République Algérienne Démocratique et Populaire
Ministére de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mouhammed Khider de Biskra
Faculté des Sciences Exactes et science Naturelle et de la Vie

Mémoire
Présenté pour l'obtention du Diplôme de Master

En Informatique
Spécialité :RÉSEAUX ET TECHNOLOGIES
DE L'INFORMATION ET DE LA COMMUNICATION

Par : GHOGGALI BRAHIM EL KHALIL

Sujet

SYSTÉME DES CRÉDITS BANCAIRE BASÉ SUR LA TECHNOLOGIE BLOCKCHAIN

Proposé et dirigé par :
MR. BELAICH HAMZA

Promotion 2019 – 2020

Résume.

Une blockchain « ou chaîne de blocs » privée est un nouvelle technologie d'opérer des transactions en toute sécurité et sans l'intervention d'une partie tierce. Il s'agit d'un grand livre comptable public consignant les transactions de manière incontestable. Les différents avantages que pourrait apporter la technologie Blockchain au secteur public, permettras la protection des données critiques, de pouvoir s'assurer de la propriété de biens, ou encore de créer un réseau puissant entre les différents services publics et surtout le stockage des données Ceci est fondamental pour plusieurs contextes au secteur publique.
En résumé, la technologie Blockchain repose sur trois grands principes techniques fondamentaux : Une architecture décentralisée ou architecture pair à pair pour assurer la résilience du système. L'utilisation de cryptographie asymétrique pour garantir la sécurité des informations (Sha256 , Rsa). le consensus, pour éliminer le risque de fraude et garantir la confiance au sein du système.
Dans ce travail on s'intéressait à l'utilisation d'une application windows forms sur la Blockchain pour la gestion des crédits des comptes bancaires (demande Montant).
La proposition donne solution au différent problème liée au domaine du banques, fraude du vol on se bassons sur des transactions similaire à la transaction du bitcoin.

Mots clés : Blockchain, Cryptomonnaie, Bitcoin,Ethereum ,Transaction .

Summary.

A private blockchain is a new technology to operate transactions securely and without the intervention of a third party. This is a big public accountant book indisputably recording transactions.
The different benefits that Blockchain technology could bring to the public sector, will allow the protection of critical data, to be able to ensure ownership of goods, or to create a powerful network between the various public services and especially the storage of data This is fundamental for many public sector contexts.
In summary, Blockchain technology is based on three major technical principles fundamental : A decentralized architecture or peer-to-peer architecture to ensure system resilience. The use of asymmetric cryptography to ensure security information (Sha256, Rsa). consensus, to eliminate the risk of fraud and ensure trust within the system.
In this work we were interested in the use of a windows forms application on the Blockchain for credit management of bank accounts (Amount request).
The proposal gives solution to the different problem linked to the banking sector, fraud of theft is based on transactions similar to the bitcoin transaction.

Keywords : Blockchain, Cryptocurrency, Bitcoin,Ethereum ,Transaction .

Remerciements.

Au préalable, nous remercions ALLAH qui nous a aidé et nous a donné la patience et le courage durant nos années d'études.

J'ai tenon d'abord à remercier très chaleureusement Mr : BELAICH HAMZA Qui a permis de bénéficier de mon encadrement.
Les conseils qu'il a prodigués, la patience et la confiance qu'il a témoignée ont été déterminants dans la réalisation de notre travail.

Mon remerciement s'étend également à tous nos enseignants pendant les années des études.

Mes grands remerciements aussi à l'équipe de département d'informatique ainsi que le membre de jury qui a pris la peine d'évaluer mon travail.

Enfin, ne souhaite exprimer ma reconnaissance envers les amis et collègues qui nous ont apporté leur soutien moral et intellectuel tout au long de ma démarche.

Un grand merci à Mr. CHAKER YOUCEFFI, M. BOUCETTA MUBAREK, M. MAHER BASSI et M. HOCINE NAOUI Pour leur confiance et leur soutien inestimable.

Dédicaces.

Je dédie ce travail :

A mes Très Chers Parents.

Tous les mots du monde ne sauraient exprimer l'immense amour que je vous porte, ni la profonde gratitude que je vous témoigne pour tous les efforts et les sacrifices que vous n'avez jamais cessé de consentir pour mon instruction et mon bien-être.

J'espère avoir répondu aux espoirs que vous avez fondés en moi. Je vous rends hommage par ce modeste travail en guise de ma reconnaissance éternelle et de mon infini amour.

Que Dieu tout puissant vous garde et vous procure santé, bonheur et longue vie pour que vous demeuriez le flambeau illuminant mon chemin.

A mes chers frères et sœurs (Soheyb, Omeyma, Newfel, et Anfel). Nulle dédicace ne saurait exprimer mon estime et mon profond amour. Vos sacrifices inoubliables, votre encouragement tout au long de ma carrière m'ont permis de concrétiser mes objectifs. Les phrases me manquent en ce moment pour vous exprimer ma grande reconnaissance et mon admiration profonde.

Je vous dédie ce travail avec tous mes vœux de bonheur, de santé et de réussite.

À tous mes amis et collègues de promotion : Farid, Moadh, Tarek, Oussama.

À tous ceux ou celles qui me sont chers et que j'ai omis involontairement de citer.

À tous ceux qui ont participé de près ou de loin à la réalisation de ce travail.

À Tous Mes enseignants tout au long de mes études.

bien sûr mon copain Ali qui travaille avec moi et qui me partage tous les mal et beaux instants.

Table des matières

Introduction Générale

La gestion et l'utilisation des données administratives peuvent être compliquées, même pour les gouvernements avancés. Les secteurs publics critiques tels que le service les crédits des comptes bancaires (Demande Montant) a tendance à construire leur propre base de données et de protocoles de gestion de l'information.
C'est un processus de prise de temps où plusieurs parties sont impliquées et qui présente également un risque de manipulation d'informations, de duplication de données et d'erreurs diverses.
Dans un tel scénario, l'information critique peut devenir très vulnérable aux fraudes et aux falsifications de données ou même devenir non-traçable.
Plusieurs vagues technologiques ont structuré les développements et Internet révolutionne les échanges entre les individus en permettant la création et la publication d'informations portées par des terminaux toujours plus variés et nombreux.
La décentralisation des bases de données sous-jacentes à une blockchain pourrait simplifier la gestion des informations fiables, ce qui permettrait aux administrateurs et même les utilisateurs d'accéder plus facilement aux données critiques du secteur tout en préservant la sécurité de ces informations.

Une blockchain est un registre numérique codé stocké sur plusieurs ordinateurs dans un réseau public ou privé.
Ce travail va essayer de combler aux objectifs suivants :

. Mettre l'accent sur le fondement théorique de la technologie blockchain
. Concevoir et réaliser un portail de gestion des crédits bancaire

Pour assurer les objectifs de notre travail, nous organisons ce mémoire en quatre chapitres :

- Le chapitre 1 introduit le concept du Blockchain, les cryptomonnaies, les caractéristiques de la blockchain, et déférente définitions sur déférente concept de base.
- Le 2eme chapitre présent les bases sur les techniques utilisé par la blockchain, Il tente de donner un aperçu global et précis de tout ce qui concerne les objectifs, le système blockchain, l'architecture, ainsi que les différents standards utilisés pour les blockchains,...
- Le 3eme chapitre Illustre la conception générale et détaillée de l'application. Il décrit l'étude conceptuelle de notre outil, ainsi que le processus de création d'une blockchain composite au niveau du code.

- Dans le 4eme chapitre, on a expliqué les crédits des comptes bancaires de la Banque. On a montré les outils utilisés pour développer les composants du système et leur réalisation.

On a terminé ce mémoire par une conclusion générale et les perspectives.

1

Blockchain

1.1 Introduction

En 2019 pas une semaine ne s'écoule sans que l'on entende parler de la blockchain dans les médias ou même au bistrot ! Il est vrai que le mot « blockchain » est sur toutes les lèvres mais pourtant peu de personnes comprennent véritablement l'enjeu de cette technologie et comment elle peut être utilisée pour réaliser [16] des transactions financières, faire des ICO (Initial coins offering), transférer des informations de manière fiable, vérifiée et sécurisée.
Les crypto-monnaies en particulier Bitcoin et ethereum sont des exemples les plus populaires qui sont liés intrinséquement a la technologie blockchain. Il est aussi le plus controversé, car il contribue à permettre à un marché mondial de plusieurs milliards de dollars des transactions anonymes sans aucun contrôle gouvernemental. [40]

Dans ce chapitre on va traité les concepts de base de la technologie blockchain.

1.2 Historique

La première blockchain est apparue fin 2008 avec la monnaie numérique bitcoin, développée par un inconnu sous le pseudonyme de Satoshi Nakamoto. Le projet bitcoin est à la base un projet politique anarcho-capitaliste, un libéralisme empreint d'individualisme, et qui a pour objectif de s'émanciper de la contrainte de l'état et des lois. Cette idéologie rejette farouchement la démocratie et fait la promotion de formes autoritaires, voire fascisantes, de gouvernement.
Dans cette vision, décentralisation est synonyme de disparition pure et simple de tout gouvernement. Remplacer des intermédiaires, au premier rang desquels les pouvoirs publics, séduit en effet les milieux ultralibéraux et libertaires [27].

1.3 Définition de blockchain

La Blockchain est fondamentalement une technologie de stockage et de transmission d'informations sécurisées, à l'image d'une base de données distribuée, en y intégrant en plus une protection cryptographique des données et en permettant la conservation de l'historique de tous les échanges effectués entre ses participants. Echange de valeurs, transfert de propriété, ou encore notarisation, ... ces transactions se réalisent grâce à une chaîne de blocs contenant les données, d'où le terme "block" -"Chain". Mais à la différence d'une base de données classique, la Blockchain introduit un nouveau type de gouvernance décentralisée, intégrée et gârce par la technologie, sans intermédiaire qui ne requiert pas la présence d'une tierce autorité de contrôle.
En remettant en cause l'utilité des acteurs de confiance traditionnelle (notaires, banques, chambres de compensation, ...), elle permet d'envisager une approche totalement nouvelle et disruptive de nos organisations [39].
Ci-dessous dans la figure 1.1 est présenté la blockchain.

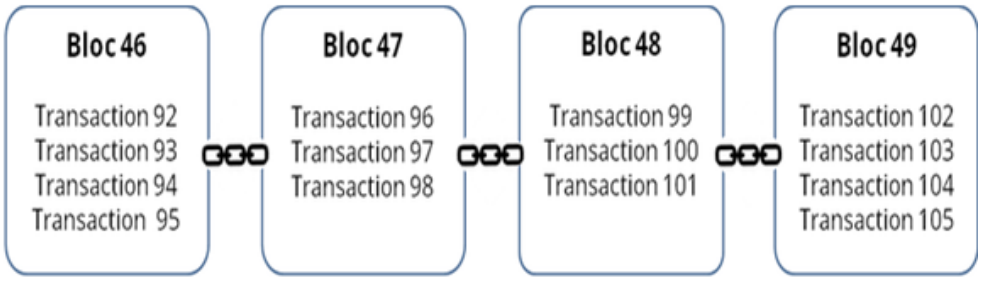

FIGURE 1.1 – *Chaîne de blocs (Blockchain France, 2016)*[39]

1.4 Structure d'une blockchain

Les blockchains sont composées de trois parties principales : [48]

1. **Le bloc :**
   Une liste des transactions enregistrées dans un grand livre (registre) sur une période donnée. La taille, la période et l'événement déclencheur pour les blocs sont différents pour chaque blockchain. Toutes les blockchains n'ont pas pour premier objectif d'enregistrer et de garantir un enregistrement du mouvement de leur crypto-monnaie. Mais toutes les blockchains enregistrent le mouvement de leur crypto-monnaie ou de leur token. Songez à la transaction comme étant simplement l'enregistrement des données. Le fait de lui affecter une valeur (comme lors d'une transaction financiére) permet d'interpréter ce que signifie cette donnée.
2. **La Chaine :**
   un hash qui relie un bloc a un autre, les enchainant mathématiquement ensemble. C'est l'un des concepts de la blockchain le plus difficile à comprendre. C'est aussi la magie qui colle des blocs ensemble et leur permet de créer une confiance mathématique.
   Le hash dans la blockchain est créé à partir des données qui se trouvaient dans le bloc précédent. Le hash est une empreinte digitale de ces données qui verrouille les blocs dans l'ordre et dans le temps.
3. **Le réseau :**
   le réseau est composé de "nœud plein" (full nodes). Songez-y comme à un ordinateur exécutant un algorithme sécurisant le réseau. Chaque nœud contient un enregistrement complet de toutes les transactions qui ont déjà été enregistrées dans cette blockchain.

1.5 Les types de la blockchain

Il existe 3 types de Blockchain

1. **Blockchain publique**
   Les blockchains tell que bitcoin, sont de grands réseaux distribués qui sont exécutés via un token ou jeton natif. Elles sont ouvertes à tous et à tous niveau, et ont un code source ouvert que leur communauté maintient à jour [44].
2. **Blockchain privée**
   Les blockchains privées ont tendance à être plus petites et à ne pas utiliser de token. Leur accès est étroitement contrôlé types de blockchains sont favorisés par les consortiums qui ont des membres affiliés qui échangent des informations confidentielles [44].
3. **Blockchain consortium**
   La blockchain "de consortium" regroupe plusieurs acteurs qui possèdent des droits et les décisions sont prises par la majorité des acteurs. Par exemple, une dizaine d'institutions financières pourraient se mettre d'accord et organiser une blockchain dans laquelle un bloc devrait être approuvé par au moins 8 d'entre elles pour être valide. C'est donc très différent de la blockchain privée et de la blockchain publique. Non seulement les participants au processus d'approbation sont limités et sélectionnés, mais ce n'est plus la règle de la majorité qui s'impose. Cette blockchain hybride est un véritable avantage pour les acteurs du secteur financier car ils opèrent dans des environnements réglementés et sont notamment obligés de connaître l'identité des participants (ce qui n'est pas le cas dans la blockchain publique) [6].

La figure 1.2 montre les trois principaux types de blockchains et les exemples associés à chacun type.

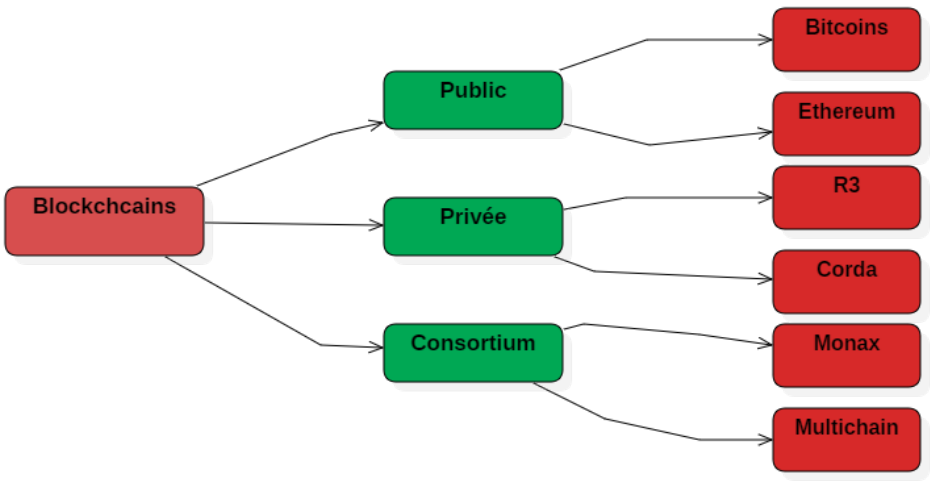

FIGURE 1.2 – *Types de blockchains et les exemples associés*

1.6 La blockchain aujourd'hui

1.6.1 Crypto-monnaies

La Blockchain fonctionne aujourd'hui dans la grande majorité des cas avec une crypto-monnaie associée.
Crypto-monnaie (Les monnaies virtuel) : permettent de transférer de l'argent sans avoir besoin de support physique et, généralement, sans faire appel à un intermédiaire. Elles doivent avoir au moins les mêmes propriétés de sécurité que les monnaies réelles : permettre les échanges, empêcher la duplication ou encore garantir l'anonymat des transactions. Récemment, plusieurs monnaies virtuelles cryptographiques ont vu le jour, telles que Ethereum, Bitcoin, Ripple, Peercoin, Primecoin ou Litecoin ?. Aujourd'hui, ce sont des monnaies alternatives, car elles n'ont de cours légal dans aucun pays, même si elles sont pour l'instant largement tolérées [14].
La blockchain est l'architecture sous-jacente de la cryptomonnaie bitcoin, qui reste aujourd'hui le cas d'usage le plus connu. La première fonction de la blockchain a donc été le transfert d'actifs financiers. Mais cette technologie ne cesse d'évoluer et est à la base de bien d'autres applications qu'un réseau de paiement [17].
Elle est aujourd'hui utilisée aussi par d'autres acteurs et les opérations et données ne sont pas nécessairement financières.
La figure 1.3 montre les top principaux crypto-monnaies qui utilise la technologie blockchain et les statistiques en milliards de dollars dans l'année 2018

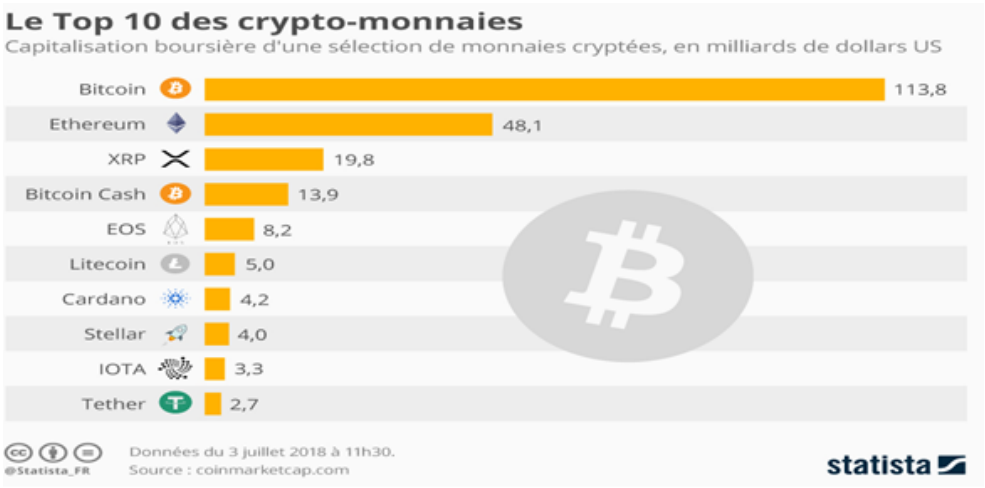

FIGURE 1.3 – *Classement des principales cryptomonnaies en termes de capitalisation au 03 juillet 2018.*

1.6.2 La blockchain Bitcoin

1.6.2.1 peu d'histoire :

Le Bitcoin n'est pas une nouvelle invention. Le concept de monnaie virtuelle a déjà été imaginé auparavant. En 1999, un inventeur crée la b-monnaie, le premier concept de crypto-monnaie, en 2005 le concept est amélioré avec le Bitgold. Ces premières versions des crypto-monnaies n'avaient pas pu être développées à cause de divers problèmes qui font qu'ils n'ont pas gagné la confiance du public. Ses problèmes résident entre autres au niveau de la sécurité et de l'authenticité ou d'un système trop complexe à utiliser. Le Bitcoin a été concu par une personne qui se fait appeler Satoshi Nakamoto et qui a réussi à résoudre ces problèmes de confiance à l'aide de la cryptographie [16].

1.6.2.2 Définition :

La blockchain est la technologie sous-jacente aux bitcoins. L'invention du bitcoin, fin 2008, avait pour objectif de montrer la faisabilité d'une monnaie basée sur un système de confiance répartie. Il s'agit d'une monnaie cryptée, dont le mécanisme de confiance est basé sur un système où le registre des transactions est réparti entre plusieurs nœuds du réseau. Les algorithmes de cryptage des transactions sont open source, ce qui renforce l'idée de confiance dans la monnaie [9].

1.6.2.3 Comment ça marche

La blockchain Bitcoin reste à l'heure actuelle la plus sécurisée. La sécurisation de son réseau s'effectue en effet via une puissance de calcul gigantesque : à titre de comparaison, début 2015 l'ensemble de la puissance de calcul de Google représentait 1% de celle de Bitcoin. Depuis, la puissance de calcul de Bitcoin a été multiplée par 4. Cela étant, Bitcoin affronte aujourd'hui certaines difficultés qui peuvent à terme remettre en jeu sa position de blockchain de référence. Au fond, la question qui agite actuellement la communauté est surtout de savoir si la blockchain Bitcoin a pour ambition de devenir incontournable ou non [20].

1.6.2.4 L'avenir du Bitcoin

Comme toute monnaie, l'avenir du Bitcoin est incertain car il dépend de plusieurs facteurs (contextes politique, social, culturel) Certains analystes affirment que le Bitcoin a un bel avenir devant lui, qu'il sera tôt ou tard accepté par tous. D'autres ne lui font pas suffisamment confiance pour miser dessus et craignent ses filiations avec les activités illégales et son caractère obscur et sans réelle réglementations efficace. Les pays qui acceptent l'utilisation du Bitcoin et de la crypto-monnaie chez eux envisagent de créer un cadre de réglementation légal et fiscal pour réguler son utilisation [16].

1.6.3 La blockchain Ethereum

1.6.3.1 Un peu d'histoire

L'histoire de l'Ethereum en tant que blockchain a beaucoup à voir avec celle du Bitcoin et de sa blockchain.
Le créateur de l'Ethereum est un jeune Russe vivant au Canada nommé Vitalik Buterin. C'est un génie de l'informatique et en 2011 il découvre et se passionne pour le Bitcoin et sa blockchain. Agé alors de 17 ans, il décide de d'étudier de près cette blockchain et fonde alors le site internet Bitcoin Magazine.
Deux ans après, alors qu'il a 19 ans et qu'il a bien baigné dans le monde du Bitcoin, il découvre très vite les limites de la blockchain du Bitcoin qui ne sert à son avis qu'à faire des transferts d'argent entre deux personnes. Il travaille alors sur une autre blockchain beaucoup plus polyvalente pour traiter une infinité d'applications décentralisées. Pour faire connaitre son projet, il publie alors en 2013 son livre blanc intitulé « A next generation of smart contracts and a decentralized application platform » ou « Une prochaine génération de contrats intelligents et une plateforme d'application décentralisée ». [16]

1.6.3.2 Définition

Ethereum est une blockchain publique, considérée comme la blockchain "montante", et par certains comme étant la plus prometteuse. Elle permet de construire des applications décentralisées. Son principe est de coupler les caractéristiques de la blockchain avec des "smart contracts", des programmes autonomes capables d'exécuter automatiquement des conditions définies en amont. Sa crypto-monnaie, l'éther, est devenue début 2016 la deuxiéme plus utilisée derriére le bitcoin. [20]

1.6.3.3 Comment ça marche

La technologie derriére Ethereum est grosso modo la même que celle utilisée par le bitcoin : il s'agit d'ordinateurs individuels qui " participent " à une unique base de données globale publique, et donc partagée entre tous. Un livre de comptes, ou un tableur géant dans lequel chaque personne intéressée entre les données qu'il souhaite et auquel tout le monde a accès.
C'est ce qu'on appelle la « blockchain ». Cette « blockchain » comprend l'historique de l'ensemble des opérations qui ont été réalisées sur la base. Cela permet d'éviter que quelqu'un ne puisse modifier cet historique de la base et de pouvoir reconstituer à n'importe quel moment les différentes opérations effectuées sur la base par les utilisateurs.[14]

1.6.3.4 L'usage de ethereum

Microsoft, qui a décidé d'utiliser Ethereum pour sa plateforme Azure blockchain-as-a-service, justifie ainsi son choix : Tandis que Bitcoin a de nombreuses utilisations intéressantes en tant que crypto-monnaie, Ethereum apporte la flexibilité que beaucoup de nos

clients recherchent. Ethereum possède une communauté vibrante de développeurs, enthousiastes et ouverts à des applications business". [20]

1.6.3.5 La différence avec Bitcoin

« La blockchain de Bitcoin a été conçue spécifiquement pour des applications monétaires, alors qu'Ethereum permet de créer tout type d'applications » explique le fondateur d'Ethereum, Vitalik Buterin. Ethereum, dont le code informatique est profondément différent de Bitcoin (il a été écrit en partant de zéro), n'a pas été construit pour concurrencer frontalement Bitcoin : il s'agit plutôt de deux utilisations différentes et complémentaires des technologies blockchains. On notera l'existence de différences idéologiques entre les deux communautés qui les entourent : celle de Bitcoin est plus d'inspiration libertarienne, centrée sur le domaine monétaire (inspirée par les théories de Hayek notamment), tandis que celle d'Ethereum vise plus à créer un nouveau web, décentralisé, plutôt qu'une nouvelle monnaie.[5]

1.7 Les blockchains par rapport à internet :

La technologie blockchain doit être comprise comme partie intégrante des systèmes informatiques de communication existants. En effet, son existence repose sur le réseau internet et sur ses protocoles. Elle présente la particularité d'utiliser un réseau pair à pair, c'est-à-dire un réseau au sein duquel chaque internaute peut être serveur ou receveur d'un autre, formant ainsi des pairs dans un modèle décentralisé. Il est alors envisageable de la situer par rapport aux autres couches technologiques des systèmes informatiques. [47]

1.7.1 Le modèle OSI

Pilier de la théorie des réseaux, le modèle « OSI » (Open Systéms Interconnection) est le standard international ISO de communication en réseau des systèmes informatiques .
Les blockchains s'ajoutent à l'ensemble de ces fonctionnalités nécessaires à la communication et à leur organisation, il convient donc de rapprocher les protocoles des blockchains des protocoles à la base du web comme TCP/IP (Transmission Control Protocol et Internet Protocol) ou HTTP, sans les mettre sur le même plan. [47]

1.7.2 Une incertitude sur la place des blockchains

Une incertitude demeure sur le niveau de couche sur lequel ou entre lesquels les blockchains viennent se placer. Elles pourraient se placer entre les couches 3 et 4, ou 4 et 5 (voire la figure 1.4), mais sans que les experts aient encore déterminé si elles s'apparentent davantage à des couches matérielles ou à des couches hautes, plus applicatives. En effet, les quatre couches inférieures sont plutôt consacrées à la communication et fournies par le

matériel et un système d'exploitation tandis que les trois couches supérieures sont davantage orientées vers les applications et donc réalisées par exemple à l'aide de bibliothèques ou de programmes spécifiques.[47]

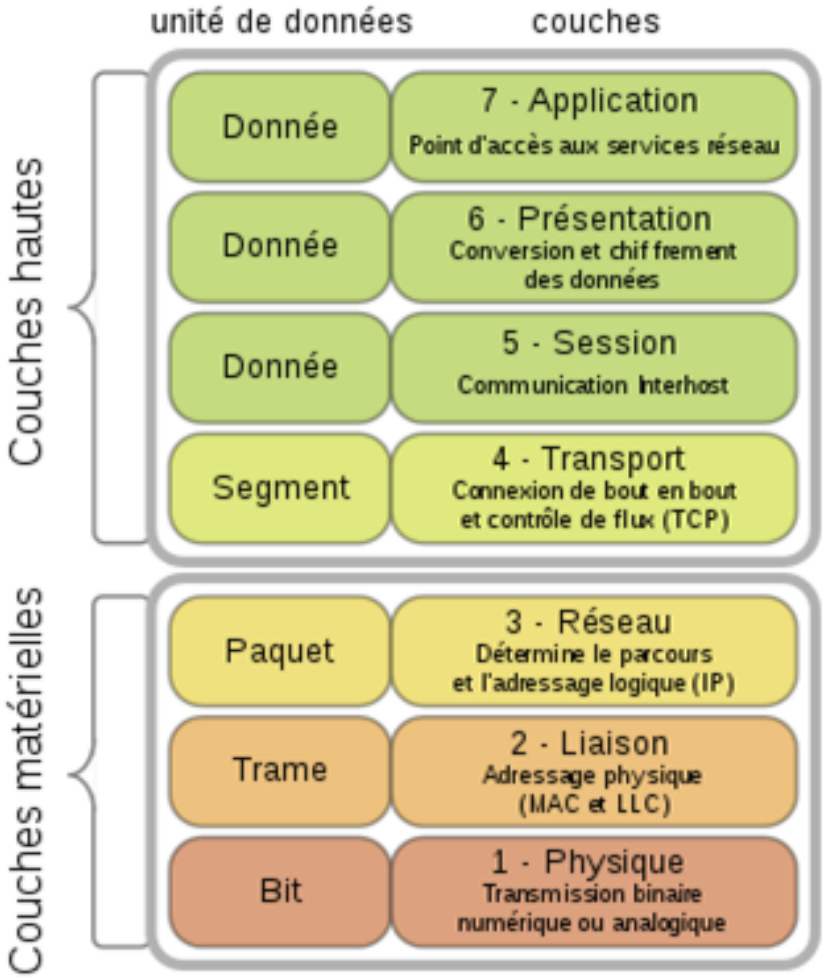

FIGURE 1.4 – *Les sept niveaux de couches du modèle « OSI »*[47]

1.8 Les caractéristiques principales de blockchain

Les caractéristiques principales de la technologie blockchain sont :

1.8.1 La désintermédiation

La technologie blockchain permet d'échanger sans le contrôle d'un tiers. La validation et l'ajout d'un bloc résultent d'un consensus entre les utilisateurs-validateurs, qui repose

sur la possibilité de vérifier leur travail de validation et qui rend inutile le contrôle par une institution de référence [12]. Tout est effectué sans l'intervention d'une autorité centrale, les utilisateurs opèrent la surveillance, et se contrôlent mutuellement, assurant la certification des sauvegardes et leurs cohérences [17].

1.8.2 La transparence

Une fois qu'un document est inscrit sur la blockchain, cela suffit à prouver que ce dernier existe bien à l'instant T et qu'il n'a pas été modifié. La blockchain est qualifiée de transparente car tout le monde peut la télécharger dans son intégralité et vérifier à tout moment son honnêteté [10]. Tous les utilisateurs de la blockchain peuvent ainsi voir les transactions présentes et passées [45].

1.8.3 La sécurité

L'hébergement décentralisé fait également de la blockchain une technologie sûre : elle rend quasi-impossible la suppression de toutes les copies des documents, qui existent sur une multitude de serveurs à travers le monde. La blockchain a une grande résistance, car toutes les données sont copiées dans les différents serveurs. Cela la rend résistante aux cyber-attaques ou au contrôle de l'état. En effet, s'il est possible de s'attaquer à un ou plusieurs ordinateurs, il est plus compliqué de s'attaquer aux blocs d'informations copiés dans l'ensemble des ordinateurs connectés au réseau. Cela offre à la blockchain un haut niveau de sécurité. La blockchain est donc considérée comme inattaquable et inviolable [33]. Cependant, cela la rend également difficilement régulable.

1.8.4 L'autonomie

La puissance de calcul et l'espace d'hébergement sont fournis par les nœuds du réseau, c'est-à-dire les utilisateurs eux-mêmes. Il n'y a donc pas besoin d'infrastructures centrales. Au sein d'une blockchain, l'infrastructure n'est plus concentrée dans les mains d'une organisation mais est, au contraire, éclatée dans l'ensemble des points du réseau. Une blockchain est donc autoportante et indépendante de services tiers [12].

1.9 L'usages de la blockchain

De nombreux cas d'usage de la blockchain ont émergé ces derniéres années. Voici quelques exemples :

1. **Les smart contrats :**
   ou contrats intelligents représentent un des cas d'usages les plus prometteurs de la Blockchain. Ce sont des programmes informatiques reposants sur la technologie Blockchain [39] et conçus pour exécuter automatiquement les termes d'un contrat dés lors que certaines conditions sont réunies. Ces programmes sont accessibles et

audit ables par toutes les parties autorisées, leur exécution est donc contrôlée et vérifiable. Enfin, la Blockchain garantit la fiabilité et l'immuabilité de ces contrats.

2. **L'automatisation du paiement des salaires :**
   La blockchain a ses racines dans les crypto-monnaies. [7] Utiliser cette technologie pour gérer la paie des salariés fait donc totalement sens.
3. **Les Assurances :**
   Le secteur de l'assurance est l'un des premiers avec le secteur financier à avoir manifesté son intérét pour la blockchain. Des modèles d'assurance Peer to-Peer avaient déjà commencé à apparaitre, la blockchain y donne un nouvel élan grâce à des systèmes d'assurance automatisés fondés sur des smart contrats. Des entités appelées "oracles" permettent ainsi de gérer les données des smart contrat et de déterminer, par exemple, si les conditions sont bien remplies pour déclencher le paiement. L'exemple souvent cité est celui de l'assurance dite indicielle ou paramétrique, autrement dit l'assurance liée a un indice tel que la température ou le niveau de pluie.[24]
4. **Santé :**
   Plusieurs cas d'usage sont envisageables dans le secteur de la santé. La blockchain pourrait notamment servir à la traçabilité des médicaments, à la sécurisation des données de santé, et à la gestion des données des patients.
   La blockchain, en tant que registre distribué, pourrait permettre aux différentes entreprises pharmaceutiques, aux régulateurs et même aux particuliers d'utiliser la même base de données, sans qu'une seule entreprise ou institution n'en soit propriétaire.
   Ce mécanisme de certification des médicaments pourrait être étendu aux données de santé au sens large. En certifiant les dossiers médicaux sur une blockchain, on ajoute une couche supplémentaire de sécurité : toute mise à jour d'un document est enregistrée dans la blockchain, sans que les documents eux- même aient besoin d'y être stockés. Il est ainsi impossible pour qui que ce soit (pouvoirs publics, institutions de santé, patients) de couvrir un changement dans un dossier médical. Dans cette optique, Guard time, une start-up spécialisée, a conclu un partenariat avec le gouvernement estonien afin de sécuriser le million de dossiers médicaux estoniens sur La blockchain [24].

1.10 Les avantages et les inconvénients de la blockchain

Quand on a parlé sur une technologie on a besoin de connaître les avantages et les inconvénients.

1.10.1 Les Avantages

Parmi les avantages de cette technologie :

1.10.1.1 Absence d'intermédiaire

La blockchain pourrait révolutionner le système monétaire car elle ne nécessite plus l'intervention d'une structure bancaire. Avec les monnaies numériques qui utilisent la technologie blockchain, il est possible de faire des transactions directement de particulier à particulier sans intermédiaire. Plus besoin de banquier, d'une administration qui note et stocke [15] toutes les informations concernant vos échanges monétaires. Toutes ces informations seront reprises dans les blocs de la chaîne. La monnaie cryptée est en quelque sorte sa propre administration bancaire.

1.10.1.2 Economie de plusieurs milliards

Selon un rapport de la Goldman Sachs, la suppression de tous ces intermédiaires pourrait faire gagner chaque année plusieurs milliards de dollars aux institutions bancaires, aux marchés financiers et à de nombreuses industries. Le rapport parle de 2 milliards de dollars pour les états-Unis et de 6 milliards à l'échelle mondiale. Mais de nombreux autres secteurs pourraient également économiser de très importantes sommes monétaires en utilisant cette technologie.

1.10.1.3 Lutte contre la fraude

Puisque la fraude est souvent une affaire de manipulation de chiffres et de lettres sur des papiers, quoi de mieux qu'une technologie avec laquelle on pourrait stocker toutes sortes d'informations sans les modifier ? La blockchain joue ce rôle. Vente de logements sociaux, arnaque au kilomètres sur véhicules d'occasion, sociétés offshores ? toutes ces informations pourraient se retrouver de façon chronologique dans un fichier sécurisé et aisément consultable.

1.10.2 Les Inconvénients

1.10.2.1 Lourdeur technologie

La transmission d'informations par la chaîne de blocs nécessite un support technologique assez important. De nombreux ordinateurs entrent en compétition pour résoudre une série de calculs qui, une fois résolus, permettent le transfert d'informations cryptées : c'est ce qu'on appelle le mining. L'ordinateur qui résout le problème est « récompensé » en monnaies numériques.
Mais ce procédé peut être lent. Une transaction en Bitcoin peut prendre jusqu'à plusieurs heures là où une simple transaction traditionnelle peut être instantanée (à condition de payer un supplément à la banque). Plus il y aura des demandes de dispositifs basés sur la blockchain, plus grand sera le nombre d'ordinateurs exploité. Ce qui aura pour conséquence de ralentir encore le système. Bien que de nouvelles approches technologiques plus rapides similaires à la Blockchain commencent à être développées, comme le Tangle, ce procédé reste encore très lent.

1.10.2.2 Aval d'une autorité

Tous les processus administratifs ne peuvent pas être remplacés par une technologie blockchain. Certains nécessitent encore l'aval d'une autorité compétente. Certaines opérations qui seraient réalisées via la blockchain ? sans intermédiaire donc n'auraient ainsi aucune valeur. Le journal suisse Le Temps donne l'exemple des transferts de propriété. Le contrat de transfert doit revêtir la forme authentique (notaire) et être vérifié par le conservateur du registre foncier. Une transaction immobilière qui ne passe que par la blockchain n'a pas de valeur .

1.10.2.3 Augmentation du chômage

De par sa simplicité et son automatisation, la blockchain pourrait remplacer de nombreux services de fonds, de comptabilité et d'administration et faire disparaître de nombreux métiers. La technologie de la chaîne de blocs pourrait envoyer plein d'employés au chômage : banquiers, comptables, assureurs, notaires et fonctionnaires. Il y a donc autant d'avantages [18] que d'inconvénients à utilisé la blockchain. Certains pensent qu'elle va révolutionner le monde industriel et économique. D'autres pensent que c'est une perte de temps. L'avenir tranchera.

1.11 Conclusion

Cette technologie est encore jeune, complexe et reste limitée à certaines communautés ou à certains secteurs. On a tout d'abord étudié le procédé technique sur lequel repose la Blockchain. Cette innovation informatique permet ainsi d'organiser les échanges de données sur un réseau [22] distribué, assurant une sécurisation des données par chiffrement, et faisant participer les nœuds du réseau pour la création de nouveaux blocs de la chaîne.

2

La sécurite de la Blockchain

2.1 Introduction

Dans le chapitre précédent, on a présenté le bagage théorique de la technologie blockchain. On a aussi présenté les différentes crypto-monnaie qui utilise par cette technologie.

La Blockchain est un protocole de gestion nuérique de données en "open source", décentralisée, distribuée, et fondée sur les échanges réalisés en P2P dans des réseaux, et permet ainsi la sécurité des données, la transparence entres les membres de la blockchain.

La blockchain est une technologie qui est structurellement accessible, partagée et sécurisée grâce aux algorithmes de consensus.
La cryptographie est le composant le plus important de la blockchain. Il est certainement un domaine de recherche en soi et est basé sur des techniques mathématiques avancées assez complexes à comprendre. On a essayé de développer une solide compréhension de certains des concepts cryptographiques dans cette section, car différents problèmes peuvent nécessiter un chiffrement différent solutions.

A travers ce chapitre on a présenté les différentes techniques de sécurité de cette technologie.

2.2 L'échange pair à pair (p2p)

2.2.1 La signification de P2P

Le pair-à-pair, peer-to-peer ou P2P (les trois termes désignent la même chose), définit un modèle de réseau informatique d'égal à égal entre ordinateurs, qui distribuent et reçoivent des données ou des fichiers. Dans ce type de réseau, comparable au réseau client-serveur, chaque client devient lui-même un serveur. Le P2P facilite et accélère les échanges entre plusieurs ordinateurs au sein d'un réseau.[37]

2.2.2 Centralisée vs Décentralisé :

La première, centralisée, laisse un ou plusieurs serveurs diriger chaque ordinateur vers ceux qui possèdent le fichier qu'il recherche. La deuxième, dècentralisée ne connaît pas de serveur fixe. Chaque ordinateur fait office de mini serveur, ce qui répartit la responsabilité, notamment dans le cas de partage illégal de documents protégés. L'une des particularités de ce type de réseau est d'offrir un relatif anonymat aux utilisateurs.[37]
Un système centralisé typique peut apparaître comme le montre la figure 2.1

FIGURE 2.1 – *Un système centralisé* [37]

Quelques inconvénients d'un système centralisé conventionnel système :[37]

- Problèmes de confiance ;
- Problème de sécurité ;
- Problème de confidentialité - la confidentialité de la vente de données est compromise ;
- Facteur de coût et de temps pour les transactions ;
- Ils sont plus vulnérables aux attaques et donc moins sécurisé.

Un système décentralisé typique peut apparaître comme le montre la figure 2.2

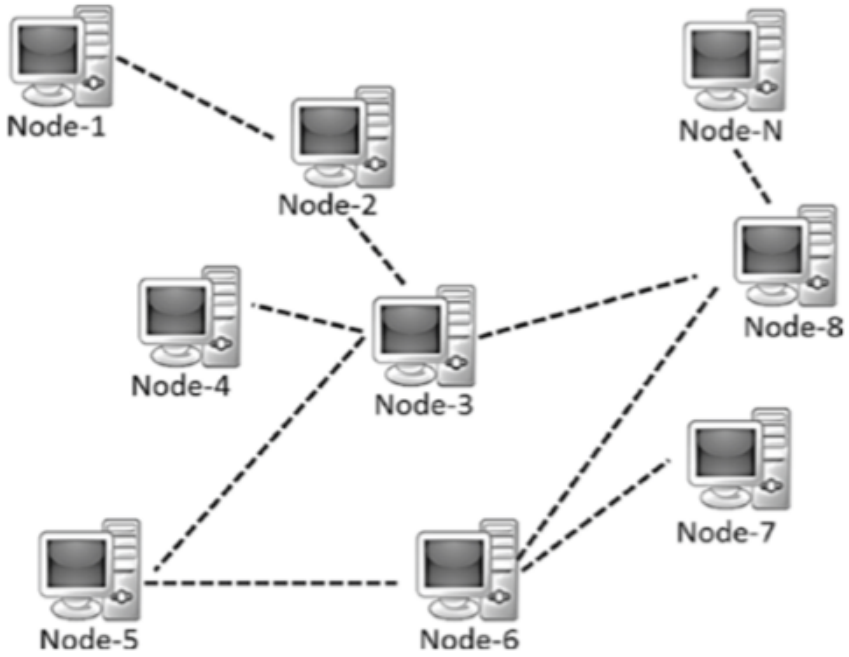

FIGURE 2.2 – *Un système décentralisé* [37]

Certains des avantages des systèmes décentralisés par rapport aux systèmes centralisés les systèmes pourraient être :[37]

- Élimination des intermédiaires ;
- Vérification plus simple et authentique des transactions ;
- Sécurité renforcée à moindre coût ;
- Une plus grande transparence ;
- Décentralisé et immuable.

2.2.3 Le rôle du P2P dans les blockchains :

Lorsqu'il crée le Bitcoin, Satoshi Nakamoto le définit en tant que Système de Cash Electronique de Pair à Pair. Le Bitcoin fut créé en tant que monnaie digitale, il peut être transféré d'un utilisateur à l'autre au travers d'un réseau P2P qui gère un registre distribué que l'on nomme blockchain.
Dans ce contexte, l'architecture P2P inhérente à la technologie blockchain est donc ce qui permet de transfèrer du Bitcoin et d'autres crypto-monnaies dans le monde, sans avoir besoin d'intermédiaires ni de serveur central. En outre, tout le monde peut configurer un nœud Bitcoin s'il veut participer au processus de vérification et de validation de blocs.

Il n'y a donc pas de banques traitantes ou enregistrant les transactions dans le réseau Bitcoin. Au lieu de cela, la blockchain agit comme un registre numérique qui enregistre

publiquement toutes les activités. En résumé, chaque nœud possède une copie de la blockchain et la compare à d'autres nœuds pour s'assurer que les données sont exactes. Le réseau rejette rapidement toute activité malveillante, ou toute inexactitude.
Dans le contexte des blockchains crypto-monnaies, les nœuds peuvent jouer une variété de rôles différents. Les nœuds complets, par exemple, sont ceux qui fournissent la sécurité au réseau via la vérification des transactions, en appliquant les règles de consensus du système.

Chaque nœud complet préserve et maintient une copie complète et à jour de la blockchain ce qui lui permet de participer à la tâche collective de vérification de l'état véritable du registre distribué.[30]

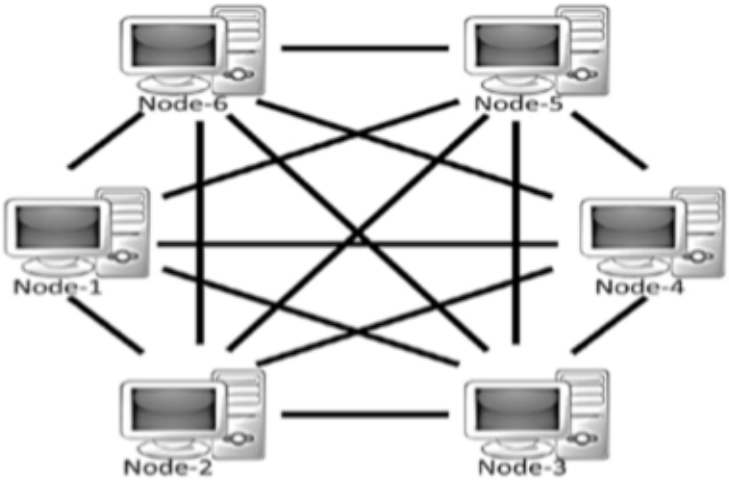

FIGURE 2.3 – *Un système décentralisé pair à pair* [37]

2.3 Le système blockchain

Pour faire partie d'un système blockchain, les entités participantes installent et exécutent chacune un logiciel qui connecte leur ordinateur ou leur serveur à d'autres participants du rèseau. En exécutant ce logiciel, les participants agissent comme des validateurs individuels, appelés nœuds de réseau. Lorsqu'un nœud se connecte au réseau pour la première fois, il télécharge une copie complète de la base de données blockchain sur son ordinateur ou son serveur.
Un système blockchain distribue typique peut apparaître comme le montre la figure 2.4

FIGURE 2.4 – *Distribution de la blockchain.*

Le réseau de nœuds gère la base de données, également appelée blockchain. Les nœuds sont des points d'entrée pour de nouvelles données, ainsi que la validation et la propagation de Nouvelles données qui ont été soumises à la blockchain.
Un bloc est créé en regroupant des transactions similaires. Ces blocs sont ajoutés dans l'ordre chronologique, d'une manière qui ressemble à une chaîne, d'où le nom blockchain. Les nœuds stockent ensuite ces nouveaux blocs sur la base de données blockchain locale sur leur ordinateur ou serveur [11].

2.3.1 Composition d'une blockchain

Une blockchain est une chaîne de blocs contenant chacun Plusieurs transactions, et qui vont être inscrits au fur et à mesure dans la blockchain par des nœuds du réseau.
L'implémentation peut différer d'une blockchain à l'autre, mais les principaux éléments D'un bloc sont les suivants :

- Index : identifier du bloc.
- Hash : clé unique basée sur le contenu bloc.
- PreviousHash : référence au hash du block précédent.
- Timestamp (horodatés) : date et heure de création du bloc.
- Data : donner entrées dans le bloc (transaction).

Le premier bloc d'une blockchain est appelé le "Genesis Block" [3].

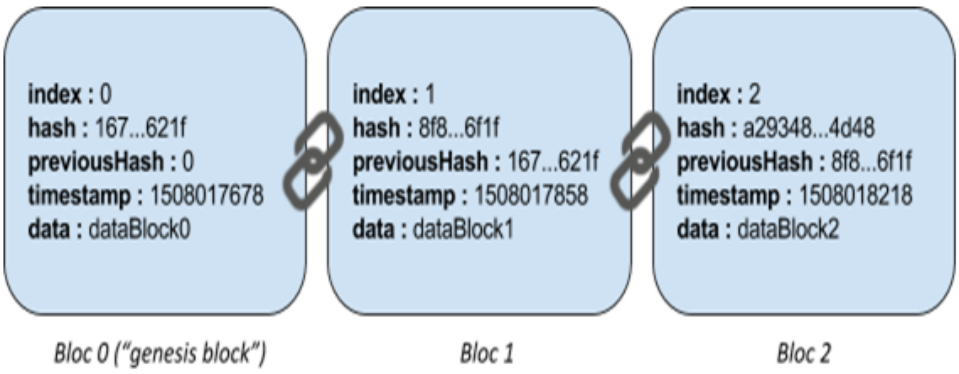

FIGURE 2.5 – *Composante de bloc.*

2.3.2 Messages

Il y'a Deux types principaux des messages sont diffusés :

- La transaction, qui représente un paiement,
- Le bloc, qui enregistre une collection de transactions.

Lorsqu'une nouvelle transaction est signée, elle est diffusée sur le réseau blockchain. Il sera ensuite collecté et enregistré dans un bloc. Chaque bloc, une fois constitué, sera à son tour diffusé. Tous ces messages sont publics et vérifiables. Ils permettent de notifier et donc de prendre à témoin tous les participants du réseau blockchain sur toute nouvelle information qui enrichit la blockchain.

2.3.3 L'horodatage

Les blocs ainsi constitués de plusieurs transactions « signées » par clés publiques sont ensuite « horodatés » (timestamp) par leur auteur. Cet aspect, appelé horodatage, est essentiel car il permet la datation relative des blocs ainsi constitués, la blockchain formant à cet égard une sorte de chronologie dans laquelle les transactions sont classées les unes après les autres.[47]

2.3.4 Fonctionnement de la blockchain

Voyons comment effectuer sur la blockchain un transfert de fonds d'une personne A vers une personne B

1. La transaction est initiée par A.
2. Un bloc est formé avec l'information " paiement de A à B ".
3. Le réseau décentralisé reçoit l'information qu'un nouveau bloc a été initialisé.
4. Tous les participants sur le réseau vérifient que le bloc (avec toutes les informations contenues) est valide.

5. Le bloc est confié à la blockchain.
6. Chacun sait maintenant que B est le nouveau propriétaire de la somme d'argent envoyée par A.

Une blockchain, ainsi que le nom l'indiquent, sert à organiser des transactions sous formes de blocs qui sont vérifiées par un grand nombre de participants. [19]
Voici le principe général d'une blockchain :

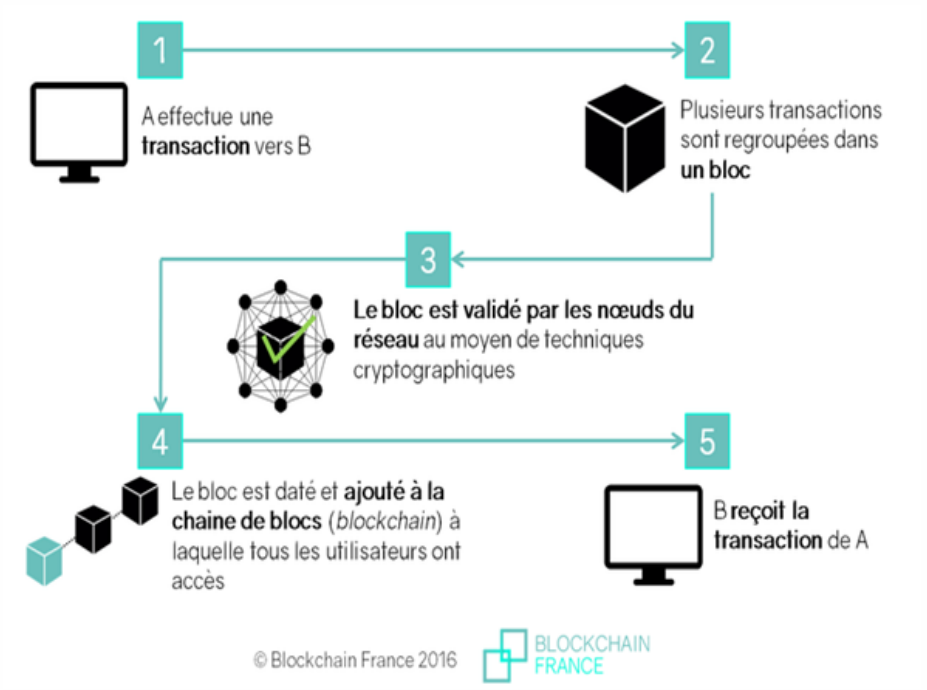

FIGURE 2.6 – *Scénario d'enregistrement d'un bloc (Blockchain France, 2016) [5]*

2.3.5 Consensus :

Le consensus désigne le mécanisme de gouvernance qui permet à une architecture Blockchain de valider la validité d'une information. La Blockchain étant basée sur une architecture décentralisée, il n'existe pas de nœud central ayant vocation à servir d'organe de contrôle pour vérifier et valider les informations stockées au sein du réseau. Cette étape de vérification est, au contraire, distribuée sur l'ensemble des nœuds, l'objectif était de faire émerger une validation globale au sein du réseau. [5]

2.3.6 Les nœuds du réseau et le consensus

2.3.6.1 Vérification des transactions

Les transactions effectuées entre les utilisateurs du réseau sont regroupées en blocs. Chaque bloc est validé par les nœuds du réseau [5]

2.3.6.2 La diffusion des blocs sur un réseau pair à pair [47]

Chaque bloc est validé par certains utilisateurs et sont transmis aux « nœuds » du réseau, c'est-à-dire aux détenteurs du registre, ce registre étant la chaîne de blocs elle-même. Cette dernière est actualisée en permanence.
Dans les blockchains dites ouvertes (permissionless), comme celle du bitcoin, n'importe quel utilisateur de l'internet peut ainsi devenir un nœud du réseau en téléchargeant le registre auprès d'un nœud existant.
Chaque nœud est connecté à plusieurs autres, appelés pairs, eux-mêmes ayant leurs propres pairs, ce qui forme un réseau pair à pair.

FIGURE 2.7 – *Diffusion d'un bloc dans le réseau* [47]

2.4 Cryptographie :

2.4.1 Généralité sur la cryptographie

2.4.1.1 Définition de la cryptographie :

La cryptographie est l'art de chiffrer, coder les messages est devenue aujourd'hui une science à part entière. Au croisement des mathèmatiques, de l'informatique, et parfois même de la physique, elle permet ce dont les civilisations ont besoin depuis qu'elles existent.

Le maintien du secret. Pour éviter une guerre, protéger un peuple, il est parfois nécessaire de cacher des choses. [26]

2.4.1.2 L'usage de la cryptographie :

La cryptographie est traditionnellement utilisée pour dissimuler des messages aux yeux de certains utilisateurs. Cette utilisation a aujourd'hui un intérêt d'autant plus grand que les communications via internet circulent dans des infrastructures dont on ne peut garantir la fiabilité et la confidentialité. Désormais, la cryptographie sert non seulement à préserver la confidentialité des données mais aussi à garantir leur intégrité et leur authenticité. [4]

La confidentialité : consiste à rendre l'information intelligible à d'autres personnes que les acteurs de la transaction.

L'intégrité : vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication.

L'authentification : consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées.

Le non répudiation : de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction.

2.4.2 Cryptographie symétrique

2.4.2.1 Définitions :

Le chiffrement dit "symétrique", qui utilise la même clé pour chiffrer et déchiffrer les messages.
Il n'existe qu'une seule clé pouvant ouvrir le cadenas, et il faut la transmettre (ou en transmettre une copie) au destinataire pour qu'il puisse l'ouvrir. [13]

2.4.3 Cryptographie Asymétrique :

2.4.3.1 Définitions :

La cryptographie symétrique consiste à chiffrer puis déchiffrer un message en utilisant la même clé et le même algorithme.
Cryptographie à clé asymétrique, également appelée « cryptographie à clè publique » est un concept révolutionnaire introduit par Diffie et Hellman. Avec ça technique, ils ont résolu le problème de la distribution des clès dans un symètrique système de cryptographie en introduisant des signatures numériques. Notez que la cryptographie à clé asymétrique n'élimine pas le besoin de symétrie cryptographie à clé. Ils se complètent généralement ; les avantages de l'un peuvent compenser les inconvénients de l'autre. [42]

Dans ce système, chaque individu souhaitant chiffrer et déchiffrer des messages doit posséder une paire de clés. Cette paire de clés est unique, et est générée par l'algorithme de chiffrement une seule et unique fois, lors de la première utilisation.
Comme nous venons de le voir, l'une d'elles sera publique et l'autre sera privée. Voici un schéma pour illustrer :

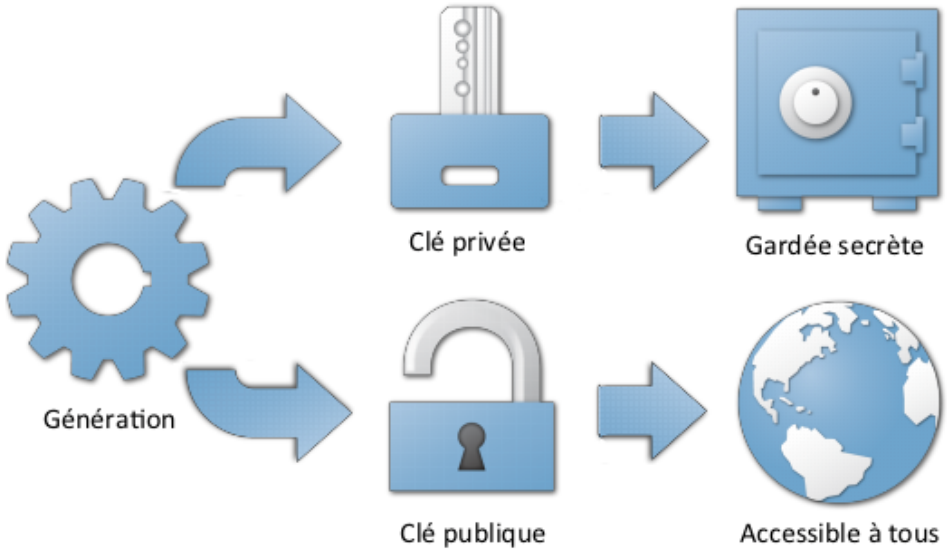

FIGURE 2.8 – *Génération des clés.*[13]

2.4.3.2 le principe du chiffrement à clé publique :

Le principe de chiffrement asymétrique (appelé aussi chiffrement à clés publiques) est apparu en 1976, avec la publication d'un ouvrage sur la cryptographie par Whitfield Diffie et Martin Hellman. Dans un crypto système asymétrique (ou crypto système à clés publiques) les utilisateurs choisissent une clé aléatoire qu'ils sont seuls à connaître (il s'agit de la clé privée).
A partir de cette clé, ils déduisent chacun automatiquement un algorithme (il s'agit de la clé publique).
Donc les clés existent par paires (le terme de bi-clés est généralement employé). Les utilisateurs s'échangent cette clé publique au travers d'un canal non sécurisé. [25]
Voilà comment cela fonctionne, toujours de manière simplifiée.

- Cet utilisateur comme le destinataire possèdent tous deux une paire de clés, et chacun connait la clé publique de l'autre.
- Afin de chiffrer un message pour le destinataire, l'utilisateur va alors utiliser la clé publique du destinataire.

. Cette clé active un algorithme, et le message écrit est alors transformé en texte incompréhensible, qui peut alors être envoyé au destinataire.

Du côté du destinataire maintenant :

. Lorsqu'il reçoit le message chiffré, le destinataire devra utiliser sa propre clé privée, celle que lui seul détient, afin d'activer l'algorithme pour le déchiffrer.

. Ainsi, même si quelqu'un intercepte le message en chemin, il ne pourra pas le déchiffrer, puisqu'il ne dispose pas de la clé privée du destinataire ! [13]

Voici un exemple pour comprendre comment un tel système travail.

Supposons qu'Alice veuille envoyer un message à Bob de manière confidentielle afin que personne d'autre que Bob ne peut donner un sens au message, alors il serait nécessité les étapes suivantes :

- Puk = clé publique.
- Prk = clé privée.

Alice - L'émetteur :

. Chiffrer le message en clair m en utilisant l'algorithme de chiffrement E et la clé publique Puk Bob pour préparer le texte chiffré c.

. c = E (Puk Bob, m)

. Envoyez le texte chiffré c à Bob.

Bob - Le récepteur :

. Déchiffrer le texte chiffré c à l'aide de l'algorithme de déchiffrement D et sa clé privée Prk Bob pour obtenir le texte en clair d'origine m.

. m = D (Prk Bob, c). [42]

Un tel système peut être représenté comme le montre la figure 2.9

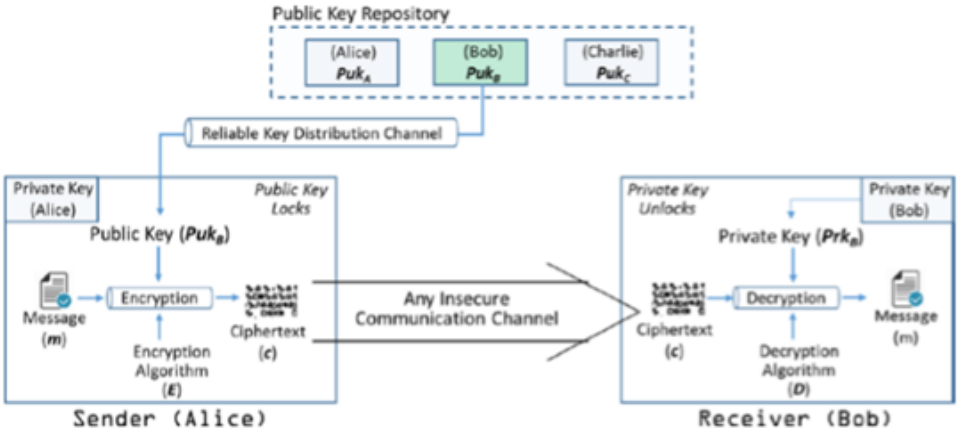

FIGURE 2.9 – *Cryptographie asymétrique pour la confidentialité.* [42]

La clé publique doit être conservée dans un référentiel public accessible à tous et la clé privée doit être conservée comme un secret gardé.
La cryptographie à clé publique fournit également un moyen d'authentification. Le destinataire, Bob, peut vérifier l'authenticité de l'origine du message m de la même manière.
Voici le schéma équivalent : [42]

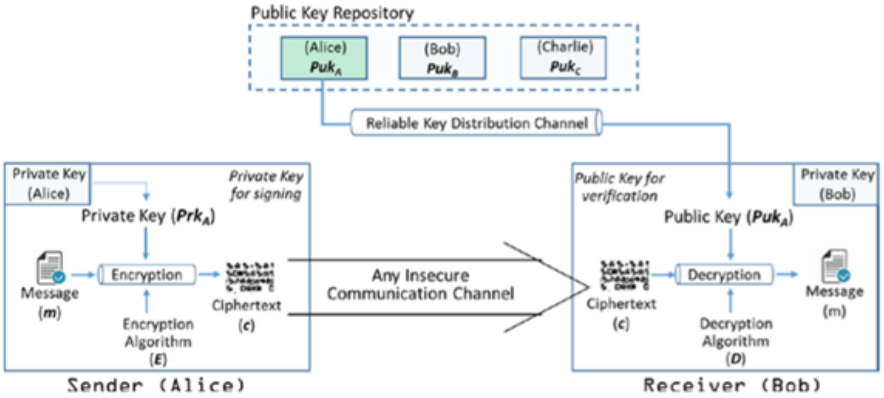

FIGURE 2.10 – *Cryptographie asymétrique pour l'authentification.*[42]

Dans l'exemple de la figure 2.10, le message a été préparé à l'aide d'Alice clé privée, afin de garantir qu'il provienne uniquement d'Alice.
Alors le message entier a servi de signature numérique. Notez que la confidentialité et l'authentification sont souhaitables. Pour faciliter cela, le cryptage à clé publique doit être utilisé deux fois. Le message doit d'abord être crypté avec le clé privée de L'émetteur pour fournir une signature numérique. Alors ça devrait être crypté avec la clé publique du récepteur pour assurer la confidentialité.
Donc Cryptographie Asymétrique utilisée deux clés : [8]

- Clé publique : Connue par tout le monde, et peut être utilisée pour crypter des messages ou pour vérifier la signature.
- Clé privée : Connue par le récepteur uniquement, utilisée pour décrypter les messages, ou pour créer la signature

2.4.4 La signature numérique :

2.4.4.1 La signification de signature numérique[36]

Les signatures numériques sont l'un des principaux aspects de la sécurité et de l'intégrité des données enregistrées sur une blockchain. Ils font partie intégrante de la plupart des protocoles de la blockchain, principalement utilisés pour sécuriser les transactions et les blocs de transactions, les transferts d'informations sensibles, la distribution de logiciels,

la gestion des contrats et tout autre cas où il est important de détecter et de prévenir toute manipulation externe.
Les signatures numériques utilisent la cryptographie asymétrique, ce qui signifie que l'information peut être partagée avec n'importe qui, grâce à l'utilisation d'une clé publique.
Les signatures numériques sont uniques au signataire et sont créées à l'aide de trois algorithmes :

- Un algorithme de génération de clé, fournissant une clé privée et publique.
- Un algorithme de signature qui combine les données et la clé privée pour créer une signature.
- Un algorithme qui vérifie les signatures et détermine si le message est authentique ou non en fonction du message, de la clé publique et de la signature.

2.4.4.2 Signature Électronique : Création

Signe (Texte clair, Clé Privée) =Signature.

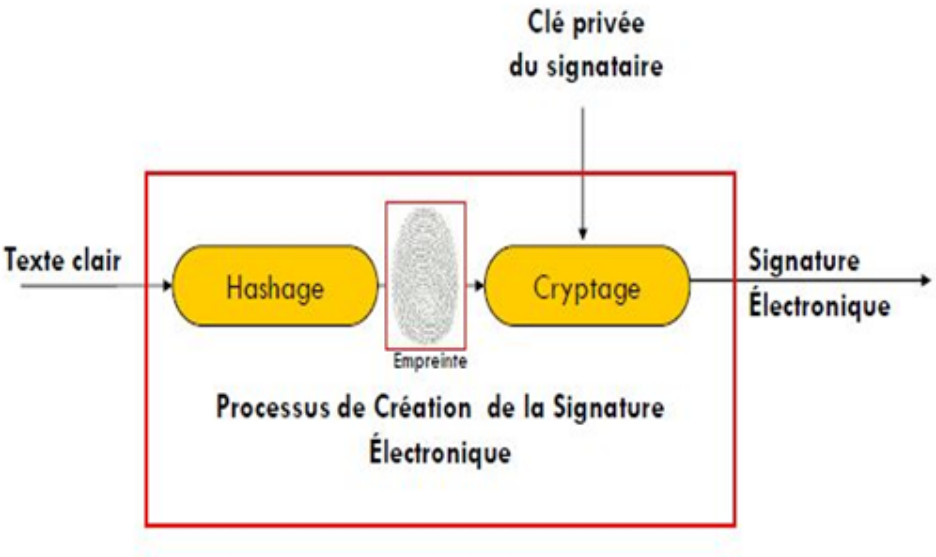

FIGURE 2.11 – *Création de signature.*[8]

2.4.4.3 Signature Électronique : Vérification

Vérifié (Texte clair, Signature, Clé publique) = Vrais/Faux.

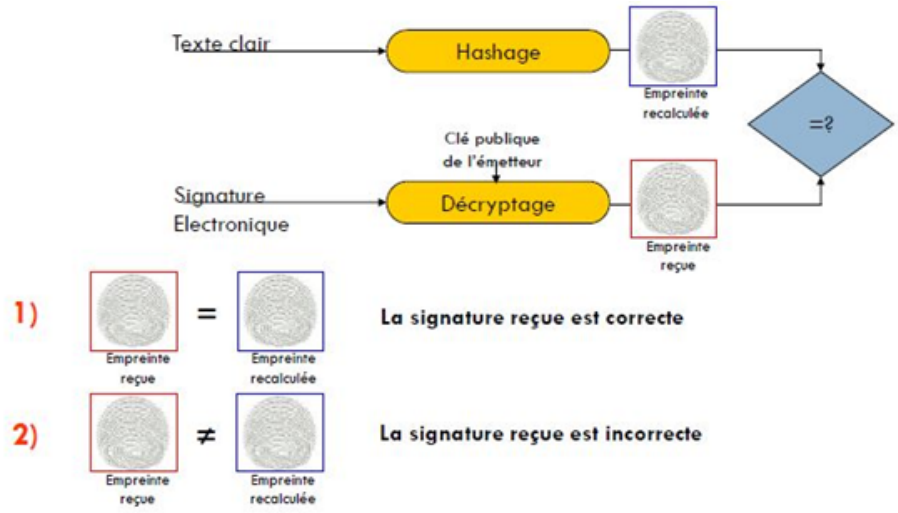

FIGURE 2.12 – *Vérification de signature.*[8]

2.4.5 Fonction de Hachage

2.4.5.1 Définition

Les fonctions de hachages sont des fonctions à sens uniques « sans collision », générant une sortie de taille fixe (appelée condensat ou empreinte), caractéristique des données fournies en entrée. Ces fonctions sont dites à sens unique car il est impossible de retrouver les données initiales à partir de l'empreinte. Une fonction est dite « sans collision » ou « injective » lorsqu'il est réputé très difficile de trouver deux sources différentes conduisant à un même résultat. [31]

Une fonction de hachage cryptographique idéale possède les quatre propriétés suivantes :

- La valeur de hachage d'un message se calcule « très rapidement » ;
- Il est par définition, impossible, pour une valeur de hachage donnée, de construire un message ayant cette valeur de hachage ;
- Il est par définition, impossible de modifier un message sans changer sa valeur de hachage ;
- Il est par définition, impossible de trouver deux messages différents ayant la même valeur de hachage. [41]

2.4.5.2 Types d'algorithme de hachage

Il existe de nombreux types d'algorithme de hachage tels que Message Digest (MD, MD2, MD4, MD5 and MD6), RIPEMD (RIPEND, RIPEMD-128, et RIPEMD-160), Whirlpool (WHIRLPOOL-0, WHIRLPOOL-T, and WHIRLPOOL) ou encore (Secure Hash

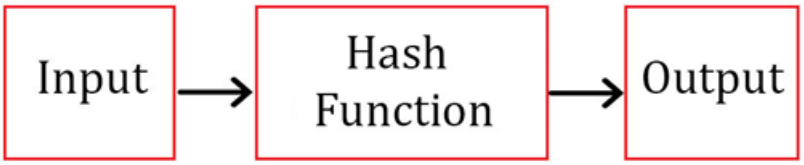

FIGURE 2.13 – *Principe de hachage.*

Function) (SHA-0, SHA-1, SHA-2, and SHA-3).
Dans l'univers des crypto-monnaies, les algorithmes de hachage les plus courant sont SHA-256 et X11. [46]

2.4.5.3 Le rôle du hachage dans l'intégrité de la chaîne de blocs [47]

Les Blocs liés entre eux par des fonctions de hachage
Chaque bloc, outre les transactions et l'horodatage, possède un identifiant (case à fond noir du bloc 90 dans le schéma ci-après), qui prend la forme d'un « hash » permettant de relier les blocs les uns aux autres. Cet hash est toujours le résultat du « hachage » du bloc précédent.
En informatique, les fonctions de « hachage » permettent de convertir n'importe quel ensemble de données numériques en un hash, c'est-à-dire en une courte suite binaire qui lui est propre.

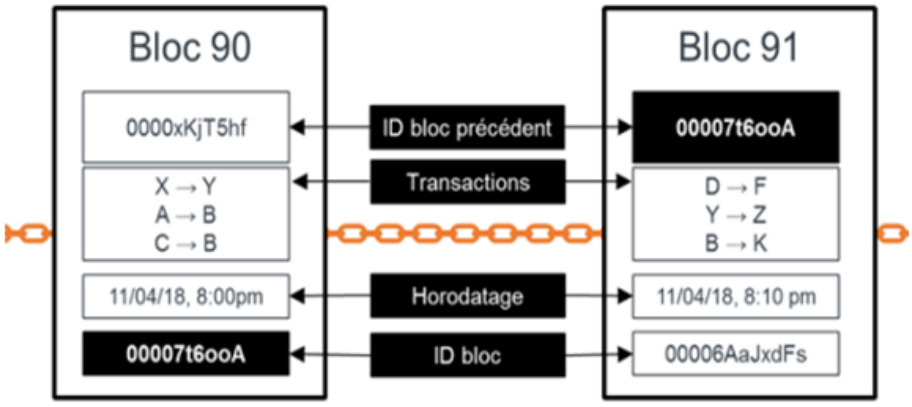

FIGURE 2.14 – *La structure d'une blockchain et le rôle des hash.*

Les Blocs son liés par leurs hashs
Dans le cas d'une chaîne de bloc, le hachage est effectué à partir du contenu du bloc, c'est-à-dire le hash du bloc précédent, un certain nombre de transactions et un horodatage

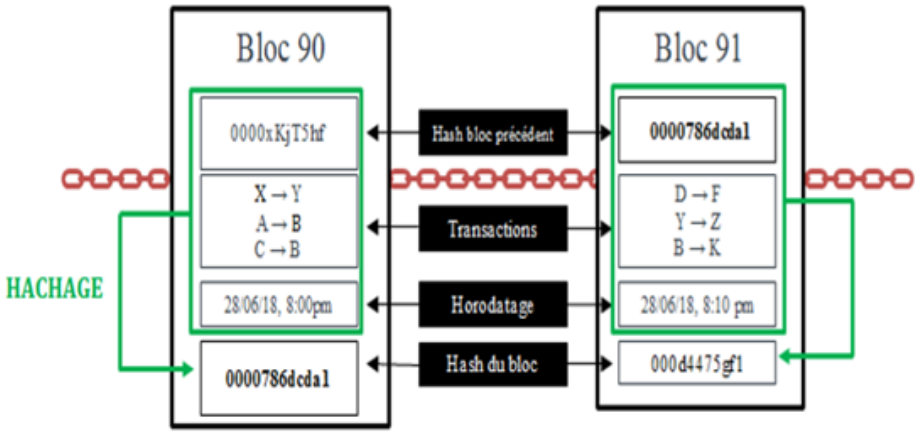

FIGURE 2.15 – *Le rôle des hashs dans les blocs.*

2.5 Conclusion

Dans ce document, on a étudié le procédé de sécurité sur lequel repose la Blockchain. La Blockchain a un impact environnemental non négligeable.
Ou tout du moins, c'est le cas aujourd'hui. Cette technologie s'appuie sur le chiffrement de données pour garantir leur protection et établir un consensus sur le réseau distribué.

3

Conception et analyse

3.1 Introduction

Dans le chapitre précédent, nous avons présenté la blockchain et les concepts liés à leurs utilisations.
A travers ce chapitre, nous avons décrit les différents composants pour implémenter notre outil dans une système des crédits de la banque. nous allons définir les objectifs (résultats attendus) et les fonctionnalités des acteurs, puis nous avons présenté la conception globale, l'architecture de notre système, et la conception détaillée du système.

3.2 Sujet du projet (Objectif)

L'objectif de cette étude est de créer un portail de gestion de crédit bancaire en utilisant la technologie blockchain.
Le rôle principal est d'ajouter de nouveaux utilisateurs, de les attribuer des comptes, d'effectuer des opérations telles que la demande de montant,la validation des transactions,vérifier les blocs et de permettre Aux clients d'accéder à leurs comptes via une application windows.

3.3 Conception Globale

La conception d'un système passe par différentes phases. On peut diviser le processus de conception en deux parties : conception générale détailler du système, L'architecture du système consiste à définir l'ensemble des composants du système et les relations qui relient ces composants.
Ces relations représentent en général, des interactions entre ces composants. L'architecture générale de notre système est représenté comme suit :

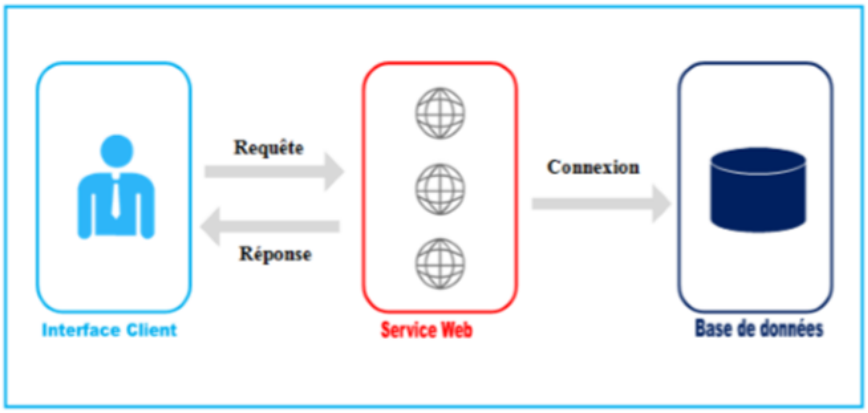

FIGURE 3.1 – *Architecture globale de l'application*

3.3.1 L'interface Client

Permet à l'utilisateur d'interagir avec le système. Les fonctionnalités offertes par cette interface permettent au client de faire plusieurs opérations tel que :

. Ajouter un nouveau compte.
. Authentification.
. Ajouter une transaction (demande montant)
. Valider les transactions.
. Vérifier la blockchain.

Une interface mal conçue peut être la cause d'erreurs catastrophiques de la part de client.

3.3.2 Services Web

Un serveur d'application va offrir un environnement pour gérer des applications accessibles depuis le Web, ces applications pourront être organisées en service.

3.3.3 Base de données

Une base de données est un ensemble structuré de données enregistrées sur des supports accessibles par l'ordinateur, et pouvant être interrogée et mise à jour par une communauté d'utilisateurs. Elle est à la forme d'une collection d'information précisée. Nous avons représenté dans la base de données un ensemble des tables des données qui nous allons utiliser dans notre application.

3.4 L'Architecture (MVC)

Le modèle-vue-contrôleur (MVC) est un modèle architectural qui sépare une application en trois composants logiques principaux : le modèle, la vue et le contrôleur.
Chacun de ces composants est conçue pour gérer des aspects de développement spécifiques d'une application.
MVC est l'un des frameworks de développement les plus fréquemment utilisés pour créer des projets évolutifs et extensibles. [50]
Notre architecture est basée sur trois couches pour offrir une plus grande souplesse d'implémentation et faciliter la réutilisation des unités existantes.

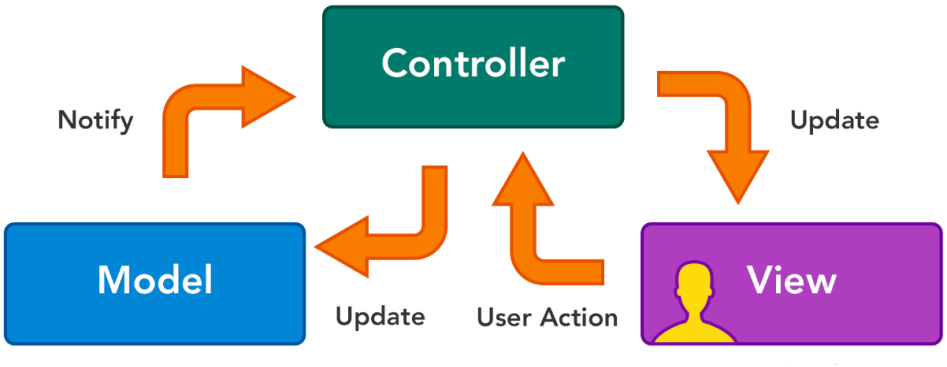

FIGURE 3.2 – *Architecture MVC* [51]

3.4.1 Couche de Vue

Une vue, autrement dit un ensemble de classes représentant les éléments de l'interface utilisateur (tous ceux que l'utilisateur voit à l'écran et avec lesquels il peut interagir : boutons, boîtes de dialogue, etc.).[52]

3.4.2 Couche de contrôleur

Un contrôleur représentant les classes qui se connectent au modèle et à la vue, et servant à la communication entre les classes dans le modèle et la vue
Le contrôleur est la partie dans laquelle nous avons traité les données après avoir recu une demande de View et avant de mettre à jour quoi que ce soit dans notre base de données avec notre modèle.[52]

3.4.3 Couche de modèle

Un modèle représentant la structure logique sous-jacente des données dans une application logicielle .
Le modèle fonctionne directement avec la base de données. Il n'a pas de traitement ni d'interface utilisateur ni des données. Dans un scénario du monde réel, vous utiliserez simplement modèle pour récupérer, insérer, mettre à jour et supprimer des données de votre base de données.[52]

3.4.4 Les avantages de l'architecture MVC

L'approche MVC offre beaucoup d'avantages lors du développement d'applications et les bénéfices sont directs :[53]

- La Séparation des tâches.
- Le Développement en parallèle.

- La Réutilisabilité et gain en temps.
- Développement Rapide et simultané.
- La possibilité de plusieurs vues.

3.5 Conception détaillée

Nous allons décrire les fonctionnalités de notre conception et les différents diagrammes essentiels

3.5.1 Le diagramme de cas d'utilisation (modélisation fonctionnelle)

Le diagramme de cas d'utilisation du client avec leurs fonctionnalités est présenté comme suit : (figure 3.3)

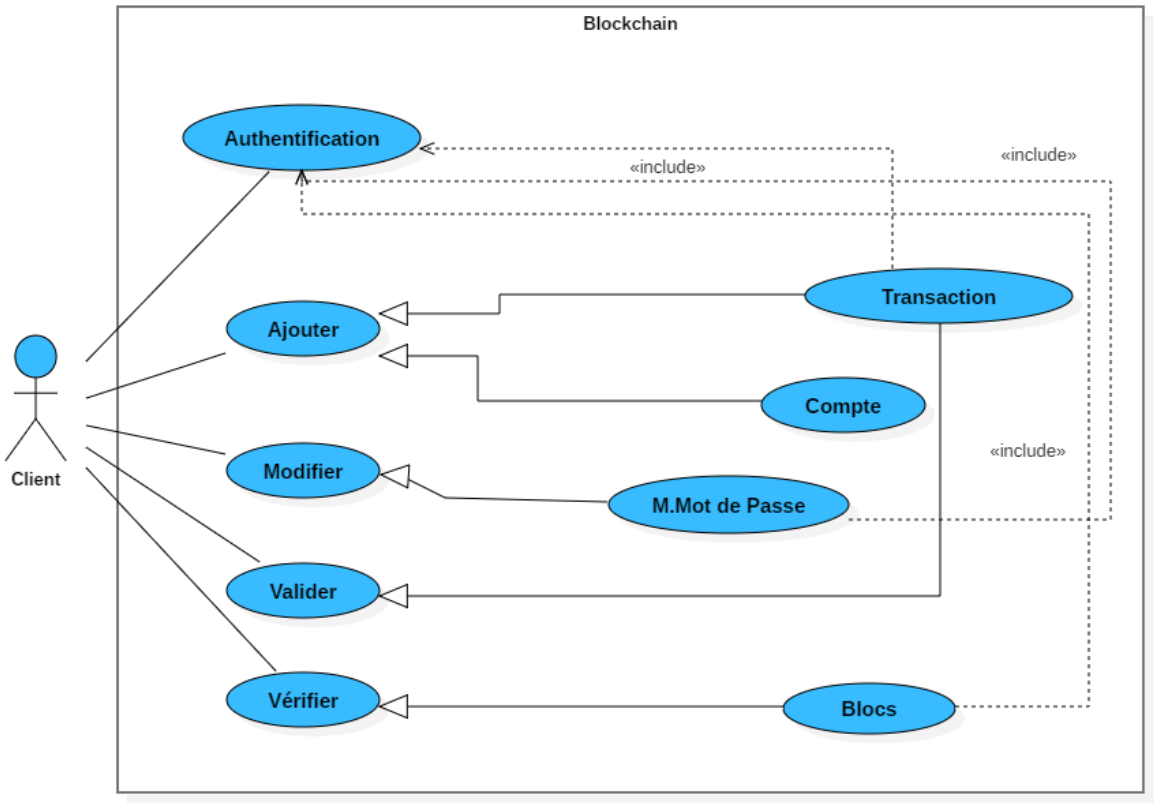

FIGURE 3.3 – *Diagramme de cas d'utilisation*

3.5.2 Le diagramme de classe (Modélisation statique)

En utilisant le diagramme de classes qui représente les entités (classes) statiques dans l'application, Notre conception est représentée comme suit (figure 3.4) Le rôle de chaque class est comme suit :

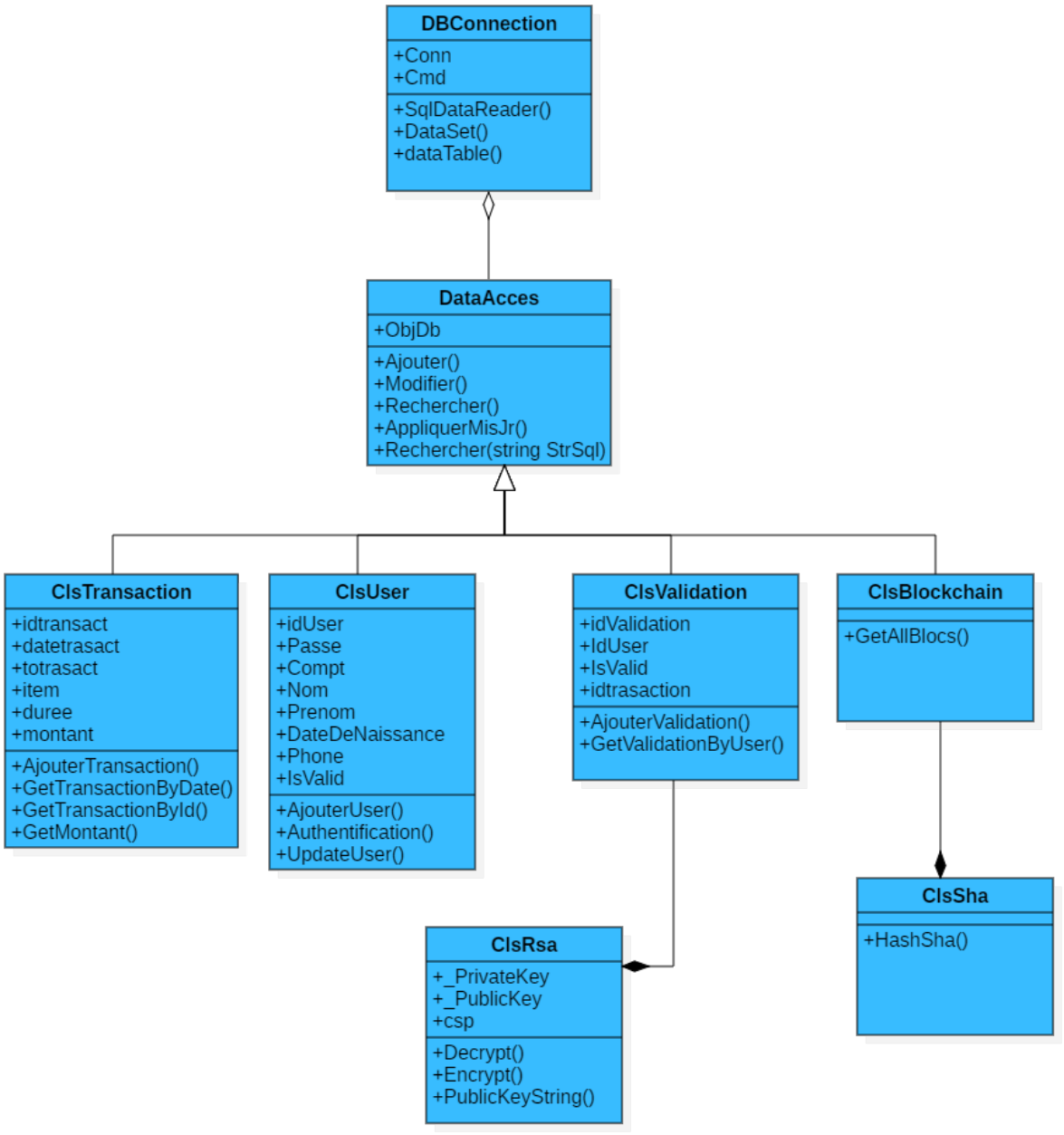

FIGURE 3.4 – *Diagramme de classe*

- La classe (ClsTransaction) : Cette classe est une représentation de la table transaction (dans la base de données) avec ses champs et toutes les opérations de base concernant le transaction (AjouterTransaction, GetTransactionById ...Etc.).
- La classe (ClsUser) : Cette classe est une représentation de la table User (dans la base de données) avec ses champs en incluant l'opération (AjouterUser,UpdateUser ,Authentification).
- La classe (ClsValidation) : Cette classe est une représentation de la table Validation (dans la base de données) avec ses champs en incluant l'opération (AjouterValidation,GetValidationByUser).
- La classe (ClsBlockchain) : Cette classe est une représentation de la Blockchain des transaction avec ses champs en incluant l'opération (GetAllBlocs).
- La classe (ClsSha) : Cette classe est contient une composition avec la class ClsBlockchain avec ses champs en incluant l'opération (HashSha) pour reliée les blocs entre eux et securisé la blockchain (transactions).
- La classe (ClsRsa) : Cette classe est contient une composition avec la classe ClsValidation avec ses champs en incluant l'opération (Encrypt,Decrypt..) pour valider les transactions par l'utilisateur.
- La classe (DataAccess) : Cette classe est une généralisation des classes mentionnées ci-dessus qui contient les opérations standards.
- La classe (DBConnexion) : cette classe contient toutes les opérations liées à la base de données.

3.5.3 Le Diagramme d'Activité (Modélisation Dynamique)

Le comportement global du notre application sera représentée par le diagramme suivant (figure 3.5)

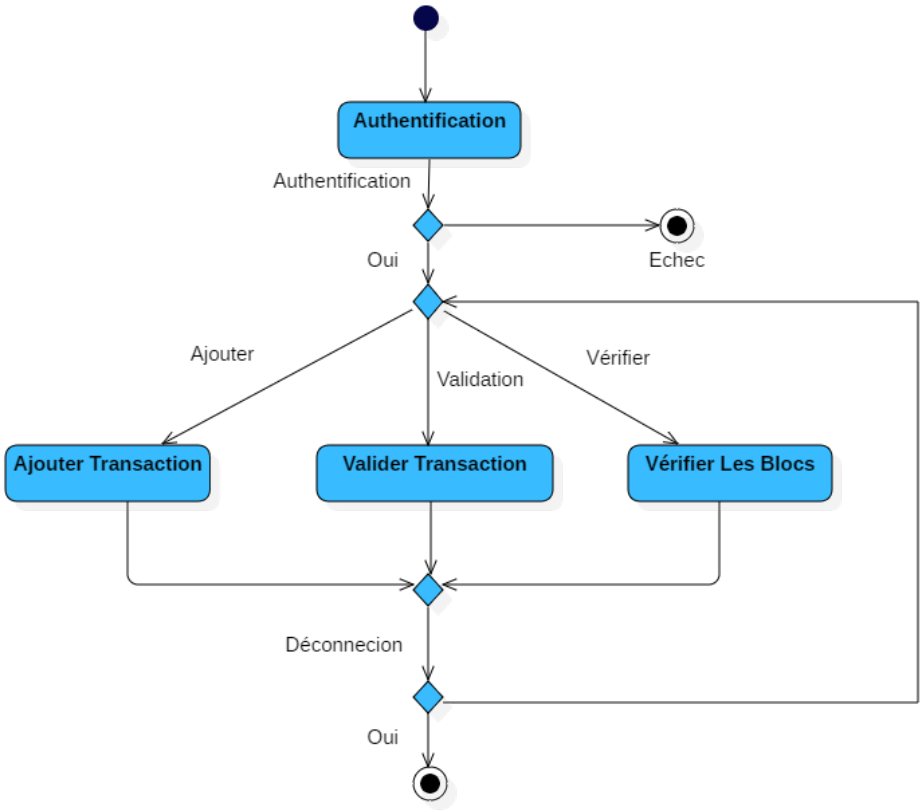

FIGURE 3.5 – *Diagramme d'Activité Dynamique Globale*

- Entrée : numéro de compte et le mot de passe (Authentification).
- Opérations : Ajouter une transaction ou valider les transactions ou vérifier les blocs...etc.
- Sortie : lorsque le client termine une opération alors il peut déconnecter comme il peut choisir une autre opération

3.5.4 Description des scénarios (Modélisation Dynamique)

Après avoir élaboré les diagrammes de classe, nous allons représenter les fonctionnalisées des Forms et la composition entre eux par les diagrammes de séquence comme suit :

3.5.4.1 Authentification

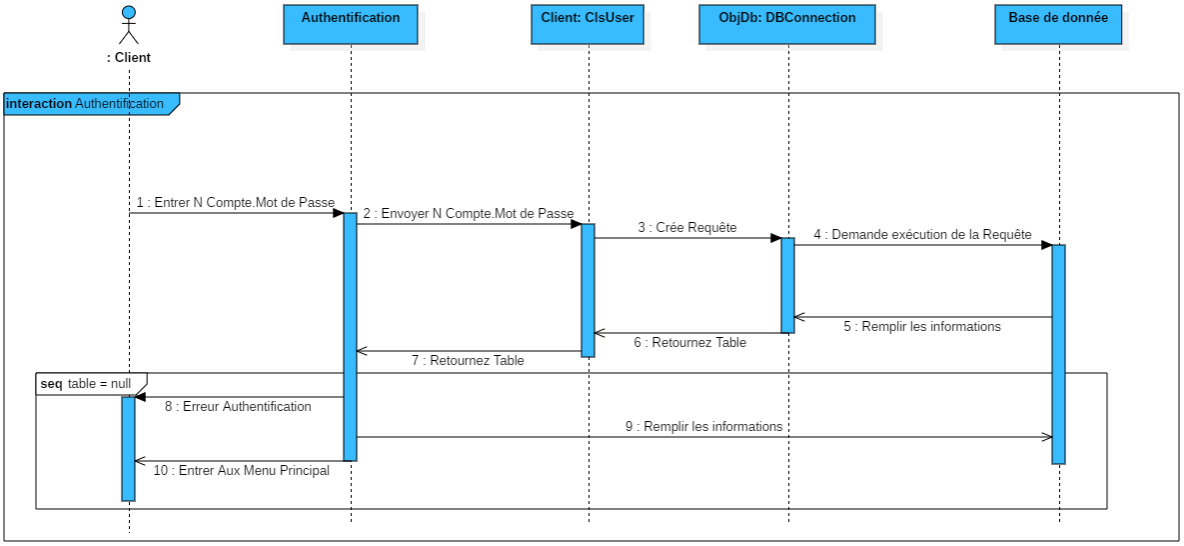

FIGURE 3.6 – *Diagramme de séquence d'Authentification*

— La Forme : Authentification

1 - Le client envoie (le NCompte et le Mot de Pass), pour faire l'authentification ,

2 - La classe ClsUser vérifie s'il peut connecter ou non par la création d'une requête,

3 - Cette requête est exécutée par l'objet DBConnection qui va interroger la base de données pour extraire l'information,

4 - Si le résultat de l'exécution de requête est négative, cela signifie qu'il ya une erreur d'Authentification,

5 - Sinon la form Authentification remplie les informations et enter au menu principal.

3.5.4.2 Nouvelle Transaction

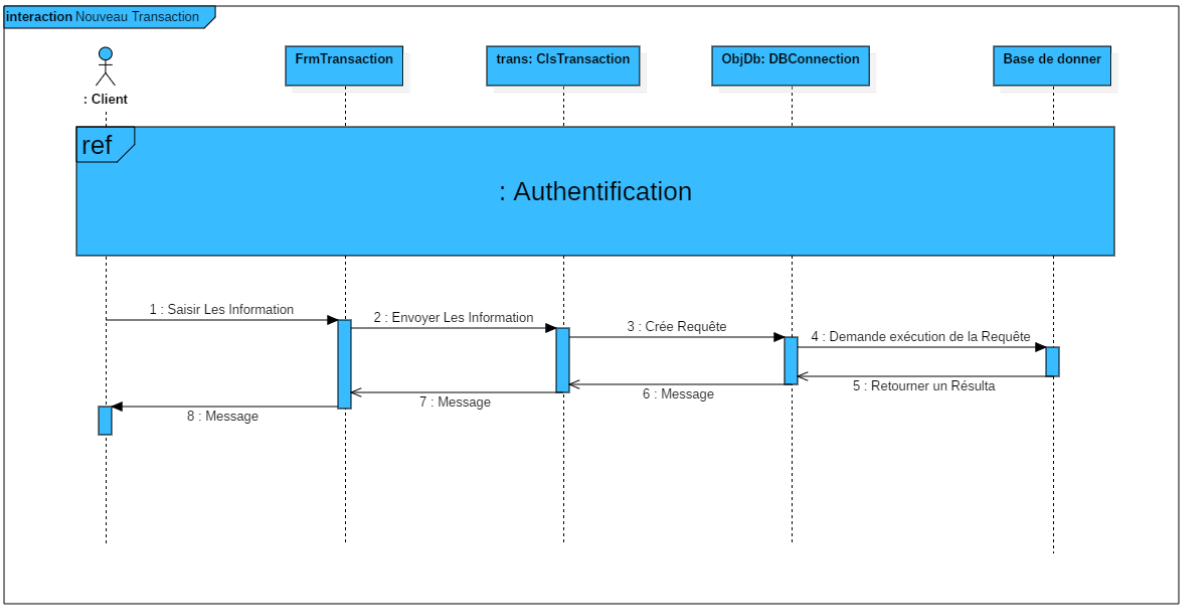

FIGURE 3.7 – *Diagramme de séquence Nouvelle Transaction*

— La Forme : Nouvelle Transaction

1 - Après l'Authentification,le client va saisir et envoie les informations pour ajouter la transaction ,

2 - La classe ClsTransaction vérifie la possibilité de la connection par la création d'une requête,

3 - Cette requête va être exécutée par l'objet DBConnection qui va interroger la base de données pour extraire l'information,

4 - Le résultat est retourné vers La forme Transaction pour répondre au client par l'envoie d'un message.

3.5.4.3 Valider les transactions

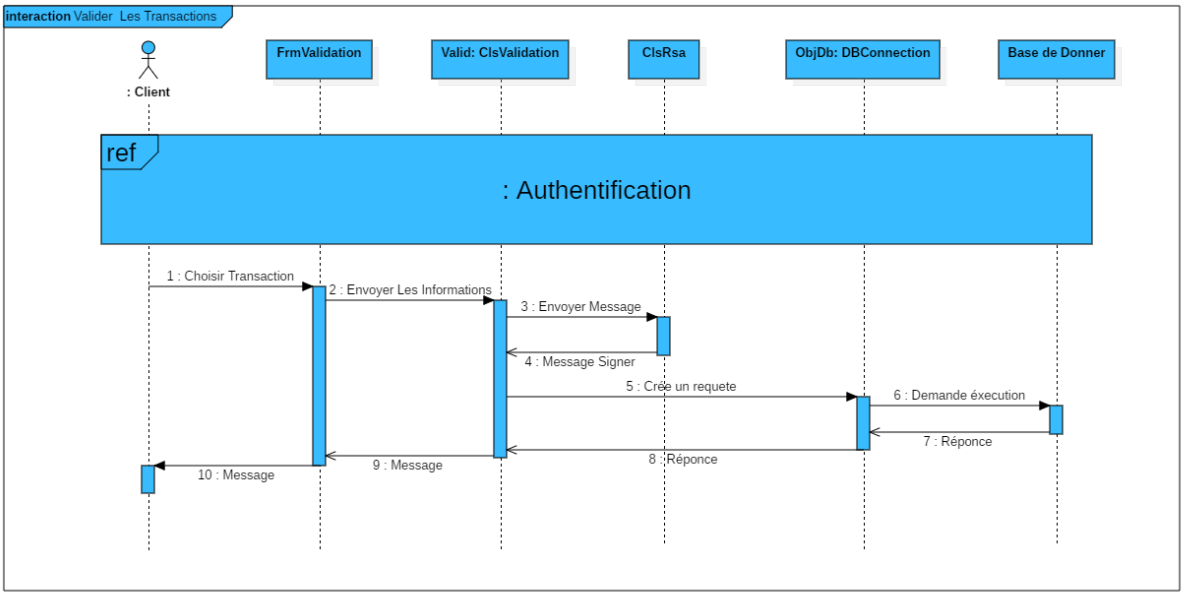

FIGURE 3.8 – *Diagramme de séquence Valider les transactions*

— La Forme : Valider les transactions

1 - Après l'Authentification,le client Choisi la transaction et envoie les informations pour valider la transaction,

2 - La classe ClsValidation envoie un message à la class Rsa,

3 - La classe Rsa retourner un message signer,

4 - La classe ClsValidation vérifie s'il peut connecter ou non par la création d'une requête,

5 - Cette requête est exécutée par l'objet DBConnection qui va interroger la base de données pour extraire l'information,

6 - Une réponse est retournée vers le client.

3.5.4.4 Afficher Les Blocs

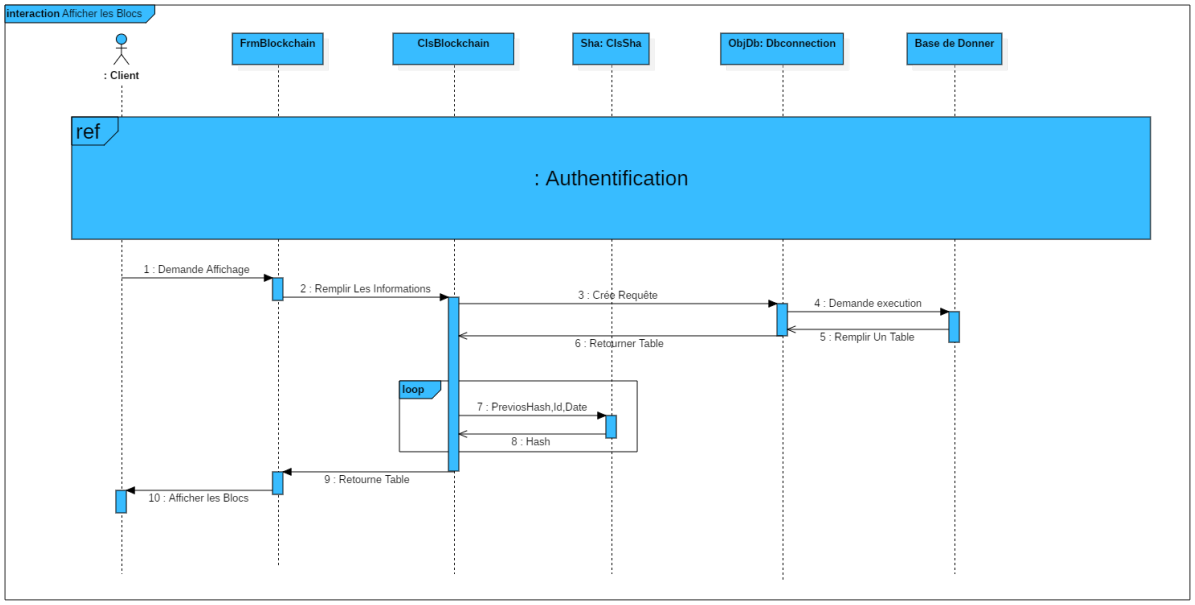

FIGURE 3.9 – *Diagramme de séquence Afficher Les Blocs*

— La Forme : Afficher Les Blocs

1 - Après l'Authentification,le client demande d'afficher et envoie les informations ,

2 - Cette requête est exécutée par l'objet DBConnection qui va interroger la base de données pour extraire l'information,

3 - La classe ClsBlockchain vérifie s'il peut connecter ou non par la création d'une requête,

4 - cette requête est exécutée par l'objet DBConnection qui va interroger la base de données pour extraire,

5 - La classe ClsBlockchain envoie (id,date,previousHash) à la classe Sha ,

6 - La classe sha retourner un message contient le hash de chaque bloc à la classe clsBlockchain,

7 - La classe clsBlockchain retourner un table vers La forme Blockchain pour afficher les blocs au client

3.6 La sécurité de l'application

La plupart des applications sont une cible privilégiée des attaques car elles sont facilement accessibles et offrent un point d'entrée lucratif, pour accéder à des données précieuses.

Ces menaces pourraient conduire à des résultats catastrophiques en particulier dans le domaine des banques.
Pour lutter contre les attaques complexes et distribuées, les entreprises ont besoin de protéger leurs applications contre des menaces nouvelles et émergentes, sans affecter Les performances ou la disponibilité des applications. Pour cela nous avons utilisé pour notre application différents niveaux de protection qui sont :

- Les données d'application (Transactions) sont cryptées par l'utilisation Le chiffrement RSA (Rivest, Shamir & Adleman) :
  En 1976, Diffie et Hellman suggérèrent la possibilité d'assurer la confidentialité sans recourir à un secret partagé, au moyen d'une clé connue de tous. Cette idée a profondément transformé la cryptographie. Le système de chiffrement à clé publique RSA, proposé en 1977 par Rivest, Shamir et Alemany, est maintenant couramment utilisé par les systèmes de chiffrement, par exemple par PGP.

Les étapes de chiffrement RSA :
Pour construire ses clés, chaque utilisateur de RSA

- Nous allons créer 2 nombres p et q, les autres nombres seront trouvés grâce à eux ;
- Calcule $n = p.q$;
- Choisit un entier e<n qui est premier avec $(p-1)(q-1)$;
- Calcule l'inverse d de e modulo $(p-1)(q-1)$;
- Publie sa clé publique, qui est formée des deux entiers e et n ;
- Conserve sa clé privée d ;
- Détruit les entiers p et q qui ne doivent pas être divulgués.

La clé publique est sous la forme (e, n), celle L'émetteur possède et que tout le monde peut avoir sans aucun problème Ce couple permettra le chiffrement de chaque message et la clé privée qui servira au déchiffrement se présente sous la forme (d, n), celle que récepteur garde précieusement. Les fonctions de chiffrage et de déchiffrage sont respectivement :

$$C(m) = m^e mood^n$$
$$(1) Chiffre Un Message$$

$$D(m) = m^d mod^n$$
$$(2) D'echiffre Un Message$$

- Nous avons utilisé la fonction de hachage SHA-256 pour relier Les blocs de la blockchain entre eux pour sécuriser les blocs.
  SHA-256 est membre des fonctions de hachage cryptographique SHA-2 .
  SHA signifies Secure Hash Algorithm.
  Les fonctions de hachage cryptographique sont des opérations mathématiques exécutées sur des données numériques ; en comparant le « hachage » calculé (la sortie

de l'exécution de l'algorithme) à une valeur de hachage connue et attendue, une personne peut déterminer l'intégrité des données. Un hachage unidirectionnel peut être généré à partir de n'importe quel élément de données, mais les données ne peuvent pas être générées à partir du hachage.
SHA-256 ou SHA-2 est la norme cryptographique moderne pour la sécurité .
L'algorithme produit une valeur de hachage de 256 bits (32 octets) de taille fixe presque unique. Il est généralement représenté par un nombre hexadécimal de 64 chiffres. [43]

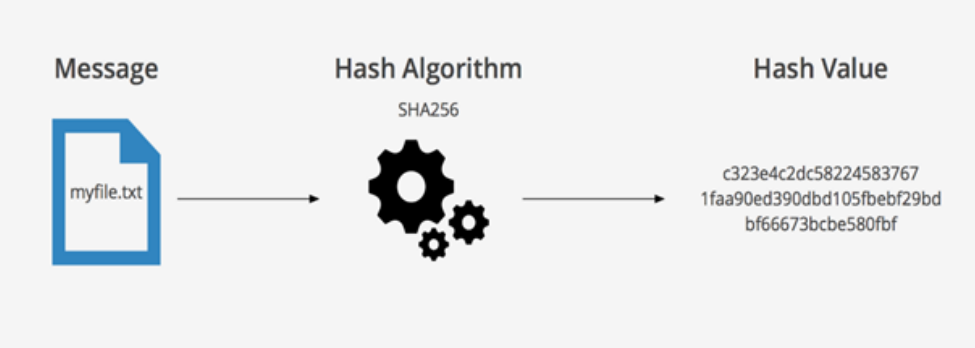

FIGURE 3.10 – *principe de SHA-256.* [49]

- Utilisation le composant data set (une image de la base de données)
- Utilisation de l'architecture MVC

3.7 La Base De Données

A partir de notre étude faite et les diagrammes UML établis, nous avons Réalisé une Base de données relationnelle qui contient des Tables pour accéder aux bases de données :

1 **Les tables**
   - Table TBtrasaction :(idtransact*, datetrasact, totrasact, item,duree,montant)
   - Table TBUser :(idUser*, Passe, Compt,Nom,Prenom,DateDeNaissance,Phone,IsValid)
   - Table TBValidation :(idValidation*, IdUser, IsValid, idtrasaction)

2 **Le Trigger**
   Un trigger est un objet de base de données (procédure) qui fonctionne comme un chien de garde pour certains événements.
   En utilisant des triggers de base de données, nous avons intercepté cet événement et lancer une action supplémentaire, comme la journalisation ou le rejet de l'action.

- Nous avons utilisé le trigger dans l'application pour le consensus, avant la transaction accéde à la blockchain doit valider les transactions Au moins plus de la moitié des gens doivent être accepté .

3.8 Conclusion

Nous avons présenté dans ce chapitre l'étude conceptuelle de notre outil qui présente l'architecture générale, MVC qui se caractérisent par des points forts(...). Et nous avons présenté aussi la conception détaillée en commençant par les diagrammes et la sécurité de lapplication , ensuit la base de données. Le prochain chapitre sert à présenter les techniques utilisées pour implémenter l'application conçue dans ce chapitre

4
Réalisation

4.1 Introduction

Dans ce chapitre, nous avons décrire la mise en œuvre des différentes étapes de notre système conçu dans le chapitre précédent. Il s'agit ici d'expliquer l'environnement matériel et logiciel sur lequel notre système a été développé. Nous avons commencé par la justification de l'environnement de développement utilisé ainsi par les outils et les langages de programmations utilisés, ensuite la plate-forme choisie et nous avons détaillé application windows réalisées par la blockchain. Et enfin présenté les applications nécessaires à l'implémentation de notre système.

4.2 L'environnement matériel de système

Notre système est développé sous l'environnement :
- Micro-Ordinator portable Dell (Inspiron 3558) : Intel(R) Core (TM) i5-5200U CPU @ 2.20 GHz (4 CPUs) RAM 4 G SSD 120 GB
- Système d'exploitation Windows 10 64 bits

4.3 L'environnement software de système

4.3.1 La plateforme .NET Framework

Le .NET Framework est une plateforme de développement largement utilisée pour la création d'applications destinées à Windows, Windows Store, Windows Phone, Windows Server et Windows Azure. La plateforme .NET Framework comprend les langages de programmation JavaScript et Visual Basic, le Common Language Runtime, ainsi qu'une abondante bibliothèque de classes [29].

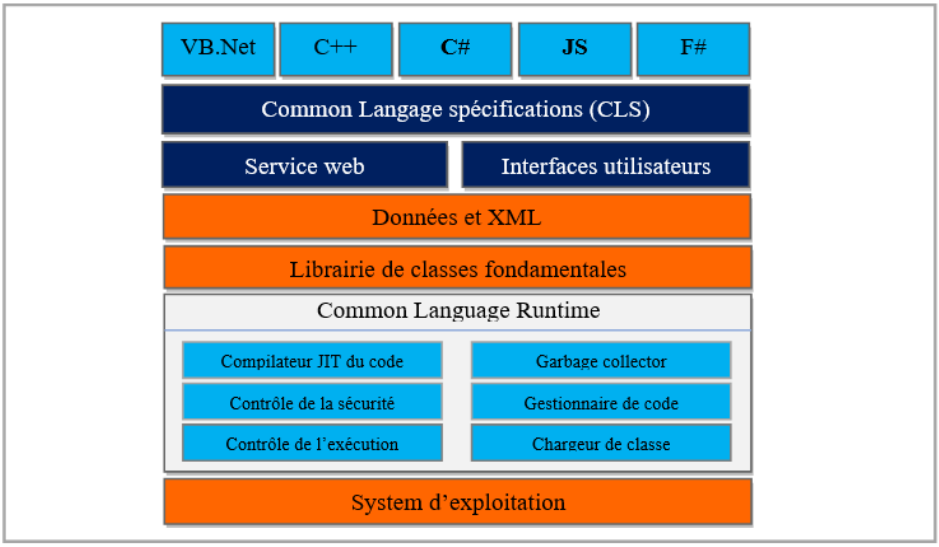

FIGURE 4.1 – *Architecteur. Net Framework [38]*

Nous avons adapté pour cette technologie pour les raisons suivantes [35] :

- Fournir un environnement cohérent de programmation orientée objet que le code objet soit stocké et exécuté localement, exécuté localement mais distribué sur Internet ou exécuté à distance.
- Fournir un environnement d'exécution de code qui minimise le déploiement de logiciels et de conflits de versions.
- Fournir un environnement d'exécution de code qui garantit l'exécution sécurisée de code y compris le code créé par un tiers d'un niveau de confiance moyen ou un tiers inconnu.
- Générer toutes les communications à partir des normes d'industries pour s'assurer que le code basé sur le Framework .NET peut s'intégrer à n'importe quel autre code

4.3.2 Le Langage C#

Le langage star de la nouvelle version de Visual Studio et de l'architecture. NET est C#, un langage dérivé du C++. Il reprend certaines caractéristiques des langages apparus ces dernières années et en particulier de Java (qui reprenait déjà à son compte des concepts introduits par Smalltalk quinze ans plus tôt) mais très rapidement, C# a innové et les concepts ainsi introduits sont aujourd'hui communément repris dans les autres langages. C# peut être utilisé pour créer, avec une facilité incomparable, des applications Windows et Web. C# devient le langage de prédilection d'ASP.NET qui permet de créer des pages Web dynamiques avec programmation côté serveur [21].

4.3.3 SQL Server

SQL Server est un système de gestion de bases de données relationnelles (SGBDR) répondant aux exigences professionnelles du stockage de données. SQL Server prend en charge nativement pour la communication de requêtes entre client et serveur :

- SQL Server intègre par défaut des outils de gestion, d'administration et de développement de bases de données.
- Déploiement par un setup, mise en œuvre et administration par des interfaces graphiques intuitives.
- Gestion avancée de la sécurité en offrant deux modes d'authentification (Authentification Windows et Authentification SQL Server).
- Coût relativement moins cher par rapport aux autres SGBD du marché [28].

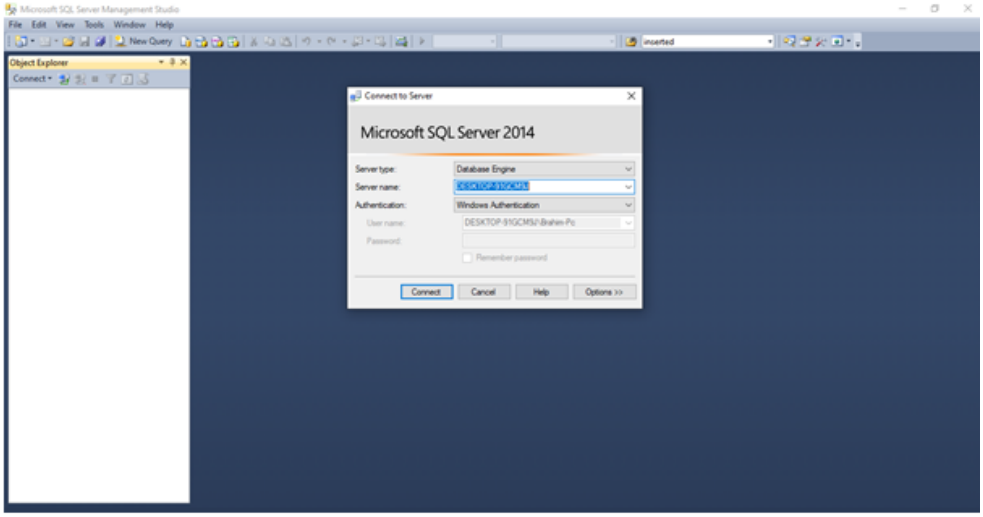

FIGURE 4.2 – *SQL Server 2014*

4.3.4 Windows Forms

Windows Forms est une bibliothéque de classes d'interface utilisateur graphique (GUI) qui est fournie dans .Net Framework.
Son objectif principal est de fournir une interface plus simple pour développer les applications pour ordinateur de bureau, tablette, PC. Il est également appelé WinForms.
Les applications développées à l'aide de Windows Forms ou WinForms sont appelées les applications Windows Forms qui s'éxécutent sur l'ordinateur de bureau. WinForms ne peut être utilisé que pour développer les applications Windows Forms et non les applications Web.
Les applications WinForms peuvent contenir différents types de contrôles tels que des labels,list boxes, button, etc.[23].nous avons apte pour cette technologie pour les raisons

suivantes :

- WindowsForms réduit considérablement la quantité de code nécessaire pour construire de grandes applications.
- Tous les processus sont étroitement surveillés et gérés par le runtime WindowsForms, de sorte que si le processus est mort, un nouveau processus peut être créé à sa place, ce qui aide à garder votre application disponible en permanence pour traiter les demandes.
- Fonctionne facilement avec ADO.NET en utilisant la liaison de données et des fonctionnalités mise en page. Il est une application qui fonctionne plus rapidement et de comptoirs de grands volumes d'utilisateurs sans avoir des problèmes de performance [2].

4.3.5 ADO.NET (ActiveX Data Objects)

ADO.NET est un ensemble de classes qui exposent les services d'accès aux données pour les programmeurs .NET Framework. ADO.NET propose un large ensemble de composants pour la création d'applications distribuées avec partage de données. Partie intégrante du .NET Framework, il permet d'accéder à des données relationnelles, XML et d'application. ADO.NET répond à divers besoins en matière de développement, en permettant notamment de créer des clients de bases de données frontaux et des objets métier de couche intermédiaire utilisés par des applications, outils, langages ou navigateurs Internet [1], on a apte pour cette technologie pour les raisons suivantes :

- Interopérabilité
- Facilité de maintenance
- Facilité de programmation
- Performances
- Evolutivité

4.3.6 Serveur IIS (Internet Information Server)

IIS est le serveur Web de Microsoft .Il contrôle les pages Web (celles évidemment qui sont hébergées sur sa machine) et envoie le HTML de ces pages Web aux navigateurs des clients qui en font la demande [21].

4.3.7 Visual studio IDE (Integrated Development Environment)

Visual Studio est un ensemble complet d'outils de développement permettant de générer des applications Web ASP.NET, des Services Web XML, des applications bureautiques et des applications mobiles. Visual Basic, Visual C# et Visual javascript utilisent tous le même environnement de développement intégré (IDE), qui permet le partage d'outils et facilite la création de solutions à plusieurs langages. Par ailleurs, ces langages utilisent les fonctionnalités du .NET Framework, qui fournit un accès à des technologies clés simplifiant

le développement d'applications Web ASP et de Services Web XML [34], les avantages suivants Visual Studio IDE :

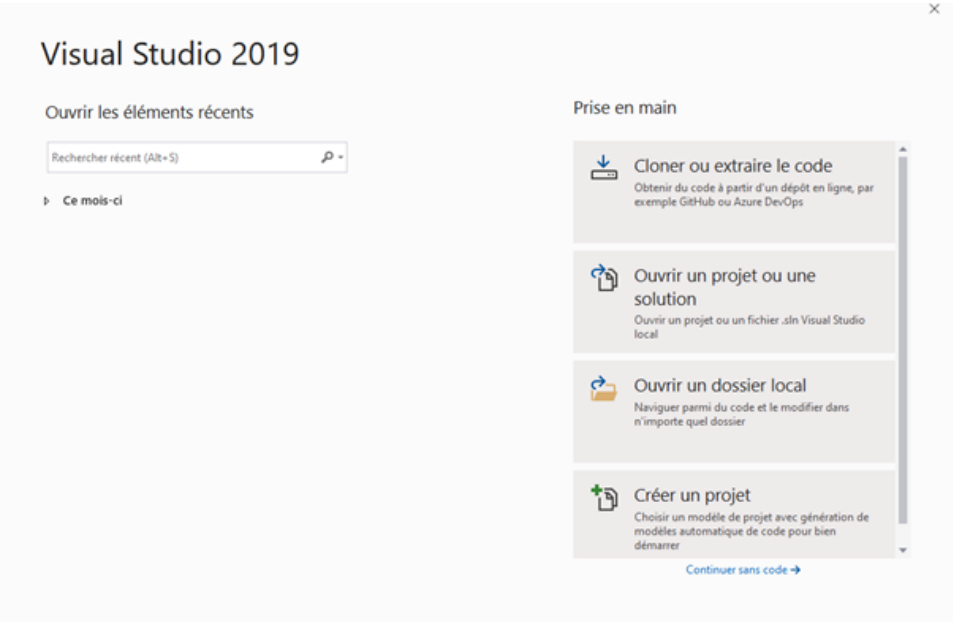

FIGURE 4.3 – *Visual studio Community 2019*

- De très nombreux outils sont disponibles et peuvent interagir.
- Design WYSIWYG des fenêtres des applications graphiques et des applications web.
- IntelliSense (auto-complétion en français).
- Personnalisation complète de VS.NET
- Extensibilité : possibilité de créer votre propre plug-in.
- IDE très optimisée : l'accès à la plupart des fonctionnalités est immédiat [32].

4.4 Réalisation

4.4.1 La Forme Authentification

La figure suivante montre La Forme Authentification :

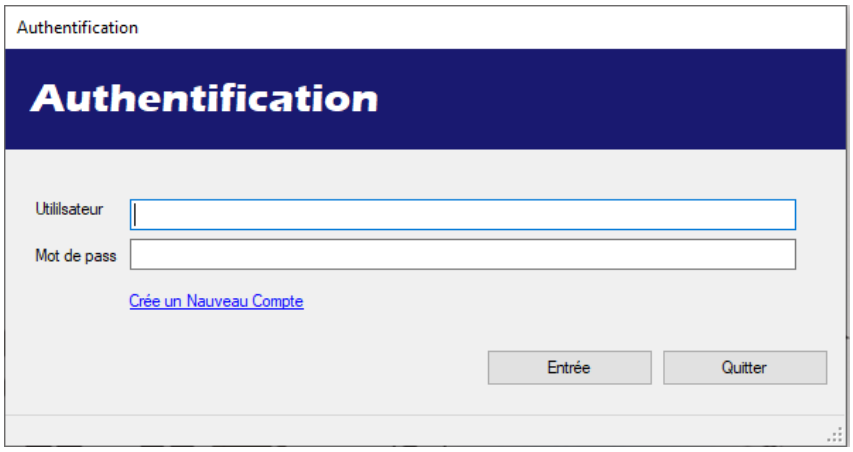

FIGURE 4.4 – L'authentification

4.4.2 La Forme Ajouter Transaction

La figure suivante montre La Forme Ajouter Transaction :

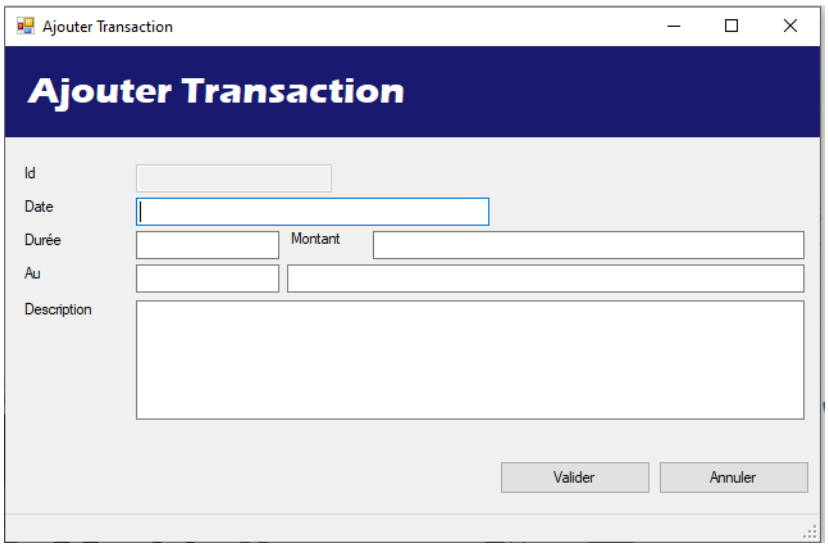

FIGURE 4.5 – Ajouter Transaction

4.4.3 La Forme Valider Les Transactions

La figure suivante montre La Forme Valider Les Transactions :

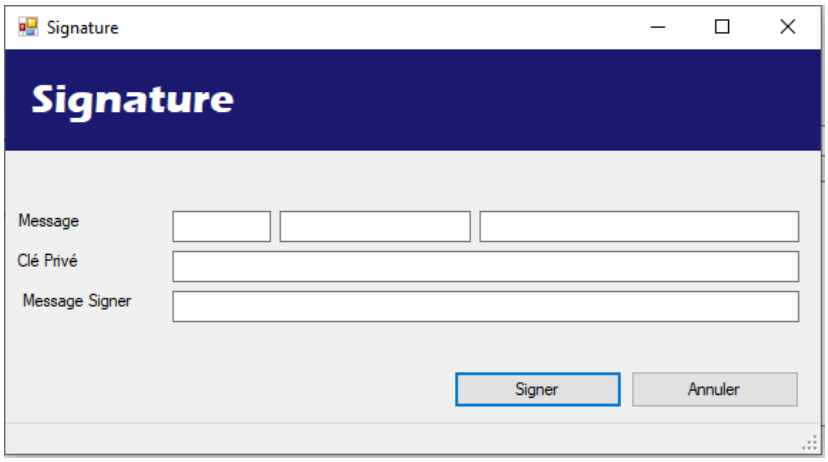

FIGURE 4.6 – Valider Les Transactions

4.4.4 La Forme Vérifier la Blockchain

La figure suivante montre La Forme Vérifier la Blockchain :

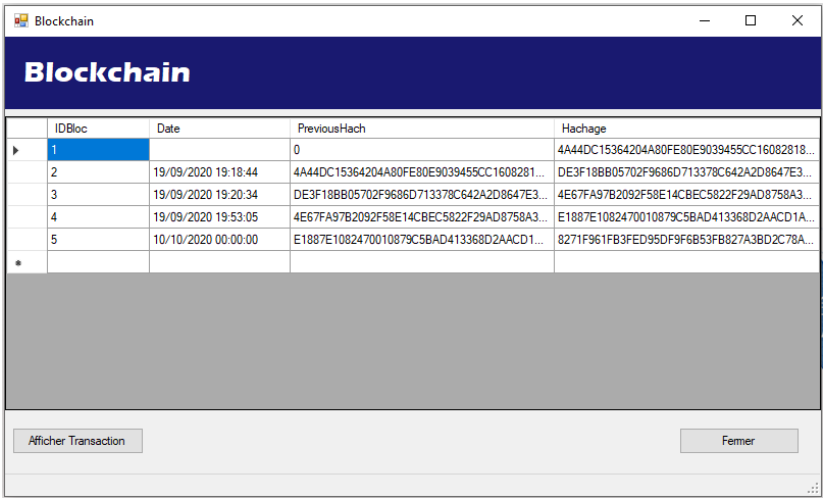

FIGURE 4.7 – Vérifier la Blockchain

4.5 Conclusion

À travers ce chapitre nous avons essayé d'implémenter les notions théorique déjà motionné au deuxième chapitre ainsi que nous avons développé le modèle proposé au troisième chapitre, en utilisant un ensemble d'outils et standard.
On est arrivé à réaliser l'application windows nécessaire et les interfaces requis pour que notre application fonctionne.

Conclusion générale et Perspectives

Le travail présenté dans ce mémoire avait pour objectif le développement d'une application qui fonctionne avec la technologie blockchain.

L'application qui se base sur la blockchain qui est une nouvelle technologie utilisée pour le sécurité l'informations grâce à leurs techniques et les points fort qu'ils se caractérisent.
En effet, on a exploré les techniques de la blockchain, leur définition et leur composition pour répondre aux besoins complexes des utilisateurs qui peuvent correspondre à l'emploi de plusieurs services.
En réponse à nos besoins, les outils. Pour cette raison on a implémenté notre modèle pour être exploité sous la plateforme et notamment on a développé la blockchain pour les crédits des comptes bancaires est assurer toutes les opérations nécessaires à travers ces application WinForms en maintenant la sécurité des procédures.
Pour réaliser notre application, on a utilisé plusieurs outils et langages de programmation.

On a envisagé que ce travail peut être étendu selon plusieurs axes :

- Selon GraphQl.
- Implémenter d'autres méthodes pouvant aider notre outil (sécurité).
- Créer la même application sur d'autres plateformes (smart mobile ...).

Annexes

— ICO : Initial Coins Offering
— OSI : Open Systéms Interconnection
— ISO : International Organization for Standardization
— HTTP : HyperText Transfer Protocol
— MD : Message Digest
— SHA : Secure Hash Function
— MVC : Model View Controller
— RSA : Rivest, Shamir,Adleman
— UML : Unifie Modelling Language
— ADO : ActiveX Data Objects
— IDE : Integrated Development Environment

Bibliographie

[1] ADO.NET (http://msdn.microsoft.com/fr-fr/library/e80y5yhx(v=vs.110).aspx)

[2] Avantages de WindowsForms (http://www.fruitymag.com/aspnet-avantagesd1358877.htm)

[3] bitcoin site official (www.bitcoin.org.fr).

[4] Bouchema, Meryem. Exploitation des transformées paramétriques dans le cryptage des images fixes. Diss. 2018. ?

[5] Blockchainfrance, (https://blockchainfrance.net), consulté le : 22/01/2020.

[6] Blockchain consortium : (https://www.journaldunet.com/economie/finance/1195520-blockchain-avril-2019)

[7] Blokchain use cases,(https://www.lafabriquedunet.fr/blog/definition-blockchain, Consulté le : 22/01/2020.)

[8] LaurentBloch, Christophe wolffhugel, natmakarevitch, Sécurité informatique : Principe s et méthodes à l'usage des DSI, RSSI et administrateurs Broché , Edition eyrolles 2013

[9] Caseau, Yves, and Serge Soudoplatoff. La blockchain, ou la confiance distribuée. Fondation pour l'innovation politique, 2016.

[10] Claire Fénéron Plisson, "L'a blockchain, un bouleversement économique, juridique voire sociétal", I2D ? Information, données & documents,(Volume 54), p. 20-22, mars 2017.

[11] Comprendre la blockchain a Richard Caetano Stratumn, CEO Livre Blanc sous Licence Creative Commons a uchange. a 2017

[12] Comprendre la blockchain, Livre blanc sous licence Creative Commons, édité par uchange.co, janvier 2016.

[13] Cryptographie,(https://openclassrooms.com/fr/courses/2990451-echangez-par-e-mail-en-toute-securite/2990481-comprenez-les\-bases-des-chiffrements-symetriques-et-asymetriques),consulter le 21/02/2020

[14] Crypto-monnaies : (https://www.ethereum-france.com), consulter le 15/02/2020

[15] Cryptoast, cryptoast.fr/blockchain-avantages-inconvenients/, consulté le : 18/02/2019.

[16] Cryptolia ; (https://www.cryptolia.fr), consulté le : 15/02/2019

[17] Delahaye, Jean-Paul. "Les blockchains, clefs d'un nouveau monde.", pour la Science 449 (2015) :80-85. ?

[18] DÉCLARATION DE RESPECT DE LA VIE PRIVÉE, (fr. express. Live/blockchain-les avantages- Et-les-inconvénients-de-cette-technologie/), consulté le : 18/02/2019.

[19] Fonctionnement de blockchain : (https://www.daf-mag.fr/Thematique/business-intelligence-1244/Breves/C-est-quoi-une-blockchain--338335.html)

[20] France, Blockchain. "La blockchain décryptée." Les clefs d'une révolution. Paris, Netexplo (2016).

[21] Gérard Le blanc : ÉDITIONS EYROLLES (C et .NET Versions 1 à 4), (www.editions-eyrolles.com)

[22] G. Ferréol, PRINCIPES CLES D'UNE APPLICATION BLOCKCHAIN,2016.

[23] https://www.geeksforgeeks.org/introduction-to-c-sharp-windows-forms-\applications

[24] La Blockchain décryptée, les clefs d'une révolution, publié par L'observation Netxplo,264 Rue du Faubourg Saint-Honoré - 75008 Paris. Mai (2016).

[25] le principe du chiffrement a clé publique (https://www.commentcamarche.net/contents/201-les-systemes-a-cle-publiques)

[26] Mammeri Ilham, GuerricheNor El Houda "Cryptographie homomorphe pour les Réseaux a Vehicular Cloud Computing a", thése de Master en Réseaux Mobiles et Services de Télécommunications, Université Abou bakrBelkaéd - Tlemcen - Faculté de TECHNOLOGIE

[27] Marion PIGNEL .LA TECHNOLOGIE BLOCKCHAIN Une opportunité pour l'économie sociale ? JUIN 19

[28] MicrosoftSQLServer (https://www.next-decision.fr/editeurs-bi/base-de-donnees/microsoft-sql-server)

[29] NET Framework (http://msdn.microsoft.com/fr-fr/vstudio/aa496123.aspx)

[30] Pair à pair (finance. Vision/fr/blockchain/peer-to-peer-networks-explained ? fbclid=IwAR1BvZIDiiGGdIk8floAt7IKNqnsBUa9xMBKz0IzB4bjRxsmWd8NPm8tnF4), consulter le (11/02/2020)

[31] Parouty, Jean-Luc, Roland Dirlewanger, and Dominique Vaufreydaz. "La signature électronique, contexte, applications et mise en oeuvre." 2003. ?

[32] Patrick Smaccbia éditions O'reilly (Pratique de .net et c)

[33] PIGNEL, Marion, and Denis STOKKINK. "LA TECHNOLOGIE BLOCKCHAIN Une opportunité pour l'économie sociale ?"

[34] Présentation de Visual Studio (http://msdn.microsoft.com/frfr/library/fx6bk1f4(v=vs.90).aspx)

[35] Qu'est-ce que le Framework .NET ? (Http://dotnet.developpez.com/faq/dotnet/?page=architecture), consulter le (07/03/2020)

[36] La signification de signature numeérique (https://www.crypto-sous.fr/blockchain-fonctionnement/signature-numerique), consulter le :16/02/2020

[37] La signification de P2P (https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203399-p2p-peer-to-peer-definition\-traduction-et-acteurs?fbclid=\IwAR0s90xGIOqsCEzVhAUeLdeO3KRiDleXTyYfuMt\RcLZ5Im408TsTn3U7DLI)

[38] R-Michel di Scala éditions Berti à Alger (Les premiers pas dans .Net Framework avec c version 2.0) Novembre 2004

[39] R. Teuscher, R. Pensec, Y. Fasla, and T. Kuselj, Blockchain La nouvelle révolution Technologique - Juin 2018,1-2.

[40] Satoshi Nakamoto. bitcoin : A peer-to-peer electronic cash system. http : //Bitcoin.org/bitcoinpdf, (Consulté le 09 février 2020).

[41] SIDI AISSA, Ikram, and Souria KEDDAR. Proposition d'un systéme a base de blockchain pour la gestion des opérations sur les véhicules au niveau national. Diss. 2018. ?

[42] Singhal, Bikramaditya, Gautam Dhameja, and Priyansu Sekhar Panda. Beginning Blockchain : A Beginner's Guide to Building Blockchain Solutions. Apress, 2018.

[43] sha-256 (https://www.w3docs.com/tools/string-sha256-generator), consulter le 21/02/2020

[44] Tiana LAURENCE - La Blockchain pour les Nuls grand format (2018, First Interactive)

[45] Thomas Dupont, a Blockchain : introduction et applications à, Etopia, 09/04/2018

[46] Types d'algorithme de hachage :(https://www.blockchains-expert.com/hachage-cryptographique-le-guide-pour-tout-comprendre), consulter le 22/02/2020

[47] VILLANI, M. Cédric, and M. Gérard LONGUET. "LES ENJEUX TECHNOLOGIQUES DES BLOCKCHAINS (CHAÉNES DE BLOCS)."

[48] Waelbroeck, Patrick. "Les enjeux économiques de la blockchain." Annales des Mines-Réalités industrielles. No. 3. FFE, 2017.

[49] Principe de sha256 (https://www.keycdn.com/support/sha1-vs-sha256)

[50] Définition de l'Architecture MVC (https://www.tutorialspoint.com/mvc_framework/mvc_framework_introduction.htm)

[51] l'Architecture MVC (https://techterms.com/definition/mvc)

[52] Les couches de MVC (https://whatis.techtarget.com/fr/definition/modele-vue-controleur-MVC))

[53] Les avantages de MVC (https://fr.quora.com/Quels-sont-les-avantages-et-inconv%C3%A9nients-du-mod%C3%A8le-MVC))

Table des figures