondie et de déterminer la méthode pour 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.

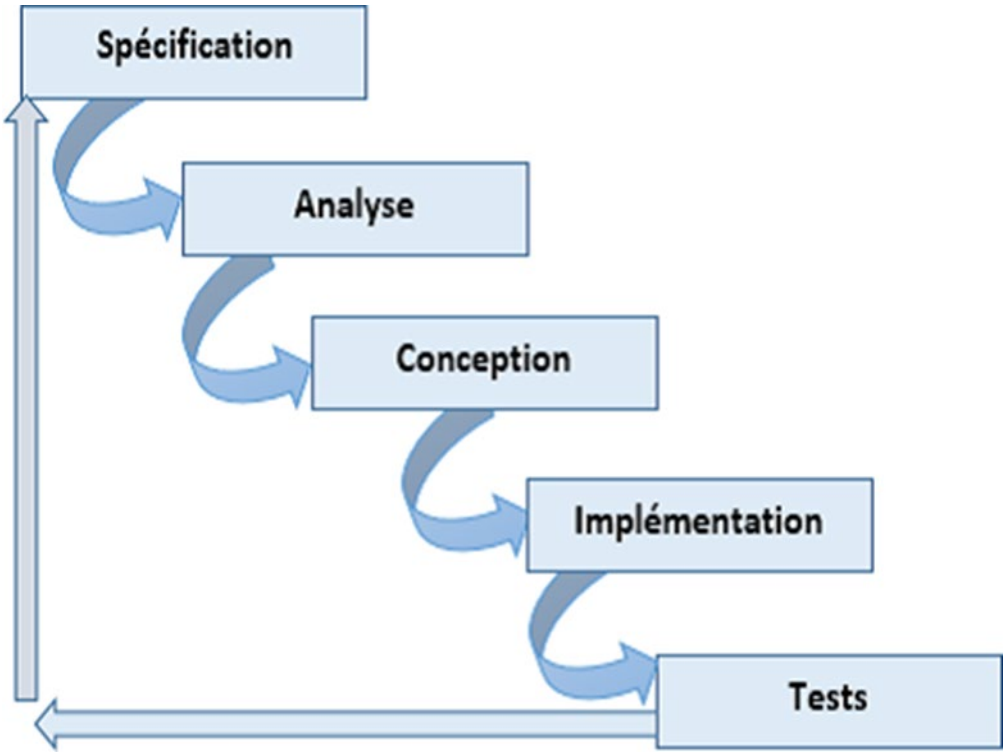

Figure 3-1 – Processus UP.

3. Unified Modeling Language (UML)

UML est un langage de modélisation graphique et textuel utilisé pour comprendre et rédiger des exigences, spécifier et documenter des systèmes, concevoir des solutions et échanger des idées [45]. UML a treize diagrammes. Pour notre système, nous utilisons les trois diagrammes de base suivants :

- Le diagramme de cas d'utilisation permet d'exprimer le comportement du système sous forme d'actions et de réactions selon le point de vue de chaque utilisateur, il définit les limites du système et sa relation avec l'environnement [46]
- Diagrammes de séquence, ces diagrammes sont des représentations graphiques des interactions entre les participants et le système dans l'ordre chronologique selon la formule UML [47].
- 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 dernies [48].

4. Identification des besoins

Besoins fonctionnels : le système doit offrir les fonctionnalités suivantes :

- Lancement du vote
- Authentification des ´électeurs

- Ajout des candidats.
- Vote.
- Affichage des résultats.

Besoins non fonctionnels : à 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 décentralise 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 sécurie et aisément consultable.

Performances : Un logiciel doit être avant tout performant c'est à -dire à travers ces fonctionnalités, 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.

5. Présentation des cas d'utilisation

5.1 Identification des acteurs du système

❖ **Electeur**

- S'authentifier (obtenir un compte).
- Accéder au système pour voter.
- Consulter les résultats de vote.

5.2 Pourquoi deux systèmes ?

Voir que la sécurité dans les systèmes de vote en ligne 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 à 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.

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 : voter
Résumé : Ce CU permet à l'acteur de voter.
Acteurs : Electeur.
Précondition : l'électeur possède un compte et le vote est lancer
Post-Condition: l'Electeur vote.
DESCRIPTION DU SCENARIO NOMINAL 01: Le système invite l'acteur a` 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 déja voté ou n'a pas un compte ou le vote n'est pas encore lancé : 01 : Le systéme affiche la page des résultats.
CU2: consulter les résultats
Résume : Ce CU permet à l'acteur de consulter les résultats de vote.
Acteurs : Electeur.

Table 3-1 – Scénario des cas d'utilisation.

6. Diagrammes de séquences

6.1Diagramme de séquence lancer le vote

Le diagramme de séquence ”Lancer le vote” présente le séquencement des interactions entre Administrateur, Electeur et le sous-systeme1, l’opérateur « 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.

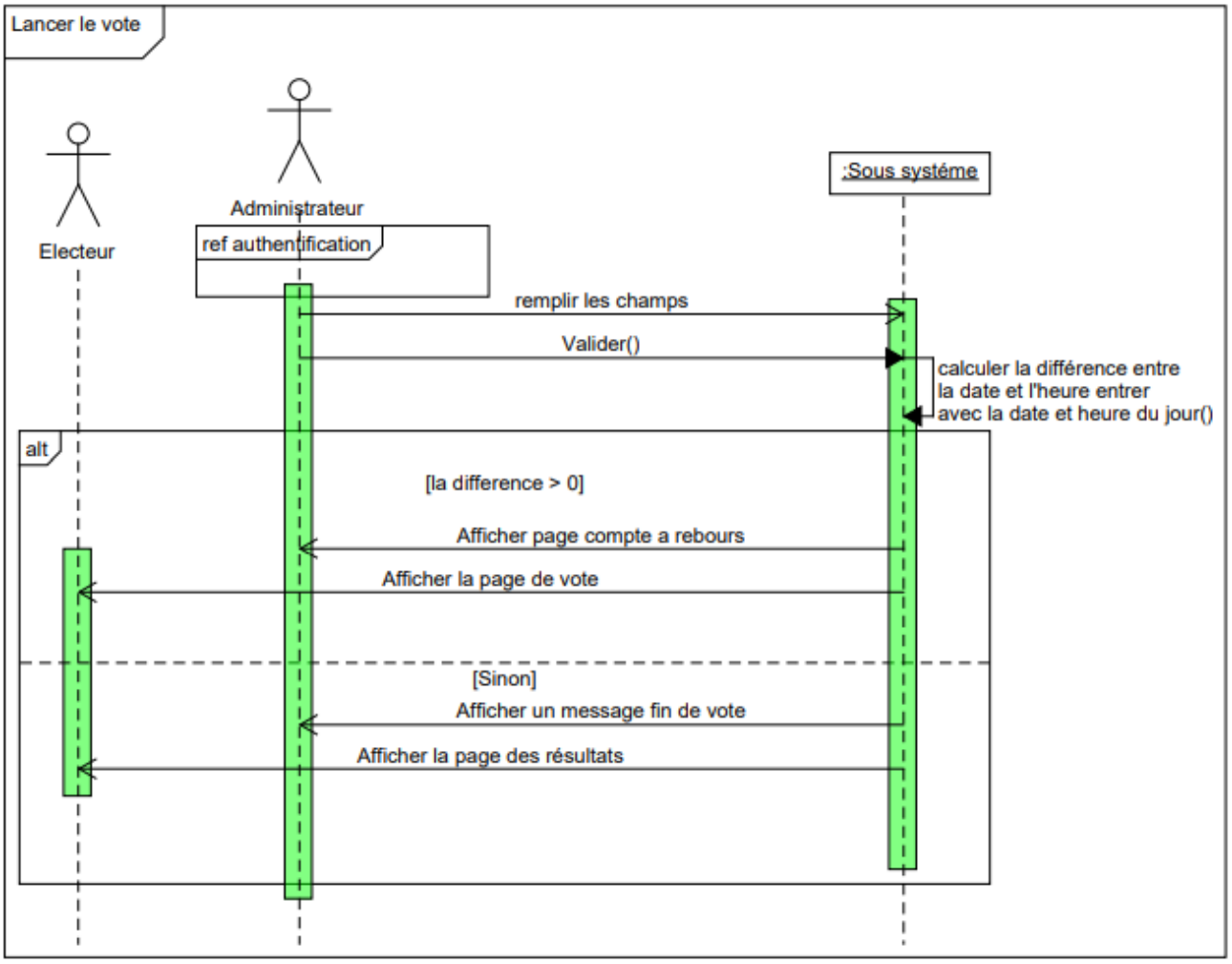

Figure 3-2 – Diagramme de séquencer lancer le vote

6.2 Diagramme de séquence voter

Le diagramme de séquence Voter présente le séquencement des interactions entre Electeur et le sous-systeme1.

L'opérateur « 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 affiche par le système si seulement si le vote est lancé, l'électeur n'a pas déjà voté et le compte est valide, sinon le système affiche la page des résultats.

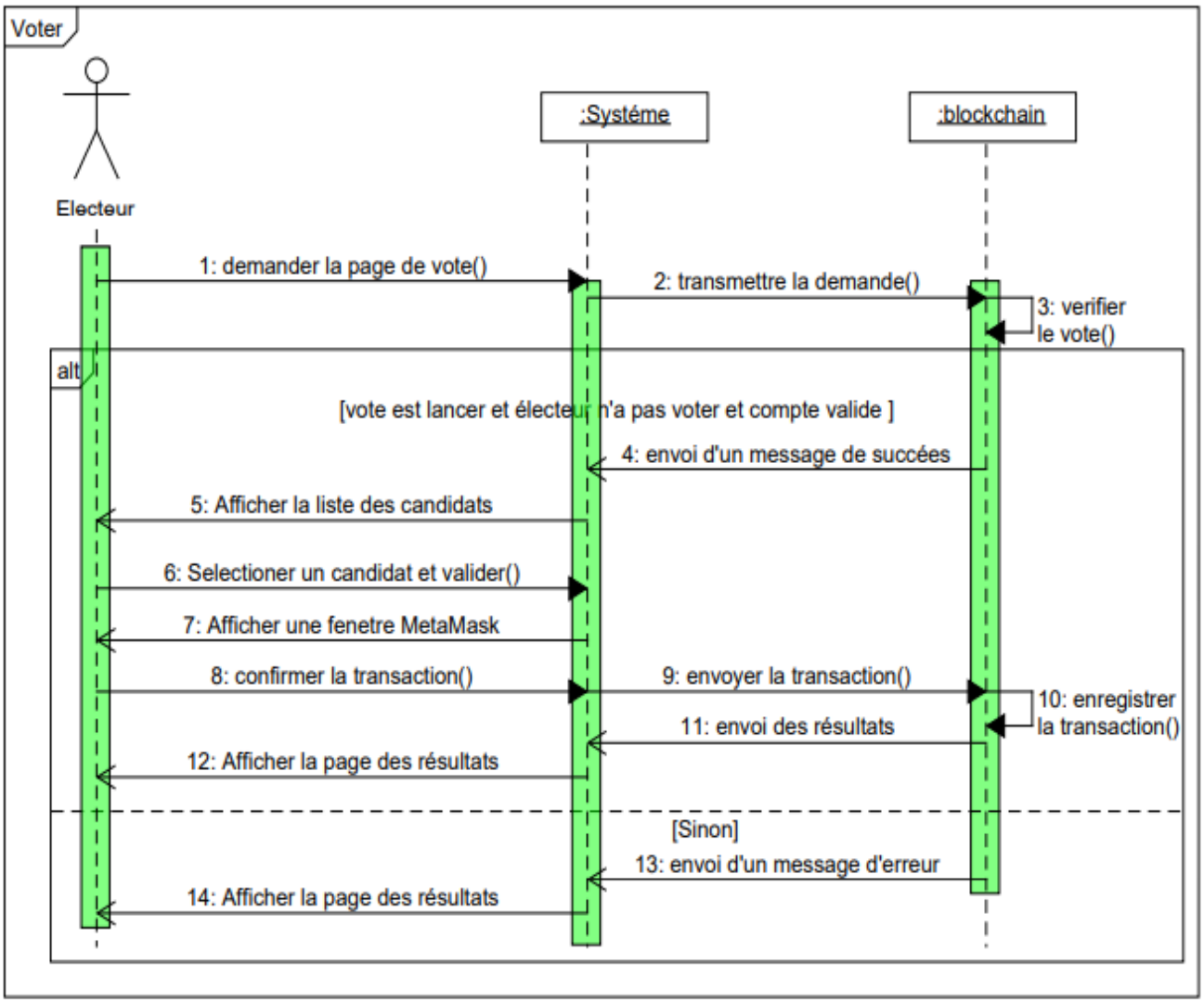

Figure 3-3 – Diagramme de séquence Voter

7. Outils de développement et langages utilisé

Sublime texte 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 [49]

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 chaine. Il vous donne la possibilité d'effectuer toutes les actions que vous feriez sur la chaine 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 [59].

Grace a 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 pour cela nous l'avons choisi.

Pour installer ganache il faut avoir

- Un processeur de 64 bits.
- 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 [50].

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 [51].

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

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... [52].

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. Ecrit en JavaScript, Remix prend en charge à la fois l'utilisation dans le navigateur et localement [53].

Nous avons choisi Remix car [54] :

- Il est très pratique et très pertinent pour apprendre à coder sur Solidity
- On y accédé 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 vraie blockchain Ethereum un smart contract directement depuis Remix, mais il peut aussi se connecter à une blockchain locale comme Ganache. Il est donc très 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 en 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 [55].

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 coté serveur comme les scripts PHP. L'exécution du code est effectuée par votre navigateur internet tel que Firefox ou Internet Explorer [56].

Web3.js : Il s'agit d'une collection de bibliothèques qui vous permettent de développer des clients qui interagissent avec l'éthéreum blockchain et effectuer des actions comme envoyer Ether d'un compte à un autre, lire et écrire des données intelligents, créer des contrats intelligents, et bien plus encore [57].

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 [58].

Solidity est de type statique, prend en charge l'héritage, les bibliothèques et les types complexes définis par l'utilisateur, entre autres fonctionnalités [58].

8. Arborescence de l'application

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

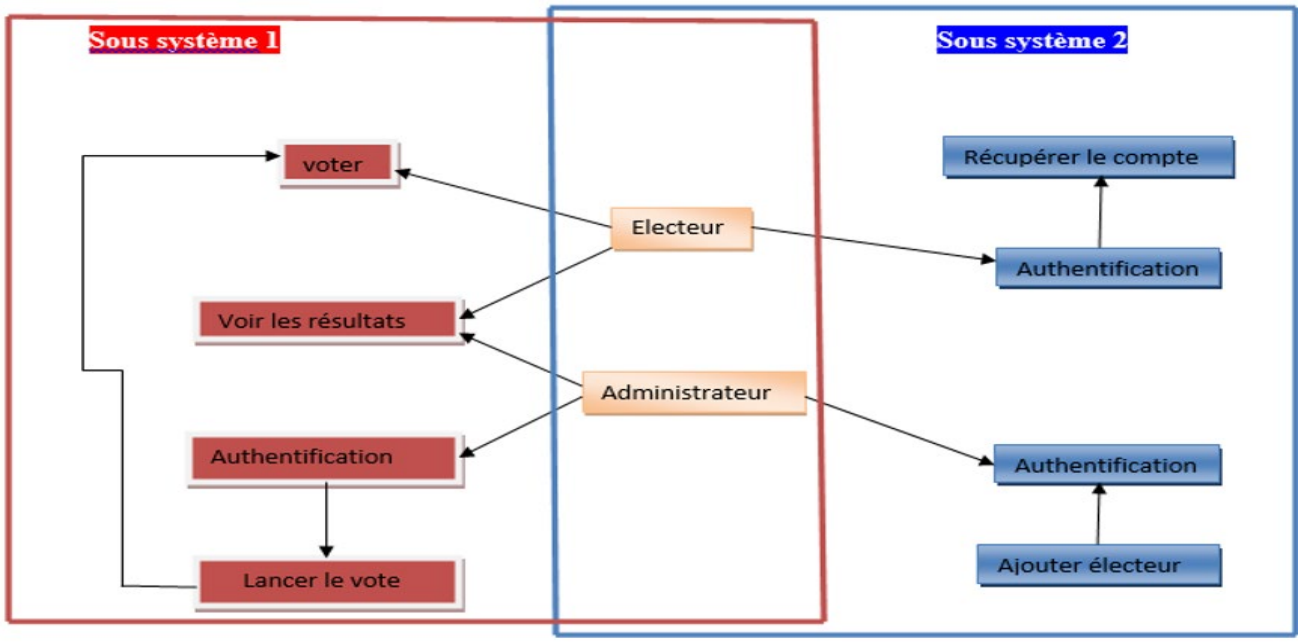

Figure 3-4 – Arborescence de l'application vote en ligne.

9. 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 truffles déjà existant. Donc, dans le dossier « election », 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 3.5).

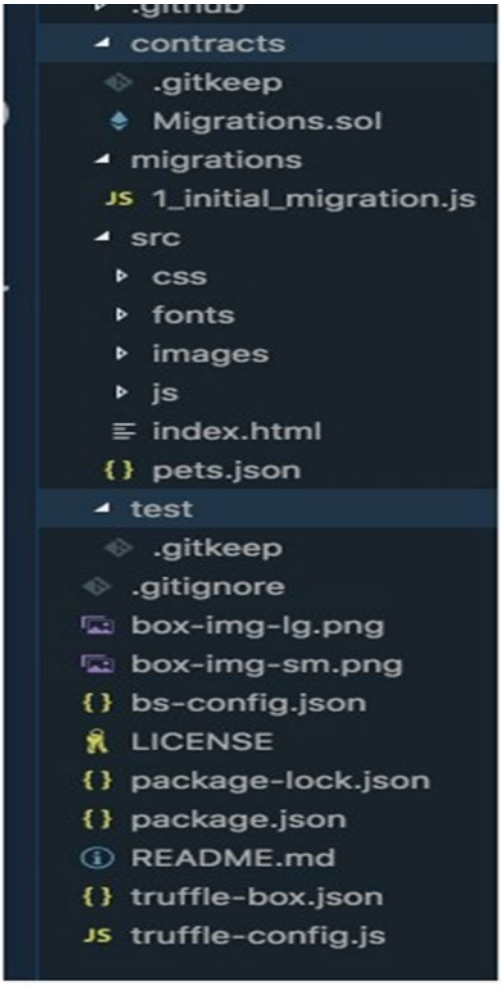

Figure 3-5 – Structure de répertoire election.

- **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 qu'il y a 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 nous 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 avons développer 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 qu'on pourra les utilisées dans le projet.

10. Présentation des interfaces de développement

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

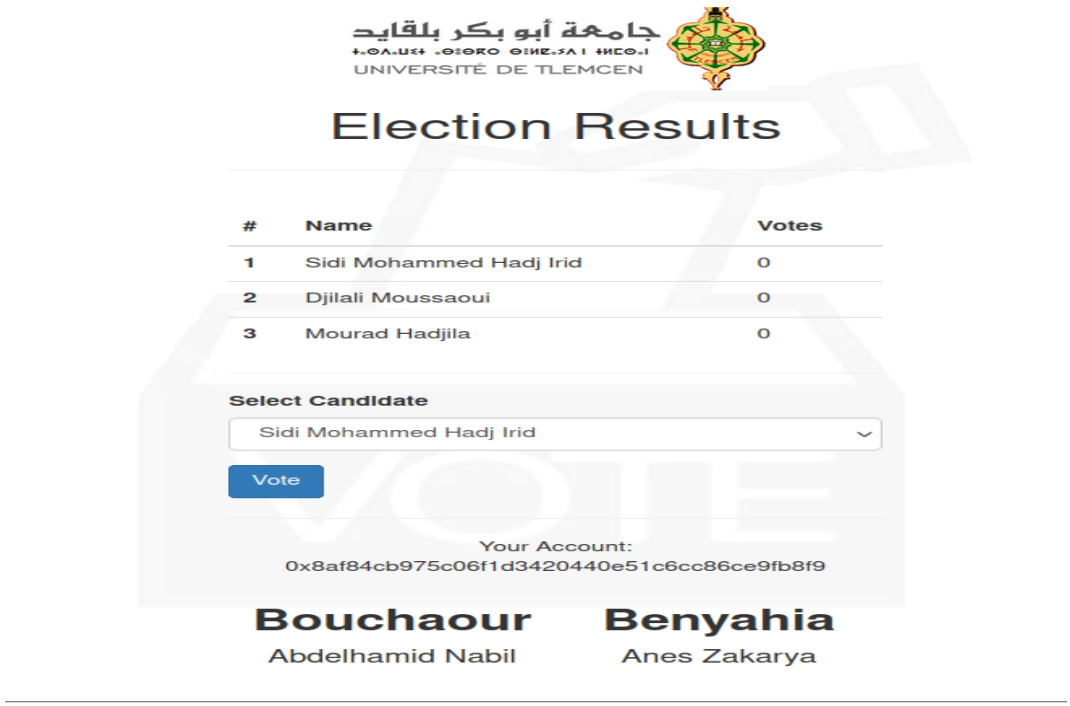

Figure 3-6 – interface principale de vote.

10.1 Présentation des interfaces pour le vote

10.1.1 Interface Connexion à la blockchain

L'électeur doit se connecter à la blockchain en utilisant l'extension MetaMask (figure 3.7.1) puis Importer le compte (figure 3.7.2) qui a été récupéré de site précédant

FIGURE 3.7.1 connecter à Metamask

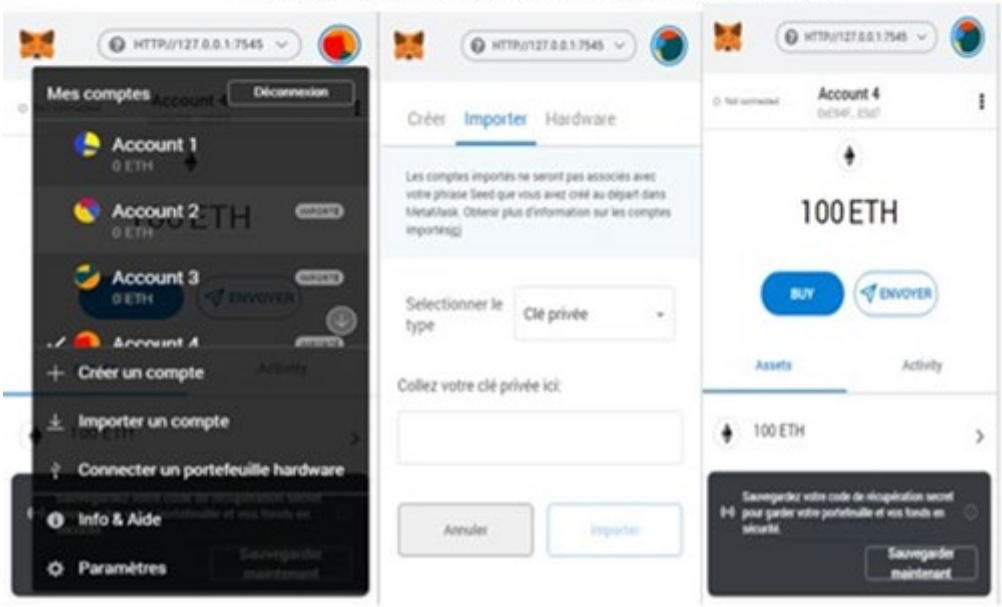

FIGURE 3.7.2 importer le compte

Figure 3-7 – Connexion à la blockchain

10.1.2 Interface principale de vote

Espace électeur (Figure 5.9).

Lorsque l'électeur accéde à son espace, le système va vérifier si le compte Metamask est autorisé pour voter

Si le compte est autorisé, l'électeur va recevoir une liste 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.

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

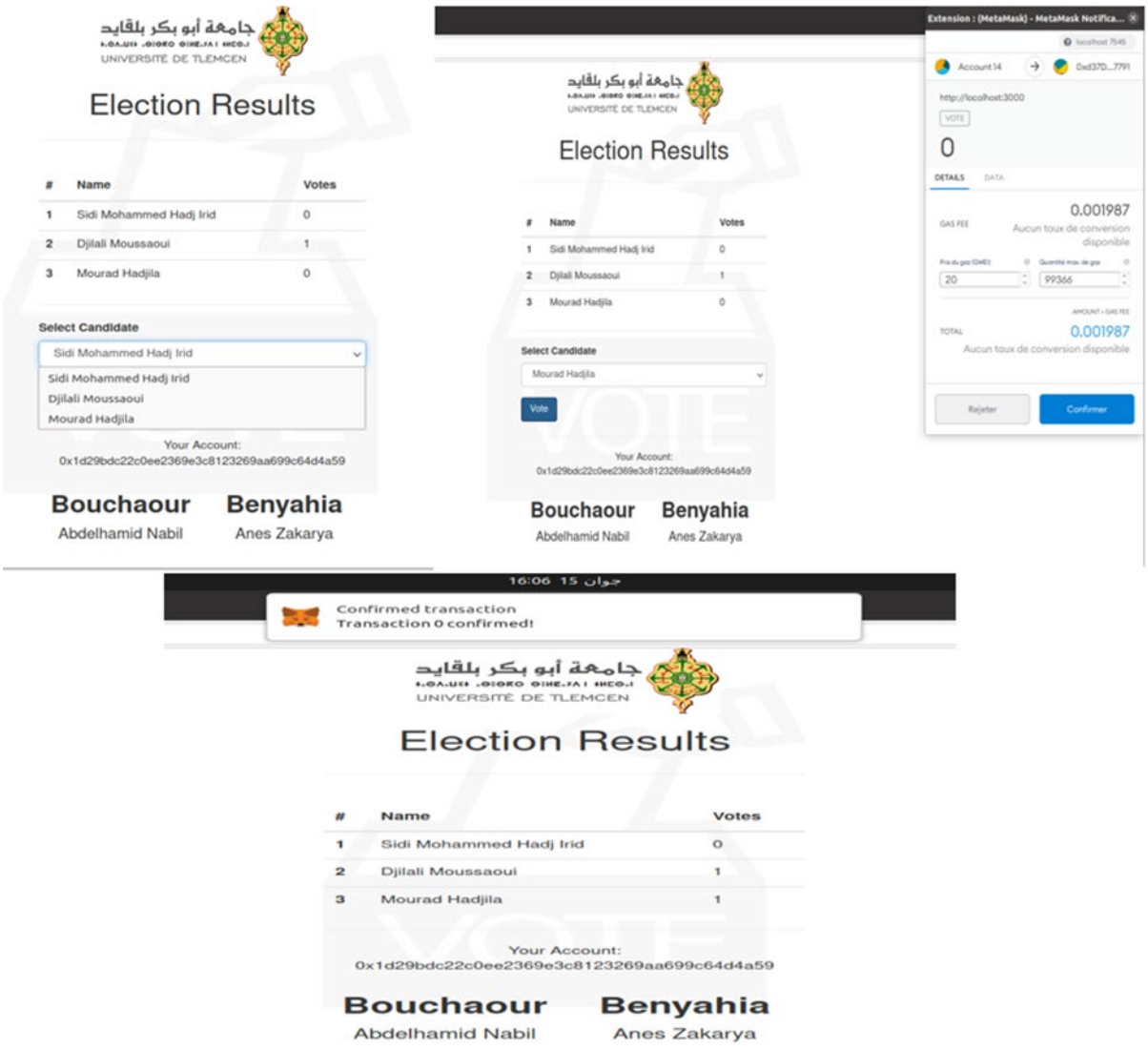

Figure 3-8 – Espace électeur

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 3.9)

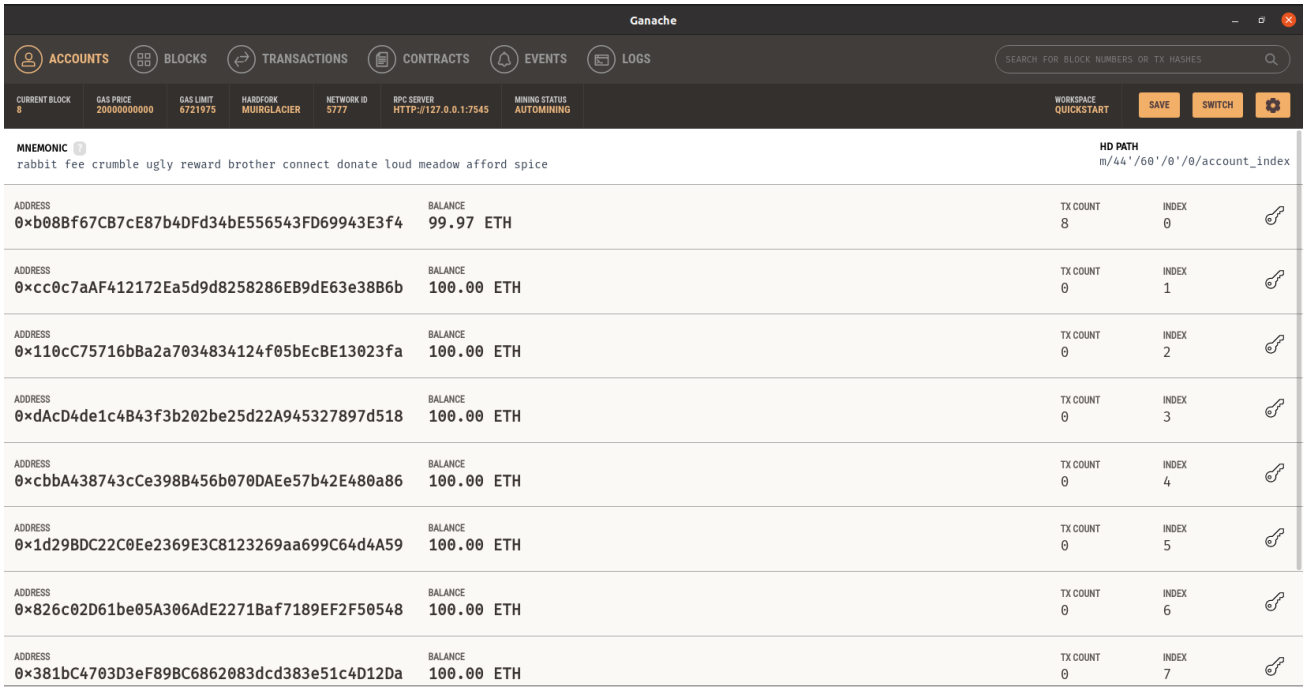

Figure 3-9 – Transactions (Ganache).

11. Perspectives

Nous ne prétendons nullement avoir répondu à tout ce qui se rapporte à cette application, celle-ci reste améliorable dans le future pour cela nous proposons :

- L'amélioration de l'interface graphique par la création d'une autre interface réservée à l'administrateur et l'électeur.
- Le perfectionnement de l'interactivité de l'interface graphique à travers le changement de couleur avant et après le vote.
- L'utilisation d'un algorithme permettant de classer les candidats selon les résultats du vote.
- Le renforcement du niveau de sécurité de l'application en faisant intervenir des experts en cyber-sécurité ...etc.

12. Conclusion

Dans ce chapitre, nous avons montré le principe de fonctionnement du système, ainsi on a 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 du vote en ligne avec la technologie de la blockchain, à travers un ensemble de captures d'écran.

Conclusion générale

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

Dans ce mémoire, nous avons exploré la blockchain et proposé une solution basée sur cette technologie. Notre proposition concerne une application pour le vote électronique.

Pour réaliser notre application du vote en ligne basée sur la blockchain. Nous avons élaboré une conception et une modélisation basée sur l'UP (Unified Process) et L'UML (Unified Modeling Language). Nous avons commencé par une étude préliminaire pour identifier les différents acteurs qui interagissent avec le système et nous avons procéder à l'analyse des besoins en spécifiant les besoins fonctionnels et non fonctionnels. Après, nous avons décrit le système à travers les diagrammes de cas d'utilisation, de séquence et de classe. L'implémentation nécessite la manipulation de l'outil spécifique à savoir la plateforme Ethereum basée sur les smart contract. L'application développée permet de garantir les besoins essentiels d'un vote démocratique.

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 de 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 développer certains points dans la partie réalisation de l'application du vote en ligne.

Bibliographie

[1] Vinay Gubta, une brève histoire de la blockchain, https : //www.hbrfrance.fr/chroniques-experts/2018/05/20131-breve-histoire-de-blockchain/ consulté le 14/05/2021

[2] Laurent Leloup, " blockchain la revolution de la confiance ", Paris, Eyrolles, 2017

[3]https://moussakayre.digital/quest-ce-que-la-technologie-blockchain-un-guide-pour-debutants/ consulté le 20/04/2021.

[4] B.Chaïmaa, B.Kawter, "Sécurisation d'un réseau bancaire avec la technologie Blockchain", mémoire, Août, 2020

[5] https://www.blocktempo.com/understand-structure-of-blockchain-bitcoin/ consulté le 28/05/2021

[6] https://www.blocktempo.com/understand-structure-of-blockchain-bitcoin/ consulté le 28/05/2021

[7] https://blockgeeks.com/guides/fr/contrats-intelligents/ consulté le 28/05/2021

[8] https://blog.toright.com/posts/5981/pow-pos-dpos-consensus-intro.html consulté le 28/05/2021

[9] Johannes Scherk B.Sc,Mag., Gerlinde Pöchhacker-Tröscher , " blockchain – technologie-feld und wirtschaftliche anwendungsbereiche ",2017.

[10] GODEBARGE Ferréol, ROSSAT Romain, "principes cles d'une application blockchain", EM Lyon Business School, Decembre 2016.

[11] Marcus O'Dair, "music on the blockchain", July 2016.

[12] Leonard Beth, Annika Cayrol, " la blockchain, une revolution pour la finance ? ", 2017

[13]C.Richter,Andre Schlieker,"Der blockchain-nebel lichtet sich auch fur die assekuranz " ,2017

[14]https://www.industrie-techno.com/article/ces-5-secteurs-que-va-revolutionner-la-blockchain.53233 consulté le 28/05/2021

[15] https://www.reply.com/de/content/healthcare consulté le 28/05/2021

[16] https://www.journaldunet.com/economie/finance/1195520-blockchain-definition-et-application-de-la-techno-derriere-le-bitcoin-juin-2021/ consulté le 15/06/2021

[17]http://www.wikiwai.com/2020/02/12/comprehension-et-conception-de-services-avec-la-blockchain-bitcoin-ethereum/

[18]https://www.slideshare.net/AmineHAMOUDA/prsentation-blockchain-v2 consulté le 15/06/2021

[19]https://www.slideshare.net/AmineHAMOUDA/prsentation-blockchain-v2 consulté le 15/06/2021

[20]https://www.lacircum.com/index.php/fr/la-crypto-monnaie-pour-les-nuls-debutants/6-blockchain-definition-expliquee consulté le 15/06/2021

[21] https://www.purevpn.fr/quest-ce-quun-vpn/protocoles/ikev2 consulté le 15/06/2021

[22] Laurent Leloup, " blockchain la revolution de la confiance ", Paris, Eyrolles, 2017

[23] https://www.blockchains-expert.com/blockchain-privee-vs-blockchain-publique/ consulté le 15/06/2021

[24] Amritha Jayanti, Bogdan Belei, "blockchain", 2020.

[25] Melanie Swan, "blockchain blueprint for a new economy", fevrier 2015.

[26] Bikramaditya Singhal, Gautam Dhameja, Priyansu Sekhar Panda, "beginning blockchain", 2018.

[27] https://www.leewayhertz.com/blockchain-platforms-for-top-blockchain-companies/ consulté le 15/06/2021

[28] Narayan Prusty, "building blockchain projects", 2017

[29] Johannes Scherk B.Sc,Mag., Gerlinde Pöchhacker-Tröscher , " blockchain – technologie-feld und wirtschaftliche anwendungsbereiche ",2017.

[30] https://en.unesco.org/sites/default/files/blockchain_glossairefrn.pdf consulté le 15/06/2021

[31]https://cdn.reseau-canope.fr/archivage/valid/feuilletage-les-risques-des-blockchains-N-11271-16257.pdf

[32] Chantal Enguehard, " vote par internet : failles techniques et recul démocratique ", université de Nantes, octobre 2007

[33] https://www.vie-publique.fr/fiches/23984-comment-se-dero consulté le 15/06/2021

[34] https://democratiedirecte.net/vote-par-internet.php consulté le 15/06/2021

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

[36]https://www.cairn.info/revue-le-journal-des-psychologues-2017-9-page-12.htm consulté le 15/06/2021

[37] Andrew Barnes, Christopher Brake, Thomas Perry, “ vote numerique avec l’utilisation de la technologie blockchain “, team plymouth pioneers - universite de plymouth,

[38] https://www.esilv.fr/portfolios/utilisation-de-technologie-blockchain-vote-electronique/ consulté le 15/06/2021

[39] https://www.dz-techs.com/fr/how-electronic-voting-works consulté le 15/06/2021

[40] Matthieu Quiniou, Christophe Debonneuil, “ glossaire blockchain “, paris,avril 2019

[41] Laurent Dehouck Etaudrey Thomas, “ les risques des blockchains “, juin 2010

[42] http ://web.cs.ucla.edu/classes/winter13/cs111/scribe/17b/ consulté le 15/06/2021

[43] Jacobson, g. Booch, j. Rumbaugh. “The unified software development process”. eyrolles, 2000

[44] https : //www.dappuniversity.com/articles/web3-js-intro, consulte le 23/06/2021

[45] Pascal Roques, “ uml2 modeliser une application web “, 4°edition 2007

[46] Jacques Lonchamp, “ genie logiciel sixieme partie la modelisation objet uml “, cours, cnam cra nancy. 2003.

[47] Josef Gabay, David Gabay, “ uml 2 analyse et conception “, Dunod, paris : 2008.

[48] https://www.supinfo.com/ consulté le 23/06/2021.

[49] https : //www.supinfo.com/articles/single/1114-sublime-text-3, consulté le 23/06/2021

[50] https : //fr.bitdegree.org/tutos/metamask/ consulté le 23/06/2021.

[51] https ://golden.com/wiki/truffle framework, consulté le 23/06/2021.

[52] https : //www.tutorialsteacher.com/nodejs/what-is-nodejs, consulté le 23/06/2021.

[53] https : //remix-ide.readthedocs.io/en/latest/ consulté le 23/06/2021.

[54] http://www.une-blockchain.fr/tutorial-developpement-solidity-remix/ consulté le 23/06/2021.

[55] https://agency-inside.com/2016/06/definition-webmarketing-bootstrap/ consulté le 23/06/2021.

[56] http ://glossaire.infowebmaster.fr/javascript/ consulté le 23/06/2021.

[57] https ://solidity.readthedocs.io/en/v0.6.11/ consulté le 23/06/2021.

[58] https://www.php.net/manual/fr/intro-whatis.php consulté le 23/06/2021.

[59] https://www.trufflesuite.com/docs/ganache/overview consulté le 23/06/2021.

[60] https ://github.com/dappuniversity/election consulté le 23/06/2021.

Code source du système vote en ligne

1. Fichier « Election.sol »

Les deux figure (Figure A1 et Figure A2) 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 A1 – 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 A2 – 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 coté 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 A3 – 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 A4 – 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 A5 – Fonction CastVote.