



Institut National des Sciences Appliquées et de Technologie

UNIVERSITE DE CARTHAGE

Projet de fin d'années

Filière : GL

Exploration de la technologie Blockchain dans un système de vote en ligne

Présenté par

Ilhem BOURIEL
Fouad WAHABI

Encadrant INSAT : **Mr YOUSFI Souheib**

Présenté le : **16/05/2017**

Table des Matières

Liste des Figures	iii
Liste des Tableaux	iv
Résumé	v
Abstract	vi
Introduction Générale	1
I Cadre du projet	3
1 Cadre général du projet	3
2 Contexte du projet	3
2.1 Problématique	4
2.2 Description du projet	4
3 Méthodologie de développement adoptée	5
4 Chronogramme des tâches	6
II État de l’art	7
1 Le vote en ligne	7
1.1 Définition	7
1.2 Domaines d’applications	7
2 La technologie Blockchain	8
2.1 Définition	8
2.2 Les principes fondamentaux de Blockchain	9
2.3 Domaines d’applications	13
2.3.1 Paiement P2P	13
2.3.2 Internet des objets IOT	13
2.3.3 Système de vote	14
2.3.4 Distribution d’énergie	14
2.3.5 Stockage des données	14
2.3.6 Contrats intelligents	15

III Étude des besoins	16
1 Étude de l'existant	16
2 Solution proposée	19
3 Analyse des besoins	21
3.1 Besoins fonctionnels	21
3.2 Besoins non fonctionnels	22
4 Modélisation des besoins	22
4.1 Diagramme de cas d'utilisation système	23
4.2 Diagrammes de séquence système	23
4.2.1 Diagramme de séquence « S'inscrire »	24
4.2.2 Diagramme de séquence « Voter »	24
IV Conception et étude technique	26
1 Conception générale	26
1.1 Architecture globale du système	26
1.2 Architecture logicielle de la partie WEB	27
2 Conception détaillée	28
2.1 Diagramme de packages	28
2.2 Diagramme de Classes	29
2.3 Diagramme de séquence objet «Payer Frais Transaction Vote»	31
V Réalisation de la solution	33
1 Étude technique	33
1.1 Environnement de travail	33
1.1.1 Environnement matériel	33
1.1.2 Environnement logiciel	34
1.2 Blockchain utilisée (Ethereum)	34
2 Réalisation de la partie WEB	35
Conclusion Générale et Perspectives	40
Bibliographie	41

Liste des Figures

I.1	La méthodologie de développement scrum	5
I.2	Diagramme de Gantt	6
II.1	Blockchain	8
II.2	Chainage des Blocks	10
II.3	Exemple d'une signature électronique d'un message envoyé	11
II.4	Envoi/Confirmation d'une transaction via la Blockchain	12
III.1	L'arbre Merkle	20
III.2	Diagramme de cas d'utilisation système	23
III.3	Diagramme de séquence « créer compte »	24
III.4	Diagramme de séquence « Voter »	25
IV.1	Architecture globale du système « InsatVoting »	27
IV.2	Architecture logicielle de la partie WEB	28
IV.3	Diagramme de packages	29
IV.4	Diagramme de classes	30
IV.5	Diagramme de séquence objet « Payer Frais Transaction Vote »	31
V.1	Formulaire de connexion	35
V.2	Menu principal	35
V.3	Création d'un vote	36
V.4	Récupération de l'adresse vers laquelle il faut envoyer des "Ethers"	36
V.5	Activation du vote après reçu les "Ethers" nécessaires	37
V.6	Le vote est activé	37
V.7	Invitation des votants	38
V.8	Invitation des votants par email	38
V.9	Affichage des resultats	39

Liste des Tableaux

III.1 Tableau comparatif des Blockchain	16
III.2 Tableau comparatif des solutions de vote existant	18

Introduction Générale

Depuis l'aube de la démocratie, les élections dans le monde ont été accusées d'illégitimité. Alors que les sociétés démocratiques à travers le monde commencent à adopter une technologie pour améliorer l'efficacité du processus électoral, beaucoup de gens découvrent que certains types de technologie peuvent être extrêmement vulnérables, ce qui pourrait avoir une influence injustifiée sur les résultats des élections. Seuls ceux qui sont avancés technologiquement se rendent compte qu'il y avait une solution technologique récemment introduite à l'humanité qui à la capacité de résoudre ces deux problèmes critiques : Le manque de transparence dans nos élections et le manque de sécurité de nos systèmes électoraux.

En utilisant cette technologie de pointe, nous pourrions obtenir une transparence dans nos élections, sans compromettre la confidentialité des électeurs, et nous permettrions de démontrer mathématiquement que les résultats des élections sont exacts. En outre, à la demande de l'électeur, il y aurait même un moyen de permettre à un électeur de voter en ligne lors d'une élection et de suivre son vote dans l'urne pour s'assurer que son vote était sécurisé et sécurisé sans être changé ou modifié dans aucun façon.

Généralement, lorsque la technologie de pointe est introduite à la masse, il y a un fardeau financier accru sur les adopteurs anticipés qui sont prêts à payer le coût plus élevé afin de profiter des avantages supplémentaires que la nouvelle technologie fournit. Contrairement à cette tendance, cette technologie particulière pourrait effectivement réduire considérablement les coûts de nos élections et libérer l'argent des contribuables pour être consacré à d'autres aspects extrêmement importants de notre société, tels que l'amélioration de la qualité de nos systèmes éducatifs ou la reconstruction de notre infrastructure qui s'écroule.

L'augmentation de la participation électorale serait également un sous-produit probable pour organiser des élections en ligne en toute sécurité. La réalité est que, dans le passé, de nombreuses entreprises ont tenté d'organiser des élections en ligne, mais elles ont échoué uniquement en raison de l'approche technologique qu'ils ont décidé de prendre et non parce que cela ne peut pas être fait. Si nous pouvons surmonter l'idée fausse selon laquelle le vote en ligne ne peut pas être fait en toute sécurité et en toute sécurité, nous pourrions encourager toute une nouvelle vague d'électeurs à voter en ligne de n'importe où dans le monde.

La technologie Blockchain a d'abord été développée en 2009 par Satoshi Nakamoto. Depuis sa publication, il a servi de base à des milliers de cryptographies dans le monde, y compris

Bitcoin et BitShares. Il a également été reconnu mondialement comme la plus sécurisée des technologies de gestion de base de données en ligne disponibles. En intégrant la sécurité de Blockchain dans la conception de notre système de vote, Follow My Vote est rapidement devenu un pionnier de l'industrie.

La technologie Blockchain est un stockage de données décentralisé qui détient un registre public des transactions formé par une chaîne de bloc. Cette chaîne peut enregistrer de nombreuses transactions : les transactions monétaires, le transfert de propriété et même le scrutin. Toutes les transactions qui se produisent sur un Blockchain standard sont vérifiées et signées avec cryptographie pour assurer la sécurité et l'anonymat. Suivre le système de **My Vote** améliore encore la sécurité en utilisant la cryptographie de courbe elliptique. Autrement dit, la cryptographie fournit la sécurité et la confidentialité, tandis que la chaîne de bloc public ajoute de la transparence et de la responsabilité.

A cet égard, nous avons développé une application de vote en ligne sécurisée qui se base sur la technologie blockchain. Le travail réalisé durant notre stage est décrit dans le présent document. Ce rapport s'articule autour de cinq chapitres.

Le premier chapitre « **Cadre du projet** » porte sur la présentation du projet et de la méthodologie de travail adoptée. Le deuxième chapitre « **État de l'art** » concerne l'étude théorique du domaine de vote en ligne ainsi que des principales techniques du protocole Blockchain. Le troisième chapitre « **Étude des besoins** » comporte l'étude, la critique de l'existant et la solution proposée ainsi que l'analyse et la modélisation des besoins fonctionnels et non fonctionnels de notre application. Le quatrième chapitre « **Conception et étude technique** » présente la conception générale et la conception détaillée du projet. Le cinquième chapitre « **Réalisation de la solution** » est consacré à exposer l'étude technique du projet ainsi que le travail réalisé tout au long de ce projet. Nous clôturons le rapport par une conclusion générale dans laquelle nous présentons une synthèse du travail réalisé ainsi que les éventuelles perspectives du projet.

Chapitre I

Cadre du projet

Plan

1	Cadre général du projet	3
2	Contexte du projet	3
2.1	Problématique	4
2.2	Description du projet	4
3	Méthodologie de développement adoptée	5
4	Chronogramme des tâches	6

Introduction

Ce chapitre amène dans un premier temps à la présentation de la problématique et l'objectif principal du projet. La deuxième partie présente la définition de la méthodologie adoptée lors de la réalisation de ce projet.

1 Cadre général du projet

Le présent projet s'intitule : Exploration de la technologie Blockchain dans un système de vote en ligne. Il a été réalisé dans le cadre d'un projet de fin d'années pour l'année universitaire 2016/2017.

2 Contexte du projet

Nous décrivons dans cette partie le sujet de notre projet.

2.1 Problématique

Les système de vote hors ligne présentent plusieurs difficultés , en effet, il faut se déplacer aux bureaux de vote en faisant recours aux entités informatisées telles qu’une autorité d’enregistrement,un appareil de vote, un tableau d’affichage et une autorité de comptage, d’où l’augmentation du coût d’établissement de la préparation des élections, la supervision et les opérations de postelection.

D’autre part, la migration vers les systèmes de vote en ligne présente bien évidemment des problèmes indéniables . En effet , Les systèmes de vote électronique existants souffrent tous d’un grave défaut de conception : ils sont Centralisés par conception, ce qui signifie qu’il existe un seul fournisseur qui contrôle les administrations système, la base de données et les sorties du système L’absence d’une production à source ouverte, vérifiable de manière indépendante, rend difficile les systèmes centralisés à acquérir la fiabilité demandée par les électeurs et les organisateurs. Cette lacune de conception limite donc les demandes de vote électronique. Le vote électronique ne vise pas à remplacer les élections traditionnelles, mais peut fournir une méthode de vote complémentaire.

Ces problèmes ont été décortiqués par des solutions proposées par le protocole Blockchain. Dans le monde de vote en ligne, ce protocole présente plusieurs avantages en supprimant les intermédiaires, diminuant les coûts, accélérant les processus et garantissant la sécurité et l’anonymat de vote.

2.2 Description du projet

En tenant compte des limites de l’utilisation de protocole Blockchain dans le domaine de vote en ligne, ce projet a été proposé. Il consiste à réaliser un PoC sur la technologie de la Blockchain réunie avec le processus de vote.

Ce PoC(Proof of Concept, en anglais : une preuve de concept est une réalisation courte d’une certaine méthode ou idée pour démontrer sa faisabilité et couvrir les différentes fonctionnalités offertes par cette dernière) sera une solution Blockchain, permettant d’avoir un produit qui répond aux besoins fonctionnels et non fonctionnels et qui peut s’adapter aux éventuelles évolutions, sur laquelle nous pouvons greffer de divers autres services.

Autrement,il s’agit d’une application web aux gens de créer des votes en lignes et de voter en payant des sommes d’argents digitales à l’aide de la Blockchain. En outre, le chargement de ces terminaux ainsi que le paiement des stations seront pair à pair et sans intervention des serveurs centralisés. Pour ce fait, les votants n’auront alors plus besoin d’un système centralisé pour

contabiliser leur vote mais pourront le faire de de manière décentralisée, autonome et sécurisée.

3 Méthodologie de développement adoptée

La réalisation d'un système informatique nécessite un bon suivi du déroulement du projet. Ceci est achevé avec les méthodologies de développement des logiciels. Il existe plusieurs méthodologies mais l'approche agile semble être la méthode la plus efficace dans notre cas parce qu'elle privilégie l'interaction entre les différentes parties concernées par le projet et surtout elle accepte les changements probables au cours du processus de réalisation. Nous avons choisi la méthodologie agile Scrum dans le cadre de notre mission et nous justifions ce choix par le fait que nous n'avons pas une visibilité claire de la portée du projet. En plus, Les besoins fonctionnels de l'application évoluent au cours de l'avancement du projet entre les travaux existants.

La méthodologie de développement scrum est présentée par la figure I.2 :

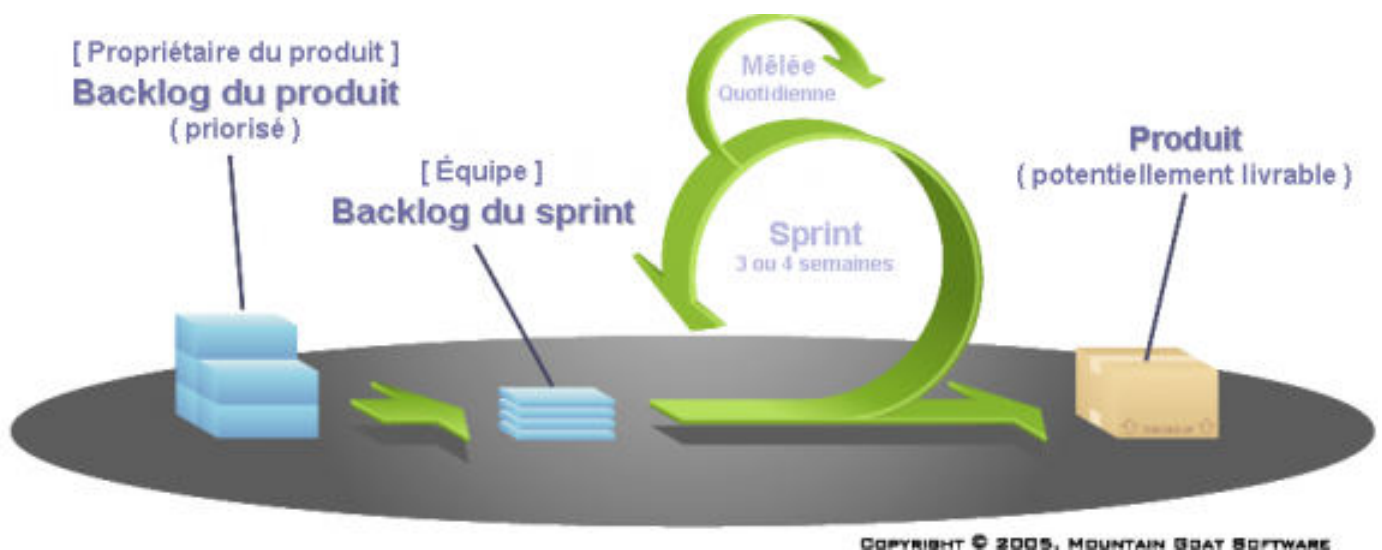


Figure I.1 – La méthodologie de développement scrum

** La répartition des rôles :

Le Scrum Master S'assure que les principes et les valeurs de Scrum sont respectés, facilite la communication au sein de l'équipe et cherche à améliorer la productivité et le savoir faire de son équipe.

L'équipe Pas de rôle bien déterminé : architecte, développeur, testeur, tous les membres de l'équipe apportent leur savoir faire pour accomplir les tâches.

Le Product Owner Expert métier, définit les spécifications fonctionnelles, établit la priorité des fonctionnalités à développer ou corriger, valide les fonctionnalités développées et joue le rôle du client.

4 Chronogramme des tâches

Dans cette partie, nous définissons la répartition des tâches du projet en fonction du temps tout au long de ces 2 mois . Cette répartition sera illustrée à travers un diagramme de Gantt décrivant le déroulement de notre projet représenté par la figure [I.2](#) :

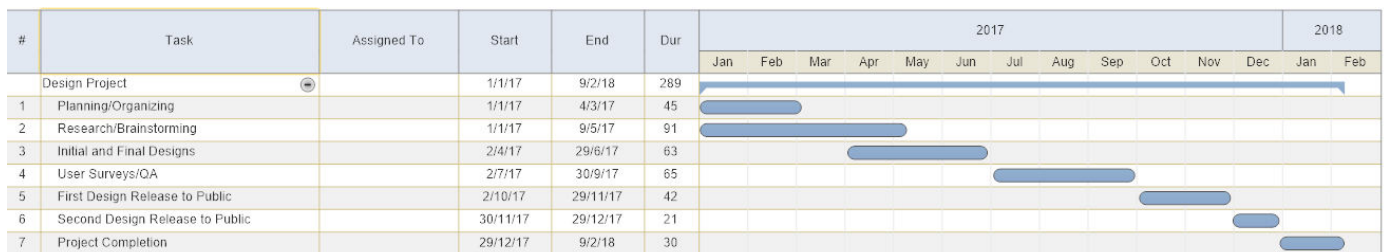


Figure I.2 – Diagramme de Gantt

Conclusion

Dans ce chapitre, nous avons donné un aperçu sur la méthodologie que nous allons adopter tout au long de ce projet. Dans le chapitre suivant, nous allons exposer le domaine de vote en ligne ainsi que les principes fondamentaux du protocole Blockchain.

Chapitre II

État de l'art

Plan

1	Le vote en ligne	7
1.1	Définition	7
1.2	Domaines d'applications	7
2	La technologie Blockchain	8
2.1	Définition	8
2.2	Les principes fondamentaux de Blockchain	9
2.3	Domaines d'applications	13

Introduction

Tout au long de ce chapitre, nous allons explorer les différentes notions en relation avec notre projet afin de le mettre dans son cadre théorique. Nous allons présenter une étude théorique des différentes technologies et principes utilisées dans le cadre de vote en ligne et la Blockchain.

1 Le vote en ligne

1.1 Définition

Le vote électronique est un système de vote dématérialisé, à comptage automatisé, notamment des scrutins, à l'aide de systèmes informatiques. Ce terme générique relève en vérité de plusieurs situations concrètes ; il peut qualifier les votes institutionnels ou l'utilisation de boîtiers de vote interactifs dans un cadre moins contrôlé.

Le vote électronique séduit par la vitesse et la simplicité de son caractère informel, pour les scrutins où le bulletin secret n'est pas requis, comme pour certains votes de parlementaires.

1.2 Domaines d'applications

Entreprise et vie syndicale :

Conseils d'administration, de surveillance, délégués du personnel...

Associatif, clubs :

Assemblées générales, élections, approbation de rapports...

Vie politique :

Primaires de partis, élections (nationales, locales, régionales, européennes...)...

2 La technologie Blockchain

2.1 Définition

La Blockchain consiste en un registre public, où est inscrit l'ensemble des échanges effectués entre les utilisateurs depuis sa création. Tous ces échanges sont consultables par toute personne inscrite dans la blockchain, et ils ne sont pas falsifiables. La particularité de la Blockchain réside d'une part dans son fonctionnement sans intermédiaire (ce qui permet par exemple d'éliminer des frais d'infrastructure), d'autre part dans sa sécurité en offrant un mécanisme informatique inédit permettant de transférer et d'enregistrer de manière ultra-sécurisée l'ensemble des échanges opérés entre les acteurs d'un même réseau qui ne se connaissent pas, indépendamment de toute autorité centrale. La figure II.1 montre le système de paiement avec Blockchain qui est géré par un réseau pair-à-pair d'utilisateurs distribués (la chaîne de blocs) plutôt que le système sans Blockchain qui est géré par une entité unique.

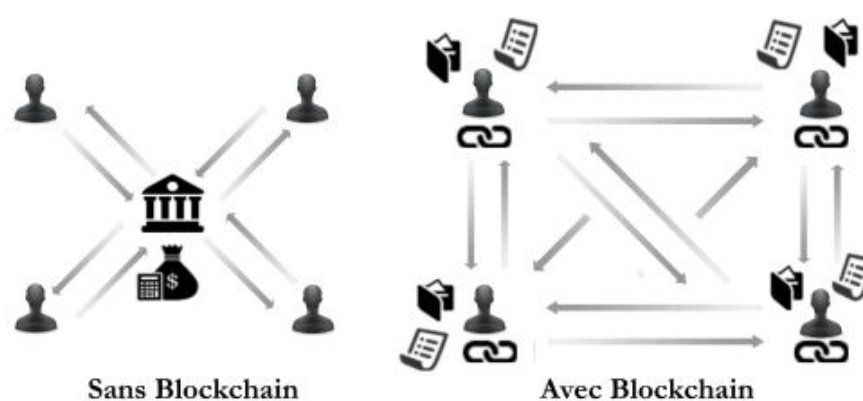


Figure II.1 – Blockchain

Historiquement, le domaine de monnaies digitales a connu plusieurs changements radicaux depuis les années 90s. En 1990, le mathématicien américain David Chaum invente DigiCash, une

monnaie électronique (centralisée et propriétaire) basée sur des protocoles cryptographiques. Après quelques années, Nick Szabo (un informaticien américain) a développé le projet BitGold, une nouvelle monnaie numérique décentralisée basée sur des chaînes infalsifiables de preuves de travail et utilisant les signatures numériques, les clés privées et publiques, etc. Le système s'est révélé cependant trop vulnérable aux attaques. Tous ces essais ont encouragé une personne avec une identité anonyme, ayant comme surnom Satoshi Nakamoto, à annoncer en 2008 la première spécification et preuve de concept de Bitcoin, une nouvelle monnaie digitale totalement basée sur une technologie révolutionnaire qui s'appelle Blockchain. Au début d'octobre 2009, il y avait publication du premier taux de change Bitcoin/Dollar dans lequel le Bitcoin a atteint les 0,001USD (Dollar américain) .

Deux ans plus tard, le Bitcoin a atteint la parité avec le dollar puis, quelques jours plus tard, avec l'euro et après quelques mois il monte à 35USD. En 2014, le cours de Bitcoin a atteint une valeur d'environ les 1200USD. Aujourd'hui, la valeur de Bitcoin devient plus ou moins stable (entre 400USD et 600USD) et des milliers de sociétés et de sites acceptent le paiement avec Bitcoin (Paypal, eBay, Braintree, Microsoft, etc) Avec le succès que Bitcoin a connu depuis sa création, la technologie derrière cette monnaie (Blockchain) a été considérée comme étant une technologie révolutionnaire et, plus que Bitcoin, il y avait plusieurs autres solutions Blockchain qui ont été développées avec des nouvelles cryptomonnaies : Ethereum, Eris, Lisk, Tendermint, etc. Toutefois, ces nouvelles Blockchains offrent d'autres avantages, tels que la vitesse accrue, une plus grande capacité de données, différentes méthodes de consensus et d'autres fonctionnalités avancées.

En effet, avec les nouvelles fonctionnalités offertes par ses différentes solutions, la technologie Blockchain couvre aujourd'hui plusieurs domaines : IoT, Finance, DAPPS (applications décentralisées), etc.

Dans notre projet, nous nous intéresserons aux applications décentralisées (DAPP) . Notre essentiel objectif est d'exploiter les contrats intelligents de la technologie **Ethereum** dans le domaine de vote électronique.

2.2 Les principes fondamentaux de Blockchain

L'adresse Blockchain :

Une adresse Blockchain est similaire à une adresse physique ou une adresse courriel. Il s'agit de la seule information à fournir pour envoyer ou recevoir des crypto-monnaies.

Le bloc :

Un bloc est un enregistrement dans la chaîne de blocs qui contient et confirme plusieurs transactions en attente. Par minage, un nouveau bloc contenant des transactions est ajouté à la chaîne de blocs toutes les périodes de temps (exemples : 10 minutes pour Bitcoin ; 10 secondes pour Ethereum...).

La chaîne de blocs (Blockchain) :

La Blockchain est défini comme étant un journal de toutes les transactions faites par ordre chronologique regroupées dans des blocks chaînés. Ce journal est public et il est partagé entre tous les utilisateurs du réseau Blockchain. La chaîne de Blocks est utilisée pour vérifier la permanence des transactions et empêcher la double dépense (dépenser des crypto monnaies auprès de deux destinataires différents au même moment).

La figure II.2 montre comment les blocks sont créés et chaînés dans une Blockchain.

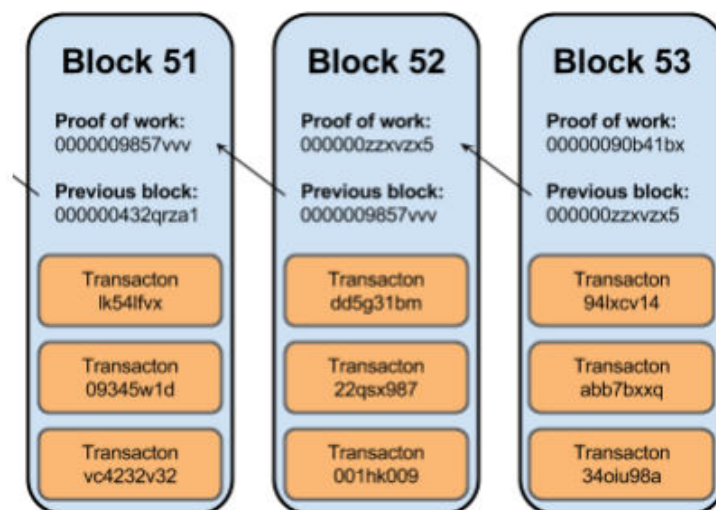


Figure II.2 – Chainage des Blocks

La transaction :

Une transaction est un transfert de valeur entre deux adresses Blockchain. Les adresses sont liées à des informations secrètes appelées clés privées ou graines qui sont utilisées pour signer les transactions, fournissant une preuve mathématique qu'elles proviennent du propriétaire de chaque adresse.

La signature empêche également toute modification de la transaction après son émission. Toutes les transactions sont diffusées entre les utilisateurs et commencent habituellement à être confirmées par un procédé nommé minage.

La clé privée :

Une clé privée est une information secrète générée avec la génération de l'adresse qui prouve le droit de dépenser des crypto monnaies sur la Blockchain grâce à une signature cryptographique. Les clés privées sont stockées en local si un explorateur logiciel en local est utilisé, tandis qu'elles sont stockées sur quelques serveurs en ligne si un explorateur Web est utilisé.

La signature :

Une signature cryptographique est un mécanisme mathématique qui permet à une personne de prouver sa propriété. Dans le cas de Blockchain, chaque adresse a une clé privée. Quand l'explorateur Blockchain signe une transaction avec la clé privée de l'adresse, le réseau entier peut voir que la signature correspond aux crypto-monnaies dépensés. Cependant, il n'existe aucun moyen de deviner cette clé privée afin de voler ces cryptomonnaies. La figure II.3 présente un exemple de signature et d'envoi/réception d'un message en utilisant les clés publique et privée. Dans le cas de la Blockchain, le message sera remplacé par la transaction à envoyer.

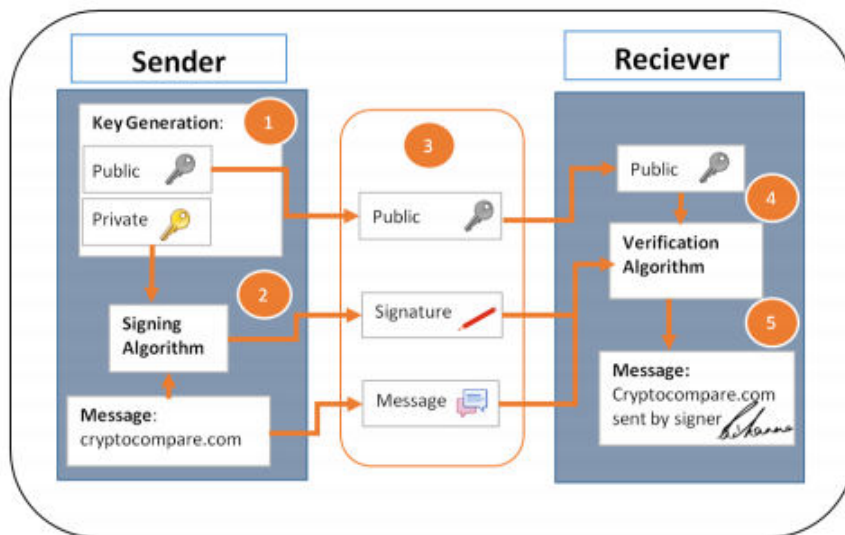


Figure II.3 – Exemple d'une signature électronique d'un message envoyé

La confirmation :

Une confirmation signifie qu'une transaction a été traitée par le réseau et que ses chances d'être renversée sont quasiment inexistantes. Les transactions reçoivent une confirmation lorsqu'elles sont incluses dans un bloc et pour chaque bloc subséquent. Chaque confirmation diminue exponentiellement le risque d'un renversement de transaction. La figure

III.3 présente les étapes de l'envoi et de la confirmation d'une transaction monétaire via la Blockchain d'une personne A à une personne B.

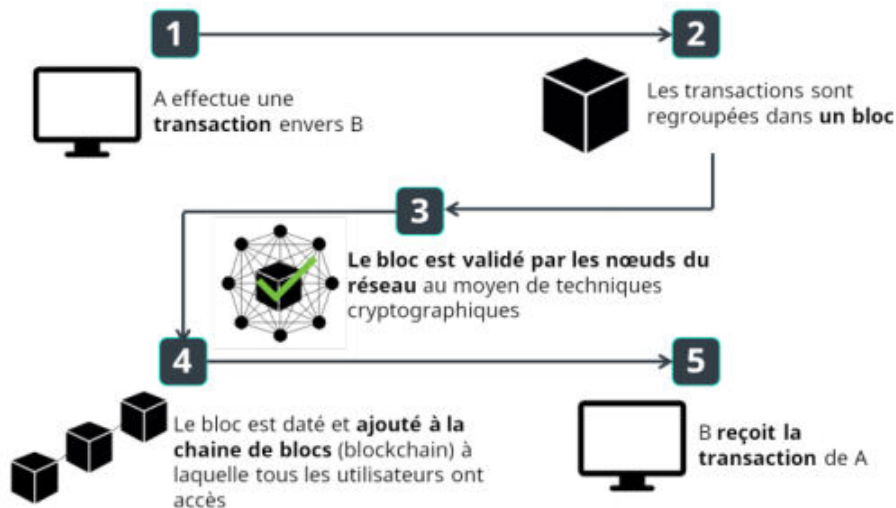


Figure II.4 – Envoi/Confirmation d'une transaction via la Blockchain

La cryptographie :

La cryptographie est une branche des mathématiques qui permet de créer des preuves mathématiques qui offrent un haut niveau de sécurité. Les commerces et banques en ligne utilisent déjà la cryptographie. Avec la technologie de Blockchain, la cryptographie est utilisée pour empêcher quiconque de dépenser les fonds provenant d'une autre adresse et pour empêcher la corruption de la chaîne de blocs.

Le minage :

Le minage de Blocks est l'utilisation de matériel informatique par des agents qui s'appellent Mineurs pour effectuer des calculs mathématiques pour le réseau Blockchain afin de confirmer des transactions et d'augmenter la sécurité. Comme récompense pour leurs services, les mineurs peuvent recevoir les frais de transaction pour celles qu'ils confirment et pour les crypto-monnaies nouvellement créés. Le minage est un marché spécialisé compétitif où les récompenses sont divisées en fonction du nombre de calculs effectués. Le minage peut être défini comme étant un système de consensus distribué utilisé pour confirmer les transactions en attente en les incluant dans la chaîne de blocs. Il impose un ordre chronologique dans la chaîne de blocs, protège la neutralité du réseau et permet à différents ordinateurs d'être en accord sur l'état du système.

Il est nécessaire que les transactions soient incluses dans un bloc qui doit correspondre à des règles cryptographiques très strictes qui seront vérifiées par le réseau. Ces règles

empêchent la modification d'un bloc antérieur car cela invaliderait tous les blocs suivants. Le minage induit également l'équivalent d'une loterie compétitive qui empêche à tout individu d'ajouter facilement des blocs consécutivement dans la chaîne de blocs. De cette façon, aucun individu ne peut contrôler ce qui est inclus dans la chaîne de blocs ni en remplacer des parties pour annuler ses propres dépenses.

Le P2P :

Le P2P (Pair à Pair) fait référence à des systèmes qui fonctionnent comme une collectivité organisée en permettant à chaque individu d'interagir directement avec les autres. Dans le cas de Blockchain, le réseau est construit de manière à ce que chaque utilisateur peut diffuser ses transactions à n'importe quel autre utilisateur de la Blockchain. Et, chose cruciale, aucune banque n'est requise en tant que tierce partie.

2.3 Domaines d'applications

La technologie Blockchain est utilisée dans plusieurs domaines, nous présentons dans la suite quelques domaines d'applications de la technologie Blockchains.

2.3.1 Paiement P2P

L'économie peer-to-peer facilitée par la chaîne de blocs a été l'un des exemples du potentiel perturbateur et innovateur de la technologie. Toutefois, l'utilisation de Bitcoin pour envoyer de l'argent dans le monde est légèrement différente de l'utilisation de Bitcoin comme monnaie. En éliminant les intermédiaires, la chaîne de blocs peut permettre des envois de fonds transfrontaliers moins chers et donc augmenter le pouvoir de dépenser des destinataires.

2.3.2 Internet des objets IOT

La technologie blockchain pourrait fournir un moyen de suivre l'historique unique des appareils individuels, en enregistrant les échanges de données entre elle et d'autres dispositifs, les services Web et les utilisateurs humains. Les exemples incluent les courriers électroniques pour transférer en toute sécurité des informations sensibles, les services d'entiercement pour transférer les droits de propriété, ou même les services d'auto-installation pour vérifier et pousser les mises à jour du logiciel régissant les autres convertisseurs numérique-analogique (Digital-to-

analog converters DAC).

2.3.3 Système de vote

Les systèmes de vote électronique existants souffrent tous d'un grave défaut de conception : ils sont propriétaires, c'est-à-dire centralisés par conception, ce qui signifie qu'il existe un seul fournisseur qui contrôle la base de code, la base de données et les sorties du système et fournit les outils de surveillance en même temps. L'absence d'une production à source ouverte et vérifiable indépendamment rend difficile pour ces systèmes centralisés d'acquiescer la fiabilité requise par les électeurs et les organisateurs d'élections. La blockchain fonctionne comme une base de données de transactions sécurisées, pour enregistrer les votes et les résultats des votes d'audit d'une manière digne de confiance.

2.3.4 Distribution d'énergie

Les nouvelles initiatives énergétiques telles que la production d'énergie domestique et l'énergie solaire communautaire comblent les lacunes de l'approvisionnement en énergie à travers le monde. Les panneaux solaires sont connectés à l'Internet avec la technologie fournie par les startups tels que Filament (voir cas d'utilisation IoT blockchain) permettant aux dispositifs électroniques traditionnels d'être connectés en ligne. Des certificats anonymes sont créés et peuvent, en théorie, être vendus à quiconque souhaite subventionner l'énergie solaire.

2.3.5 Stockage des données

Les services de stockage cloud actuels sont centralisés - les utilisateurs doivent donc faire confiance à un seul fournisseur de stockage. Avec Blockchain, cela peut devenir décentralisé. Alors que certaines industries traditionnelles telles que les banques ont déjà prouvé bénéficier d'un stockage de données décentralisé, certains domaines tels que l'industrie de la santé sont sur le point d'éprouver un changement perturbateur. toutes les informations sensibles qui sont associées à la santé : l'identité, les maladies, les traitements, le paiement, etc qui pourraient être privés sécurisés et stockés grâce à blockchain.

2.3.6 Contrats intelligents

Les contrats intelligents sont des états contractuels auto-exécutables, stockés sur la chaîne de blocs, que personne ne contrôle et que chacun peut donc avoir confiance. Une caractéristique importante d'un contrat intelligent est la capacité de réduire les risques par une exécution non discriminatoire. L'absence d'agent de contrepartie centrale peut permettre à ces contrats de desservir les marchés avec une plus grande efficacité .

Conclusion

Lors de ce chapitre, nous avons défini, en détail, les différentes technologies et notions intégrées dans notre projet, ce qui va nous permettre par la suite d'attaquer l'étude des solutions existantes sur le marché de Blockchain et de vote en ligne en décrivant les limites de chacune.

Chapitre III

Étude des besoins

Plan

1	Étude de l'existant	16
2	Solution proposée	19
3	Analyse des besoins	21
3.1	Besoins fonctionnels	21
3.2	Besoins non fonctionnels	22
4	Modélisation des besoins	22
4.1	Diagramme de cas d'utilisation système	23
4.2	Diagrammes de séquence système	23

Introduction

Au niveau de ce chapitre, nous commençons par une étude des solutions existantes sur le marché. Ces solutions concernent d'une part la technologie Blockchain d'autre part celles qui utilisent cette technologie dans le vote en ligne. Ensuite, nous présentons une critique des solutions proposées. Celle-ci nous a conduits à dégager les besoins fonctionnels et non fonctionnels liés à notre projet ainsi qu'une analyse détaillée des fonctionnalités les plus importantes offertes par notre système . Ces besoins sont analysés et spécifiés dans la deuxième partie de ce chapitre.

1 Étude de l'existant

Depuis la création de la première Blockchain liée au protocole Bitcoin, un certain nombre d'autres Blockchains indépendants ont émergé ces dernières années comme Ethereum, Eris, Lisk, Tendermint, etc. Chaque type de Blockchain a ses propres caractéristiques ainsi que des avantages et des inconvénients. Le tableau [III.1](#) présente une comparaison entre les différentes solutions et protocoles Blockchain existantes.

Tableau III.1 – Tableau comparatif des Blockchain

III.1 Étude de l'existant

Technologies	Avantages	Inconvénients
Bitcoin	<ul style="list-style-type: none"> - Elle est la plus utilisée dans le monde. - Son implémentation est compatible avec plusieurs types de systèmes d'exploitation : Linux, POSIX, Windows, OS X. - Sa monnaie est acceptée par une large collection de sociétés et de sites de paiement digitale. 	<ul style="list-style-type: none"> - Le temps de validation des transactions est assez long presque égale 10minutes . - Elle ne permet pas de créer des contrats intelligents. - Elle est dédiée principalement au domaine de finance. - Elle est écrite seulement en C++ - Le consensus utilisé est le preuve de travail, PoW : Proof of Work
Ethereum	<ul style="list-style-type: none"> - Le temps de validation des transactions est court qui est presque égale à 10secondes . - Elle permet la manipulation des contrats intelligents et des DAPPS (Decentralized Applications) - Elle est facile à implémenter sur des différents types d'OS comme Linux, POSIX, Windows, OS X, etc , en offrant une compatibilité avec plusieurs types de Blockchains : publiques, privées, consortium - Elle est écrit en plusieurs langages C++, Go, JavaScript, Python, Java 	<ul style="list-style-type: none"> - Le consensus utilisé « actuellement » est le PoW ce qui peut entraîner une possibilité d'attaque 51 pour-cents
Eris	<ul style="list-style-type: none"> - Elle est conçu pour habilitier le prototypage rapide, et le bon fonctionnement des applications basées sur des contrats intelligents 	<ul style="list-style-type: none"> - Elle utilise seulement les Blockchains privés. - Son implémentation reste restreinte aux développeurs d'Eris technologies, la société qui a lancé le projet Eris.
Tendermint	<ul style="list-style-type: none"> - Elle utilise plusieurs types de Blockchains : publiques, privées, consortium. - Les blocks sont validés dans un temps très court presque égale à 1seconde - Elle utilise le Proof of Stake (PoS) 	<ul style="list-style-type: none"> - Elle utilise des mineurs propres à elle pour la validation la création de richesse est limitée à Tendermint seulement. - Elle est dédiée principalement au domaine de finance.

Pour la réalisation de notre projet, nous avons opté pour la Blockchain Ethereum dès qu'elle présente plusieurs avantages qui facilite la création des votes életroniques dont on peut citer les contrats intelligents. Pour le domaine de vote en ligne, il existe plusieurs acteurs qui ont implémenté des solutions et des PoCs basées sur le protocole de Blockchain. Par la suite, nous présentons, dans le tableau III.2, les solutions les plus utilisées ainsi que les limites de chaque solution :

Tableau III.2 – Tableau comparatif des solutions de vote existant

Solution	Description
Flux	Le Flux Party a été formé à la fin de 2015 comme un nouveau concept en démocratie avec l'objectif déclaré de retourner le pouvoir démocratique aux électeurs individuels. Dans le cadre du modèle Flux, les représentants du Flux élus voteront sur les projets de loi avant qu'ils ne soient dirigés par un vote majoritaire des membres Flux, en utilisant l'application Flux sécurisée.
V-Initiative	PublicVotes est une application de vote basée sur Ethereum, une nouvelle plateforme de nouveaux contrats intelligents. Grâce à Ethereum, PublicVotes est en mesure de créer un système de vote probable et transparent. Tous les votes sont enregistrés publiquement sur Ethereum Blockchain et peuvent être consultés et audités par tout le monde.
PublicVotes	Bien que la blockchain de Bitcoin présente un large éventail de bénéfices, un inconvénient en tant qu'opérateur électoral est qu'il n'est pas anonyme, mais pseudonyme, ce qui signifie que l'identité de l'utilisateur n'est pas entièrement protégée du public. Les pseudonymes, les identifiants d'utilisateur et les adresses IP peuvent être visualisés et éventuellement tracés par d'autres utilisateurs. Pour renforcer la vie privée, V-Initiative protège l'anonymat des électeurs en utilisant Zero Coin et une cryptographie sans connaissance du savoir, en partenariat avec le logiciel de masquage IP, TOR.
FollowMyVote	FollowMyVote propose une plateforme de vote en ligne open-source et transparente, fondée sur une blockchain.

Le vote en ligne ne résoudrait certes pas le problème de l'abstention dans son ensemble. La question de fond, celle de l'offre politique elle-même et de l'adhésion à ceux qui l'incarnent aujourd'hui, resterait à résoudre.

2 Solution proposée

Dans le cadre de notre projet , nous avons implémenté une solution de vote en ligne qui n'est qu'un POC (preuve de concept). Ce Poc couvre toutes les fonctionnalités de la Blockchain Ethereum en insistant sur la sécurité l'anonymat de vote par l'utilisation de plusieurs techniques de cryptographie. Cette solution sera générique, évolutive ayant des informations techniques pour l'analyse de la Blockchain utilisée.

Par ailleurs, le processus implémenté tout au long de ce projet est le suivant :

Récupération de la liste des candidats :

Chaque candidat (C) attribue une clé publique KeyC à l'électeur et publie partout un vanity Bitcoin adress comme 1Martin .., c'est-à-dire, une adresse préparée par les organisateurs pour le candidat Martin. Pour le secret de chaque bulletin(ballot) , chaque KeyC est différent pour chaque électeur, de sorte que le candidat doit générer n clés publiques KeyC pour n électeurs. Chaque candidat doit publier aux organisateurs Merkle Root comprenant toutes ses clés publiques KeyC. Alternativement, l'application de vote peut générer les clés KeyC au nom du candidat,mais cette option pourrait être évitée pour réduire la nécessité de faire confiance aux organisateurs. À l'aide de la demande de vote, chaque électeur devrait pouvoir vérifier que son vote est tenu en compte en visualisant sa clé KeyC dans le hash tree.

Chaque électeur (B) est également assigné par les organisateurs d'élections (association A) une Clé publique KeyA et une valeur nonce qui peut être utilisé par l'électeur comme une clé d'accès secrète pour ouvrir son compte. Ces clés d'accès seront envoyées en toute sécurité par les organisateurs à chaque électeur. La liste des électeurs peut être représentée dans un Merkle tree . L'application donne à chaque électeur la liste des hachages intérieurs, reliant sa clé publique KeyA au Merkle root. Avec l'arbre Merkle (Merkle tree) publié par l'application et avec le calcul standard des formules données , la liste des électeurs peut être vérifiée de façon indépendante par toutes les parties . L'électeur peut vérifier le chemin de son nœud de feuille à la racine de Merkle et s'assurer que le nombre de noeuds feuilles est égal au nombre d'électeurs.

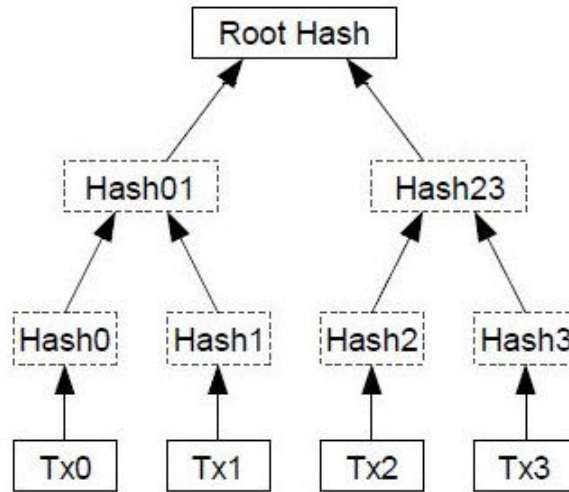


Figure III.1 – L'arbre Merkle

Préparation du bulletin de vote :

Avant le jour de l'élection, avec les clés publiques A, B et C enregistrées par l'application, l'application peut créer une adresse 2-sur-3 multisignature et une transaction lui envoyant un bitcoin micropayment (prix d'un timbre-poste) à la confirmation de l'électeur de son vote. Le vote de l'électeur a maintenant une représentation cryptographiquement sûre dans cette transaction, qui est diffusé aux noeuds de réseau bitcoin par l'application. À ce stade, il convient de noter que l'électeur peut vérifier indépendamment et immédiatement que son vote a été soumis au réseau bitcoin en consultant l'adresse multisignature avec n'importe quel explorateur de bloc bien que la transaction est encore non confirmée, elle s'affiche dans 2 à 3 s au plus après avoir confirmé son vote. Après quelques heures, le bulletin de vote est enregistré de façon sécurisée sur le blockchain avec une augmentation du nombre de confirmations réseau.

comptage des votes :

À la fin de l'élections, l'application peut simplement afficher les résultats compilés de son base de données. Par rapport à un système traditionnel, propriétaire, la fonctionnalité ajoutée est la capacité d'afficher une adresse multisignature financée pour chaque vote enregistré. Le blockchain ne dit pas grand chose de cette adresse jusqu'à ce que ses coins soient dépensées pour une autre adresse. Les résultats des élections seront vérifiés de façon indépendante au cours de la prochaine et dernière étape.

Affichage des résultats :

C'est l'étape dans laquelle on expose une preuve durable et facilement vérifiable que le comptage des votes est totalement crédible et non falsifié. Disons que l'un des candidats est Martin : Martin a annoncé une spéciale bitcoin vanity 1Martin sur les réseaux sociaux pendant la campagne électorale. Pour chaque électeur, l'application utilise les deux clés privées correspondant à KeyB et KeyC, respectivement, pour signer une transaction, dépenser les coins du compte de la 2-de-3 multisignature adresse vers l'adresse "1Martin". Un observateur peut utiliser Merkle tree publié par le candidat avant l'élection pour vérifier la validité des hachages internes reliant KeyC à la racine Merkle (Merkle root). Similaire les vérifications appliquées à KeyA et KeyB permettront à l'observateur d'affirmer la validité de l'adresse multisignature. Un écart entre le nombre de votes fourni le jour du scrutin et les transactions blockchain pourraient être repérées facilement avec n'importe quel logiciel explorateur de blocs. Toutefois, il est impossible pour un observateur de lier une multisignature adress à un électeur dans la mesure où KeyB ne peut pas être lié à l'identité de l'électeur par l'observateur. Ce système utilise davantage la signature numérique par rapport à la signature manuelle : une signature numérique n'identifie son auteur qu'avec son consentement, si et elle révèle son identité. Les votes, tout en préservant le secret des bulletins de vote, sont parfaitement vérifiables par les candidats et les électeurs, indépendamment de toute organisation. Pour compléter les opérations post-election, les organisateurs collectent les fonds de l'adresse 1Martin et des vanity adresses des autres candidats qui ont été préparés dans la période pré-élection.

3 Analyse des besoins

L'objectif de ce projet est la conception et la réalisation du application web de vote en ligne « InsatVoting », Cette application est divisée en deux parties : partie web, utilisée comme moyen de vote et de création des votes, et une partie d'infrastructure, permettant d'exploiter un contrat intelligent intitulé Evote stocké sur la blockchain.

3.1 Besoins fonctionnels

L'application doit répondre à un ensemble de besoins fonctionnels. Nous présentons ces besoins par acteur :

Administrateur de vote :

Cet acteur peut créer un vote ,saisir la liste des candidats ainsi que inviter les votants concernés par email. A la fin de vote , il peut afficher les resultats de vote .

Le votant :

Après avoir reçu une invitation de vote de la part de l'administrateur , le votant doit finaliser son inscription par le remplissage du formulaire d'inscription. Une fois son inscription est confirmée, le votant peut voter plusieurs fois et seul son dernier vote qui sera comptabilisé.

3.2 Besoins non fonctionnels

Notre application met l'accent sur plusieurs besoins non fonctionnels, qui se rapportent à des spécifications et des concepts de securité :

Utilisabilité :

L'application web doit offrir une interface conviviale, responsive, ergonomique et facile à manipuler par les utilisateurs afin de faciliter la navigation.

Evolutivité :

Le code doit être clair pour permettre de futures évolutions ou améliorations et l'ajout des modules et des nouvelles fonctionnalités doit être facile et souple.

Sécurité :

L'application doit garantir plusieurs critères de vote. En effet , elle doit assurer l'anonymat de vote çad personne ne doit être capable de faire le rapprochement entre l'électeur et son vote, l'éligibilité parce que seuls les votants éligibles peuvent voter.En plus ,il n'y aura pas de résultat partiel.

Performance :

Les performances d'exécution de l'application « InsatVoting » doivent être optimales et le temps de réponse doit être le plus court possible..

4 Modélisation des besoins

Nous allons modéliser les besoins de l'application à travers un diagramme de cas d'utilisation système, qui nous permet d'avoir une vision globale du fonctionnement de notre application, et des diagrammes de séquences système, qui nous permettent de détailler les cas d'utilisation de ce dernier.

4.1 Diagramme de cas d'utilisation système

Les besoins fonctionnels de notre module peuvent se résumer par le diagramme de cas d'utilisation système illustré par la figure III.2

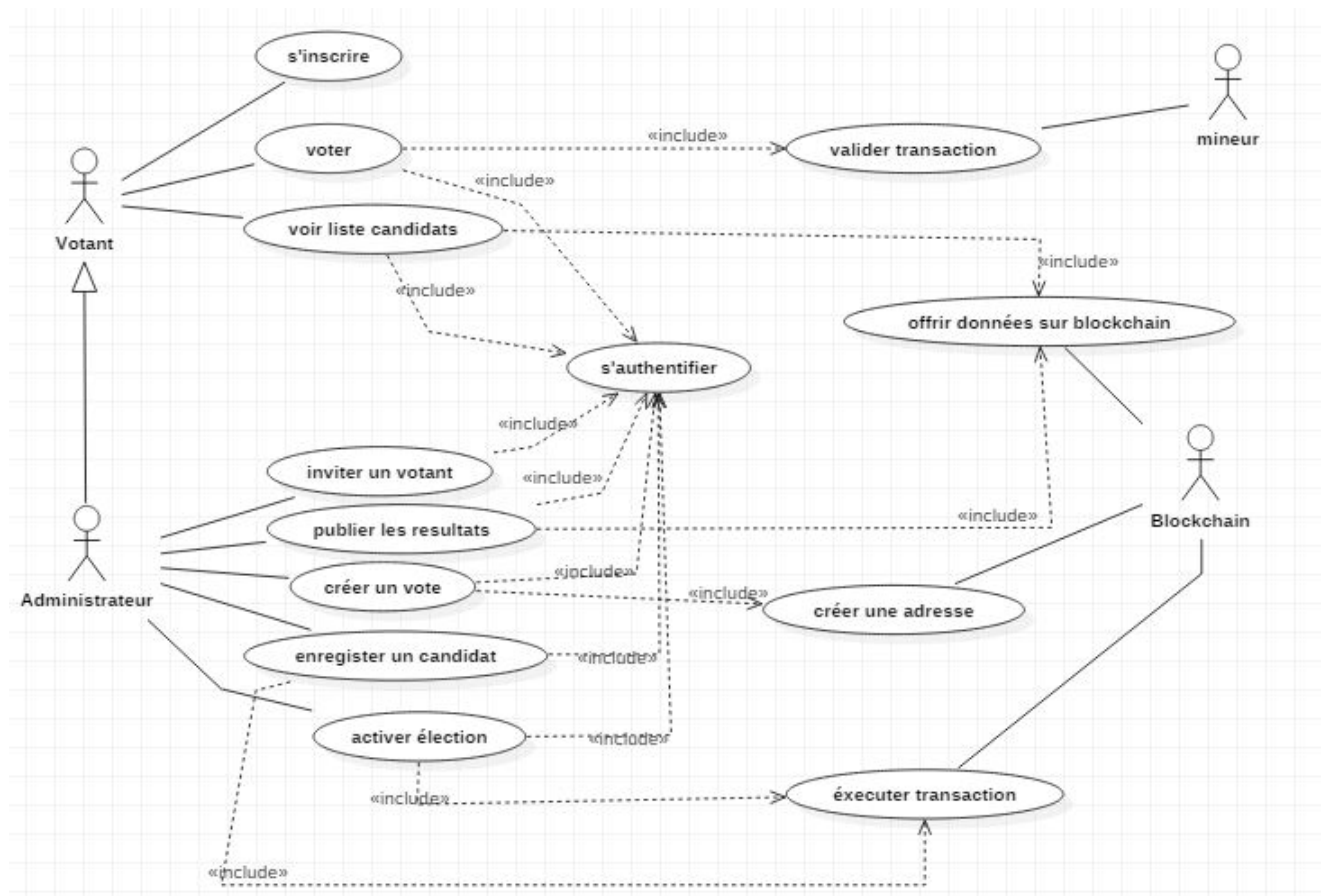


Figure III.2 – Diagramme de cas d'utilisation système

Nous notons que les besoins « voir liste candidats », « publier les resultats », « créer un vote » et « activer élection » exigent l'intervention de l'acteur secondaire « Blockchain » et que le besoin « voter » exige l'intervention de l'acteur secondaire « Mineur » afin de valider la transaction sur la blockchain.

4.2 Diagrammes de séquence système

Au cours de ce paragraphe, nous détaillons les fonctionnalités les plus importantes offertes par « InsatVoting » à savoir la création des comptes et l'opération de vote.

4.2.1 Diagramme de séquence « S'inscrire »

Dans la figure III.3 nous exposons l'opération de création d'un compte sur la Blockchain Ethereum à travers un diagramme de séquence

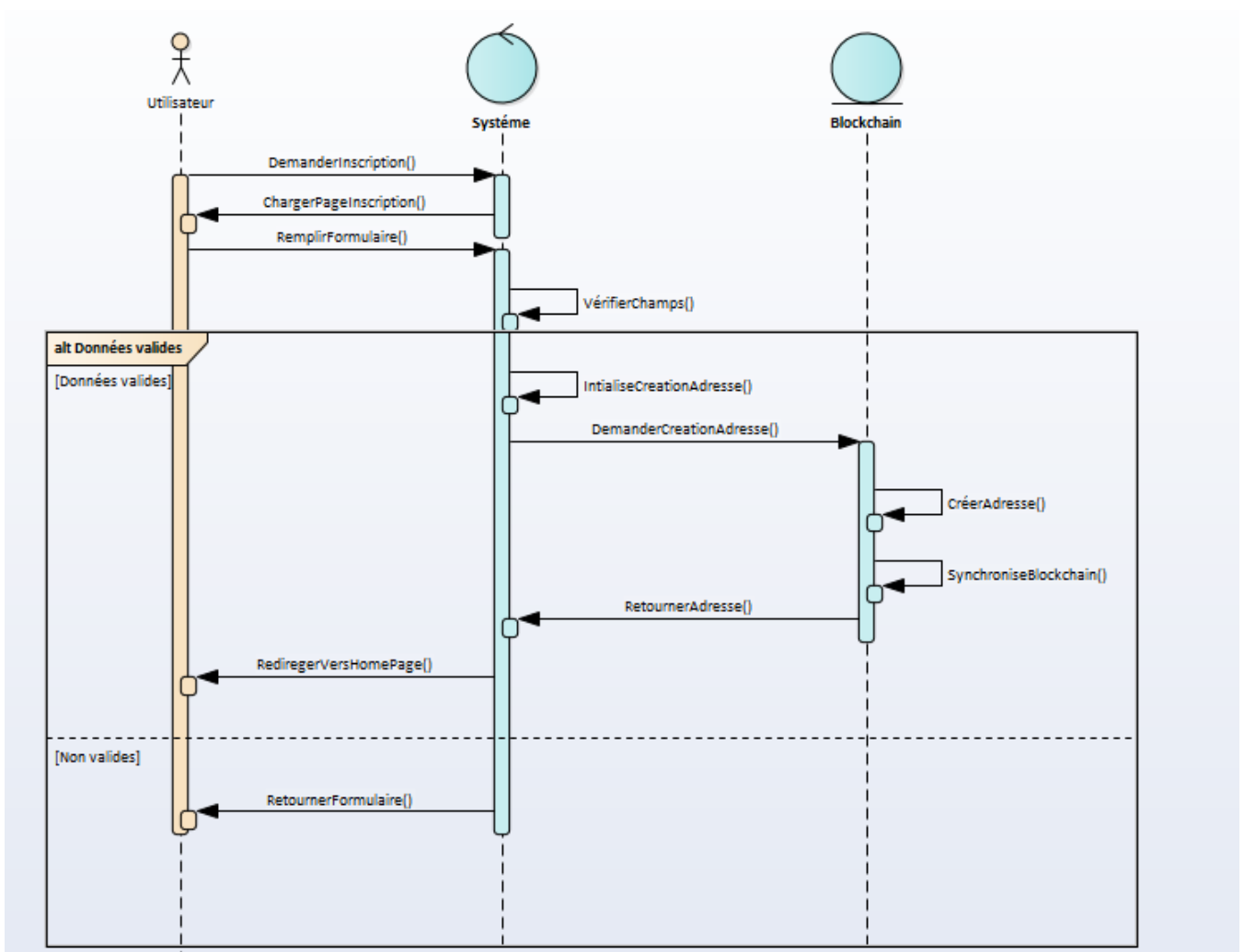


Figure III.3 – Diagramme de séquence « créer compte »

4.2.2 Diagramme de séquence « Voter »

Dans la figure III.4, nous exposons l'opération de vote à travers un diagramme de séquence

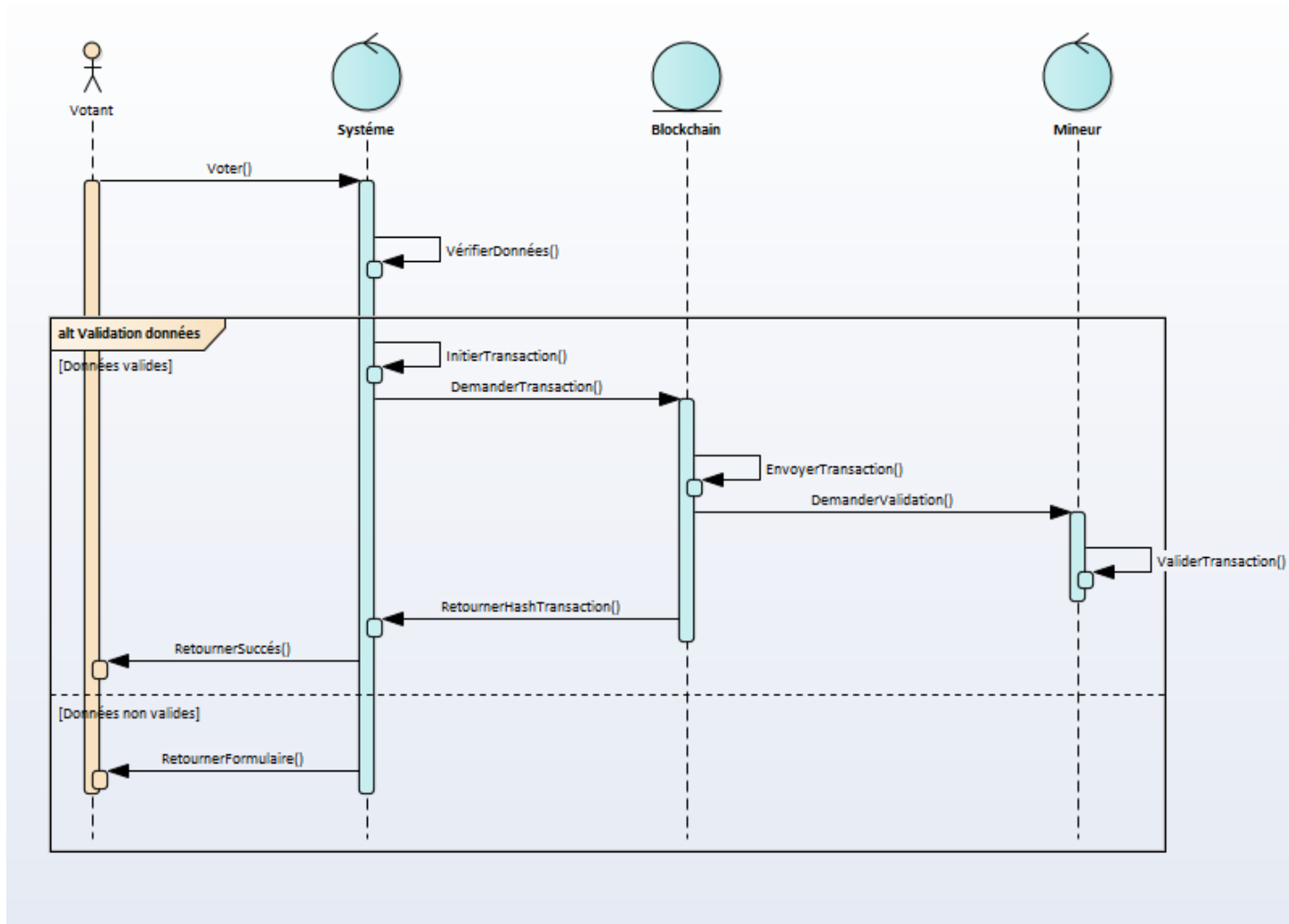


Figure III.4 – Diagramme de séquence « Voter »

Conclusion

Dans ce chapitre, nous nous sommes intéressés à l'étude de l'existant ainsi que l'analyse des besoins fonctionnels et non fonctionnels de notre application. Nous avons détaillé les fonctionnalités les plus importantes offertes par « InsatVoting » à savoir la création des comptes et l'opération de vote . Dans le chapitre qui suit, nous allons entamer la partie conception de « VotingInsat ».

Chapitre IV

Conception et étude technique

Plan

1	Conception générale	26
1.1	Architecture globale du système	26
1.2	Architecture logicielle de la partie WEB	27
2	Conception détaillée	28
2.1	Diagramme de packages	28
2.2	Diagramme de Classes	29
2.3	Diagramme de séquence objet «Payer Frais Transaction Vote»	31

Introduction

Dans ce chapitre, nous enchaînerons dans un premier lieu avec la partie conception générale à travers laquelle nous exposons les architectures globale et détaillée du notre système. Dans un second lieu, nous présentons la conception détaillée dans laquelle nous exposons les diagrammes nécessaires pour mieux expliquer le fonctionnement du système.

1 Conception générale

1.1 Architecture globale du système

Comme nous avons mentionné dans le chapitre précédent, « InsatVoting » comporte deux parties : une partie WEB et une partie blockchain. La structure générale de ces parties est illustrée dans la figure [IV.1](#)

La partie WEB est composée de 2 modules :

Module D'administration :

qui crée les élections , ajoute les candidats , inviter les votants et publier les résultats.

Module Votant :

qui permet l'inscription des votants ainsi que le vote.

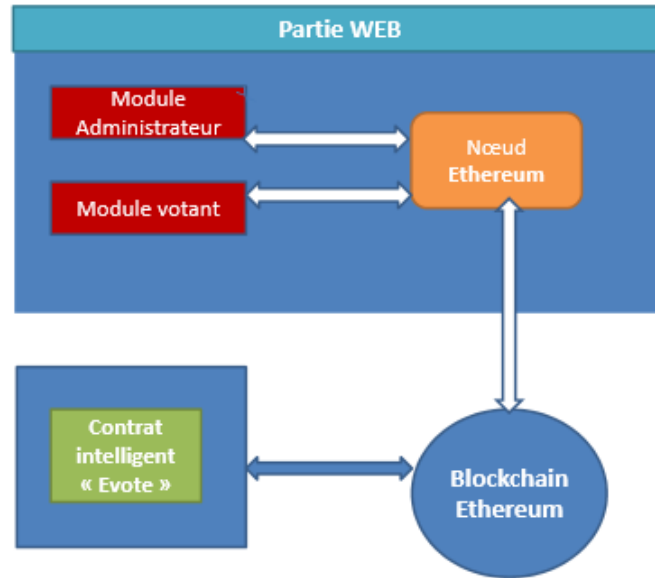


Figure IV.1 – Architecture globale du système « InsatVoting »

La seconde partie est celle de la blockchain dans laquelle on trouve le contrat "Evote" en cours d'exécution par les mineurs.

1.2 Architecture logicielle de la partie WEB

L'architecture logique de la partie web de notre application est une architecture qui comporte 3 couches comme le montre la figure IV.2 :

L'architecture de l'application WEB respecte le modèle MVC en ajoutant quelques spécifications de la plateforme logicielle utilisée. Le choix de l'architecture WEB est basé sur la Blockchain utilisée (Ethereum) et la décision finale était la plateforme de développement **MeteorJS** dès qu'elle présente plusieurs avantages :

- Compatibilité avec la Blockchain Ethereum .
- Permet la création des applications WEB temps réel.
- Multi-plateformes (mobile, desktop, tv).

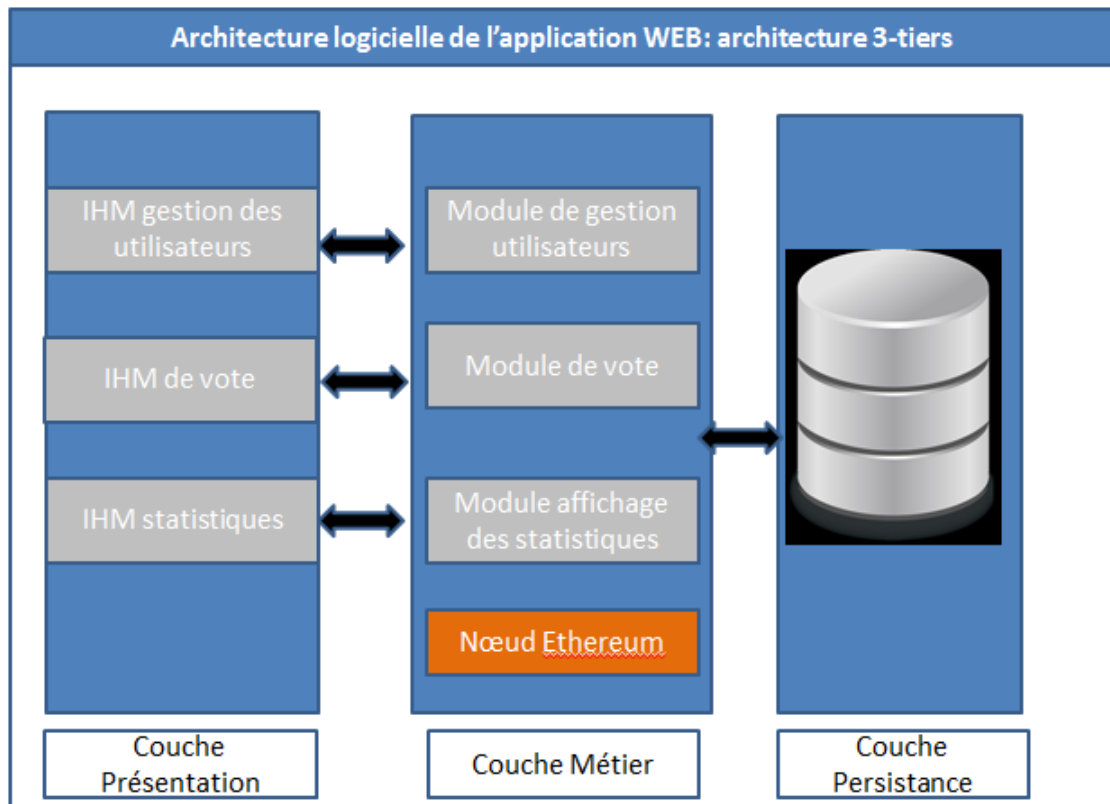


Figure IV.2 – Architecture logicielle de la partie WEB

2 Conception détaillée

Dans cette partie nous allons présenter une conception détaillée de la partie WEB à travers un diagramme de packages et un diagramme de classes.

- Les diagrammes doivent être clairs, lisibles et bien expliqués, sans pour autant nous submerger de détails. Des explications trop longues deviennent ennuyeuses ;
- Si un diagramme est trop grand, vous pouvez le diviser, le représenter sous forme de plusieurs diagrammes, ou vous abstraire de certains détails. Si c'est impossible, imprimez-le sur une grande page (A3), quitte à le plier ensuite. Le plus important est que tous les mots soient lisibles.

2.1 Diagramme de packages

Le diagramme de packages représenté par la figure IV.3 rassemble toutes les packages qui ont assuré les fonctionnalités offertes par notre application. Ces packages sont décrites comme suit :

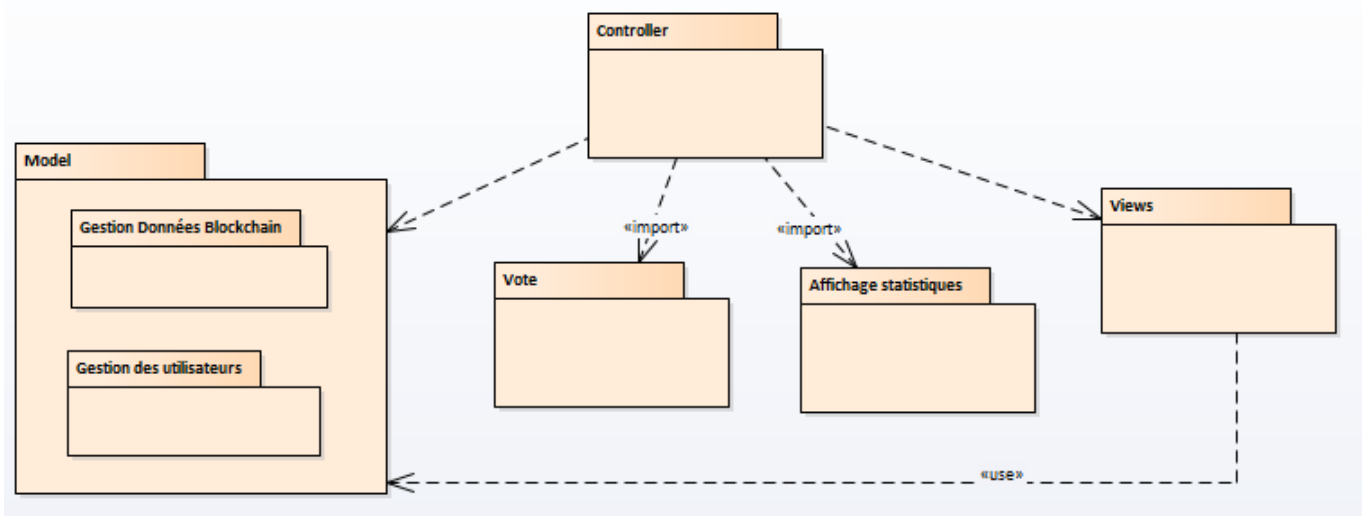


Figure IV.3 – Diagramme de packages

- **Controlleur**, comportant les composants utilisés pour gérer la partie commande de notre système.
- **Views**, contient les éléments de la couche présentation.
- **Model**, comporte les composants de l'accès à la partie données .
- **Vote**, composé de l'ensemble des traitements inclus dans l'opération de vote.
- **Affichage statistiques**, c'est le package ayant les unités d'affichage des statistiques.
- **Gestion des utilisateurs**, contient les classes et les associations manipulant les comptes des utilisateurs : authentification, création, etc.
- **Gestion des données blockchain**, permettant la manipulation de données issues de la Blockchain et leurs traitement et préparation pour les adapter par la suite à l'affichage des statistiques.

2.2 Diagramme de Classes

Nous présentons par la suite le diagramme de classes illustré dans la figure [IV.4](#) :

Blockchain :

C'est la classe qui comporte les informations relatives à la blockchain utilisée.

Block :

Elle présente des informations relatives aux blocks constituant la blockchain. Une blockchain est un ensemble de blocks chaînés chronologiquement.

Mineur :

Cette classe comporte les informations relatives aux mineurs. Elle est en relation «use»

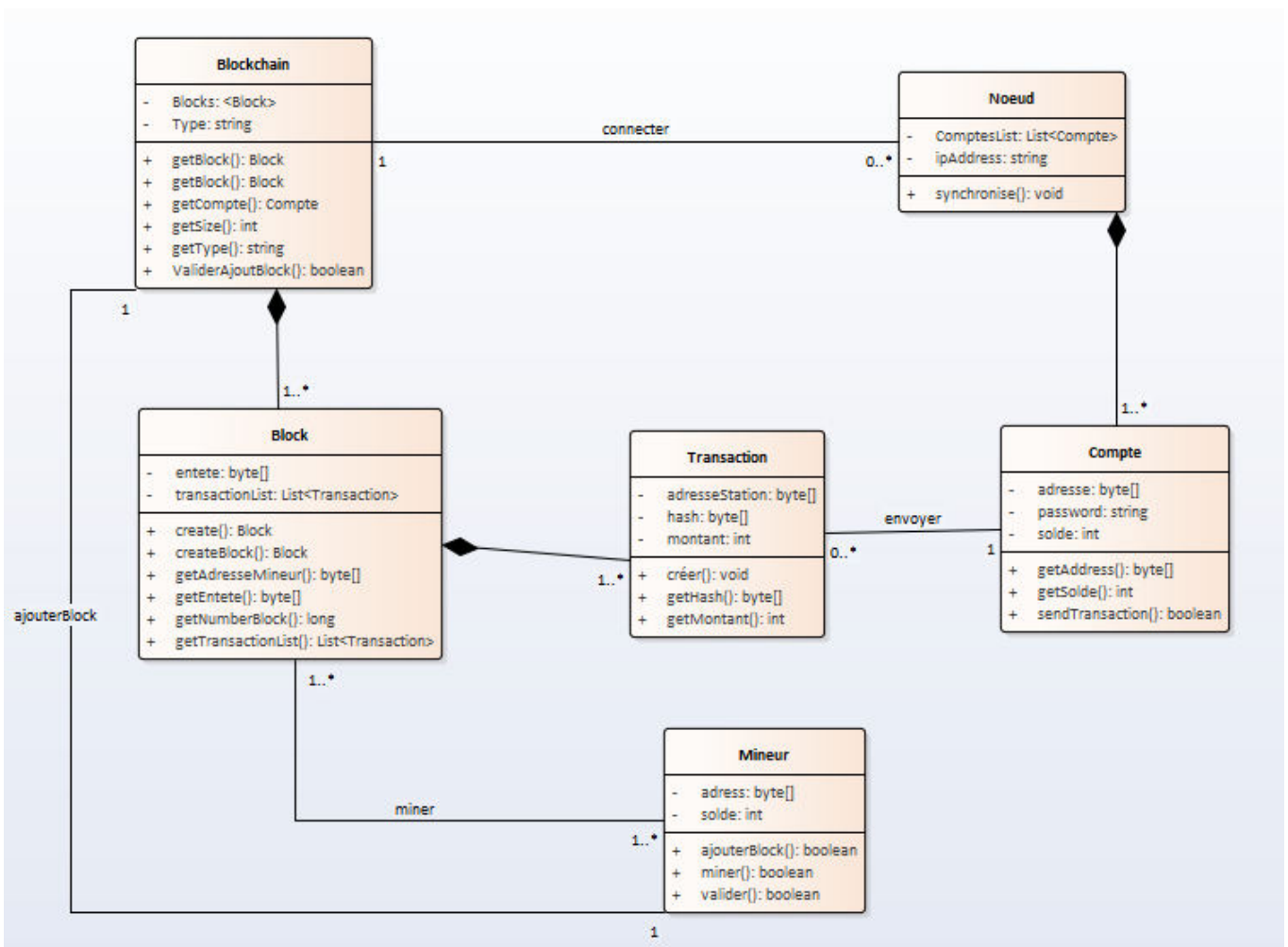


Figure IV.4 – Diagramme de classes

avec la classe block dès qu'elle utilise dans l'une de ses méthodes des blocks comme argument. D'un côté, un mineur peut ajouter des blocks à la blockchain à condition qu'il a terminé le premier et a l'accord de l'ensemble des autres mineurs. De l'autre côté, pour qu'il soit récompensé, le mineur doit récolter les transactions qui circulent dans la blockchain et les mettre dans un block et le valider, alors valider les transactions, à l'aide des calculs mathématiques et il doit le retourner à la blockchain pour vérifier son travail, cette opération s'appelle « minage ».

Transaction :

Elle présente des informations relatives aux transactions de la blockchain. Les transactions sont regroupées dans des blocks et elles sont aussi chaînées chronologiquement. utilisée.

Compte :

C'est la classe qui contient les informations relatives à un noeud Blockchain. Un noeud est composé de plusieurs comptes et il permet la synchronisation avec la Blockchain et l'intégration du notre serveur d'application dans le réseau P2P de Ethereum.

Noeud :

C'est la classe qui contient les informations relatives à un compte Ethereum créé par notre système tel que son mot de passe, son adresse et son solde..

2.3 Diagramme de séquence objet «Payer Frais Transaction Vote»

Pour mieux comprendre le déroulement de paiement du service de vote de « VotingInsat », nous présentons par la suite la figure IV.5 qui montre les différentes interactions entre les objets pour payer les frais de l'exécution d'une transaction.

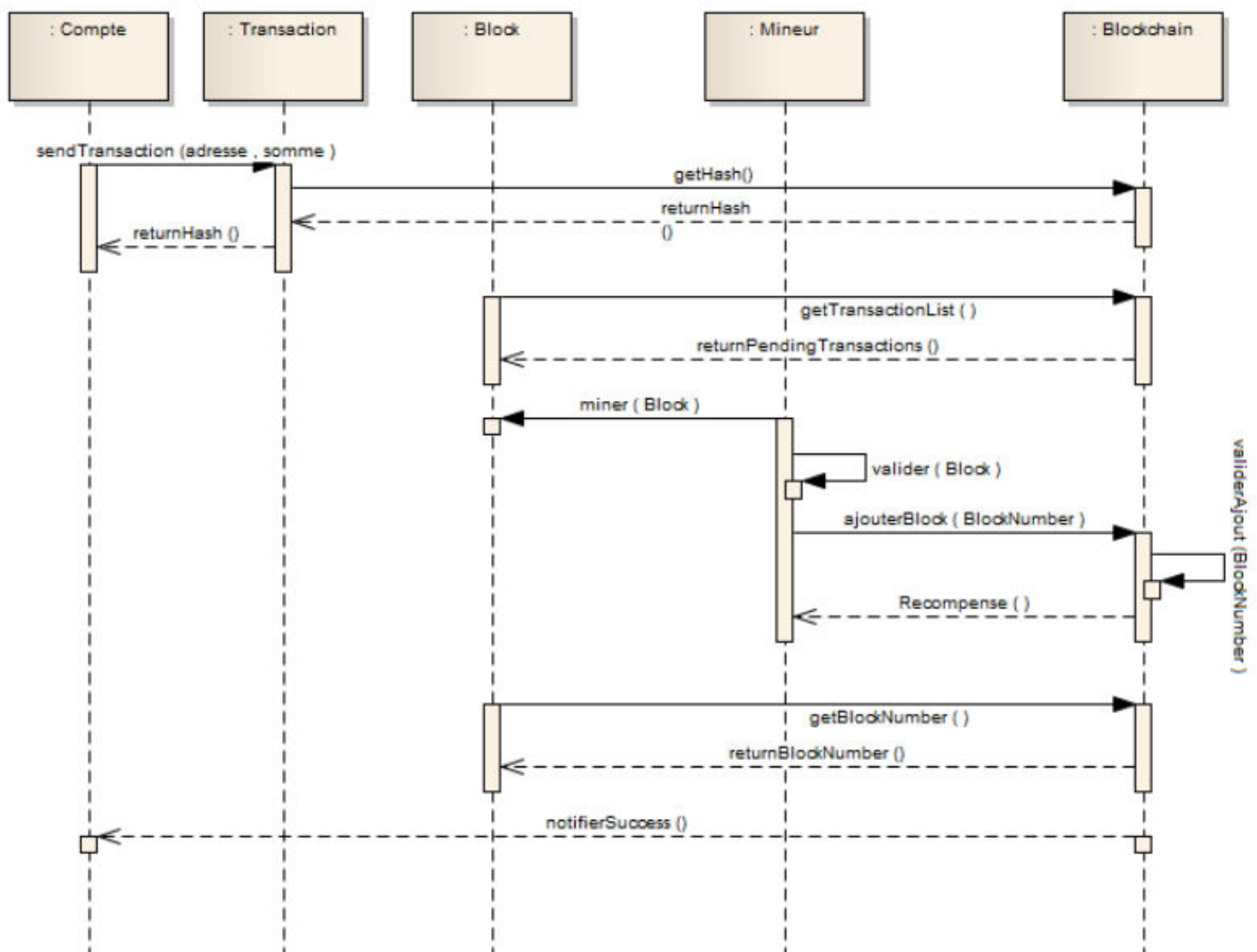


Figure IV.5 – Diagramme de séquence objet « Payer Frais Transaction Vote »

Conclusion

Dans ce chapitre, nous avons établi les principaux composants du système interagissant entre eux afin de réaliser ses fonctions. Le chapitre suivant présentera l'environnement du travail et les différentes technologies utilisées ainsi qu'une présentation de la réalisation de la solution «VotingInsat».

Chapitre V

Réalisation de la solution

Plan

1	Étude technique	33
1.1	Environnement de travail	33
1.2	Blockchain utilisée (Ethereum)	34
2	Réalisation de la partie WEB	35

Introduction

Ce chapitre constitue le dernier volet de ce rapport. Il a pour but d'exposer le travail réalisé tout au long de ce projet. Il est consacré à présenter une étude technique des différentes technologies utilisées, les principales interfaces de l'application WEB du système « InsatVoting » à travers des captures d'écrans.

1 Étude technique

Dans ce paragraphe, nous exposons les environnements logicielle et matérielle de notre application ainsi que les différentes technologies et langages utilisés pour sa réalisation.

1.1 Environnement de travail

1.1.1 Environnement matériel

Le projet a été réalisé sur une machine virtuelle Linux utilisée comme étant un serveur d'application dont les caractéristiques sont :

- 4 Go RAM
- 100 GB ROM
- Linux Mint

1.1.2 Environnement logiciel

Dans cette partie, nous présentons les différents langages que nous avons utilisés tout au long de notre projet.

HTML :

C'est un langage de balisage permettant de structurer systématiquement et de mettre en forme le contenu des pages WEB.

CSS :

permet de mettre en forme des documents Web, type page HTML ou XML.

Bootstrap :

représente un ensemble qui contient des codes HTML et CSS, des formulaires, boutons, outils de navigation et autres éléments interactifs.

JavaScripts :

est un langage de programmation de scripts principalement utilisé dans les pages web interactives.

Truffle :

est un environnement de développement, un cadre de test et un pipeline d'actifs pour Ethereum, afin de faciliter la vie en tant que développeur Ethereum.

TestRPC :

est un client Ethereum basé sur Node.js pour le test et le développement.

1.2 Blockchain utilisée (Ethereum)

Ethereum propose plusieurs avantages pour les machines connectées qui permettent la bonne gestion des messages et de données échangées entre les différents noeuds (machines) de sa Blockchain. Contrairement à la majorité des Blockchains existantes, Ethereum intègre des contrats intelligents qui permettent d'exposer des méthodes qui sont appelées dynamiquement par d'autres contrats ou par des agents externes. Ethereum est donc un protocole conçu pour construire des applications décentralisées (Dapps) dans des situations où la sécurité doit être au rendez-vous. En effet, Ethereum offre la possibilité d'utiliser différents types de Blockchain (testrpc,public, testnet, privée, consortium). Notre application est basée sur le réseau TESTRPC : — Il utilise pour les phases de tests. — Il offre des faux éthers pour les tests. — Il a les mêmes caractéristiques que le réseau réel. — Il est ouvert à tout le monde. — Il peut être par la suite simplement migré vers les blockchains privées ou sur le réseau Ethereum réel.

2 Réalisation de la partie WEB

Cette partie a pour but d'exposer les différentes parties de notre application par un enchaînement de captures d'écrans.

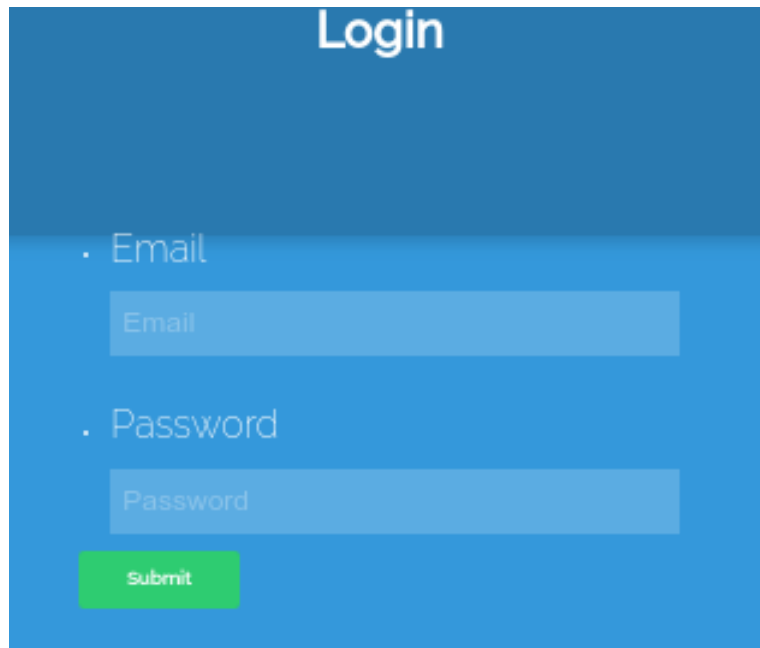
A screenshot of a web application's login page. The page has a solid blue background. At the top center, the word "Login" is written in white. Below it, there are two labels: "Email" and "Password", each preceded by a small white dot. Under the "Email" label is a light blue rectangular input field with the placeholder text "Email". Similarly, under the "Password" label is a light blue rectangular input field with the placeholder text "Password". At the bottom center, there is a green rectangular button with the word "Submit" in white.

Figure V.1 – Formulaire de connexion

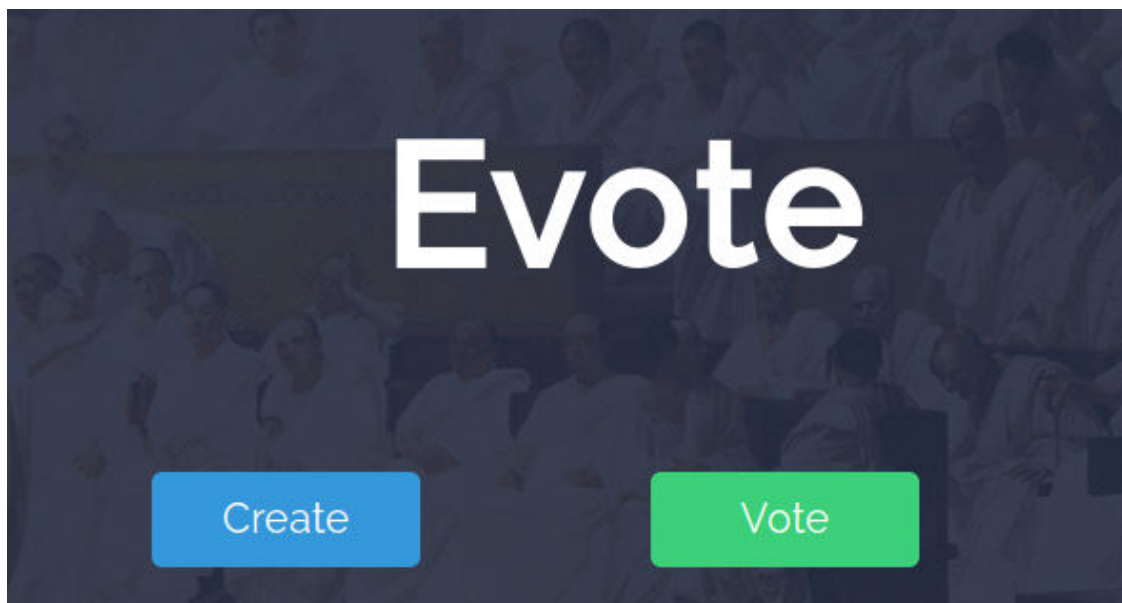
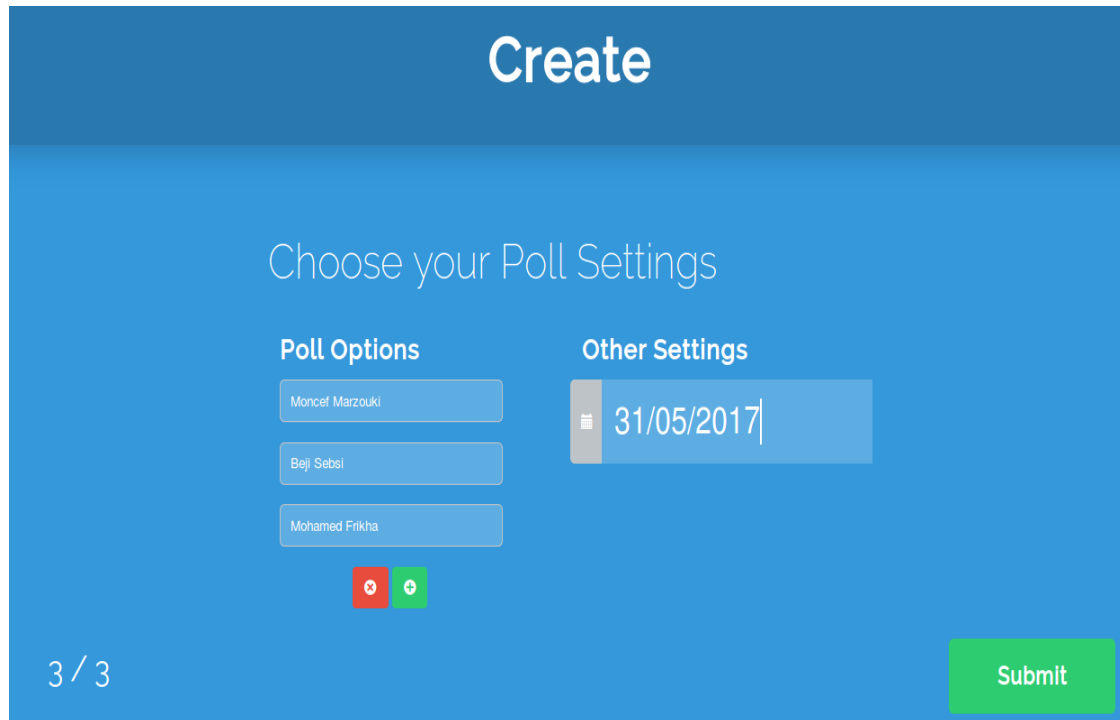


Figure V.2 – Menu principal



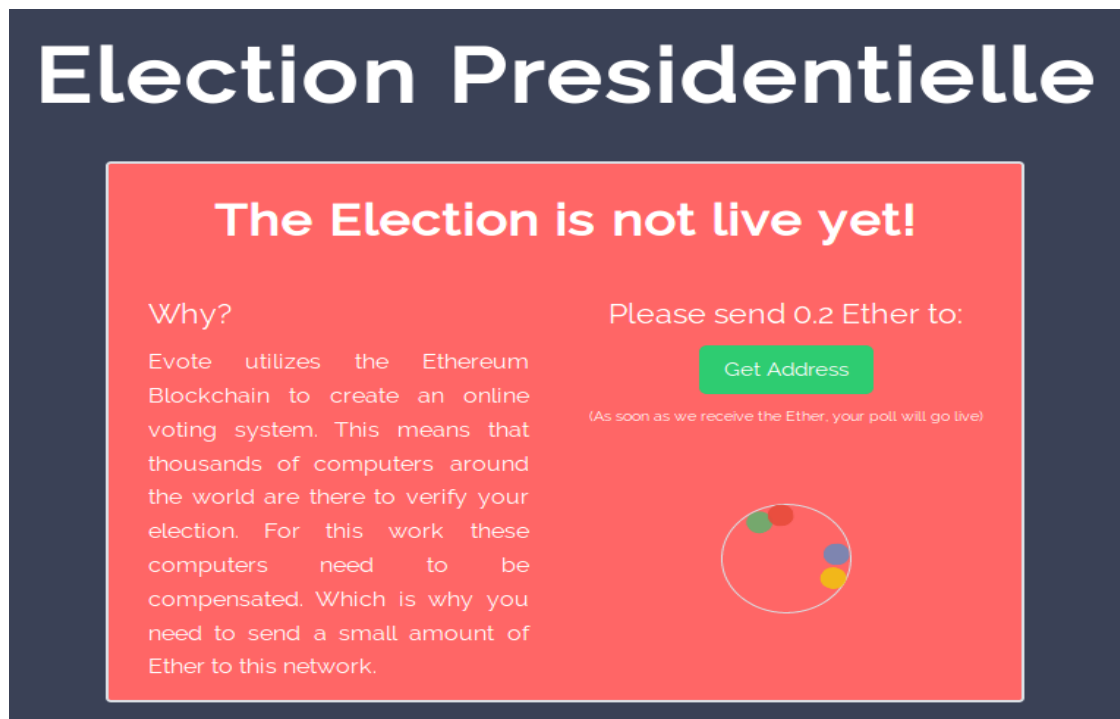
The screenshot shows a web interface titled "Create" with a subtitle "Choose your Poll Settings". It is divided into two main sections: "Poll Options" and "Other Settings".

Poll Options: This section contains three input fields with the names "Moncef Marzouki", "Beji Sebsi", and "Mohamed Frikha". Below these fields are two small buttons: a red one with a minus sign and a green one with a plus sign.

Other Settings: This section contains a date input field showing "31/05/2017".

At the bottom left, there is a page indicator "3 / 3". At the bottom right, there is a green "Submit" button.

Figure V.3 – Création d'un vote



The screenshot shows a dark blue background with the title "Election Presidentielle" in large white letters. Below the title is a red rectangular box containing the following text:

The Election is not live yet!

Why?

Evote utilizes the Ethereum Blockchain to create an online voting system. This means that thousands of computers around the world are there to verify your election. For this work these computers need to be compensated. Which is why you need to send a small amount of Ether to this network.

Please send 0.2 Ether to:

[Get Address](#)

(As soon as we receive the Ether, your poll will go live)

Below the text, there is a circular graphic with four colored dots (green, red, blue, yellow) arranged in a square pattern.

Figure V.4 – Récupération de l'adresse vers laquelle il faut envoyer des "Ethers"

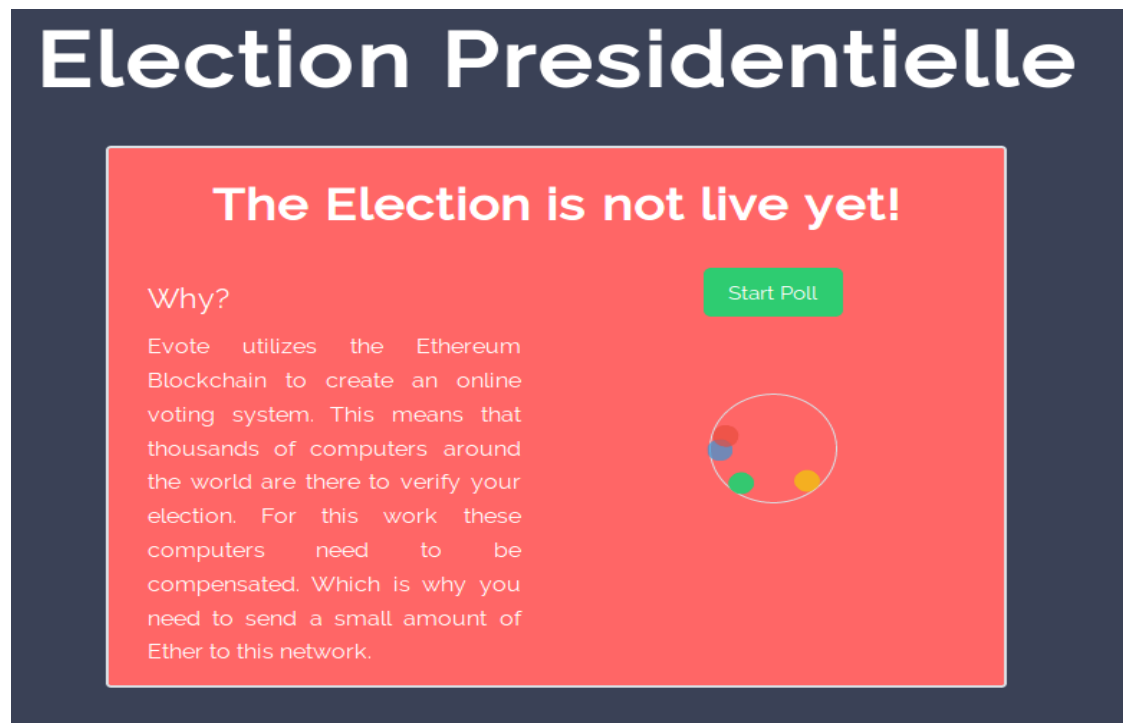


Figure V.5 – Activation du vote après reçu les "Ethers" nécessaires

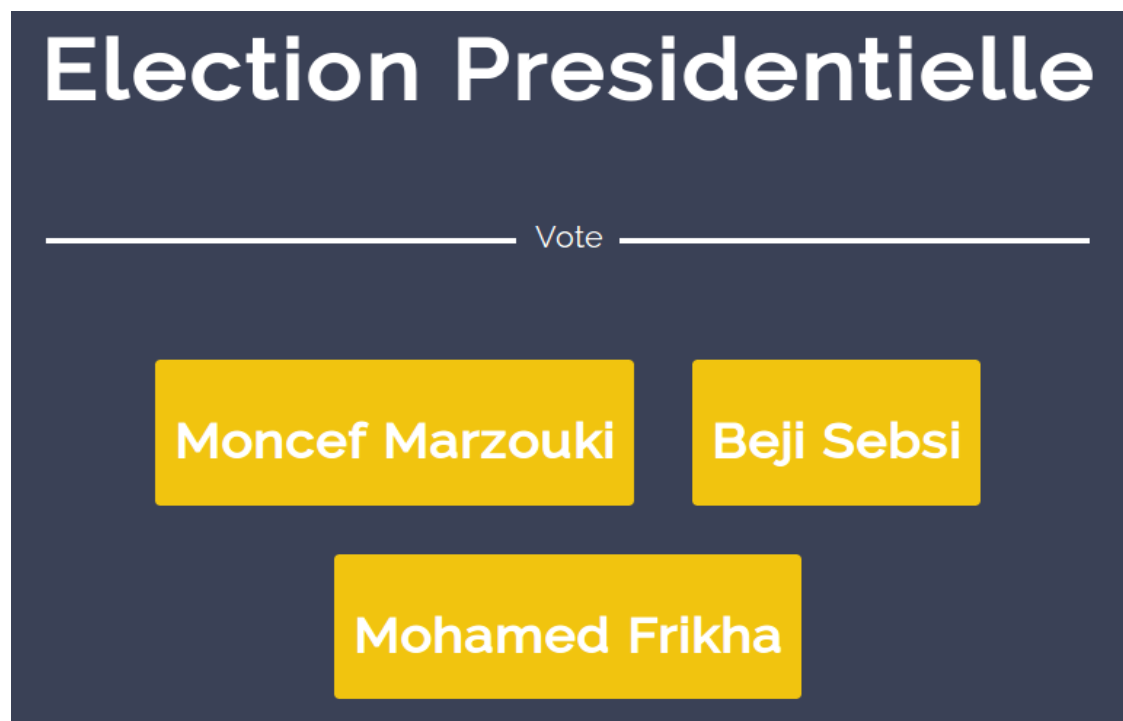


Figure V.6 – Le vote est activé

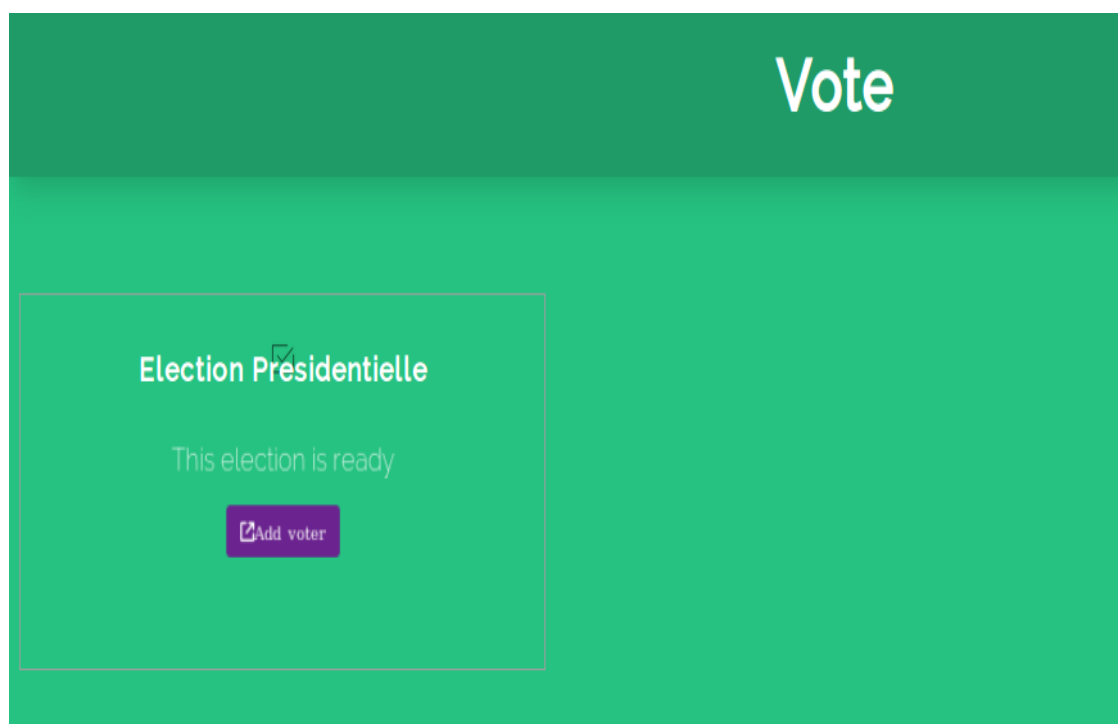


Figure V.7 – Invitation des votants

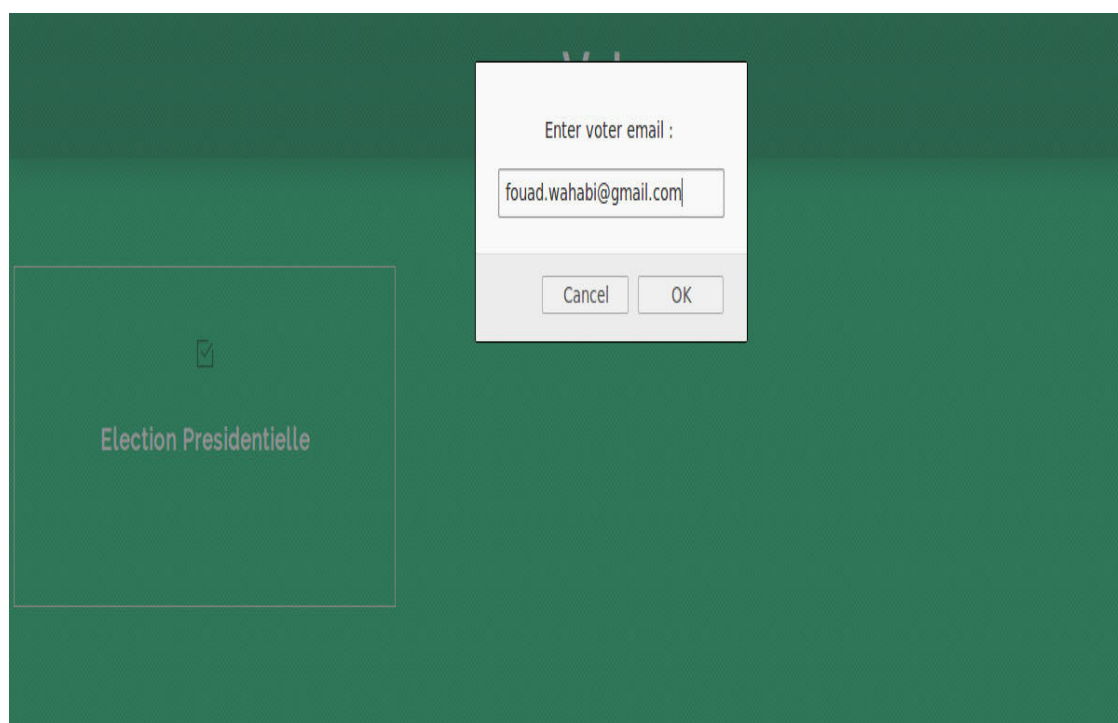


Figure V.8 – Invitation des votants par email

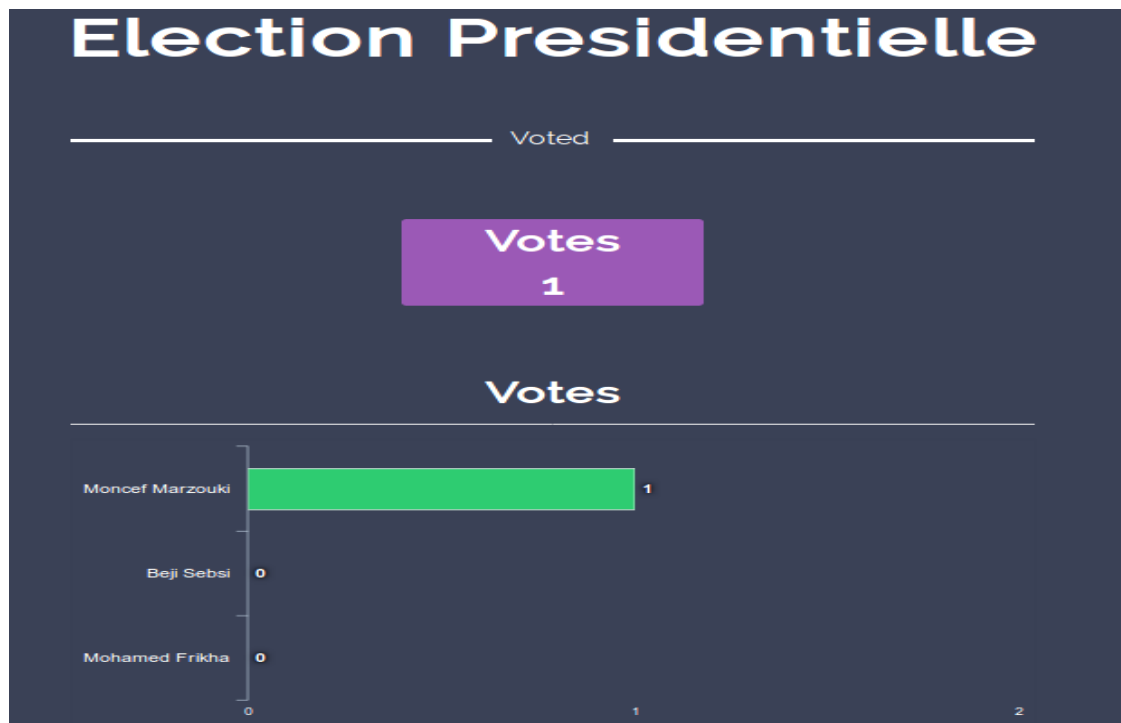


Figure V.9 – Affichage des resultats

Conclusion

Dans ce chapitre, nous nous sommes intéressés à la réalisation des fonctionnalités de notre solution. Nous avons décelé cette réalisation à travers un ensemble d'interfaces accompagnées de descriptions.

Conclusion Générale et Perspectives

La situation actuelle de Blockchain ressemble à celle d'Internet dans les années 1990 - avec son lot d'espoirs, d'attentes parfois exagérées, de scepticisme aussi, mais avec un potentiel certain.

Dans ce contexte, notre projet de fin d'années vise à réaliser un PoC sur la technologie Blockchain, ce qui va permettre à répondre aux besoins et s'adapter aux éventuelles évolutions de notre institut.

Cette application permet d'utiliser un contrat intelligent, et de réaliser l'opération de vote d'une façon directe, décentralisée et surtout sécurisée.

Pour atteindre cet objectif, nous avons tout d'abord étudié la technologie Blockchain et les solutions existantes pour le domaine de vote en ligne. Ensuite, nous avons déterminé les différents besoins et exigences relatifs à l'application pour aboutir à la partie conception qui met l'accent sur l'aspect statique et dynamique du système. Puis, nous avons enchainé avec une étude technique dans laquelle nous avons présenté l'environnement de travail et les technologies utilisées pour la réalisation du projet. Enfin, nous avons abordé la partie réalisation à travers laquelle nous avons décrit les différentes fonctionnalités de notre application.

Pour conclure, notre application a bien résolu les besoins demandés et nous a donc permis d'atteindre les objectifs fixés à savoir la conception et le développement d'un PoC sur cette technologie permettant sa compréhension et son utilisation pour d'autres applications.

Néanmoins, ce travail est ouvert à de nouvelles perspectives. L'intégration des contrats intelligents de la technologie Ethereum va permettre de faciliter la création des applications totalement décentralisées, les DAPPs, et d'aider les clients Blockchain de créer des Organisations autonomes décentralisées (DAOs : Decentralized Autonomous Organizations, en anglais) sur la Blockchain. Une DAO n'existe que sur la blockchain Ethereum et ses participants n'interagissent entre eux que sur elle.

Bibliographie

- [1] [https ://www.ethereum.org/](https://www.ethereum.org/)
- [2] [http ://www.agiliste.fr/introduction-methodes-agiles/](http://www.agiliste.fr/introduction-methodes-agiles/)
- [3] [https ://blockchainfrance.net](https://blockchainfrance.net)
- [4] [http ://www.zdnet.fr/actualites/vote-electronique-la-blockchain-a-la-rescousse](http://www.zdnet.fr/actualites/vote-electronique-la-blockchain-a-la-rescousse)
- [5] [https ://openclassrooms.com/courses/apprenez-a-programmer-en-java/modelisation-uml](https://openclassrooms.com/courses/apprenez-a-programmer-en-java/modelisation-uml)
- [6] [https ://www.maddyness.com/technologie](https://www.maddyness.com/technologie)
- [7] [http ://www.cryptos.net/technologie-block-chain-lavenir-democratie-numerique/](http://www.cryptos.net/technologie-block-chain-lavenir-democratie-numerique/)
- [8] [https ://www.lesechos.fr](https://www.lesechos.fr)