REPUBLIQUE DU CAMEROUN
Paix-Travail-Patrie
****
MINISTERE DES POSTES ET TELECOMMUNICATIONS
****
ECOLE NATIONALE SUPERIEURE DES POSTES, DES TELECOMMUNICATIONS ET DES TIC
****

REPUBLIC OF CAMEROON
Peace-Work-Fatherland
****
MINISTRY OF POSTS AND TELECOMMUNICATIONS
****
NATIONAL ADVANCED SCHOOL OF POSTS, TELECOMMUNICATIONS AND ICT
****

SUP'PTIC

IMPLEMENTATION DE LA BLOCKCHAIN POUR LA SECURITE ET LA TRACABILITE DES TRANSACTIONS FINANCIERES: CAS DE l'APPLICATION MOBILE « DirectCash » D'ALLIANCE FINANCIAL Sa

Mémoire de fin d'études/Master of Engineering

Présenté et soutenu par NGOUAHA MBIKAKEU Ronald

Matricule : 13T31D33

Option: Sécurité des réseaux et des systèmes

En vue de l'obtention du :

Diplôme de Master 2 en Télécommunications

Sous la supervision

Académique de:

Dr. Georges Bell B

Enseignant à ENSP, Cryptologue.
belltver@yahoo.fr

Professionnelle de:

M. Chrétien TABETSING

Directeur Général d'Alliance Financial.
chretien.tabesting@gmail.com

Dédicace

À MES TRES CHERS PARENTS, M. & MME NGOUAHA

Remerciements

Nous adressons aussi nos remerciements chaleureux :

Au Directeur de SUP'PTIC de Yaoundé, Monsieur **Félix Watching** pour son engagement permanent et sa dévotion inconditionnelle au bon fonctionnement de l'Institution ;

A Monsieur **TABETSING Chrétien** titulaire d'un DEA en informatique et Doctorant en Informatique de l'Université de Paul Sabatier (Sciences) Toulouse en France, Diplômé de l'Ecole Supérieur de Commerce de Toulouse, notre encadreur professionnel, qui nous a accueillis dans son entreprise, d'abord comme stagiaire, ensuite comme collaborateur. Vous n'avez ménagé aucun effort à nous insérer dans votre équipe en nous guidant tous les jours afin de faire de nous, des ingénieurs complets.

Au Docteur **Georges Bell B**, notre encadreur académique ; pour avoir accepté de diriger ce travail malgré ses innombrables obligations, il a su renoncer à une large partie de leur temps pour nous encadrer et nous guider ;

Un tel voyage, aussi solitaire soit-il, n'aurait pas été possible sans le soutien patient et indéfectible de nos proches. Cette aventure fut partagée d'un bout à l'autre avec nos parents papa Joseph et maman Odette, notre chef de famille papa Georges, notre ange gardien et mère maman Josephine, notre oncle papa Florent, notre oncle papa André, notre tante maman Florence qui nous ont apportés le soutien financier, moral, psychologique et logistique. Que notre entourage familial, amical et professionnel, dont les encouragements n'ont jamais fait défaut, soit également remercié ici.

Une pensée particulière aux enseignants de l'école des Postes, toutes nos considérations à ces personnes qui ont participés à faire de ces deux années de Master, une expérience inoubliable.

Je remercie également les rencontres fructueuses avec les collègues d'Alliance Financial SA, ils ont été très ouverts à nos questions, sans oublier de remercier fortement Bakota Yves, Ingénieur Développeur, Elvire Matchum, responsable exploitation de la plateforme;

À nos frères et sœurs pour leur amour, leurs encouragements inconditionnels et leur désir de nous voir aller le plus loin possible;

À tous nos camarades de promotion avec qui nous avons partagé des moments inoubliables ces dernières années ;

À tous ceux qui nous ont encouragés, soutenu et aidé, de près ou de loin, dans l'élaboration de ce projet, trouvent ici nos sincères remerciements et l'expression de notre profonde gratitude.

Nos sincères remerciements

Résumé

La sécurité informatique est devenue une réelle préoccupation pour les entreprises envisageant d'ouvrir sur internet un service en ligne. Des précautions en termes de sécurité ne sont plus à négliger car ces dernières années, les menaces informatiques sont de plus en plus courantes. En effet Alliance Financial Cameroun propose à sa clientèle une gamme de services financiers accessible en ligne par l'intermédiaire d'une application mobile « DirectCash ». Cette application offre la possibilité d'envoyer de l'argent, de payer ses factures d'électricité et d'eau, d'acheter du crédit de communication et de s'interconnecter avec d'autres plateformes de payement mobile à l'instar d'Orange Money et de Mobile Money. Nonobstant toutes les précautions prises pour garantir la sécurité et la traçabilité des transactions financières de ses clients, il en ressort qu'Alliance Financier n'est véritablement pas à l'abri des attaques informatiques qui sont de plus en plus croissantes.

Le présent mémoire propose une solution de sécurité semblable à la blockchain de la crypto-monnaie[1] Bitcoin, afin de maintenir un niveau de sécurité et de traçabilité élevé des transactions financières opérées par les clients d'Alliance Financial. Un audit de sécurité a été réalisé sur l'architecture du système d'information d'Alliance Financial. Cet audit nous a permis de mieux comprendre l'origine du problème à résoudre tout en se conformant aux normes internationales à l'instar de la famille ISO 2700X. Cette analyse a conduit à la conception d'un nouveau système d'information encore plus sécurisé que le précédent afin de juguler ce problème. Le langage UML est alors utilisé pour monter les diagrammes jugés pertinents pour la mise en place de la solution, notamment le diagramme des cas d'utilisation, les diagrammes de séquences, le diagramme des classes, et les diagrammes d'activités.

Le nouveau système d'information comporte d'une part une infrastructure à clef publique utilisée pour la gestion des clefs permettant de chiffrer les transactions et de garantir l'identité de chaque client d'Alliance Financial. D'autre part nous avons doté notre système d'une base de données des transactions financières, distribuée, partagée entre les sites de l'entreprise. L'écriture et la lecture des données sont faites au moyen de procédés cryptographiques complexes afin d'assurer l'intégrité de son contenu.

Nous comptons étendre notre solution en direction d'autres secteurs d'activité comme les banques et les chaines de productions où des données sensibles sont constamment manipulées.

Mots clés : transactions financières, attaques informatiques, blockchain, sécurité, traçabilité.

[1] une monnaie électronique pair à pair et décentralisée dont le code source se base sur les principes de la cryptographie pour valider les transactions et émettre la monnaie elle-même.

Abstract

IT security has become a real concern for companies considering opening a new online service on the Internet. Security precautions should no longer be neglected because in recent years, computer threats have increased and are still increasing further. Indeed, Alliance Financial Cameroon offers its customers a range of financial services accessible online through a mobile application called "DirectCash". This application offers the possibility to send money, pay electricity and water bills, buy communication credit and interconnect with other mobile payment platforms such as Orange Money and Mobile Money. Notwithstanding all the precautions taken to guarantee the security and traceability of its customers' financial transactions, it appears that Alliance Financier is not really immune to computer attacks that are constantly growing every day.

This thesis proposes a security solution similar to the Bitcoin cryptology blockchain to maintain a high level of security and traceability of financial transactions operated by Alliance customers. A security diagnose was carried out on the architecture of Alliance's information system. This diagnose allowed us to better understand the origin of the problem to be solved while complying with international standards such as ISO27001. This analysis led to the design of a new information system that is even more secure than the previous one in order to overcome this problem. The UML language is then used to build the diagrams deemed relevant to the implementation of the solution, namely the utilisation cases' diagram, sequence's diagrams, class' diagram, and activity's diagrams.

The new information system includes a public key infrastructure used for key management to encrypt transactions and guarantee the identity of each Alliance Financial customer. In addition, we have equipped our system with a database of financial transactions, distributed and shared between the company's sites. Data are written and read using complex cryptographic processes to ensure the integrity of its content.

We intend to extend our solution to other sectors of activity such as banks and production chains where sensitive data is constantly manipulated.

Keywords: financial transactions, computer attacks, blockchain, security, traceability.

Sommaire

Table des figures

Liste des tableaux

Glossaire

ART	Agence de Régulation des Télécommunications.
API	Interface de Programmation Applicative
AES	Advanced Encryption Standard
Btc	Bitcoin
CA	Certificate Authority
CAMTEL	Cameroon Telecommunication
DES	Data Encryption Standard
DSA	Digital Signature Algorithm,
EIA	Energy Information Administration
GATT	General Agreement on Tariffs and Trade
Ghz	Giga Hertz
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICP	Infrastructure à Clef Publique
IDEA	International Data Encryption Algorithm
IIS	Internet Information Services
ISMS	Information Security Management System
ISO/IEC	Organization for Standardization / International Electrotechnical Commission
LAN	Local Area Network
MERISE	Méthode d'Etude et de Réalisation Informatique pour les Systèmes d'Entreprise
MD 5, 2, 3	Message Digest 5, 2, 3
MDC	**Modification Detection Code**
MINFI/ DGTCFM	Ministère des Finances du Cameroun: Direction Générale du Trésor, de la Coopération Financière et Monétaire
MIT	Massachusetts Institute of Technology
OCSP	Online Certificate Status Protocol
OMC	Organisation Mondiale du Commerce

P2P	Peer-to-Peer
PKI	Public Key Infrastructure
RC 2, 4, 5	Rivest Cipher 2, 4, 5
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
RSA	Rivest Shamir Adleman
SI	Système d'information
SHA 1, 256	Secure Hash Algorithm 1, 256
SQL	Structured Query Language
SSL/TLS	Secure Sockets Layer/ Transport Layer Security
SWIFT	Society for Worldwide Interbank Financial
TIC	Technologies de l'information et de la communication
TLS par PSK	Transport Layer Security for Pre-Shared Key
TLS par SRP	Transport Layer Security for Secure Remote Password
UML	Unified Modeling Language
WAN	Wilde Area Network
XML	Extensible Markup Language

Introduction générale

Au début des années 1980, Internet servait surtout à relier des chercheurs. À cette époque, la circulation des documents ne posait aucun problème de confidentialité et les données traversaient le réseau en clair [15]. Si, au début, les protocoles Internet n'ont évolué que pour faire face à l'accroissement du nombre d'utilisateurs, l'ouverture du réseau à un usage commercial a modifié les comportements. Comme des informations confidentielles circulent sur les liaisons, la sécurité des communications est devenue une préoccupation importante des utilisateurs et des entreprises. Tous cherchent à se protéger contre une utilisation frauduleuse de leurs données ou contre des intrusions malveillantes dans les systèmes informatiques. La tendance actuelle est de mettre en place des protocoles sécurisés qui luttent contre les usurpations d'identité ou l'espionnage des données privées.

Par ailleurs, une multitude de virus[2] se propagent à l'insu des utilisateurs, principalement dans les fichiers téléchargés. Les virus sont susceptibles de détruire des documents ou même de provoquer la perte totale des informations stockées dans les machines. Les machines des internautes sont également vulnérables à l'infection par des logiciels espions, les spywares[3]. Ces logiciels sont installés sans l'autorisation de l'utilisateur, ce dernier n'ayant aucun moyen de se rendre compte de leur présence. Une fois logés dans une machine, les spywares collectent des informations concernant les habitudes de connexion de l'utilisateur, repèrent les logiciels installés et utilisés sur le poste de travail, recueillent les mots de passe... N'étant pas considérés comme des « codes dangereux », ils ne sont pas détectés par un antivirus classique et doivent être éradiqués par des logiciels spécifiques [16].

D'une manière générale, plus un système d'information est ouvert sur l'extérieur, plus il est vulnérable aux agressions et plus il convient de le protéger. Une politique de sécurisation d'un réseau ou d'une machine combine plusieurs méthodes pour rendre une intrusion très difficile, voire impossible. De nombreux outils sont utilisés pour répondre aux attentes en sécurité pour ces systèmes d'informations: l'utilisation des firewalls était souvent recommandée. Cependant, la présence d'un firewall procure un faux sentiment de sécurité, car il est trop souvent perçu comme la panacée des solutions de sécurité. Or il ne couvre que certains aspects de la protection globale en particulier, celle que nécessite une application web complexe ouverte sur internet. En effet, certaines attaques

[2] Un virus est un automate auto réplicatif à la base non malveillant, mais aujourd'hui souvent additionné de code malveillant (donc classifié comme logiciel malveillant), conçu pour se propager à d'autres ordinateurs en s'insérant dans des logiciels légitimes, appelés « hôtes ».

[3] Un logiciel espion (aussi appelé mouchard ou espiogiciel) est un logiciel malveillant qui s'installe dans un ordinateur ou autre appareil mobile, dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance.

ne peuvent pas être arrêtées par un firewall pour la simple raison qu'elles sont noyées au milieu des requêtes http, qui sont bien sûr autorisées à travers le firewall.

Des avancées en sécurité informatique ont conduit à la mise en place de plusieurs autres outils pouvant contrer les attaques susceptibles d'outrepasser un firewall ; notamment les firewalls applicatifs et des logiciels de protections des applications web de type « reverse-proxy intelligent[4] ». Nonobstant tous ces outils de sécurité implémentés et vu les attaques informatiques qui ne cessent de se perfectionner chaque jour, les applications web n'en demeurent toujours pas à l'abri.

En 2008, Satoshi, la mystérieuse figure derrière la blockchain Bitcoin, trouve un moyen plus efficace pour sécuriser des applications web en optant pour la décentralisation complète des données à traiter. De ce fait, la sécurité dans le processus de traitement de l'information circulant dans le réseau dépend d'un consensus mutuel entre l'ensemble des nœuds de ce réseau. La puissance de calcul de chaque nœud est tellement énorme qu'il serait très difficile, voire impossible qu'une attaque informatique puisse aboutir. C'est à la lumière de cette technologie mise en place par Satoshi que plusieurs autres applications décentralisées vont être créées afin d'assurer une sécurité optimale quant à la manipulation des données au sein d'un réseau.

Nous avons pris comme exemple la blockchain Bitcoin, parce qu'elle offre un moyen sûr pour sécuriser les transactions financières en les inscrivants dans un grand livres qui est partagé par tous les nœuds de son réseau.

La présente étude vise à transformer l'application web d'Alliance Financial, en une application web décentralisée comme celle de la blockchain Bitcoin. En optant pour ce choix, nous aurons la possibilité d'assurer une intégrité et une traçabilité absolue des transactions financières des clients d'Alliance Financial.

La suite de ce document est organisée de la manière suivante :

- Le premier chapitre présente le cadre d'étude, l'état de l'art et les applications basées sur la blockchain. Il pose aussi le problème principal de l'étude et fixe les objectifs poursuivis.
- Le second chapitre présente l'approche méthodologique adoptée et développe l'architecture conceptuelle de la solution proposée. Il présente ensuite les différents outils de conception et de modélisation avant de développer les principaux diagrammes de modélisation du système.
- Le troisième et dernier chapitre expose et commente les principaux résultats obtenus.

[5] Elément essentiel de la sécurisation d'une architecture Web, il sert à la fois de passerelle de sécurité, d'outils de répartition de charge et d'accélération Web

CHAPITRE 1: Contexte, Problématique et Etat de l'art

Dans ce chapitre, nous allons tout d'abord présenter le cadre de notre travail, Alliance Financial Cameroun. Ensuite, nous présenterons les services proposés par Alliance à travers l'application mobile « DirectCash ». Un audit de sécurité sera élaboré conformément à la norme ISO 2700X afin de critiquer les mesures de sécurité implémentées par Alliance pour garantir la sécurité de ses services. Le rapport de cet audit nous indiquera le problème principal de notre étude. Des hypothèses de recherche seront ainsi émises. Ceci nous permettra en outre, de présenter nos objectifs, les résultats attendus et nous ferons enfin un état de l'art sur la blockchain.

1.1 Contexte

1.1.1 Présentation du cadre de travail

1.1.1.1 Historique d'Alliance Financial

Alliance Financial Cameroun est une société anonyme de transfert d'argent, de change de devise et de monétique, agréée par l'arrêté N° 00000086/MINFI/SG/DGTCFM du 17 Avril 201, au capital social de 200.000.000 FCFA. En 2015, Alliance Financial Cameroun, est agréée auprès de l'ART (Agence de Régulation des Télécommunications) afin de proposer à sa clientèle d'autres services à forte valeur ajouté à travers les TIC. Cet agrément lui donne l'autorisation de concevoir des solutions numériques autours du mobile comme moyen pour effectuer ces services de transferts de fonds et, « DirectCash » en est une solution. A partir de cette période, DirectCash est utilisée dans toutes les agences d'Alliance Financial réparties sur le territoire. En 2016, la vulgarisation de l'économie numérique contraint les entreprises IT, à concevoir d'avantage des services numériques et qu'Alliance Financial s'est arrimée à cette nouvelle donne. Ainsi plusieurs autres services ont été intégrés à cette application. En fait, Alliance Financial Cameroun est intégrateur et agrégateur de solutions mobiles ou web visant l'inclusion financière.

1.1.1.2 Présentation du centre de déroulement du stage

Nous avons, lors de notre séjour à **Alliance Financial Cameroun** effectué le stage au centre technique de développement et de pilotage des projets dont l'organigramme est donné par la figure ci-dessous :

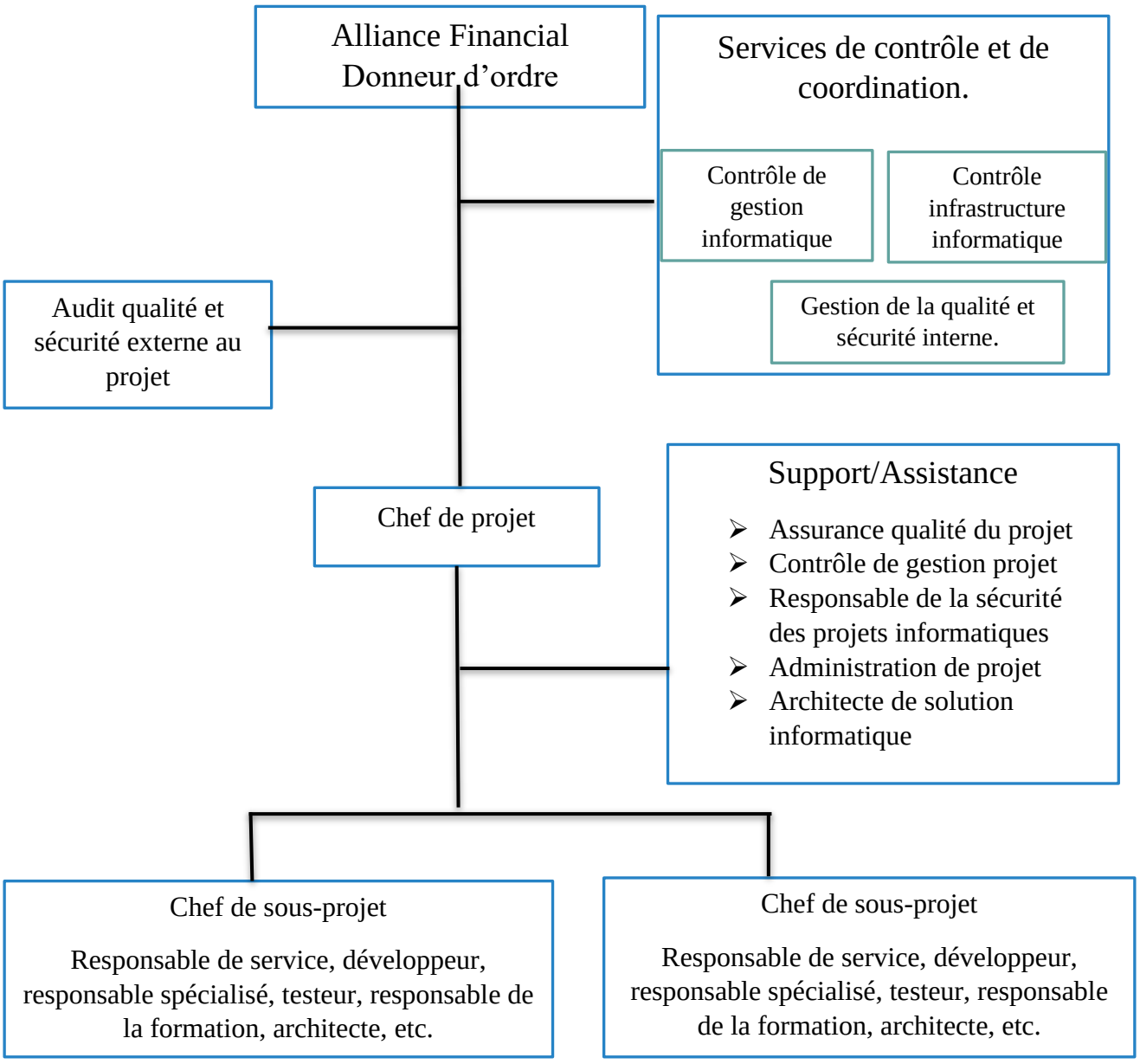


Figure 1: organigramme du centre de déroulement du stage

1.1.1.3 Présentation des services d'Alliance Financial Sa

Les services d'Alliance Financial disponibles au niveau de ses agences sont:

- Le change de devises: le change est une opération qui consiste à convertir une monnaie en une autre monnaie moyennant un coût qui est négocié le jour du change.
- La recharge des cartes visa,
- La vente des cartes visa prépayées,
- Autres services contenus dans son application « DirectCash »

1.1.1.4 Présentation de l'application « DirectCash »

« DirectCash » est une application mobile, offrant les services suivants :

- Le transfert d'argent,
- Le payement de facture d'eau et d'électricité,
- Le réabonnement aux bouquets de télévision Canal+,
- Les opérations de dépôt et de retrait d'argent via Mobile Money (MTN Cameroun) et Orange Money (Orange Cameroun),
- La recharge des cartes visa et Master,
- L'achat du crédit de communication pour tous les opérateurs téléphonique confondus (MTN, Orange, CAMTEL, Yoomee)
- L'achat du crédit de communication pour les autres opérateurs à travers le monde (412 opérateurs au total)

L'utilisation de cette application requière au préalable la création d'un compte, après quoi le client devra ravitailler ce compte-là pour pouvoir bénéficier des services cités plus haut.

1.1.2 Audit de sécurité du système d'informations d'Alliance Financial

La loi n°2010/012 du 21 décembre 2010 relative à la Cyber sécurité et à la Cybercriminalité au Cameroun définit l'audit de sécurité comme un examen méthodique des composantes et des acteurs de la sécurité, de la politique, des mesures, des solutions, des procédures et des moyens mis en œuvre par une organisation, pour sécuriser son environnement et effectuer des contrôles de conformité de son système d'information [8].

1.1.2.1 **Etude des normes d'audit relatives à la sécurité**

L'organisation internationale de normalisation (ISO) a réservé la série ISO/IEC 27000 pour une plage de normes dédiée au pilotage de la sécurité de l'information.

Chaque norme porte sur les aspects spécifiques suivants de la sécurité de l'information :

ISO 27001 : Modèle d'établissement, de mise en œuvre, d'exploitation, de suivi, d'examen, de maintien et d'amélioration de systèmes de gestion de la sécurité de l'information.

ISO 27002 : Liste de centaines de mesures et mécanismes de contrôle susceptibles d'être adoptés suivant les lignes directrices de la norme ISO 27001.

ISO 27003 : Conseils et lignes directrices quant à la mise en œuvre de système de sécurité de l'information, particulièrement en ce qui concerne la boucle d'amélioration continue.

ISO 27004 : Instruments de mesure et indicateurs d'évaluation de la gestion de la sécurité de l'information (publication de la norme à venir).

ISO 27005 : Instrument de définition du processus de gestion des risques du système de gestion de la sécurité de l'information, notamment le relevé des actifs, des menaces et des vulnérabilités (publication de la norme à venir).

ISO 27006 : Lignes directrices à suivre pour accréditer les entités qui offrent le service de certification et d'inscription relativement à un système de gestion de la sécurité de l'information. Les lignes directrices précisent les éléments à observer en plus des exigences stipulées dans la norme ISO 17021.

ISO 27007 : Rentrée très récemment en période d'étude, cette norme va être un guide spécifique pour les audits d'ISMS, notamment en support à l'ISO 27006.

Au Cameroun, la réalisation d'un audit de sécurité informatique est obligatoire et est imposé, selon le décret N°2012/1643/PM, du 14 juin 2012, aux organismes suivants :

- Les opérateurs de réseaux publics de télécommunications et fournisseurs des services de télécommunication et d'Internet,
- Les entreprises dont les réseaux informatiques sont interconnectées à travers des réseaux externes de télécommunication,
- Les entreprises qui procèdent au traitement automatisé des données personnelles de leurs clients dans le cadre de la fourniture de leurs services à travers les réseaux de télécommunications.

De ce point de vue, l'audit de sécurité se présente comme une nécessité, pour répondre à une obligation règlementaire [8]. Pour mener notre mission d'audit, nous utiliserons comme références, les normes ISO 27001 dans sa version 2013 et la norme ISO 27002 dans sa version 2005. Nous tenons à préciser le cadre très restreint de cette mission d'audit, qui nous a permis d'évaluer les problèmes liés à la sécurité et à la traçabilité des transactions financières opérées par les clients d'Alliance Financial par le biais de son application « DirectCash ».

1.1.2.2 Description des systèmes d'information

Tableau 1: Composants du système d'information d'Alliance Financial

Logiciels	
Nom	
Microsoft IIS 8.5 	**Description** : Application d'hébergement des sites web et des services d'Alliance Financial, l'API Rest[5] y est hébergé.
	Environnement de développement : C++
	Développée par /Année : Microsoft /2015
	Nombre d'utilisateurs : Equipe développeurs d'Alliance
	Inclus au périmètre d'audit : Non
SQL Serveur  version 2017	**Description** : serveur de base de données.
	Environnement de développement : C++, C#
	Développée par /Année : Microsoft /2016
	Nombre d'utilisateurs : Equipe développeurs d'Alliance
	Inclus au périmètre d'audit : Oui
Applications	
Nom	
Web Services  API RestFul	**Description** : Interface d'interconnexion utilisant le protocole http pour l'échange de données entre l'application client « DirectCash » et les services d'Alliance Financial
	Environnement de développement : C#
	Développée par /Année : Equipe développeurs d'Alliance/2016
	Nombre d'utilisateurs : tous les clients d'Alliance Financial
	Incluse au périmètre d'audit : Oui
DirectCash 	**Description** : Application mobile utilisée par les clients de l'entreprise et proposant ses services. Elle communique avec le serveur d'Alliance Financial par l'intermédiaire de l'API RestFul.
	Environnement de développement : Java/XML
	Développée par /Année : Equipe développeurs d'Alliance /2016
	Nombre d'utilisateurs : tous les clients d'Alliance Financial
	Incluse au périmètre d'audit : Oui

[5] REST est un style d'architecture logicielle définissant un ensemble de contraintes à utiliser pour créer des services web. Les services web conformes au style d'architecture REST, aussi appelés services web RESTful, établissent une interopérabilité entre les ordinateurs sur Internet.

Serveurs	
Nom	
Host-235-188.mtn.cm 	**Adresse IP** : XXX.XXX.XXX
	Système d'exploitation: Windows server 2012 R2
	Fonctionnalités : contient le serveur de base de donnée SQL server, hébergement des sites et des services d'Alliance via IIS, Firewall Windows applicatif pour le filtrage des ports non autorisés aux utilisateurs externes.
	Propriétés: **Processeur :** intel®Xeon® avec une fréquence de 2.53GHz **Ram** : 16 Giga, **Disque Dur** : SATA 2Tera octet
	Inclus au périmètre d'audit : Oui
Infrastructure Réseau et sécurité	
Aucun	

1.1.2.3 Schéma synoptique de l'architecture du réseau

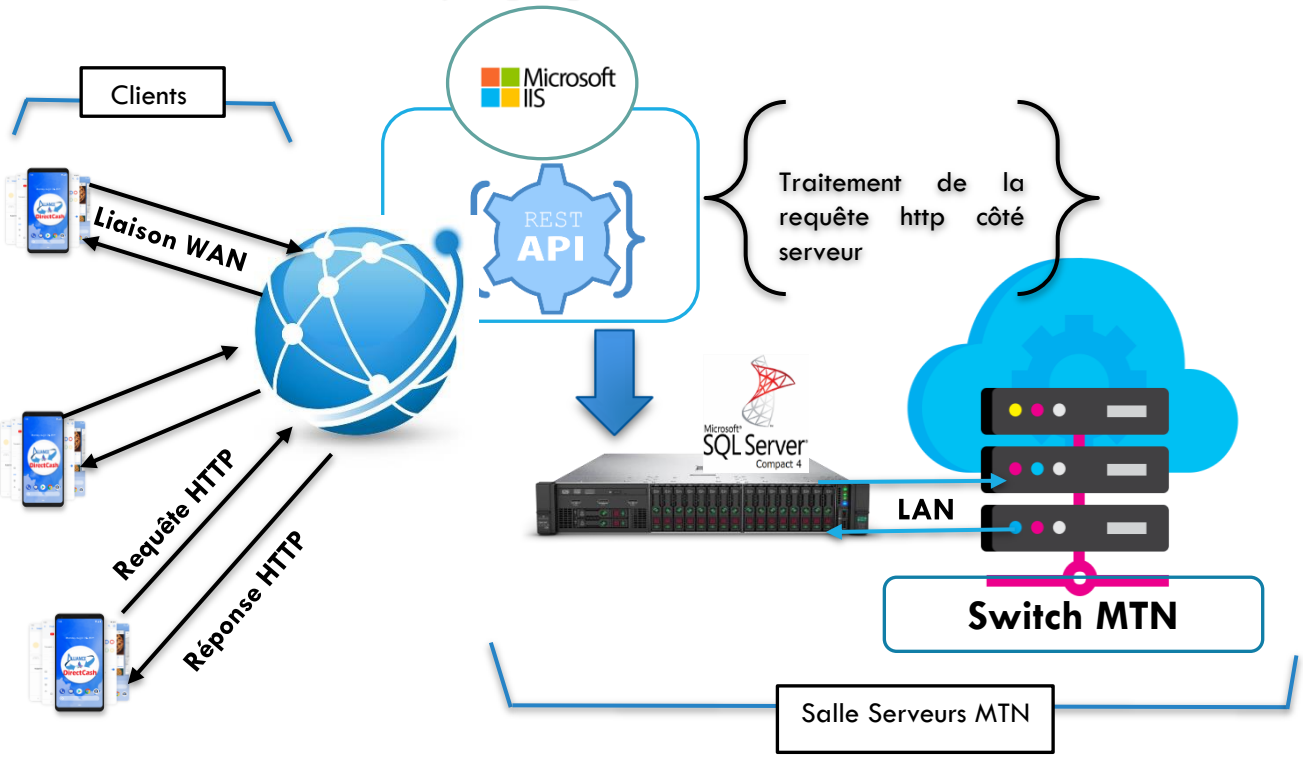


Figure 2: Schéma synoptique du système d'information d'Alliance Financial

1.1.2.4 Présentation détaillée des résultats de l'audit

Tableau 2: Audit de sécurité détaillé sur le système d'information d'Alliance Financial

Domaine	Critères d'audit	Résultats de l'audit (constats)	Appréciation	Description des vérifications effectuées
A.12.3.1 **Sauvegarde des informations**	Des copies de sauvegarde des informations, des logiciels et des images du système doivent être prises et testées régulièrement conformément à une politique de sauvegarde.	**Bonnes pratiques identifiées**		
		1. La sauvegarde des données liées aux services d'Alliance est faite aléatoirement et, aucune procédure de sauvegarde n'est prédéfinie.	Seulement une partie des données pourront être récupérées si le serveur d'Alliance se grille.	Les données sur la consommation des clients sont notées dans un registre et à la demande du directeur général.
		2. Utilisation du système RAID (Redundant Array of Independent Disks) 1-mirroring dans le serveur.	Les données sont stockées simultanément sur deux disques. Un servant de backup	
		Vulnérabilités enregistrées		
		1. Absence des sites de Backup pour la sauvegarde des données.	Les données des clients pourront être divulguées ou être perdues à jamais.	L'entreprise n'a qu'un seul site.
		2. Les sauvegardes sont faites sur les postes de travail personnel des développeurs d'Alliance		

A.14.1.3 **Protéger les échanges de données des services applicatifs.**	Les informations impliquées dans les transactions du service d'application doivent être protégées afin d'évité une transmission incomplète, un mauvais acheminement, une modification non autorisée des messages, une divulgation ou une rediffusion non autorisée des données.	**Bonnes pratiques identifiées** 1. le flux d'informations sur la liaison WAN reliant les clients et le serveur d'Alliance est chiffré.	Cette pratique assure la confidentialité et l'intégrité des données échangées entre l'application Directcash et le serveur d'Alliance.	La connexion entre l'application mobile « DirectCash » et les services d'Alliance se fait via le protocole HTTPS (SSL/TLS).
		Vulnérabilités enregistrées 1. Seul les services d'Alliance ont une configuration SSL/TLS, les clients n'en ont pas pour se connecter à ces services.	Le chiffrement SSL (sans utilisation de certificats clients X.509) ne concerne que la confidentialité, et ne protège pas contre des intrusions.	Dans le code source de l'application « directcash », aucune configuration SSL/TLS n'est faite pour communiquer avec les services d'Alliance.

1.1.2.5 Appréciation des risques liés aux vulnérabilités du système d'Alliance

Référence de la vulnérabilité: Absence des sites de Backup pour la sauvegarde des données relatives aux soldes des comptes et aux transactions des clients.
Scénario de risque : Perte des données de l'entreprise
Composante(s) du SI impactée(s) : Serveur de base de données
Impact(s)/Conséquence(s) d'exploitation des vulnérabilités associées : Alliance perdra toutes les traces sur le solde des comptes de ses clients.
Gravité du risque : Très élevé, Alliance enregistrera d'énormes pertes financières à haute des soldes des clients non connus.
Recommandation : Etablir une politique de sauvegarde permettant de conserver en temps réel les données de l'entreprise sur d'autres sites distant.

Tableau 3: Appréciation des vulnérabilités du système d'information d'Alliance Financial

Référence de la vulnérabilité: l'application « Directcash » ne prévoit pas de certificats SSL client pour l'interconnexion aux services d'Alliance.
Scénario de risque : Accès par une personne non autorisée
Composante(s) du SI impactée(s) : l'API d'interconnexion aux services d'Alliance
Impact(s)/Conséquence(s) d'exploitation des vulnérabilités associées : Usurpation d'identité du serveur ou des clients de l'entreprise par une personne non autorisée.
Complexité d'exploitation de(s)s vulnérabilité(s) : Une tierce personne pourra se faire passer pour Alliance Financial et les clients d'Alliance lui transféreront toutes les informations sur leur compte (Identifiant et mot de passe).
Gravité du risque : élevé, mais qui ne bloque pas les services d'Alliance
Recommandations : **1-** implémenter un système de gestion de clés cryptographiques pour chaque client d'Alliance Financial, **2-** introduire entre les clients et le serveur d'Alliance, un proxy afin de préserver l'identité du serveur.

1.1.2.6 Synthèse des résultats de l'audit

Durant notre mission d'audit, nous nous sommes uniquement intéressés sur les moyens employés par Alliance Financial pour sécuriser les transactions financières de ses clients et ensuite sur la politique de sauvegarde mise en place pour avoir une traçabilité de ces transactions. Il en ressort que les moyens employés pour assurer cette sécurité ne sont pas fiables et donc ne garantissent pas une sécurité optimale. Aussi, à travers la mission d'audit nous avons constaté qu'aucune politique de sauvegarde de données des transactions n'est explicitement définie, de ce fait Alliance n'a pas les moyens d'avoir une traçabilité sans faille de ces transactions. C'est aussi sur la base de se présent rapport d'audit que va s'appuyer notre projet.

1.2 Problématique

1.2.1 Problème

Eu égard de la mission d'audit présenter au paragraphe **1.1.2**, il en ressort que : l'architecture du système d'information élaborée par Alliance Financial Sa n'assure pas une sécurité et une traçabilité des transactions financières de ses clients via son application mobile « DirectCash ».

1.2.2 Question de recherche

Du problème explicité précédemment, une question de recherche se dégage :

Comment peut-on redéfinir l'architecture du système d'information d'Alliance Financial, pour qu'elle puisse répondre aux exigences en sécurité et en traçabilité des transactions financières de ses clients depuis son application « DirectCash » ?

1.2.3 Hypothèse de Recherche

La technologie blockchain, dispose d'un système d'information hautement sécurisé qui permet d'assurer à la fois une sécurité et une traçabilité sans faille des transactions financières. Nous pouvons nous appuyer sur cette technologie pour reconstruire le SI d'Alliance Financial.

1.3 Objectifs

1.3.1 Objectif général

L'objectif général visé par cette étude est d'implémenter un système d'information semblable à celui de la blockchain Bitcoin regroupant des entités qui pourront assurer d'une part la sécurité des transactions financières et d'autre part assurer leur traçabilité.

1.3.2 Objectifs spécifiques

De cet objectif général découlent les objectifs suivants :

- Définir dans un premier temps la nouvelle architecture du SI d'Alliance Financial,
- Implémenter une infrastructure à clé publique (ICP) qui va assurer un contrôle d'accès hautement sécurisé des clients aux services d'Alliance par l'intermédiaire des certificats SSL.
- Concevoir une base de données distribuée et hautement sécurisée qui va regrouper en temps réel les transactions financières des clients.
- Concevoir une application web qui va présenter le contenu de la base de données mentionnée plus haut,
- Concevoir une application web qui va nous permettre de gérer le cycle de vie des certificats SSL délivrés aux clients.

1.3.2 Résultats attendus

À la fin de cette étude,

- ✓ nous comptons présenter la nouvelle architecture du SI d'Alliance,
- ✓ nous aurons une application mobile « DirectCash » intégrant un certificat SSL pour l'interfaçage avec les services d'Alliance,
- ✓ nous aurons une base de données distribuée à accès sécurisé, regroupant les transactions d'Alliance,
- ✓ nous aurons une application web facilitant la gestion du cycle de vie des certificats SSL clients et affichant toutes les transactions financières des clients.

1.4 Etat de l'art

1.4.1 Historique la BlockChain

1.4.1.1 Tiers de confiance, monnaie et propriété

Jusqu'au XVII ème siècle, le modus-operandi est le troc[6], puis les premières pièces de monnaies sont battues au Moyen-Orient et des unités de compte interopérables sont mises en place. Viennent ensuite les monnaies fiduciaires où la valeur est détachée du support physique, et enfin, l'époque que nous connaissons avec la digitalisation des moyens de paiement [12].

Parallèlement, la notion de propriété se développe, portée par les écrits de Rousseau et Locke. La consolidation des États européens favorise la création des premiers registres nationaux, comme le cadastre napoléonien. Ce cadastre répond au besoin d'un document de référence utilisable lors des transactions entre particuliers. Il est adopté car le pouvoir de l'Empire et de son administration le rend «digne de confiance ». Comme le rappelle son étymologie latine, la confiance est le cœur de la monnaie fiduciaire**.** Contrairement à une pièce de métal, la valeur intrinsèque d'un billet de banque est nulle [12]. C'est la confiance dans le fait que sa valeur nominale est partagée par tous qui compte. Pour que cette confiance soit maintenue, les monnaies fiduciaires sont adossées à des institutions (d'abord des villes puis des États et enfin des organisations internationales). C'est la naissance des banques centrales. Un tiers de confiance est alors une condition sine qua non au développement de la monnaie et de la propriété [12].

[6] Le **troc** est l'opération économique par laquelle chaque participant cède la propriété d'un bien (ou un groupe de biens) et reçoit un autre bien. Le troc fait partie du commerce de compensation avec l'échange de services au pair.

1.4.1.2 La virtualisation des transactions

Les modalités de transaction se complexifient et suivent les évolutions de l'économie. Portés par les premiers accords **GATT**[7] de 1947 et l'abandon de l'étalon-or à Bretton-Woods en 1948, le commerce international et la division internationale du travail s'accélèrent tout au long de la deuxième moitié du XXème siècle [12]. L'augmentation des transactions transfrontalières génère une augmentation du risque et, de facto, fait appel à de nouveaux tiers de confiance. C'est le sens de la création du système interbancaire SWIFT[8] en 1977 ou de l'OMC[9] en 1995, par exemple.

La mission de ces tiers de confiance est double : apporter les conditions d'un échange sécurisé, sans risque de perte pour les acteurs économiques (principe d'une chambre de compensation), et fluide. L'échange doit être le moins coûteux et le plus rapide possible.

1.4.1.3 L'Innovation au service de la confiance

Deux innovations vont bouleverser la manière dont la confiance est générée : l'avancée de la cryptographie et les architectures informatiques distribuées**.**

Parallèlement, les architectures distribuées s'imposent comme une référence en termes de stabilité et de sécurité.

Le meilleur exemple de ces caractéristiques est né dans les laboratoires du CERN[10] au début des années 1990: le web (HTML). Réseau ouvert et décentralisé, il a prouvé sa robustesse en ne connaissant aucune rupture majeure depuis plus de 20 ans. En termes de sécurité, le fait qu'aucune attaque informatique ne soit parvenue à mettre à mal l'ensemble des noms de domaines souligne de manière empirique cette robustesse.

Cryptographie et architectures distribuées sont génératrices de confiance ex-nihilo. Elles vont converger pour former la couche technologique du Bitcoin: la Blockchain.

En 2008, Satoshi Nakamoto, la mystérieuse figure derrière l'invention de Bitcoin, publie «*Bitcoin: A Peer-to-Peer Electronic Cash System*» [2]. Il y expose une méthode pour résoudre un problème cryptographique sur lequel aucunes issues n'avaient été trouvées depuis plusieurs décennies, le problème du double paiement et le problème des Généraux Byzantins. Celui-ci empêchait à deux agents d'échanger des actifs, comme une monnaie par exemple, sans le passage par un tiers de confiance. La solution repose sur l'architecture décentralisée qui supporte Bitcoin: la chaine de blocs, ou blockchain.

---

[7] Le General Agreement on Tariffs and Trade (GATT, en français): accord général sur les tarifs douaniers et le commerce) est signé le 30 octobre 1947 par 23 pays, pour harmoniser les politiques douanières des parties signataires.

[8] La Society for Worldwide Interbank Financial Telecommunication.

[9] L'Organisation mondiale du est une organisation internationale qui s'occupe des règles régissant le commerce international entre les pays

[10] L'Organisation européenne pour la recherche nucléaire

Cette découverte est historique dans la mesure où elle autorise ce qui était auparavant impossible : deux agents qui ne se connaissent pas peuvent échanger des actifs sans que la transaction ne soit validée par une autorité centrale.

1.4.2 Présentation de la technologie blockchain

1.4.2.1 Concept et définition

Littéralement, une blockchain désigne une chaine de blocs, des conteneurs numériques sur lesquels sont stockées des informations de toutes natures: transactions, contrats, titres de propriétés, œuvres d'art… L'ensemble de ces blocs forme une base de données semblable aux pages d'un grand livre de comptes. Ce livre des comptes est décentralisé ; c'est-à-dire qu'il n'est pas hébergé par un serveur unique mais par une partie des utilisateurs. Les informations contenues sur les blocs sont protégées par plusieurs procédés cryptographiques innovants si bien qu'il est impossible de les modifier a posteriori.

1.4.2.2 Précisions techniques en partant de l'origine des Blockchains : le Bitcoin

Afin de mieux comprendre le fonctionnement technique de la Blockchain, nous nous intéresserons au système sous-jacent au Bitcoin, expliqué par Satoshi Nakamoto, dans sa publication « Bitcoin : A Peer-to-Peer Electronic Cash System », disponible sur le site www.bitcoin.org [2].

Tout d'abord, le Bitcoin est une crypto-monnaie inventée en 2008, et dont le logiciel open source est publié en 2009. Une monnaie cryptographique, ou crypto monnaie, est une monnaie électronique sur un réseau Peer-to-Peer[11] ou décentralisé (chaque client, appelé nœud, est également un serveur). Afin de sécuriser cette monnaie, le système de transaction repose sur le concept de blockchain, basé en partie sur des procédés de cryptographie.L'intention de Satoshi Nakamoto a été de créer un système de paiement électronique, pouvant se passer de l'intervention des institutions financières. Ils'agissait donc, pour Satoshi Nakamoto de permettre l'utilisation d'une monnaie virtuelle[12], limitant les problématiques liés au traitement des transactions de payements opérées en ligne par l'intermédiaire des institutions :

- Le caractère irréversible des transactions,
- le coût de fonctionnement des institutions financières qui engendre des frais supplémentaires sur le coût des transactions,

[11] Le pair à pair (en anglais *peer-to-peer*, souvent abrégé « P2P ») est un modèle de réseau informatique où chaque entité du réseau est à la fois client et serveur contrairement au modèle client-serveur. Les termes « pair », « nœud », et « utilisateur » sont généralement utilisés pour désigner les entités composant un réseau P2P.

[12] La monnaie virtuelle est une unité de compte n'ayant pas de statut légal, à ce titre ces monnaies ne sont pas régulées par une Banque centrale et ne sont pas délivrées par des établissements financiers

Il propose ainsi un système basé sur des preuves cryptographiques, censées remplacer la confiance accordée aux institutions financières. Ce système a pour objectif de répondre à plusieurs enjeux :

- Une transaction entre deux parties sans tiers de confiance,
- Des vendeurs protégés contre d'éventuelles fraudes grâce à une impossibilité de supprimer ou modifier une transaction,
- Pas de double dépense possible grâce à l'horodatage des transactions.

a- Déroulement des transactions

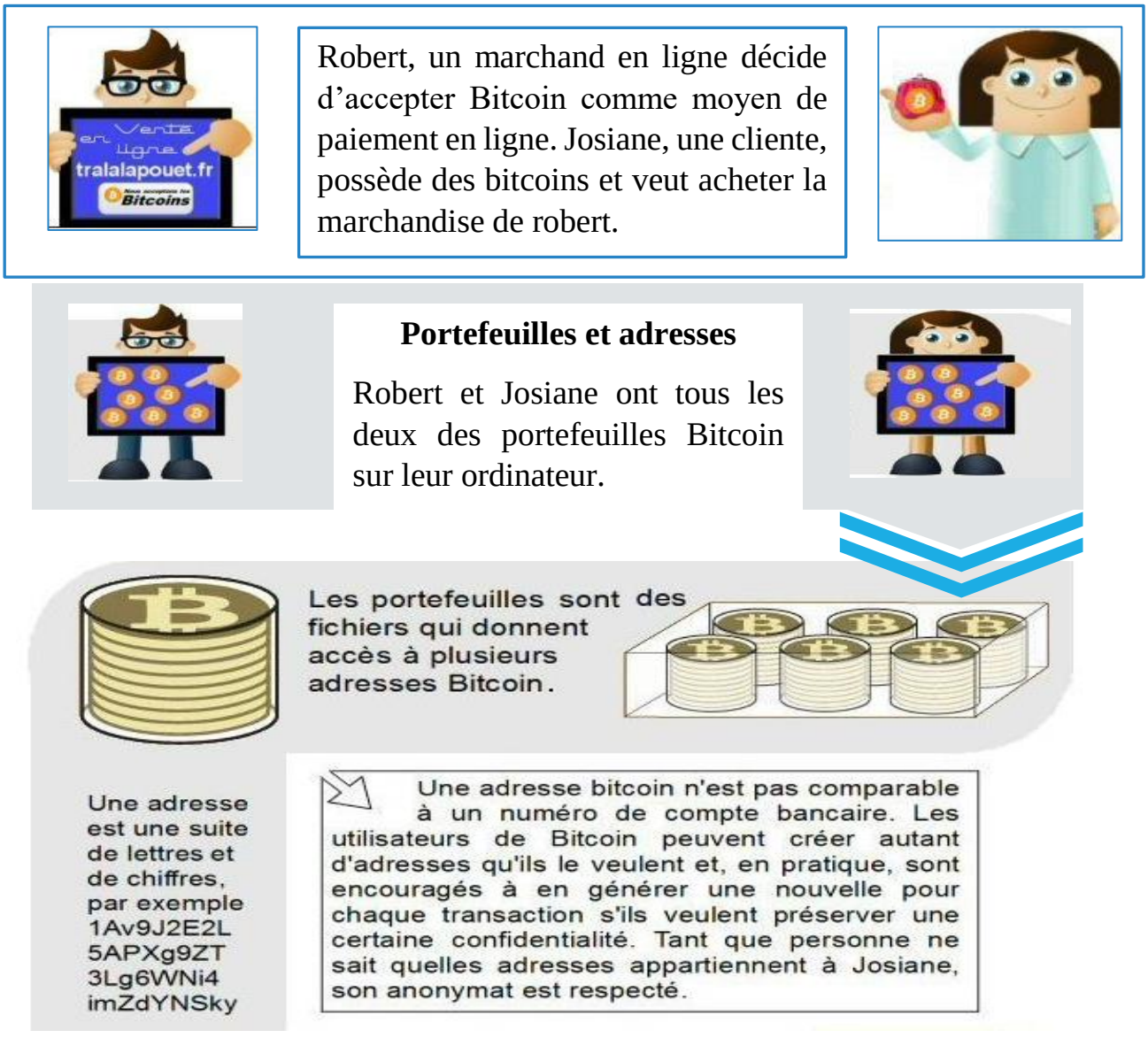


Figure 3: Déroulement des transactions dans la blockchain Bitcoin (étape 1)

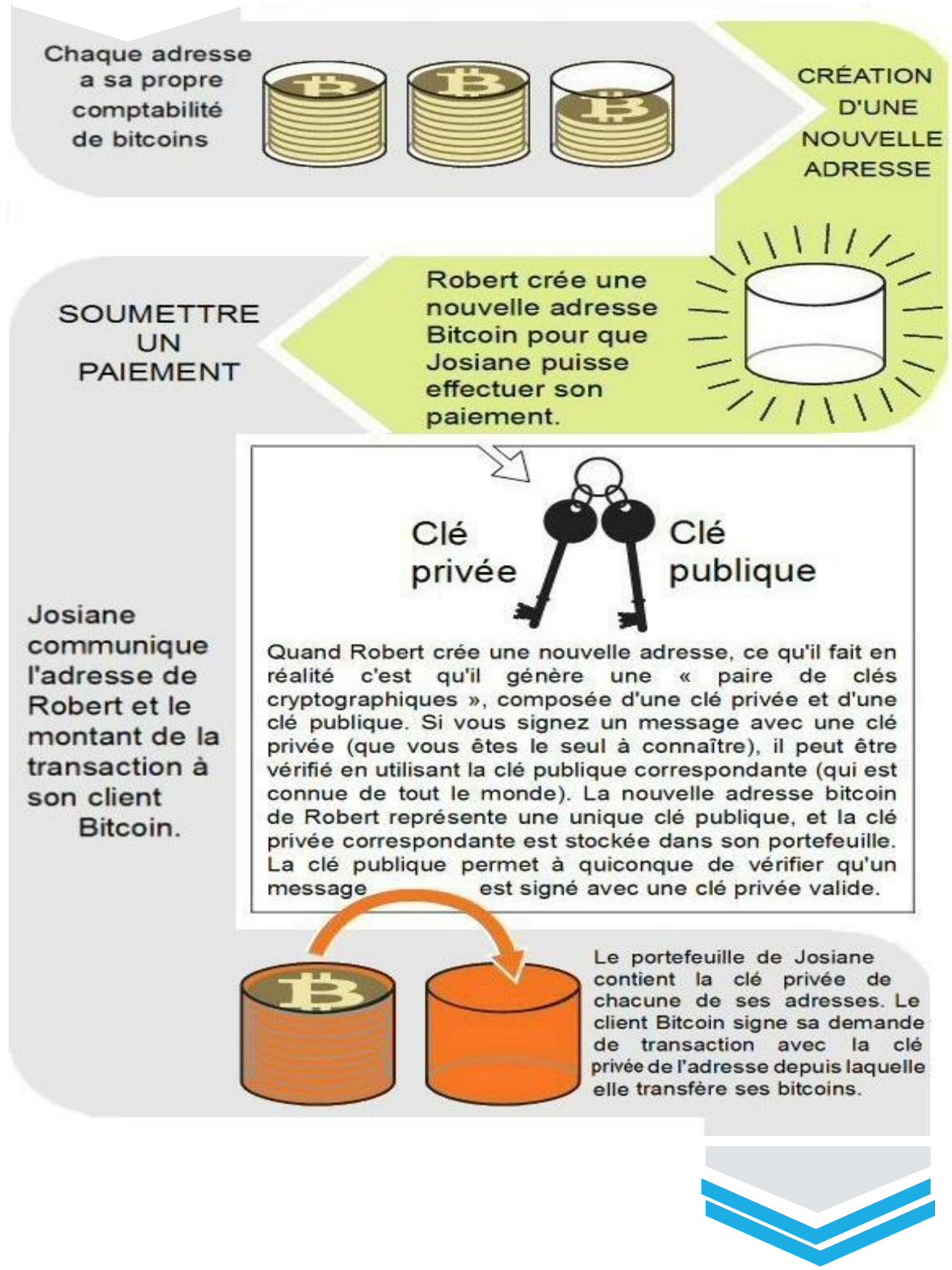


Figure 4 : Déroulement des transactions dans la blockchain Bitcoin (étape 2)

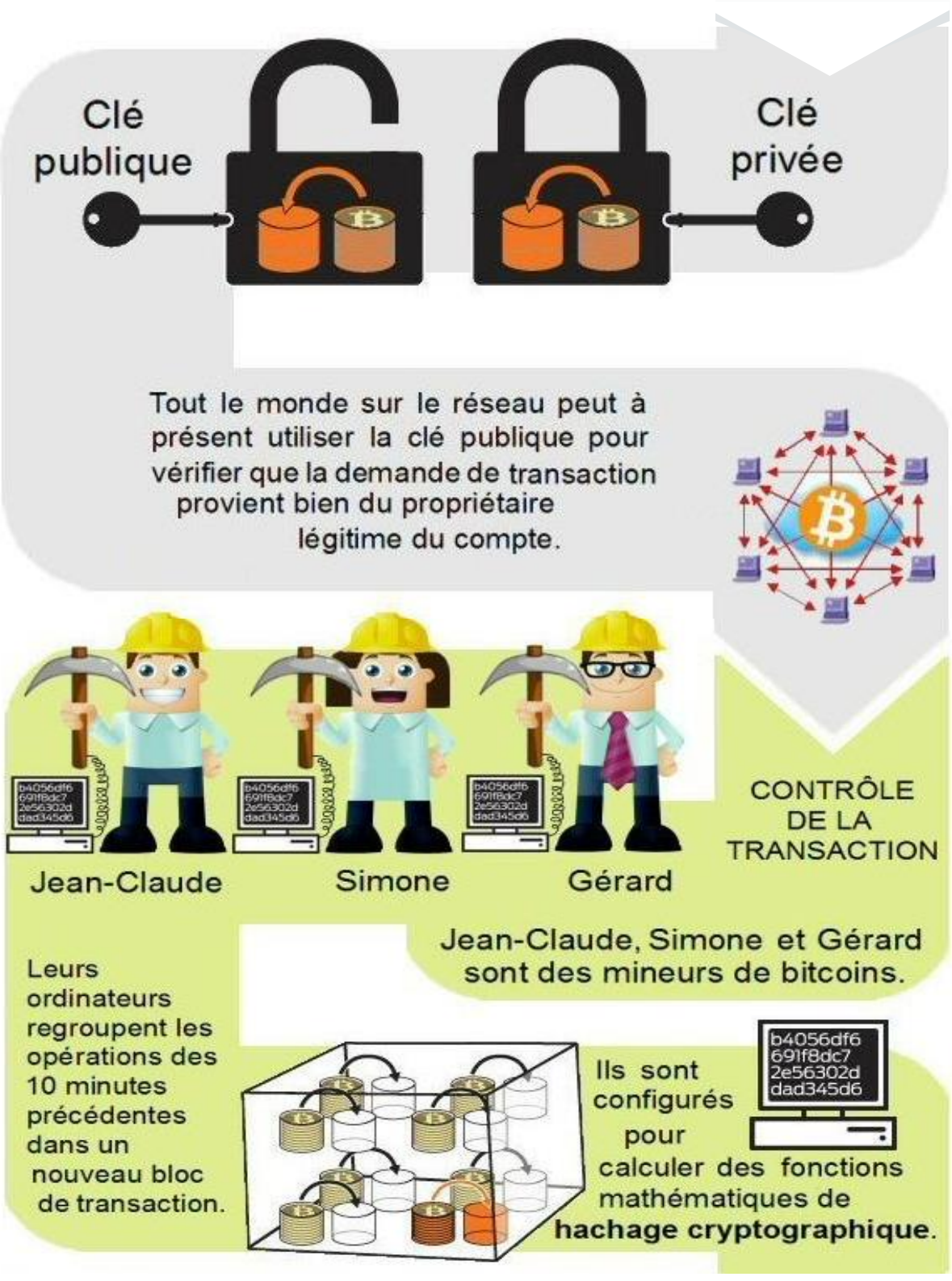


Figure 5: Déroulement des transactions dans la blockchain Bitcoin (étape 3)

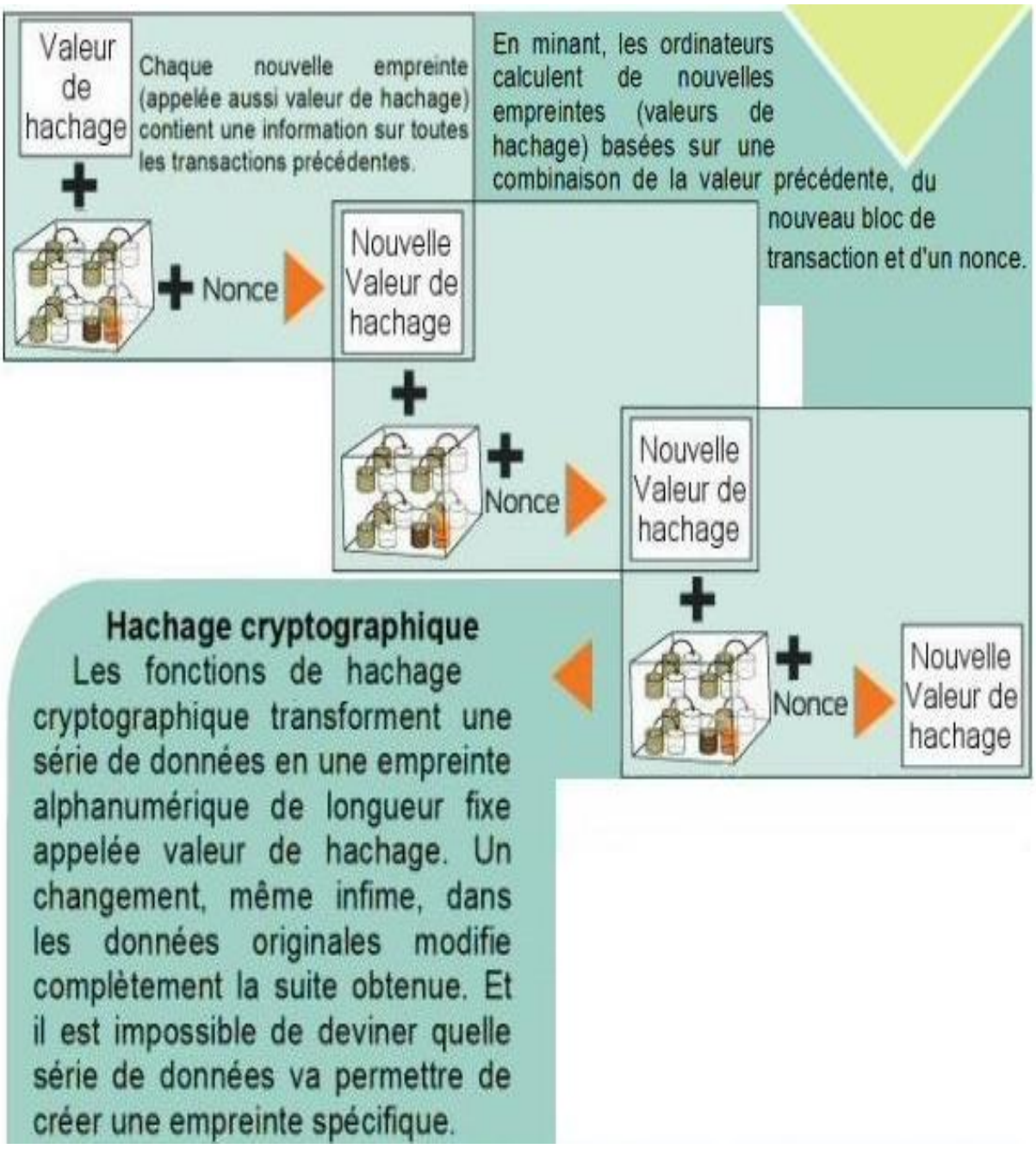


Figure 6: Déroulement des transactions dans la blockchain Bitcoin (étape 4)

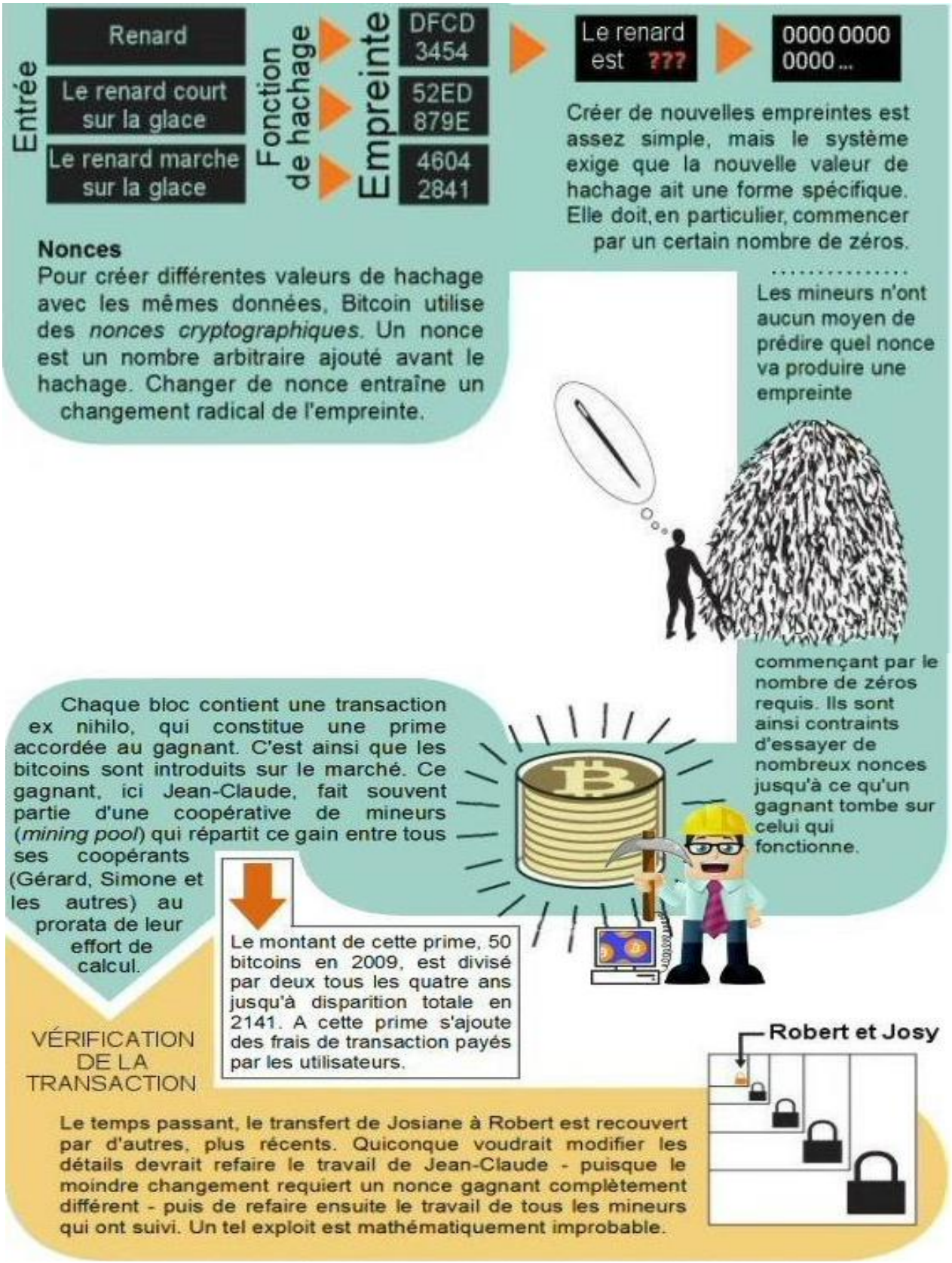


Figure 7: Déroulement des transactions dans la blockchain Bitcoin (étape 5)

b- L'horodatage

La solution imaginée repose donc sur un service d'horodatage. Ce serveur fonctionne de la manière suivante, dans le cas général :

- Le serveur réunit un ensemble d'objets (transactions) et prend l'empreinte (Hash) de cet ensemble
- Il annonce ensuite cette empreinte sous la forme d'un message sur un forum Usenet (système de réseau de forums)
- Chaque horodatage contient l'horodatage précédent, ce qui constitue une chaine de blocs horodatés, d'où le terme de Blockchain

Ainsi, chaque nouvel élément vient confirmer l'élément précédent.

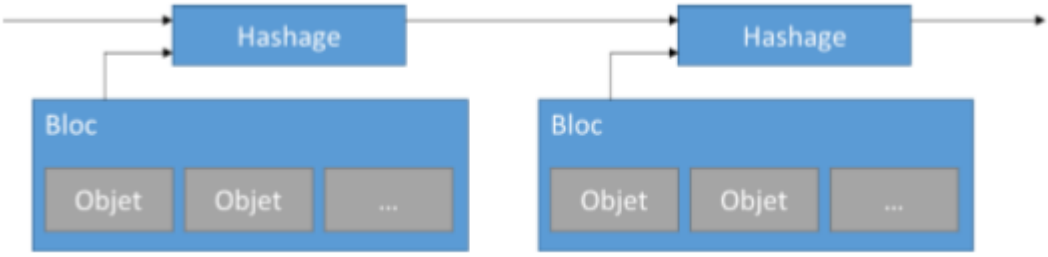


Figure 8: Illustration de l'horodatage

Le principe de l'empreinte (hash) est défini dans le paragraphe suivant. Afin de comprendre le schéma précédent, l'empreinte d'une donnée (un fichier, un dossier, une image, …) est unique. Ainsi, deux blocs avec des transactions identiques, mais qui possèdent des prédécesseurs différents n'ont pas la même empreinte. De même, si deux blocs possèdent les mêmes transactions, mais dans un ordre différent, alors ces deux blocs n'ont pas la même empreinte. Ainsi, une blockchain est identifiable par son empreinte unique.

c- Preuve de travail

Le paragraphe précédent présente le concept de la solution proposée par Satoshi Nakamoto. En réalité, le système (l'ensemble des nœuds du réseau participant à l'élaboration de la blockchain), a besoin d'avoir une preuve de la véracité des informations du bloc qui doit être ajouté. Ceci passe ainsi par le concept de « preuve de travail ».

Afin de créer un serveur d'horodatage dans un système qui est celui imaginé, c'est-à-dire un système reposant sur un réseau peer-to-peer distribué, la preuve donnée par un message sur un forum **Usenet** ne convient pas. Il faut donner une preuve de l'authenticité suffisante d'un bloc**.** La preuve de travail est donc l'algorithme permettant le consensus de l'ensemble des nœuds du réseau sur le bloc qui fait foi.

Ainsi, afin d'être authentifié, une transaction doit être intégrée à un bloc contenant d'autres transactions. La validation de ce bloc est réalisée par le procédé cryptographique appelé **preuve de travail**. Ce procédé a pour but de trouver un double hash en **SHA-256** correspondant au bloc en cours, à partir du bloc qui le précède. Un hash correspond à l'identité, appelée également empreinte d'un fichier. Un bloc possède donc un unique hash. **SHA-256** est une fonction qui, à chaque donnée, associe un unique nombre, qui est l'identité de ces données. Le moindre bit modifié dans les données de départ change le résultat de la fonction **SHA-256**.

Ainsi, afin d'ajouter un nouveau bloc à la chaîne de blocs, les nœuds participant à la création de la chaîne (les mineurs) doivent lancer un procédé cryptographique : le calcul du hash du bloc. Ce procédé a pour but de convertir des données en une suite pseudo-aléatoire de chiffres. Il est impossible de modifier les données en entrée de l'algorithme pour obtenir un résultat précis. Ceci est dû au caractère aléatoire de l'algorithme.

Dans l'exemple suivant, la complexité (nombre de zéros en début de hash requis pour attribuer un hash à un nouveau bloc) est de 10. L'encadré ci-dessous montre l'activité des mineurs pour l'ajout d'un bloc sur la blockchain.

Ainsi l'algorithme proposé est le suivant :
1) Calcul de :
$fonction\ hash\ (Bloc + infos\ mineur + hash\ bloc\ précédent + \mathbf{nbre\ aléatoire\ 1}) < C$
Avec C : la valeur dépendant de la complexité. Par exemple, si la complexité est de 10, il faudra trouver un h inférieur à 0000000000fffffffffffffffffffffffffffffffffffffffffffffffffffffff. Le calcul s'effectue en hexadécimal (base 16), c'est-à-dire en une base allant de 0 à f. La fonction hash est aléatoire, ainsi la seule méthode de résolution de cette inéquation est de recommencer le calcul jusqu'à trouver la solution.
2) Recommencer le calcul de l'inégalité précédente en modifiant uniquement le nombre aléatoire, tant que la condition n'est pas réalisée
3) Lorsqu'une solution est trouvée, le bloc ainsi formé peut être envoyé à tous les nœuds du réseau

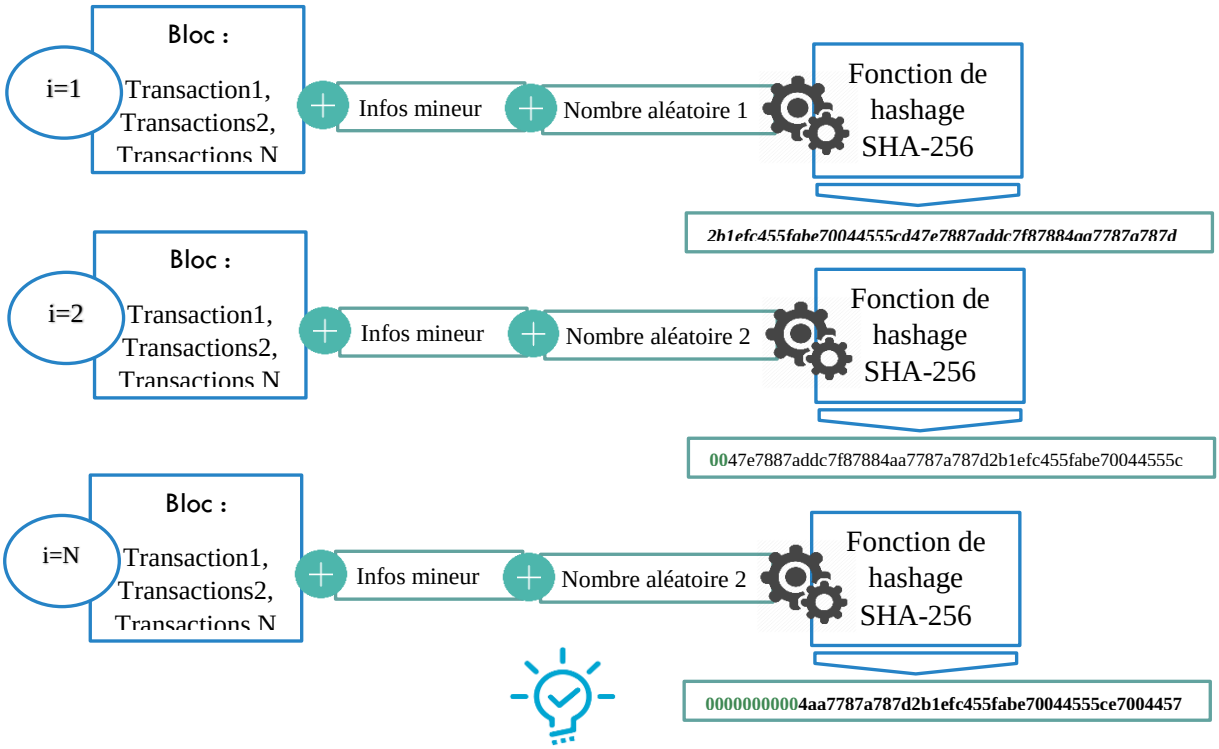


Figure 9: Réalisation de la preuve de travail trouvée en N essais

Afin d'arriver au nombre de zéros requis, le mineur doit réaliser un certain nombre de fois le calcul du hash de la combinaison bloc + informations liées au mineur + nombre aléatoire correspondant à l'essai. Une fois que le résultat donne le hash avec la difficulté requise, le mineur qui a réussi l'opération envoie cette information au réseau distribué.

Si plusieurs mineurs arrivent à un résultat à un temps très proche, une nouvelle branche pourra être créée :

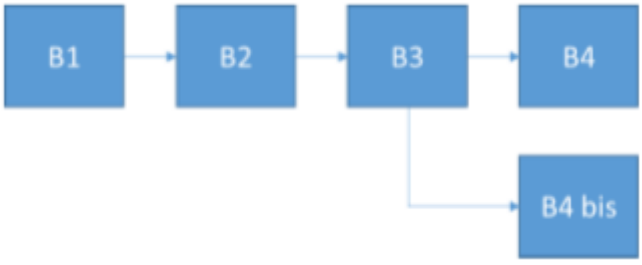


Figure 10: Exemple d'une nouvelle branche pour la chaîne

Lorsqu'il y a un bloc supplémentaire sur une branche plutôt qu'une autre, alors la branche secondaire est abandonnée, et seule la branche principale prévaut.

La récompense délivrée aux mineurs était de 50 Bitcoins (btc) par bloc miné initialement (en 2008) [2]. En 2012, la rémunération a été divisée par 2, soit 25 btc par bloc miné.

Tous les 210 000 blocs minés (soit environ 4 ans), la rémunération est divisée par 2. Ainsi, le minage rapportera de moins en moins de btc et les frais de transaction seront le principal moyen de pouvoir générer de nouveaux Bitcoins.

Le graphique ci-dessous représente le nombre de bitcoins créés en fonction du temps. On remarque notamment que la quasi-totalité des bitcoins sera créée avant 2040, soit environ 21 000 000 de bitcoins.

$$\sum_{n=0}^{\infty} \frac{210000 \times 50}{2^n} = 210000 \times 50 \times \frac{1}{1-\frac{1}{2}} = 21000000$$

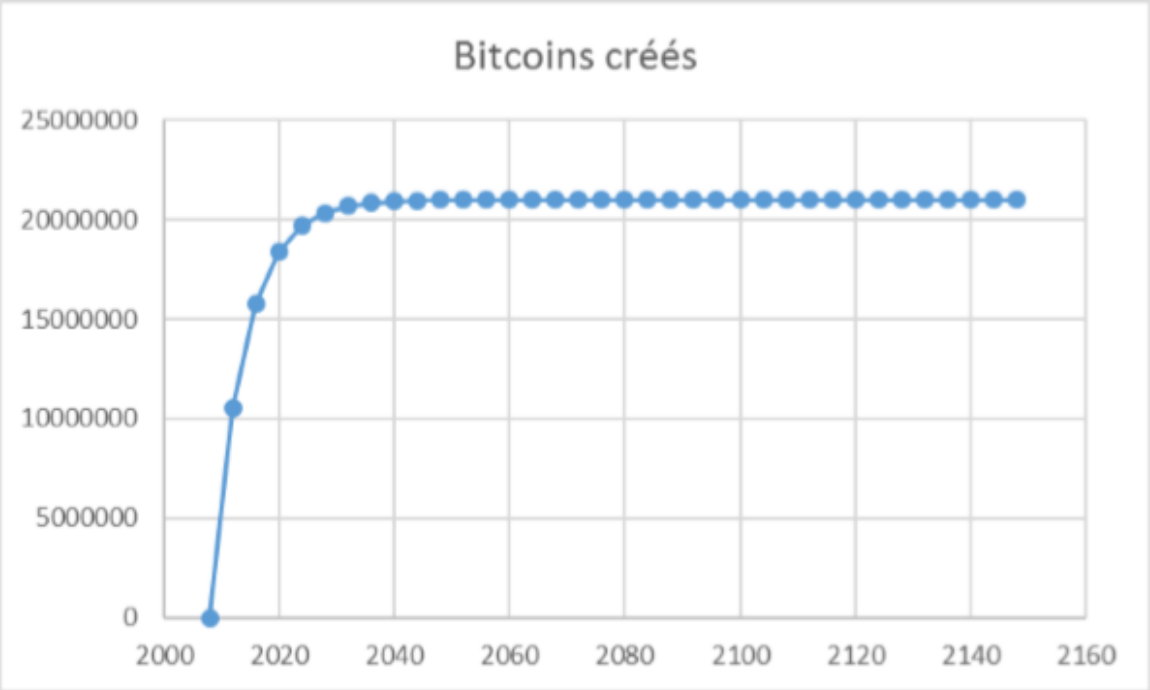


Figure 11: Courbe d'évolution du nombre total de Bitcoin

d- Les types de blockchain

Le concept originel de la blockchain incluait une validation prenant en compte l'ensemble des nœuds du réseau. Entre autres, la blockchain elle-même, ainsi que la validation des blocs qui la constituent, s'effectuait de manière totalement partagée, et donc publique.

Certaines institutions, intéressées par cette nouvelle technologie, ont cependant été méfiantes quant au caractère public proposé par la blockchain à son état d'origine.

De nouveaux concepts ont ainsi émergé, suite à ce besoin identifié. Il s'agit des blockchains « privées », ou « de consortium ». Une blockchain de consortium est une blockchain qui se base sur un procédé de validation des blocs qui est restreint à un certain nombre de nœuds définis. La capacité de lire l'ensemble de la blockchain peut être réservée à certains nœuds particulier, la consultation sera donc privée ; elle peut être aussi disponible pour l'ensemble des nœuds, auquel cas la consultation de la blockchain est publique.

La blockchain peut également être séparée en plusieurs parties : certaines données peuvent être consultées publiquement, tandis que d'autres ne sont disponible que sur un réseau privé, la consultation est, dans ce dernier cas, hybride.

Une blockchain privée, quant à elle, réserve le processus de validation à un acteur unique, les consultations pouvant être privées, publiques, ou hybrides

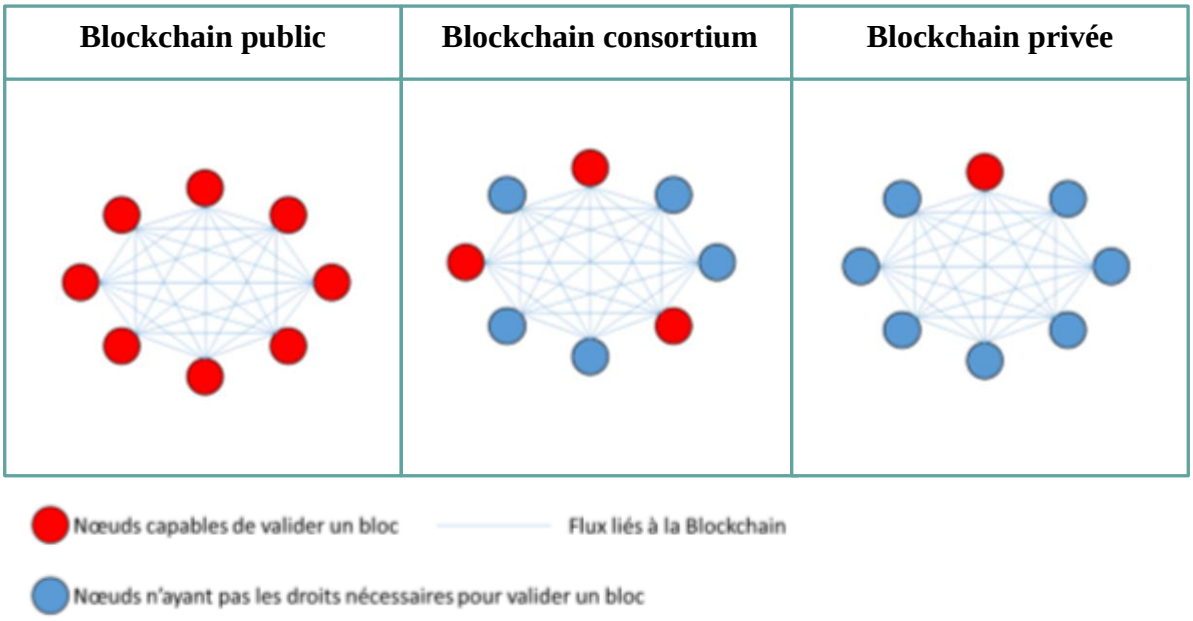


Figure 12: Types de blockchain selon le mode de validation de blocs

1.4.3 Les limites de la blockchain

S'agissant des blockchains publiques, elles présentent de multiples limites, tant dans l'aspect technique que dans l'esprit qui les anime. L'absence de toute gouvernance centralisée est un vrai frein au déploiement de tels systèmes sur certains secteurs qui posent également des questions de souveraineté et de protection des utilisateurs. D'un point de vue technique, le coût énergétique et la fiabilité des blockchains publique apparaissent comme de réelles limites, tout comme certaines caractéristiques techniques actuelles (temps de latence, volume de transactions, etc).

1.4.3.1 Coût du système et consommation énergétique élevée

Du fait du mécanisme de preuve de travaille, bitcoin apparait aujourd'hui comme un gouffre énergétique. Pour rappel, ce mécanisme de consensus consiste à appliquer une fonction de hachage à un bloc auquel on ajoute un nonce[13], et ce de manière répétée afin de trouver le nonce qui permettra d'obtenir un hash respectant une certaine propriété mathématique. Concrètement, il s'agit de faire fonctionner un processus en continu pour lui faire calculer des hash jusqu'à parvenir à valider un bloc. Ce travail a un coût, car faire tourner des processus est un procédé gourmand en énergie. En effet, les hashs calculés ne présentent, en eux-mêmes, aucun intérêt mais ne servent qu'à prouver, dans un sens, que le mineur est prêt à dépenser de l'énergie et en payer le coût pour parvenir à valider un bloc.

Certains sites ont proposé diverses estimations de la consommation en électricité nécessaire pour faire fonctionner la blockchain bitcoin. Citons par exemple le calcul par le site de bitcoin.fr [4] qui estime la consommation de bitcoin entre 2,15 et 5,4 milliards de kilowattheures par an, soit une puissance comprise entre 0,25 et 0,62 gigawatts. A titre de comparaison, si l'on se réfère aux données fournies par l'EIA (Energy Information Administration), quant à la consommation d'électricité en 2014, une consommation de 2,15 milliards de kilowattheures est équivalente à la consommation électrique totale du Gabon, alors que le Honduras a une consommation proche des 5,3 milliards. Le calcul de la consommation électrique du minage sur bitcoin est fondé sur trois valeurs : la consommation du matériel de minage, sa puissance de calcul et le nombre de hashs calculés sur le réseau bitcoin, estimé à environ deux millions cinq cent mille terahashs par seconde [5]. Le calcul prend en compte deux matériels de minage différents : le AntMiner S7, qui consomme dix watts pour une puissance de calcul de 4.86 terahashs par seconde ; et le AntMiner S9, qui consomme 1375 watts pour une puissance de calcul de quatorze terahashs par seconde. On peut donc estimer la puissance totale requise par chacune des deux machines pour effectuer la totalité des calculs sur le réseau de bitcoin.

[13] en cryptographie, un nonce est un nombre aléatoire destiné à être utilisé au trop une seule fois

1.4.3.2 Limites techniques

Si l'on se concentre plus spécifiquement sur bitcoin, qui demeure la blockchain réalisant le plus de transactions, on observe également une limite technique majeure :

- le temps de latence pour valider les transactions.

Un bloc étant validé en moyenne toutes les dix minutes, cela représente le temps minimal à attendre avant qu'une transaction que l'on vient de réaliser soit écrite sur la blockchain. Pour autant, il est recommandé d'attendre environ une heure, afin que cinq à six blocs aient été validés, rendant le facto quasiment impossible qu'une chaîne plus longue se développe et devienne la chaîne principale au risque d'invalider la transaction. Cependant, un temps de latence d'une heure avant d'être assuré qu'une transaction a été passée est une vraie limitation technique. Ceci n'est pas un frein au développement de systèmes d'échanges impliquant de grosses transactions, mais il paraît difficile d'envisager faire du paiement à grande échelle ou du micro paiement avec un tel temps de validation.

- La gestion des clés privées.

Toujours en prenant comme référence le bitcoin, chaque portefeuille virtuel appartenant aux participants de la technologie est sécurisé par un couple de clé privée et publique. La clé publique est connue de tous, alors que la clé privée est uniquement détenue par le détenteur du portefeuille de sorte que seule cette clé permet l'utilisation des fonds stockés. Ceci implique que la perte de la clé privée entraine la perte de l'intégralité des fonds en bitcoins. Aucun système de recouvrement au niveau de cette blockchain n'a était mis en place pour favoriser la récupération des clés perdues.

1.4.4 Autres applications de la blockchain

Les applications de la blockchain ne sont pas limitées aux cryptomonnaies. Deux grands domaines d'application pressentis sont la gestion de l'identité et la gestion d'une supply-chain. Pour la gestion d'identité, nous pouvons citer par exemple :

- **Dock.io**, qui est une plateforme permettant de centraliser les différents profils d'un utilisateur sur les plateformes professionnelles comme linkedIn dans un profil unique adossé à la blockchain ethereum.
- **Everledger** est une blockchain privée, de la galaxie hypedger, assurant la traçabilité des diamants.

En effet, Everledger propose une blockchain, Diamond Time-lapse, permettant de suivre les diamants tout au long de leur parcours depuis la mine jusqu'en bijouterie. Elle est basée sur la technologie hyperledger d'IBM. Elle appartient donc à la galaxie des blockchains privées. Lorsqu'un utilisateur veut connaître la provenance d'un diamant, il entre son identifiant et obtient ainsi tout son parcours détaillant sa mine d'origine, l'ensemble des artisans l'ayant manipulé à chaque étape de la fabrication ainsi que ses

différentes caractéristiques après chaque étape (poids, couleur, type de coupe, pureté et taille).

1.4.5 Les spécificités du projet par rapport aux solutions existantes

Dans les paragraphes précédents, nous avons présenté la technologie de blockchain de référence (Bitcoin) tout en mettant en exergue ses avantages et ses inconvénients. Comme inconvénients, nous avons noté une gabegie énergivore pour la consommation électrique, un temps de latence élevé pour la validation des transactions, et une mauvaise gestion des clefs ayant comme impacte la perte des fonds en Bitcoin. Eu égard de ces différentes limites, la solution que nous comptons mettre en place comportera : un serveur de clefs qui va faciliter la gestion des clefs des clients d'Alliance Financial, un temps de latence relativement très élevé pour le traitement des transactions, et une consommation d'énergie très basse.

1.5 Conclusion chapitre

Dans ce chapitre, il a été question pour nous de présenter dans un premier temps notre cadre de travail. Ensuite nous avons présenté les services proposés par Alliance Financial. Nous avons après ciblé le problème principal de notre étude afin de proposer la solution idéale à concevoir. Une étude des solutions existantes nous a permis de comprendre la difficulté de la solution à concevoir car celle-ci devra se distinguer des autres. Cette solution est donc une blockchain, caractérisée par un temps de latence très bas pour le traitement des transactions financières, une gestion efficace des clefs et une consommation en énergie très basse. Cette solution sera donc modélisée dans le chapitre qui suit.

CHAPITRE 2: Méthodologie

Notre thème est centré sur deux aspects : la sécurité et la traçabilité des transactions financières des clients d'Alliance. De ce fait, il convient de modéliser succinctement la solution indiquée pour répondre au problème de sécurité, puis celle indiquée pour résoudre les problèmes de traçabilité. Dans un premier temps, nous allons modéliser l'Infrastructures de Gestion de Clefs (ICP) qui sera la solution aux problèmes de sécurité et dans un deuxième temps, nous allons modéliser la blockchain qui va répondre aux besoins en termes de traçabilité des transactions financières.

2.1 Modélisation de l'Infrastructures à clé publique (ICP)

2.1.1 Analyse de l'existant

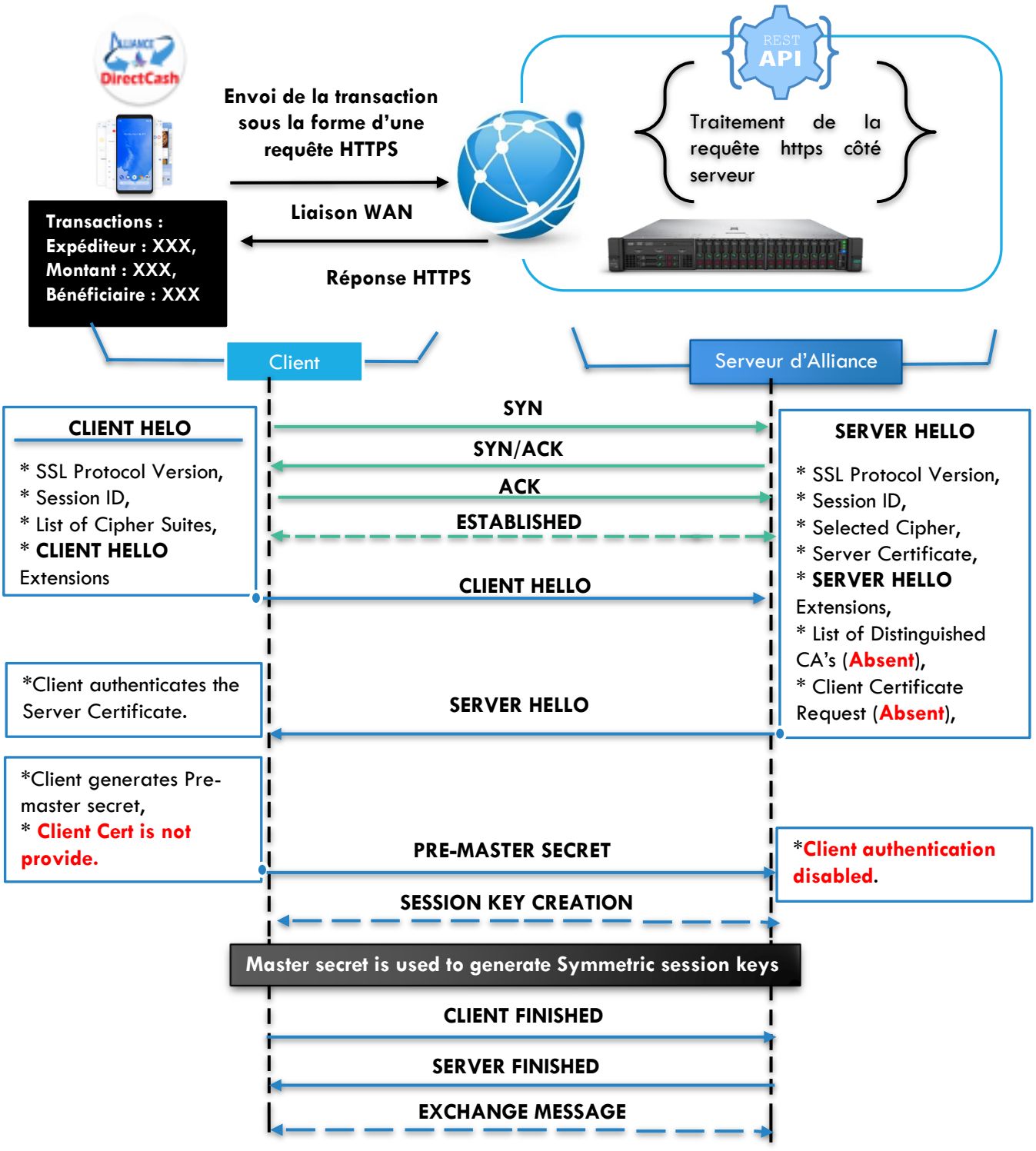


Figure 13: Illustration de la faille de sécurité pour l'authentification des cleints dans le protocole HTTPS

Observations et interprétations :

La demande d'authentification des clients via leur certificat SSL n'est pas activée au niveau du serveur. Cette configuration est donc vulnérable à l'attaque de « **l'homme du milieu** » (man in the middle) [13]. En effet, il suffit que le serveur intercepteur possède lui aussi un certificat serveur et que le client clique sur « Accepter » lorsque son navigateur lui propose d'utiliser ce certificat pour dialoguer avec le serveur distant légitime. C'est ce que fera tout utilisateur qui n'a aucune connaissance de ce problème de sécurité. Il ne reste plus qu'au serveur intercepteur de déchiffrer d'un côté et rechiffrer de l'autre, à la volée.

Le seul moyen de se prémunir contre ce type d'attaque est d'imposer une authentification du côté client par l'utilisation de certificats clients **X.509**. Le serveur intercepteur ne pourra alors plus se faire passer pour le client auprès du serveur distant légitime car il ne dispose pas de la clé privée du client. L'attribution dudit certificat au client, exige la mise en place d'une infrastructure à clé publique.

A titre de rappel, une infrastructure à clé publique *(ICP)* est un ensemble de rôles, de politiques et de procédures nécessaires pour créer, gérer, distribuer, utiliser, stocker, révoquer des certificats numériques et gérer le chiffrement à clé publique.

En cryptographie, une ICP est un arrangement qui lie les clés publiques aux identités respectives des entités (comme les personnes et les organisations). La liaison est établie par un processus d'enregistrement et de délivrance de certificats auprès d'une autorité de certification (AC) et par celle-ci. Selon le niveau d'assurance de cette liaison, celle-ci peut être réalisée par un processus automatisé ou sous supervision humaine [13].

2.1.2 Architecture des composants de la PKI

Notre PKI contient plusieurs composants essentiels à son bon fonctionnement.

Une Autorité d'enregistrement : (Registration Authority - RA) Son principal rôle est de vérifier la demande d'enregistrement (*Certificate Signing Request - CSR*) d'un nouvel utilisateur dans l'infrastructure.

Une Autorité de Certification : (Certificate Authority - CA) Son principal rôle est de générer un certificat pour l'utilisateur. Le certificat contiendra des informations personnelles sur l'utilisateur mais surtout sa clef publique et la date de validité. L'autorité de certification signera ce certificat avec sa clef privée, ainsi ce certificat sera certifié authentique par lui-même.

Un Annuaire : Son rôle est de stocker les certificats révoqués et par la même occasion, les certificats en cours de validité afin d'avoir un accès rapide à ces certificats. De plus, l'annuaire peut stocker les clefs privées des utilisateurs dans le cadre du recouvrement de clef. Sachant que les certificats sont largement distribués, l'annuaire est une solution pour les mettre à disposition.

Un serveur OCSP (Online Certificate Status Protocol) : En effet, les autorités de certification doivent constamment mettre à jour leurs listes de certificat en cours de validité et les utilisateurs doivent constamment interroger l'autorité de certification pour vérifier la validité d'un certificat. Si les demandes ne sont pas synchronisées, alors un certificat révoqué pourra être considéré comme valide. **OCSP** est considéré comme un répondeur afin de connaître les listes de révocation. C'est pourquoi, la liste de révocation de la PKI est le seul élément devant disposer d'un service d'annuaire obligatoirement connecté à Internet.

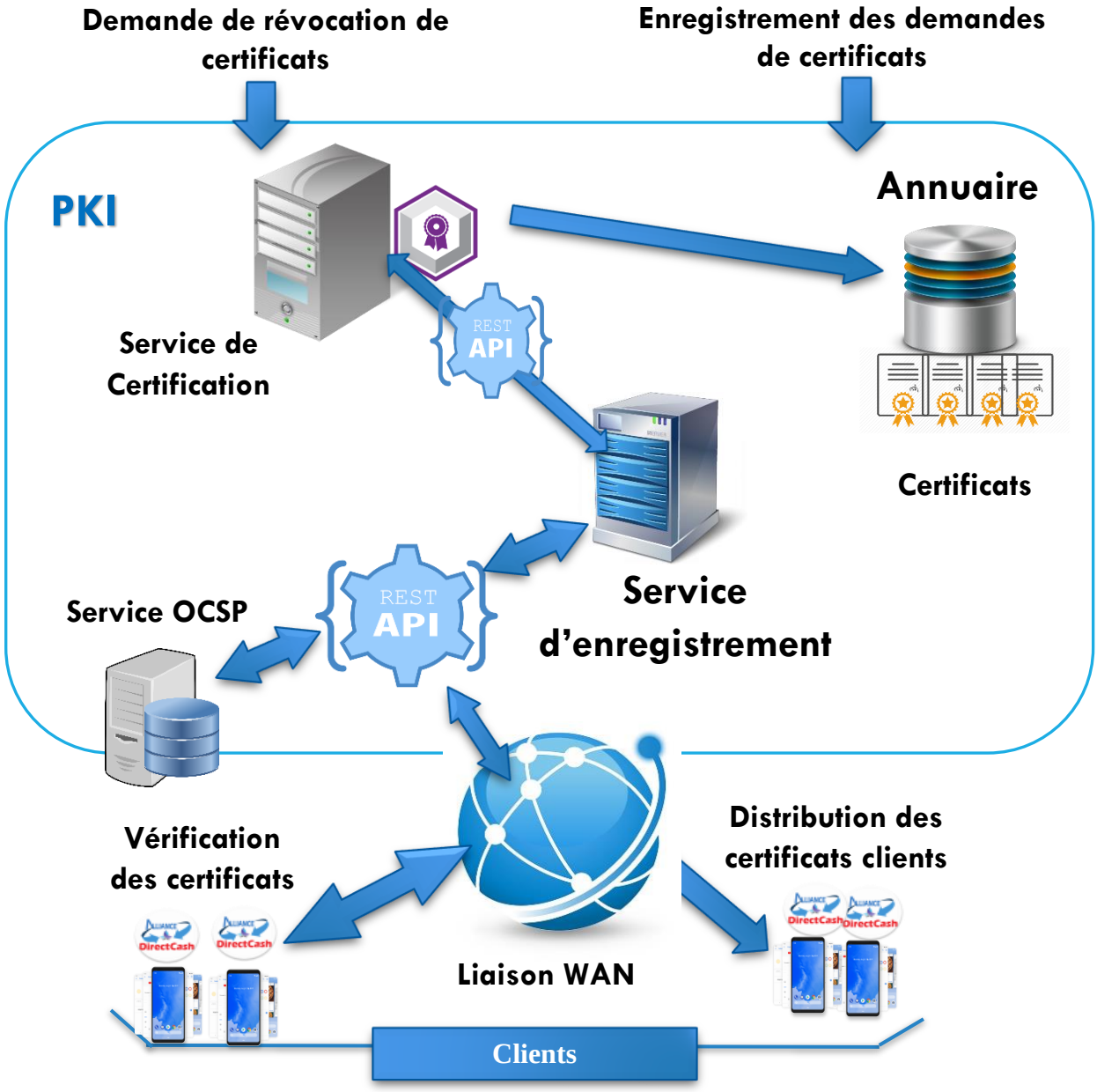


Figure 14: Architecture des composants de l'infrastructure à clef publique

2.1.3 Le modèle de confiance de la PKI

Il existe plusieurs modèles pour structurer les autorités de certifications : Le modèle hiérarchique, le modèle Peer-to-Peer[14], le modèle Bridge[15] [14]. Notre choix a été porté sur le **modèle hiérarchique** pour ça simplicité de mise en œuvre par rapport aux autres modèles.

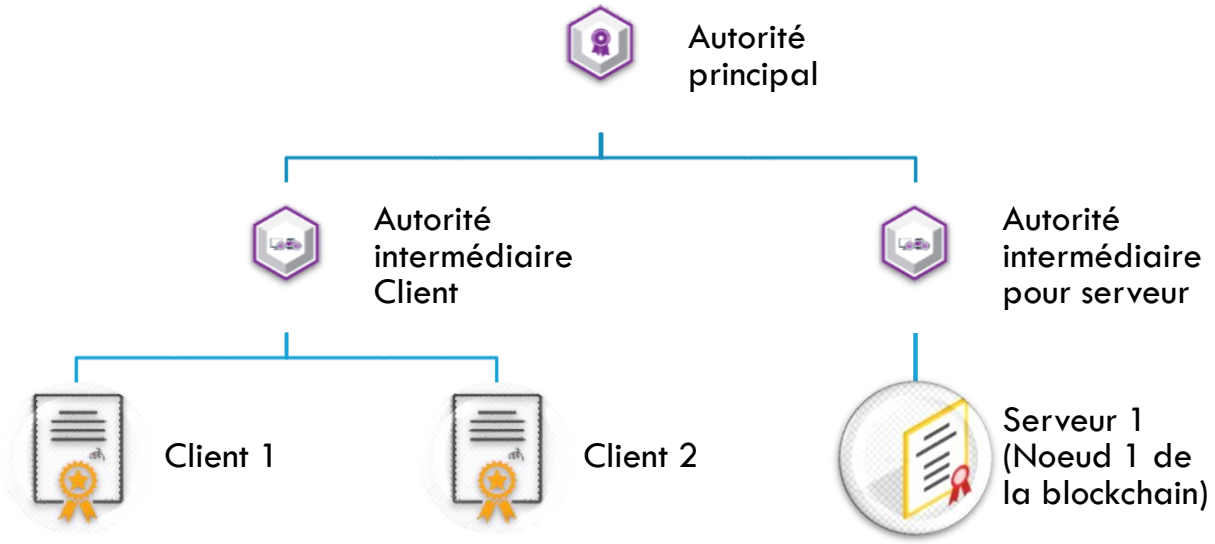


Figure 15: Chaine de confiance de la PKI

Les **autorités intermédiaires client et serveur** soumettent leurs clefs publiques à l'autorité principale qui leur a généré un certificat. **L'autorité principale** peut être définie comme le plus haut niveau d'autorité. C'est le seul composant qui a un certificat auto-signé[16]. Un certificat auto-signé est le seul certificat qui permet d'assurer l'intégrité et non l'authenticité, d'où la chaîne de confiance. Par conséquence, les **autorités intermédiaires client et serveur** deviennent des CA subordonnées de l'autorité principale.

[14] Le modèle Peer-to-Peer permet que différentes autorités de certification soient au même niveau. Si des autorités de certifications sont au même niveau, les certificats qu'elles génèrent sont co-signé.
[15] Le *modèle en pont* ou Bridge est une alternative aux deux autres modèles. En effet, le modèle hiérarchique ne permet pas d'avoir une structure stable et le modèle Peer-to-Peer nécessite un nombre important d'échange entre les autorités. Le modèle en pont ressemble fortement au modèle Peer-to-Peer sauf qu'il permet de limiter les échanges entre les autorités. Le nombre d'échange entre les autorités est réduit car il ne faut plus échanger la clef publique avec toutes les autres autorités mais uniquement avec l'autorité pont.
[16] En cryptographie et en sécurité informatique, un **certificat racine** est un certificat électronique non signé ou auto-signé qui identifie une autorité de certification (AC).

2.1.4 Choix des outils de conception de la PKI

2.1.4.1 Choix des outils d'implémentation.

a- Choix de la boite à outils de chiffrement implémentant les protocoles TLS et SSL,

IL existe plusieurs librairies de chiffrement implémentant les protocoles TLS et SSL, parmi lesquelles :

- OpenSSL

OpenSSL est une boîte à outils de chiffrement comportant deux bibliothèques (libcrypto fournit les algorithmes cryptographiques et libssl implémente le protocole de communication Transport Layer (TLS) ainsi que son prédécesseur Secure Layer (SSL)) et une interface de commande (openssl).

OpensSSL supporte un grand nombre de :

- **Types de chiffrement :**

AES, Blowfish, Camellia, SEED, DES, IDEA, RC2, RC4, RC5, Triple DES, etc.

- **Fonction de hachage cryptographique :**

MD5, MD4, MD2, SHA-1, SHA-2, RIPEMD-160, MDC-2, etc

- **Types de cryptographique à clé publique :**

RSA, DSA, Diffie-Hellman, courbe ellitique, etc

- GnuTLS

NGU Transport Layer Security Library est une implémentation libre des protocoles SSL et TLS. GnuTLS est distribuée sous la forme d'une bibliothèque (libgnutls) permettant au programme qui l'utilise de disposer de protocoles de communication sécurisée, et de diverses interfaces en ligne de commande. Les fonctionnalités fournies par GnuTLS sont :

- Protocoles SSL 3.0, DTLS, TLS 1.0, TLS 1.1 et TLS 1.2 ;
- Authentification TLS par SRP ;
- Authentification TLS par PSK ;
- Mécanisme d'extension TLS ;
- Compression TLS ;
- Prise en charge des certificats X.509 et OpenPGP.

- LibreSSL : est une boîte à outils de chiffrement implémentant les protocoles SSL et TLS et résultant d'un fork de la populaire OpenSSL par le

projet OpenBSD à la suite de la découverte de la faille Heartbleed[17] [9] en avril 2014. LibreSSL contient les fonctionnalités standards de la librairie OpenSSl, à la seule différence qu'elle est d'avantage plus sécurisée et plus pratique.

Il existe plusieurs autres librairies TLS/SSL prenant en charge les certificats X.509, mais notre choix a été porté sur la librairie openSSL, pour son interopérabilité avec plusieurs plateformes de programmations et sa notoriété.

b- Choix du format et configuration des certificats générés par la PKI,

Les certificats électroniques respectent des standards spécifiant leur contenu de façon rigoureuse. Les deux formats les plus utilisés aujourd'hui sont :

- **X.509**, défini dans la RFC 5280 ;
- **OpenPGP**, défini dans la RFC 4880.

La différence notable entre ces deux formats est qu'un certificat X.509 ne peut contenir qu'un seul identifiant, que cet identifiant doit contenir de nombreux champs prédéfinis, et ne peut être signé que par une seule autorité de certification. Un certificat OpenPGP peut contenir plusieurs identifiants, lesquels autorisent une certaine souplesse sur leur contenu, et peuvent être signés par une multitude d'autres certificats OpenPGP, ce qui permet alors de construire des toiles de confiance[18].

Notre choix a été porté pour le format X.509 car selon notre contexte, nos certificats seront signés par une seule autorité.

c- Choix de l'environnement de développement,

- Environnement côté serveur :

1. Logiciels :

NodeJs

NodeJs est une plateforme logicielle libre et événementielle en JavaScript, orienté vers les applications réseau qui doivent monter en charge. Elle utilise la machine V8 et implément sous licence MIT les spécifications CommonJS. Parmi les modules natifs de Node.js, on retrouve http qui permet le développement de serveur HTTP. Il est donc possible de se passer de serveurs web tels que Nginx[19] ou Apache lors du déploiement de sites et d'applications web développés avec Node.js.

[17] **Heartbleed** est une vulnérabilité logicielle présente dans la bibliothèque de cryptographie open source OpenSSL à partir de mars 2012, qui permet à un « attaquant » de lire la mémoire d'un serveur ou d'un client pour récupérer, par exemple, les clés privées utilisées lors d'une communication avec le protocole Transport Layer Security (TLS).

[18] La toile de confiance permet de vérifier la relation entre une clé publique et une identité numérique.

[19] NGINX est un logiciel libre de serveur Web ainsi qu'un proxy inverse écrit par Igor Sysoev, dont le développement a débuté en 2002 pour les besoins d'un site russe à très fort trafic.

Concrètement, Node.js est un environnement bas niveau permettant l'exécution de JavaScript côté serveur.

2. Libraires :

Les librairies sont des outils préconfigurés qui peuvent accomplir une ou plusieurs fonctionnalités ciblées.

Désignation/Version	Description
body-parser /1.0	Permet d'accéder au corps d'une requête http.
cluster / 0.7.7	Permet de virtualiser un processus maître en un ou plusieurs processus esclave(s).
crypto / 1.0.1	Contient les fonctions de hachage cryptographique comme le SHA, MD5, etc.
express / 4.15.2	Permet de créer des serveurs http.
fs-extra /2.0.x	Permet de lire ou d'écrire sur un fichier (Créer un certificat, lire la clé d'une autorité).
request /2.83.0	Permet de construire les requêtes http (POST, GET, PUT, UPDATE, DELETE, etc.
swagger-ui-express/4.0.1	Permet de prévisualiser l'ensemble des requêtes http configurées au niveau du serveur.

- Environnement côté client :

1. Logiciels

Java pour Android :

Java est un langage de programmation orienté objet. La particularité et l'objectif central de Java est que les logiciels écrits dans ce langage doivent être facilement portables sur plusieurs systèmes d'exploitation en occurrence Android.

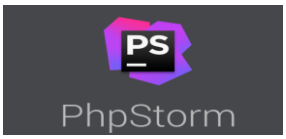
XML :

L'***Extensible Markup Language***, généralement appelé XML (Langage de balisage extensible, en français) est un métalangage informatique de balisage générique qui dérive du SGML.

2. Librairies

Désignation/Version	Description
retrofit/1.0.0	retrofit est une bibliothèque qui rend la mise en réseau des applications Android plus facile et surtout plus rapide.
Json /1.0.1	Permet de construire le corps des requêtes http en objet.

d- Logiciels de programmation



Editeur de code Multi langages pour les applications orientées WEB : JavaScript, PHP, etc.

Editeur de code pour les applications mobile sous Android

e- Logiciel de modélisation

Logiciel de modélisation pour les diagrammes d'UML

2.1.4.2 Choix des outils de modélisation PKI.

a- Choix de la méthode de modélisation

Deux approches méthodologiques proposent des visions différentes pour modéliser la réalité. La première apporte une approche relationnelle (MERISE), tandis que la deuxième est orientée « objet » (UML). Pour la modélisation de notre système, nous avons choisi langage de modélisation UML. En effet, UML se définit comme un langage de modélisation graphique et textuel destiné à comprendre et décrire des besoins, spécifier et documenter des systèmes, esquisser des architectures logicielles, concevoir des solutions et communiquer des points de vue[11].

b- Analyse des besoins en sécurité pouvant être accomplis par la PKI

Pour l'entreprise, elle voudrait une PKI qui soit à mesure de :

- proposer une interface de demande et d'enregistrement des certificats numériques clients et serveurs,

- proposer une interface de validation des certificats,
- proposer une interface de publication des certificats numériques,
- proposer une interface de contrôle des statuts des certificats,
- proposer une interface de révocation des certificats numériques

c- Diagramme d'activité pour la génération de la PKI.

Il s'agit pour nous de présenter les étapes majeures de création de notre PKI.

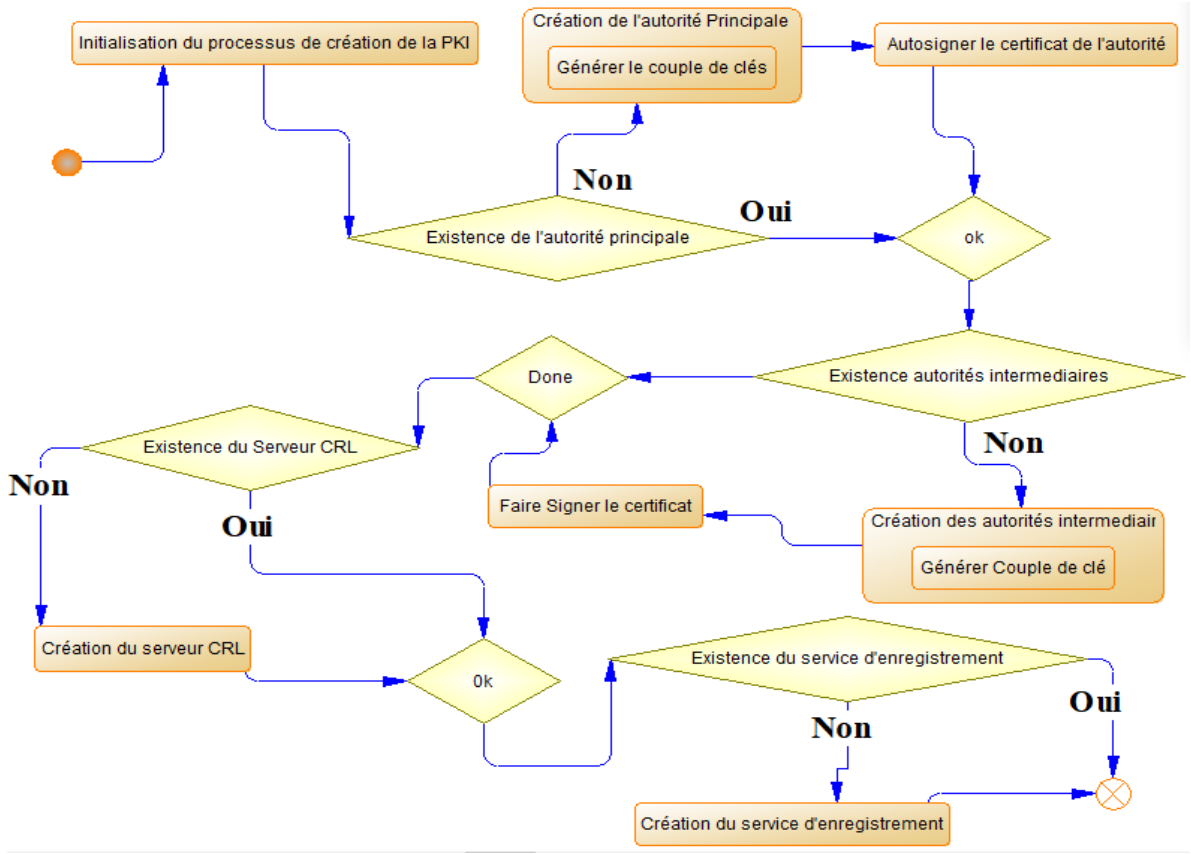


Figure 16: Illustration du processus de mise en place de la PKI

d- Diagramme de cas d'utilisation

* Acteurs du système

- Les clients d'Alliance,
- Le système lui-même

* Cas d'utilisations

- **S'authentifier** : le client renseigne ses paramètres de connexion aux services d'Alliance (Identifiant, mot de passe),

- **Demande de certificat** : le client formule une requête de demande de certificat au format *PCKS#10*.
- **Vérifier l'état de son certificat :** le client peut à tout moment vérifier si son certificat est encore en cours de validité.
- **Enregistrer les demandes de certificats :** le système enregistre les demandes de certificats par les clients.
- **Valider les certificats :** le système valide les demandes de certificats en imposant sa signature.
- **Sauvegarder les certificats :** le système sauvegarde les certificats nouvellement créé.
- **Révoquer les certificats :** le système peut révoquer un certificat

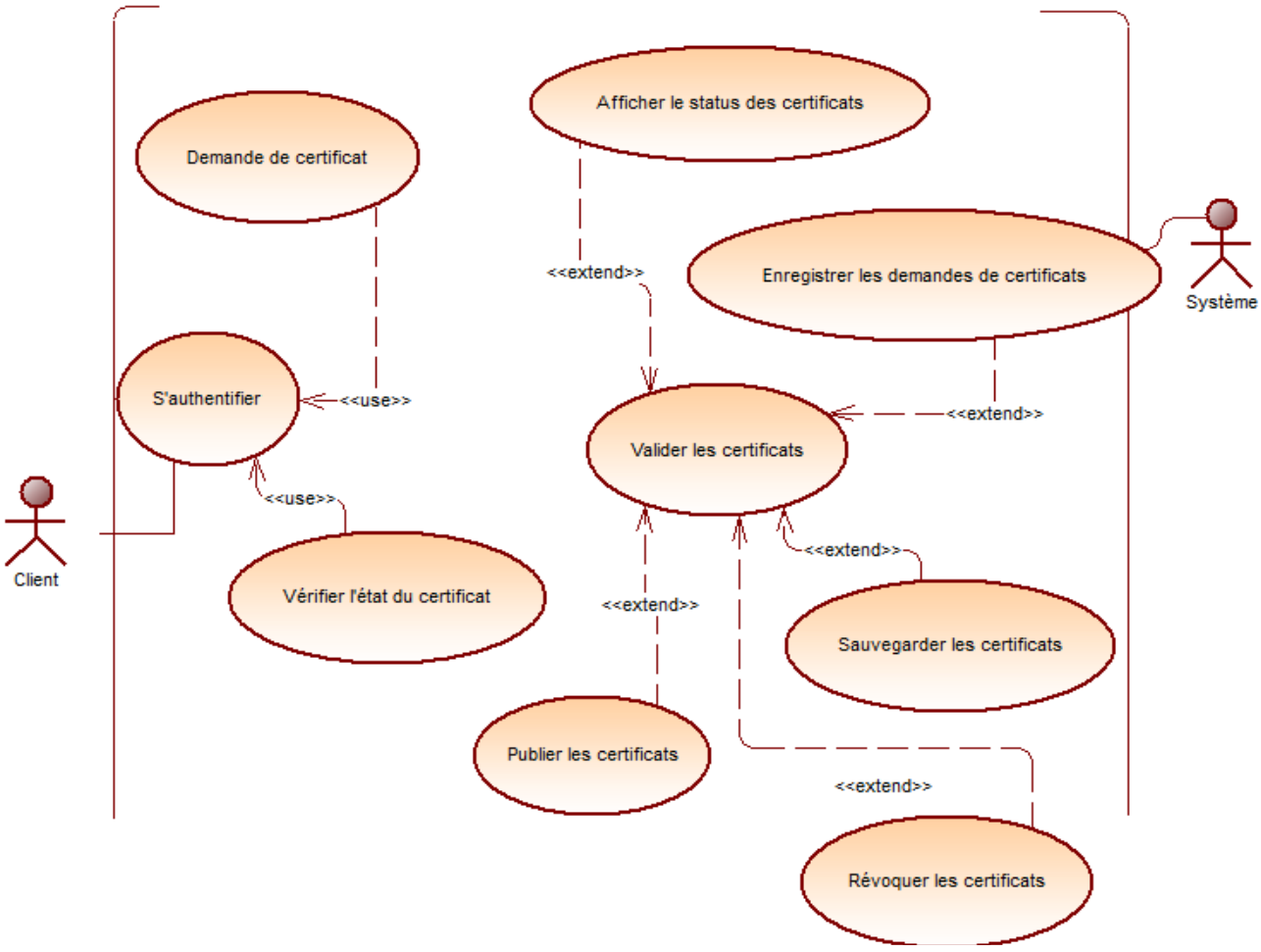


Figure 17: diagramme des cas d'utilisation de la PKI

e- Diagramme de séquence

Le diagramme de séquence permet de montrer les interactions d'objets dans le cadre des scénarii cités plus haut. Pour des raisons de simplification, nous allons choisir

la représentation de deux d'entre eux à savoir le scénario de demande d'un certificat, et celui de vérification du statut d'un certificat.

Ainsi, voici comment se présente le scénario de « demande d'un certificat »

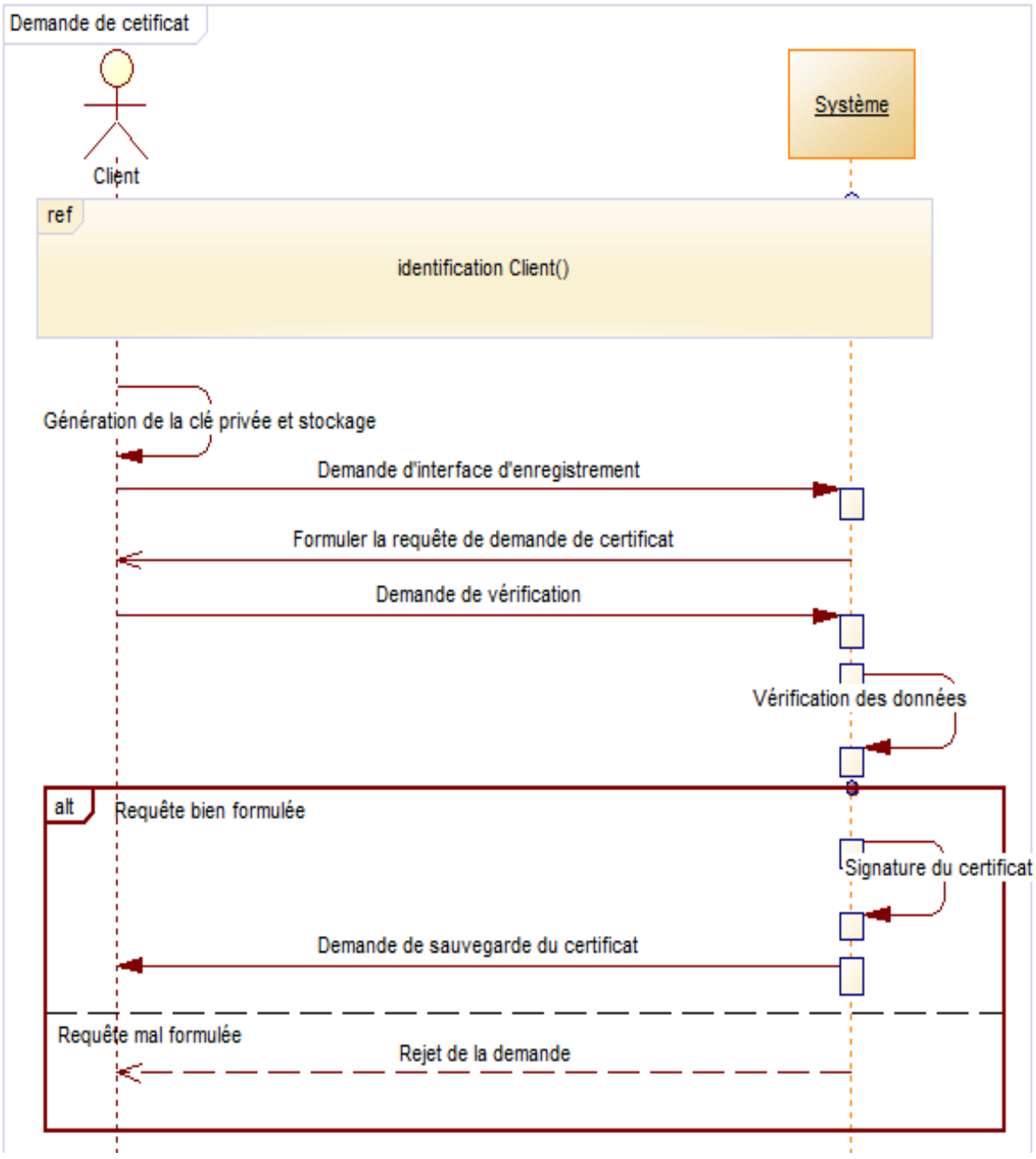


Figure 18: Illustration du processus de demande d'un nouveau certificat

De même, le processus de « vérification du statut d'un certificat » fonctionne comme suit :

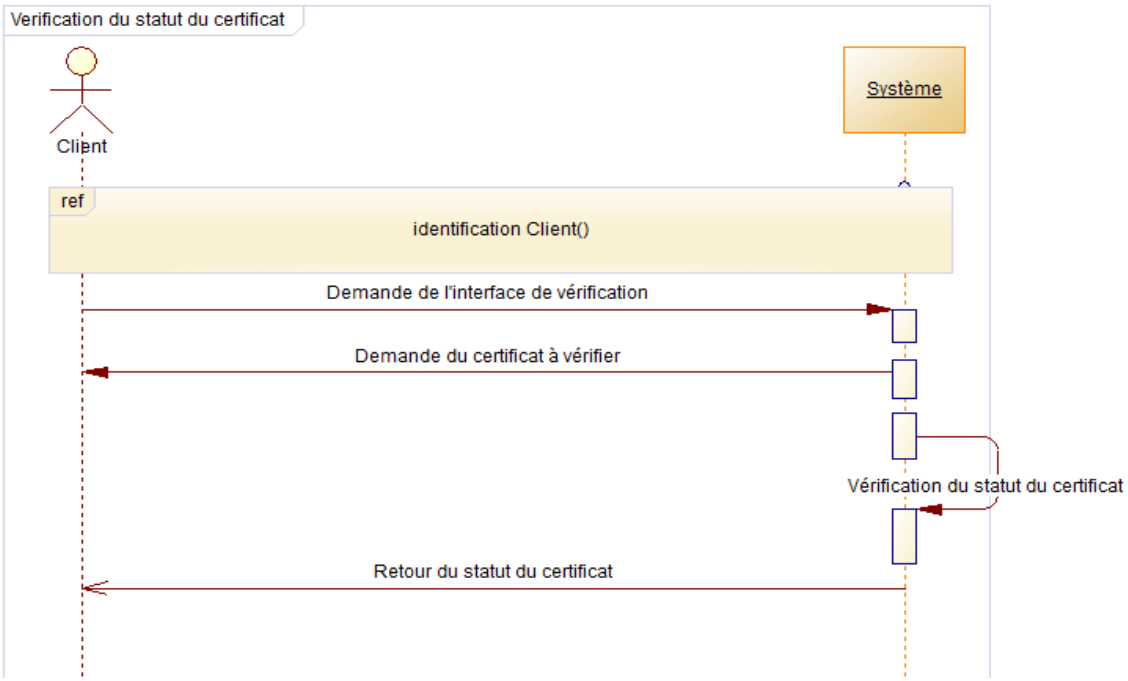


Figure 19: Illustration du processus de vérification du statut d'un certificat SSL

f- Diagrammes d'activité

* cas d'utilisation demande de certificat

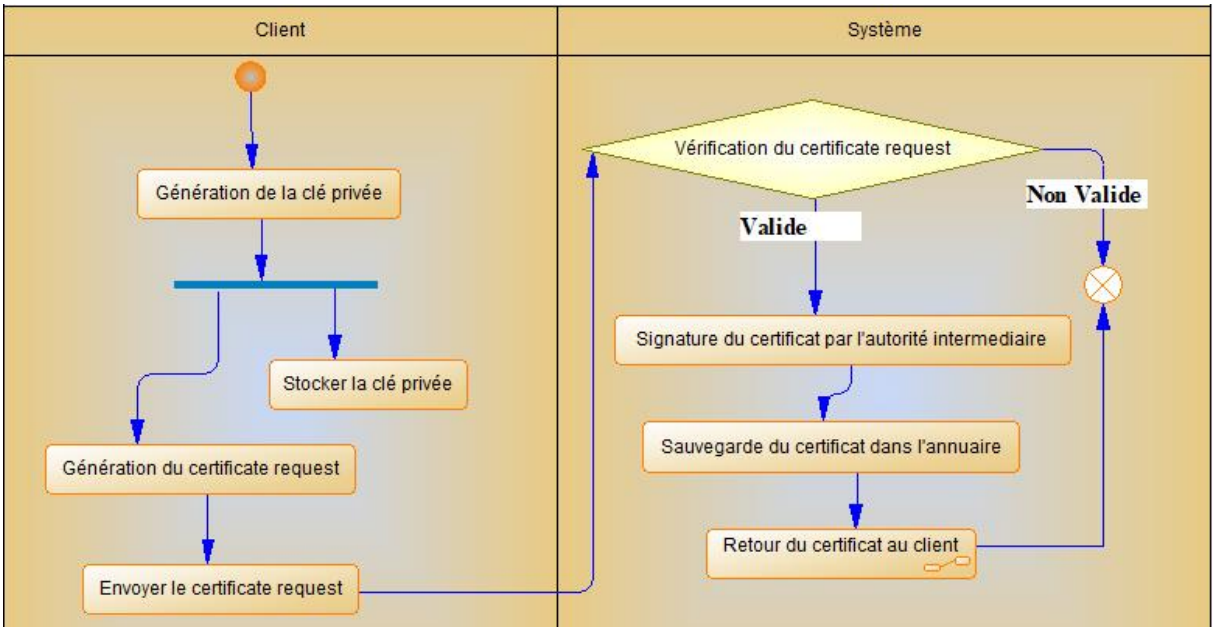


Figure 20: Diagramme d'activité présentant le processus de demande d'un certificat

* cas d'utilisation vérifier statut certificat.

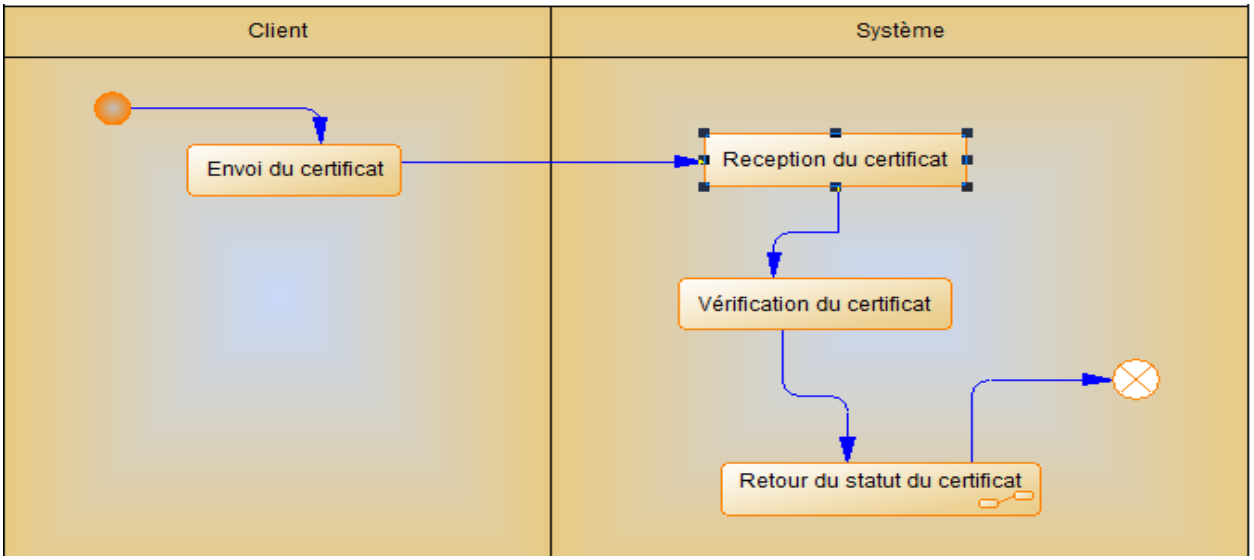


Figure 21 : Diagramme d'activité présentant le processus vérification du statut d'un certificat

g- Quelques commandes OpenSSL

*Commande OpenSSL pour la demande de certificat

```
function createCSR(info, name, passphrase, folder, cb) {
    folder = folder.replace(/\\/g, '/');
    const subj = '-subj "/C=' + info.C + '/ST=' + info.ST + '/L=' + info.L + '/O=' + info.O + '/OU=' + info.OU + '/CN=' + info.CN + '"';
    exec('openssl req ' + subj + ' -new -sha256 -key ' + name + '.key.pem -out ' + name + '.csr.pem -passin pass:' + passphrase, {
        cwd: folder
    }, function(err, stdout, stderr) {
        callback(cb, err, stdout, stderr);
    });
}
```

*Commande OpenSSL pour la validation du certificat

```
function createCertificate(caConfigFile, caExtensionType, caPassword, csrFileName, certFileName, lifetime, folder, cb) {
    folder = folder.replace(/\\/g, '/');
    caConfigFile = caConfigFile.replace(/\\/g, '/');
    exec('openssl ca -config ' + caConfigFile + '.cnf -extensions ' + caExtensionType + ' -days ' + lifetime + ' -notext' +
        ' -md sha256 -in ' + csrFileName + '.csr.pem -out ' + certFileName + '.cert.pem -passin pass:' + caPassword + ' -batch', {
        cwd: folder
    }, function(err, stdout, stderr) {
        callback(cb, err, stdout, stderr);
    });
}
```

*Commande OpenSSL pour la vérification du statut d'un certificat

```
function verifyWithCA(issuerFile, caCert, folder, cb) {
    issuerFile = issuerFile.replace(/\\/g, '/');
    caCert = caCert.replace(/\\/g, '/');
    folder = folder.replace(/\\/g, '/');
    exec('openssl verify -CAfile ' + issuerFile + '.cert.pem ' + caCert, {
        cwd: folder
    }, function(err, stdout, stderr) {
        callback(cb, err, stdout, stderr);
    });
}
```

*Commande OpenSSL pour la révocation d'un certificat

```
function revokeCertificate(serialNumber, passphrase, folder, cb) {
    folder = folder.replace(/\\/g, '/');
    exec('openssl ca -config openssl.cnf -revoke ./certs/' + serialNumber.toString() + '.pem -passin pass:' + passphrase, {
        cwd: folder
    }, function(err, stdout, stderr) {
        callback(cb, err, stdout, stderr);
    });
}
```

2.1.5 Conclusion

Cette première partie de la méthodologie de notre travail a été consacrée à la conception d'une infrastructure à clé. Ce module en réalité comprend plusieurs parties. Il s'agit d'une autorité de certification racine, de plusieurs autorités de certifications intermédiaires, des serveurs applicatifs d'enregistrement de demandes de certificats, d'un serveur applicatif pour la vérification des statuts des certificats. L'utilisation des diagrammes de classe nous a permis de mieux comprendre comment les échanges se font entre les clients demandeurs de certificats et la PKI. Les certificats ainsi générés par la PKI ont pour principal rôle de permettre une authentification forte entre les clients d'Alliance Financial et son serveur de sorte que leurs identités ne soient usurpées ou volées encours d'échange. Quelques commandes openSSL, ont ainsi été présentées pour illustrer comment le certificats sont créés, signés et révoqués. Mais ce qui est aussi important à noter, c'est qu'en réalité, la PKI que nous venons de concevoir va intervenir dans le processus de validation des transactions par les nœuds de la blockchain. La suite de ce chapitre sera donc réservée à la modélisation d'entités de la blockchain.

2.2 Modélisation de la blockchain

2.2.1 Analyse de l'existant

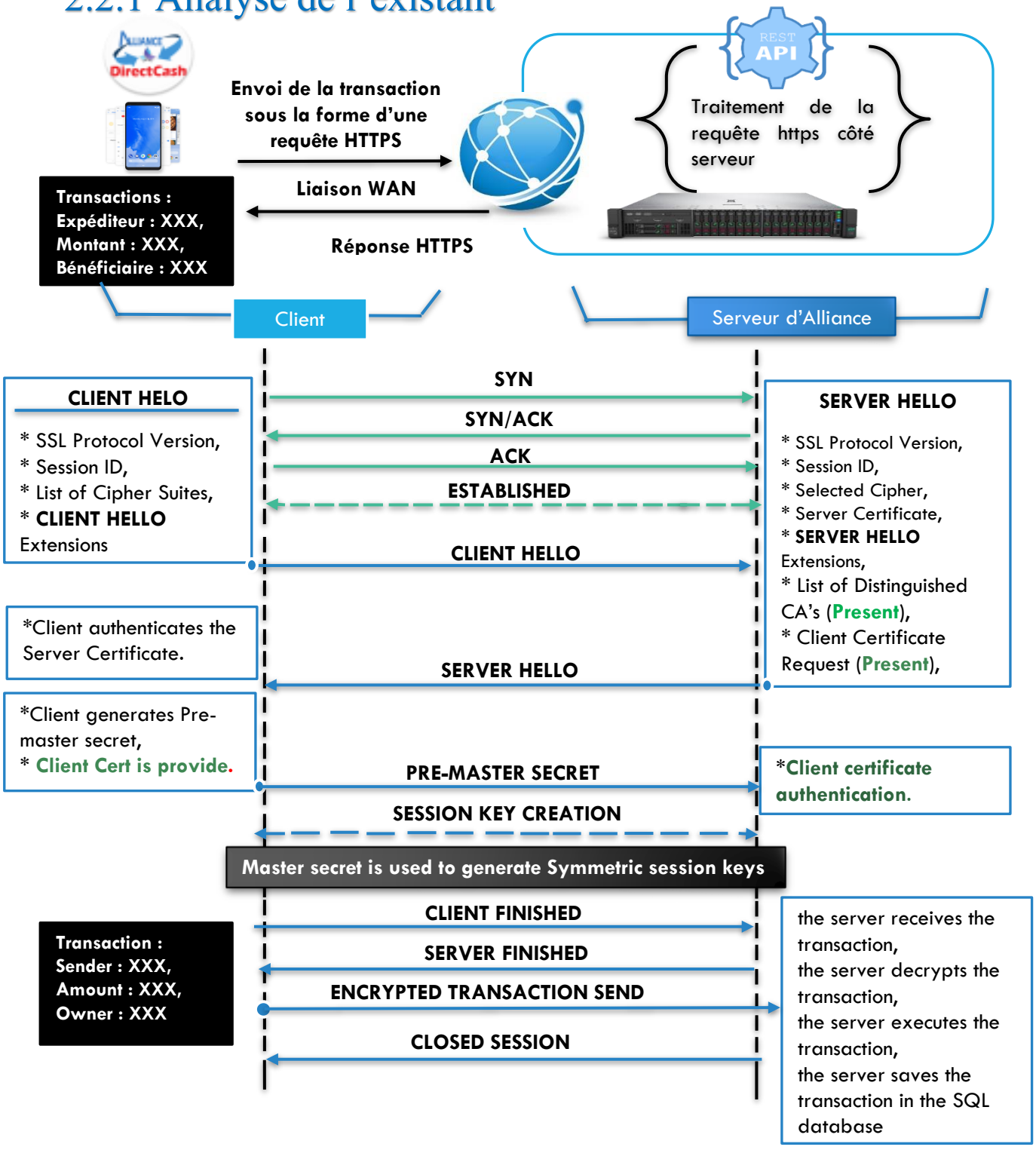


Figure 22: Illustration du problème de traçabilité des transactions financières

Observations et interprétations :

Les clients utilisent un certificat numérique pour communiquer avec le serveur. L'utilisation d'un certificat SSL côté client permet de préserver l'identité du client au près du serveur et assure une communication sécurisée des échanges. Au niveau du serveur, aucun système d'horodatage des transactions n'est mis sur pieds. Le serveur se contente d'enregistrer les transactions dans une base de données. Le risque que présente une telle pratique est qu'un intrus peut rejouer les transactions d'un client plusieurs fois en direction du serveur et à son avantage [15].

C'est donc sur la base de ce constat que nous allons introduire la deuxième technologie appelée « blockChain. L'objectif principal visé par l'implémentation de cette technologie est d'empêcher les « attaques par rejeu[20] » en mettant sur pieds un système d'horodatage pour la traçabilité des transactions. En plus de sauvegarder les transactions dans la base de données SQL, nous allons les stocker dans une base de données distribuée, partagée uniquement par les sites de l'entreprise. Le stockage des transactions se fera par l'utilisation de méthodes cryptographiques afin d'empêcher que les transactions ne soient falsifiées ou rejouées.

2.2.2 Choix des outils de conception de la Blockchain

2.2.2.1 Choix de l'environnement de programmation.

Nous avons utilisé les mêmes outils de programmation que ceux de la PKI pour concevoir notre application web Blockchain (voir paragraphe **2.1.4.1 c)**.

2.2.2.2 Choix des outils de modélisation PKI.

a- Choix de la méthode de modélisation

Pour la modélisation de notre blockchain, nous avons choisi le langage de modélisation UML pour les mêmes motifs cité plus haut au paragraphe **2.1.4.2 a**.

b- Analyse des besoins en traçabilité pouvant être accomplis par la blockchain

Alliance Financial voudrait un système qui soit à mesure de :

- Horodater les transactions,
- Empêcher la falsification des transactions,

c- Modélisation des blocks et des transactions de la blockchain

Il s'agit pour nous de recenser les entités participant à la blockchain et de définir les relations entre les entités. L'utilisation d'un diagramme de classe s'impose.

[20] Une **attaque par rejeu** (en anglais, replay attack ou playback attack) est une forme d'**attaque** réseau dans laquelle une transmission est malicieusement répétée par un attaquant qui a intercepté la transmission. Il s'agit d'un type d'usurpation d'identité.

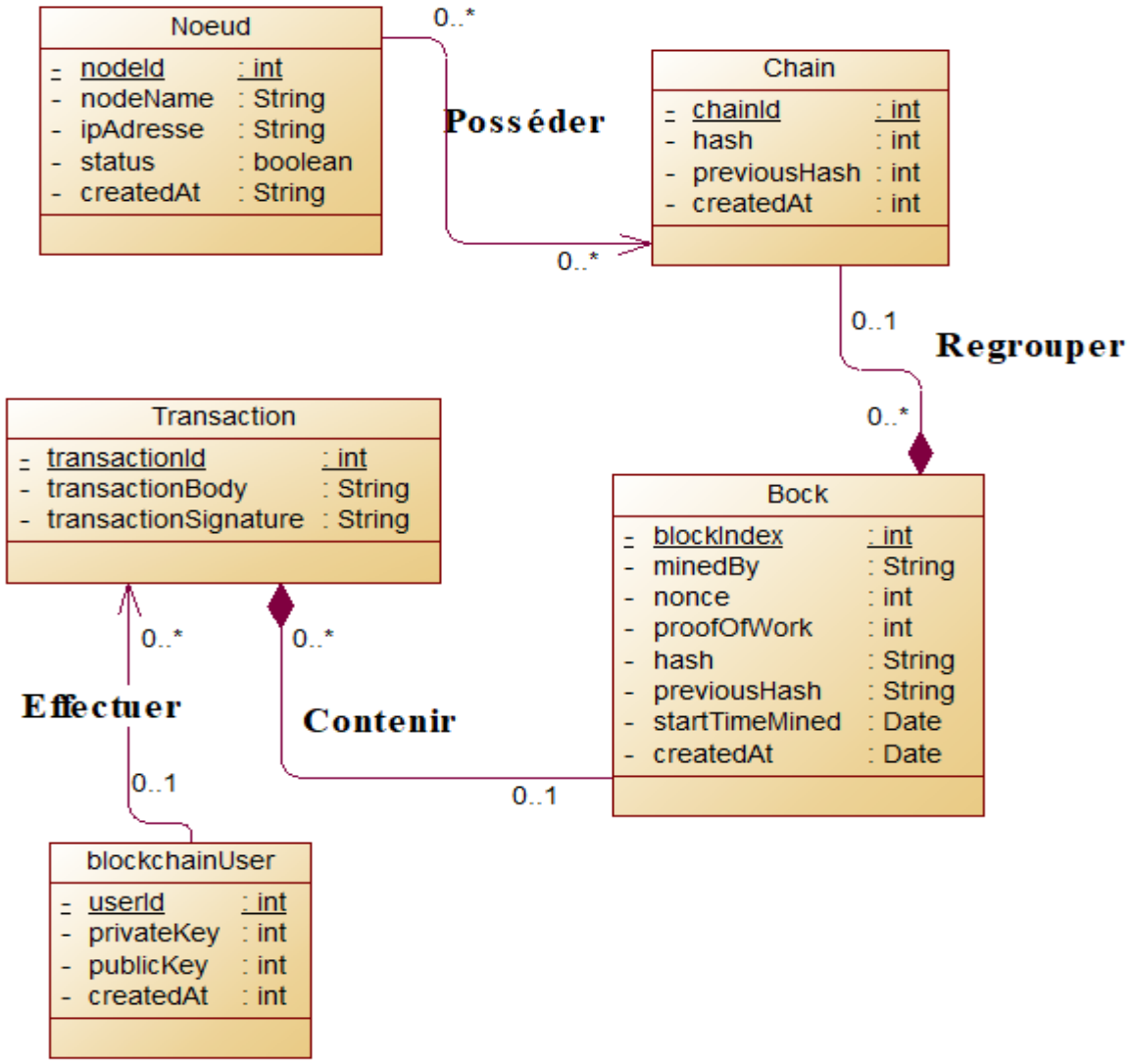


Figure 23: Diagramme de classe pour modélisation des relations entre les entités de la blockchain

d- Les fonctionnalités des entités de la blockckain

Il s'agit pour nous de présenter les différents rôles que vont jouer chaque entité de la blockchain. Pour cela, nous les avons matérialisés avec un diagramme de cas d'utilisations.

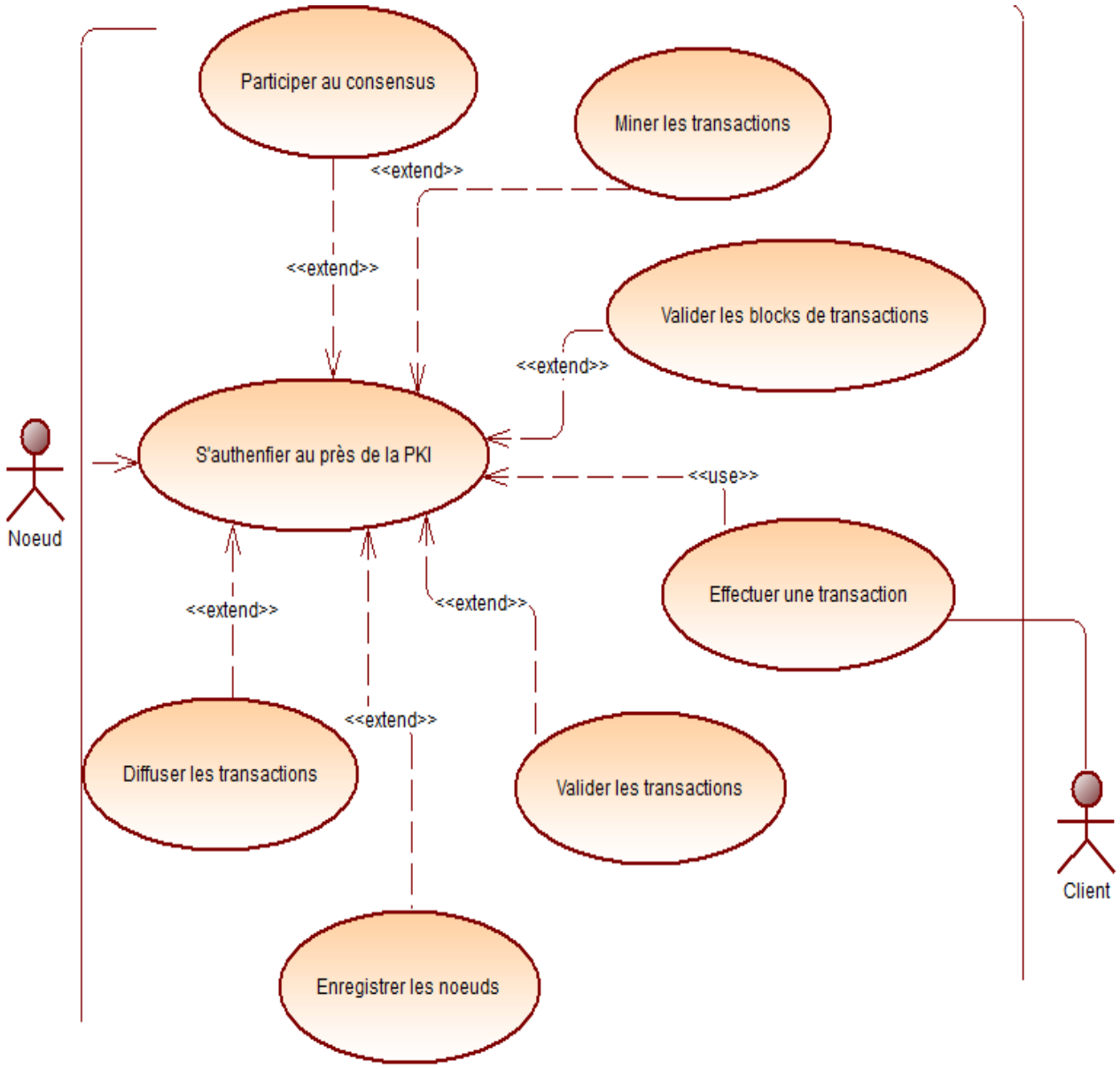


Figure 24: Diagramme des cas d'utilisations de la blockchain

Pour chaque cas d'utilisations, nous allons illustrer comment se fait l'échange des informations.

* Cas d'utilisation « **Effectuer une transaction**»

La transaction est effectuée par les clients d'Alliance Financial depuis une application mobile. Chaque client possède une paire de clefs privée et publique. La clé publique est utilisée pour signer chaque transaction avant de l'envoyer vers le serveur. De cette manière, le serveur pourra vérifier si la transaction provient bien du client,

qu'elle n'a pas été altérée en cours de route et qu'aucune information sur la transaction n'a été dérobée.

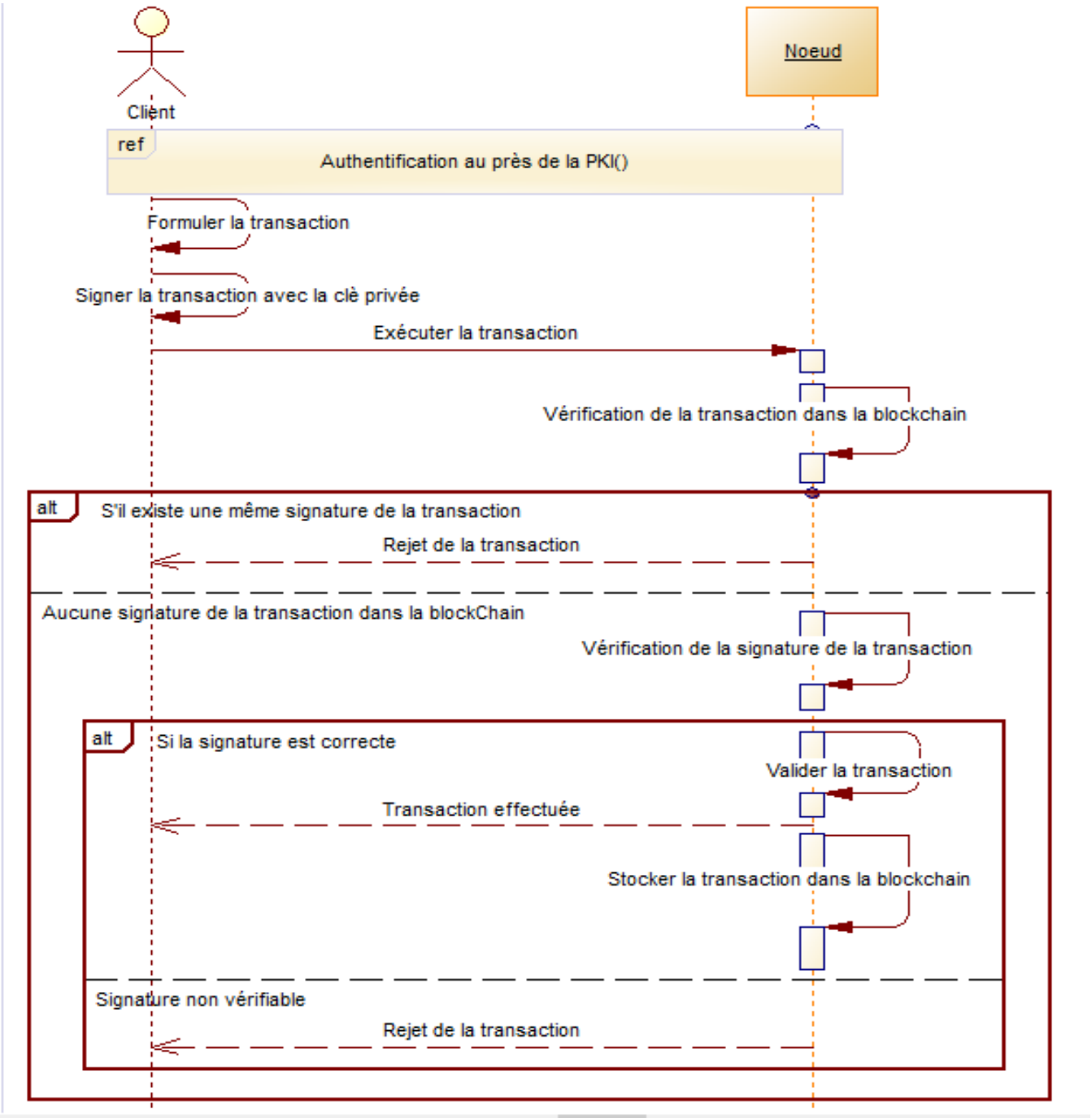


Figure 25: Illustration du processus de la validation, puis d'enregistrement d'une transaction dans la blockchain

* Cas d'utilisation « **Miner les transactions**»

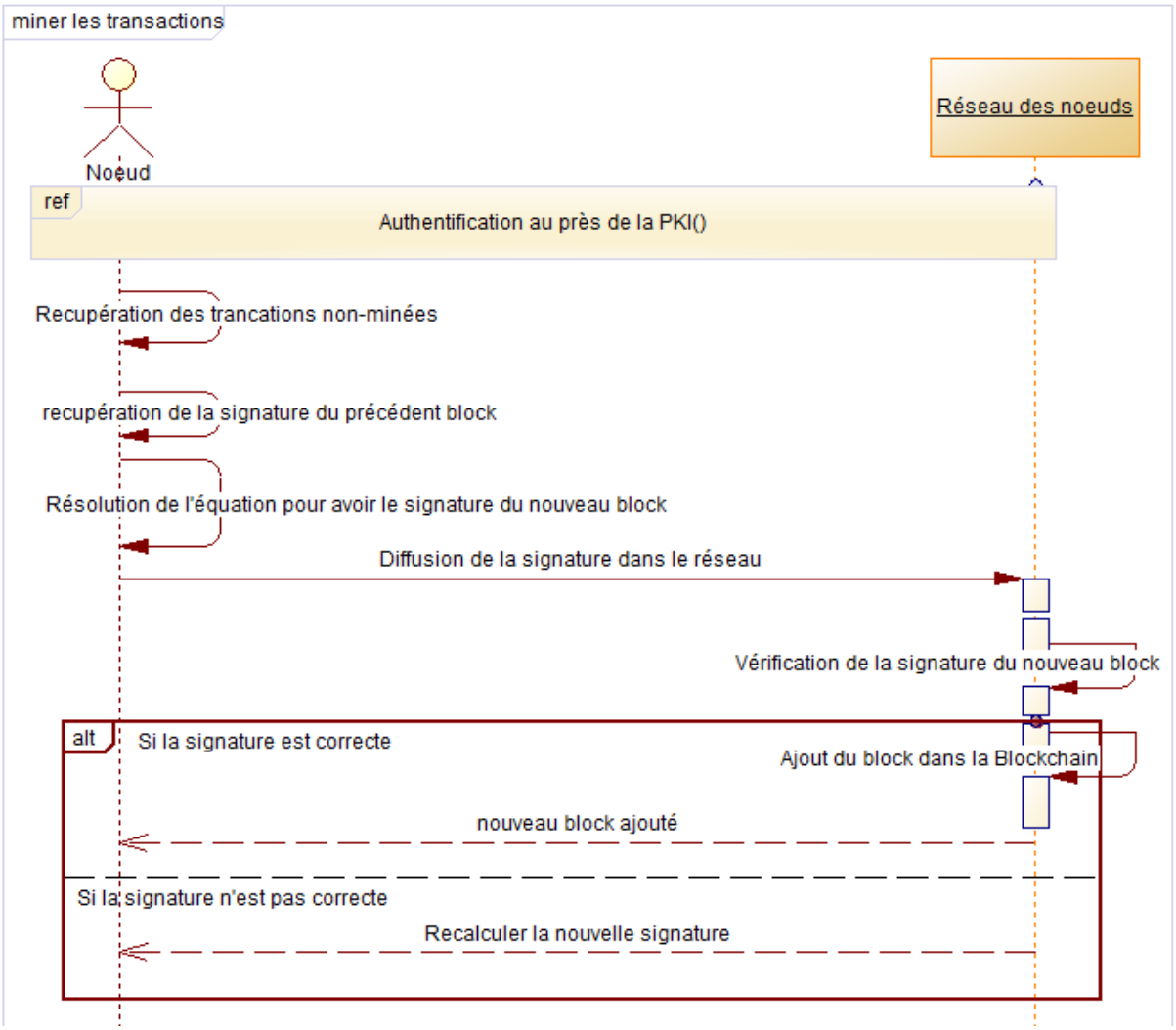


Figure 26: Illustration du processus de minage des transactions par un nœud

NB : le processus permettant de déterminer la signature d'un nouveau block afin de le sceller est décrit au paragraphe **1.4.2.2 d** plus haut. En effet il s'agit pour chaque nœud de résoudre l'équation suivante :

Sha256 (*Bloc*+*infos mineur*+*hash bloc précédent*+i) =*C*

i ϵ N et ***C*** est un nombre hexadécimal commençant par **5 zéros, 5** étant **la difficulté** de la blockchain. Cette difficulté dépend de la puissance de calcul de chaque nœud. Plus elle est grande, plus le nœud prend beaucoup de temps à sceller le bloc. Nous avons mis le niveau de difficulté à 5 parce que notre serveur n'est pas assez puissant. Mais dans les normes, un niveau de difficulté **≥15** renforce d'avantage la sécurité des blocks.

Lorsqu'un nœud réussit à trouver la solution (c'est-à-dire le i correspond), il annonce directement aux autres nœuds du réseau en envoyant le « **i** » et le « **C** ». Les

autres nœuds doivent à leur tour vérifier si la solution trouvée résout l'équation précédente. Après vérification, le nouveau block est ainsi ajouté à la blockchain.

* Cas d'utilisation « **Participer au consensus**»

A titre de rappel, le « consensus » est une opération qui consiste à déterminer la chaine la plus longues et honnête posséder par les 51% des nœuds du réseau.

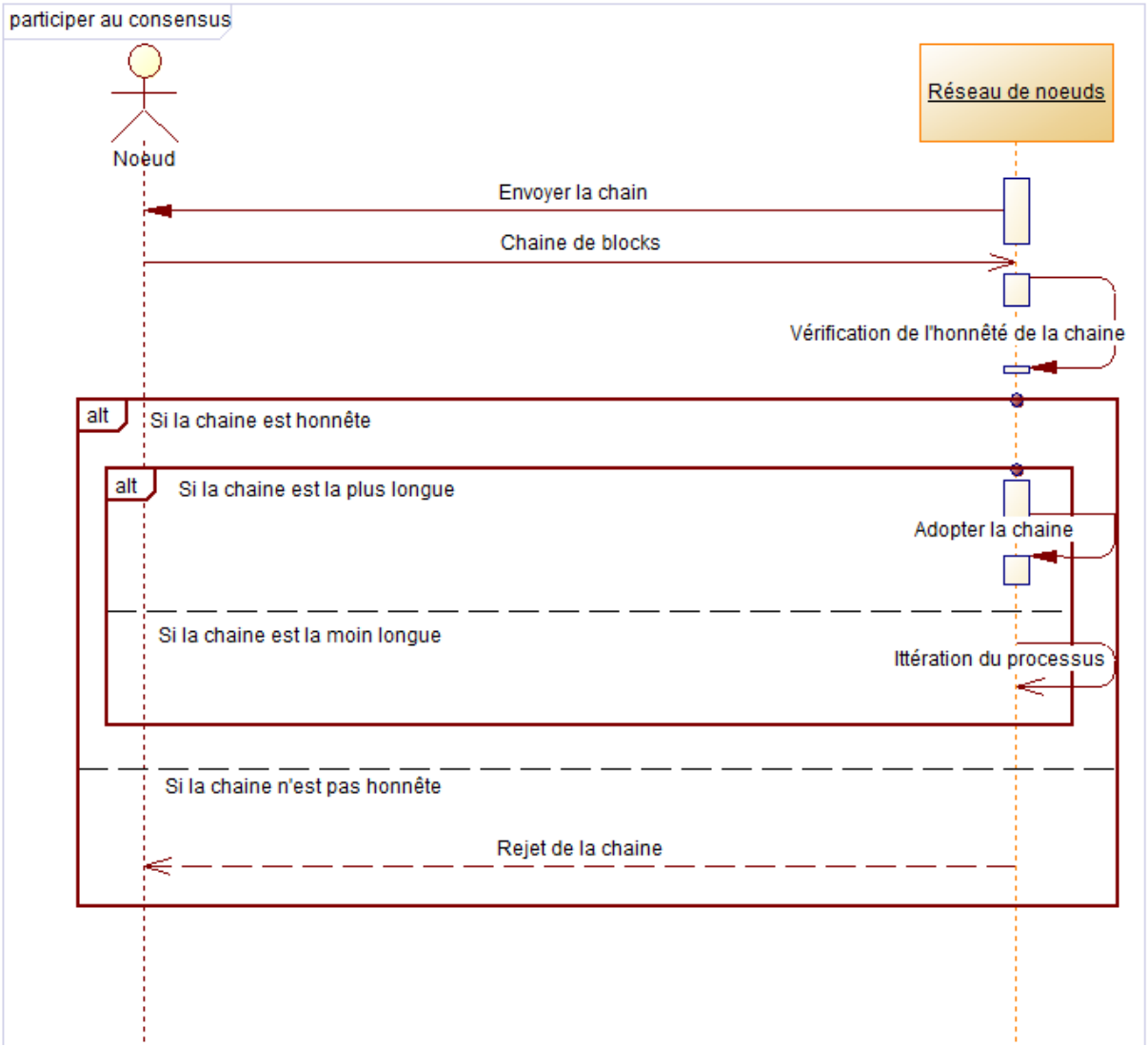


Figure 27: Présentation d'un consensus dans une blockchain

L'activité des nœuds se résume comme suit :

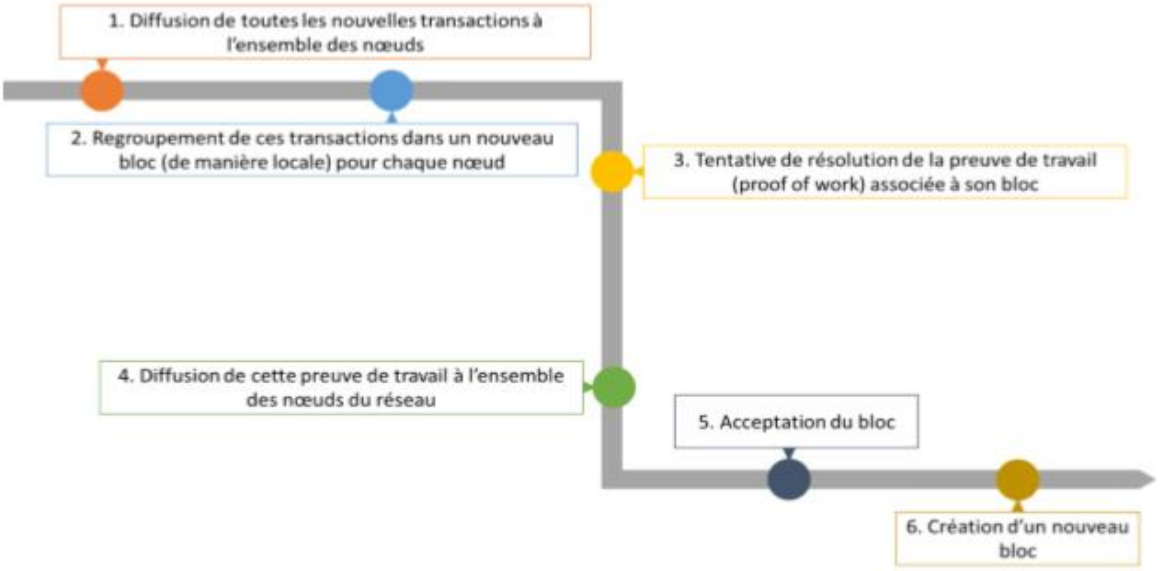


Figure 28: Résumé de l'activité des nœuds dans une blockchain

e- Processus de vérification des transactions.

La vérification des transactions va être facilitée par l'utilisation de *l'arbre de Merkle*. La technique consiste à calculer successivement plusieurs empreintes par regroupement jusqu'à trouver l'empreinte racine pour un ensemble de transactions contenues dans un bloc. Avec cette technique, pour vérifier la transaction « Tx0 » par

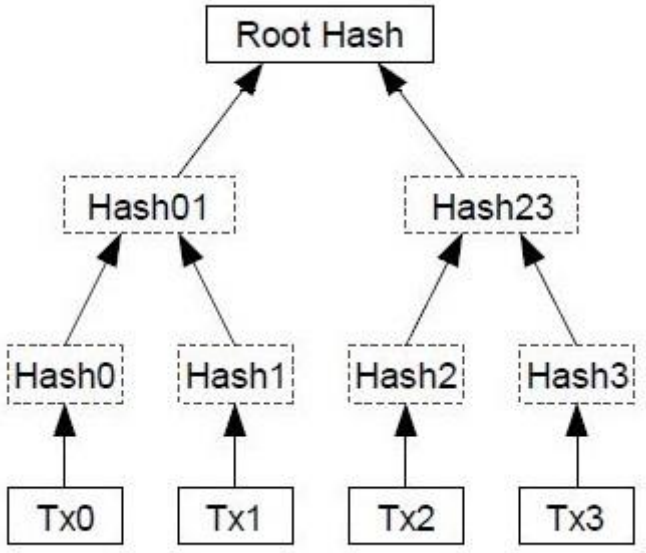


Figure 29: Arbre de Merkle

exemple, il suffit de se positionner sur la branche « Hash01 » comme le montre la figure ci-dessus.

2.2.3 Autres spécifications techniques.

2.2.3.1 Choix du matériel.

Le matériel informatique recommandé pour la mise en place de cette solution est décrit comme suit :

Tableau 4: Caractéristiques du matériel de minage

Désignation	Antminer S7
Modèle	AMS7473
Taux de hash	4.73 TéraHashs/s
Tension d'entrée	11.60 ~ 13.00 V
Consommation d'énergie	1293 Watt
Dimension	301 mm(L)*123(W)*155mm(H)
Coût unitaire	1000 Euro hors taxe
Poids	4 Kg
Quantité	2

2.2.3.2 Fréquence de minage des transactions.

Nous allons supposer qu'au cours de la journée une certaine quantité de transactions est traitée par chaque nœud du réseau de la blockchain. Ceci nous permettra d'évaluer l'activité de chaque mineur et d'estimer leur consommation en énergie.

Année 1:

Tableau 5: Prévision du trafic année 1

Quantité moyenne des transactions par jours	1000 Transactions/Jrs, soit 1000 clients, soit 1 transaction par client
Fréquence de minage par jours	12 fois/jour, soit un intervalle de temps de 2h.
Nombre moyens de hashs nécessaires pour chaque minage	2 terahashs/opération de minage
Nombre moyens de hashs générés par jours	14 terahashs/jour
Consommation d'énergie moyenne d'un nœud par jour	1914 Watt/Jour/Noeud
Consommation d'énergie annuelle	1.396.878 Watt/an

Année 2:

Tableau 6: Prévision du trafic année 2

Quantité moyenne des transactions par jours	3000 Transactions/Jrs, soit 1500 clients, soit 2 transactions par client.
Fréquence de minage par jours	12 fois/jour, soit un intervalle de temps de 2h.
Nombre moyens de hashs nécessaires pour chaque minage	2 terahashs/opération de minage
Nombre moyens de hashs générés par jours	14 terahashs/jour
Consommation d'énergie moyenne d'un nœud par jour	1914 Watt/Jour/Noeud
Consommation d'énergie annuelle	1.396.878 Watt/an

Année 3:

Tableau 7: Prévision du trafic année 3

Quantité moyenne des transactions par jours	15000 Transactions/Jrs, soit 3000 clients, soit 5 transactions par client
Fréquence de minage par jours.	10 fois/jour, soit un intervalle de temps de 1h.
Nombre moyens de hashs nécessaires pour chaque minage.	2 terahashs/opération de minage
Nombre moyens de hashs générés par jours	14 terahashs/jour
Consommation d'énergie moyenne d'un nœud par jour.	1914 Watt/Jour/Noeud
Consommation d'énergie annuelle.	1.396.878 Watt/an

2.3 Architecture de déploiement de la solution

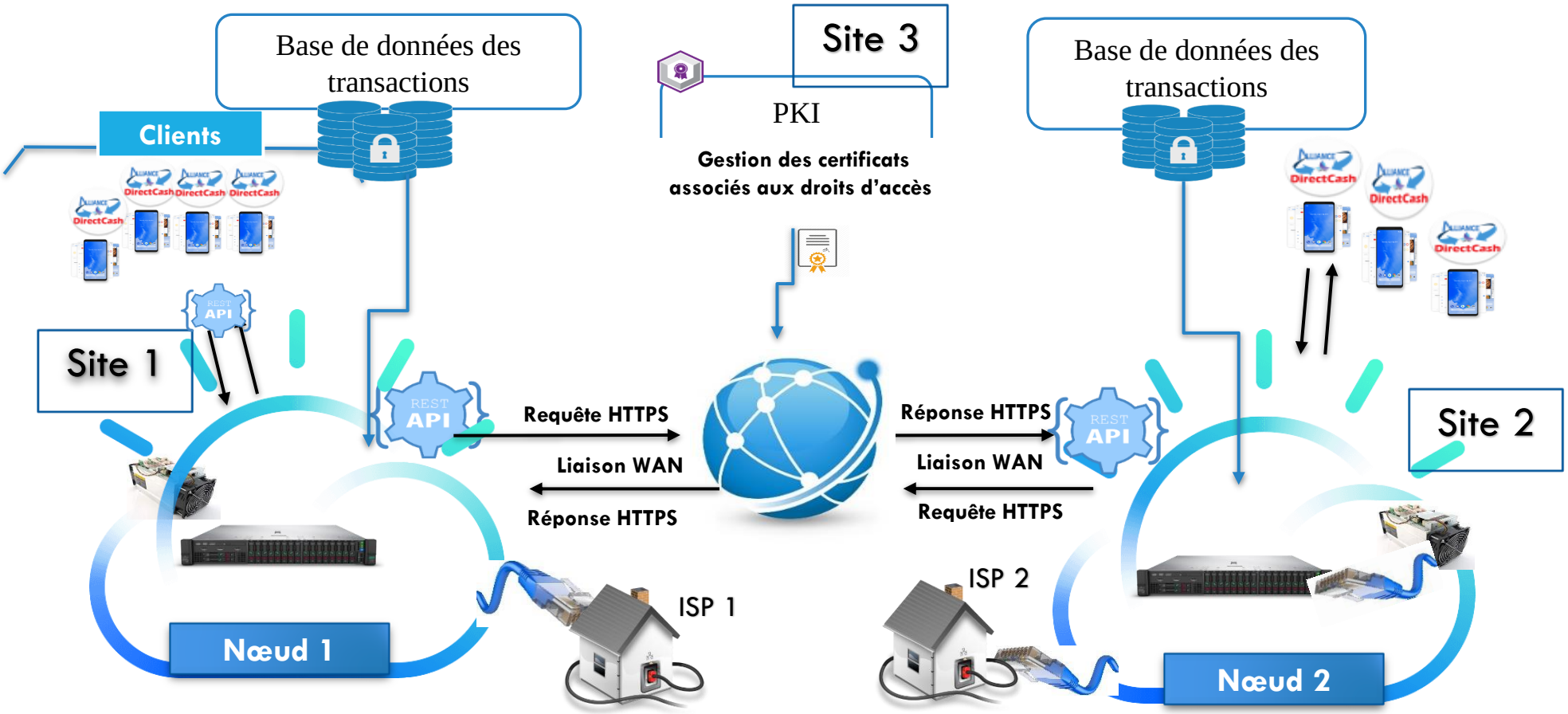


Figure 30: Architecture de déploiement de notre solution

Commentaires :

Cette architecture met en exergue trois sites. Dans chaque site, se trouve une machine serveuse abritant les services de l'entreprise et un mineur dont la fonction principale sera de miner les transactions financières (pour les sites 1 et 2).

1 Les serveurs doivent avoir une adresse IP publique au près d'un fournisseur d'accès internet (FAI ou ISP en anglais). Cette adresse IP sera utilisée dans les configurations de l'application « DirectCash » au niveau de son module de connexion aux services d'Alliance Financial.
2 Les sites 1 et 2 valident et minent transactions financières, puis participent au consensus permettant d'assurer leur intégrité.
3 Chaque client est interconnecté au plus à un site (le site 1 ou le site 2) afin de bénéficier des services de l'entreprise.
4 Le site 3 représente l'infrastructure à clé publique pour la gestion des certificats SSL pour les clients et les serveurs qui doivent aussi pouvoir s'authentifier mutuellement.
5 La demande de certificat par les clients auprès de l'infrastructure à clé publique se fait par l'intermédiaire des sites 1 ou 2.
6 Les sites 1 et 2 ont en temps réel une copie de la base de données des transactions financières dont ils ont la charge d'assurer leur intégrité.

2.4 Conclusion du chapitre

Ce chapitre était réservé à la conception de la solution évoquée dans le chapitre précédent. Cette solution regroupe deux modules. Le premier module est une infrastructure à clé publique. Cette infrastructure a pour rôle de fournir des certificats numériques aux clients d'Alliance, lesquelles serviront à signer leurs transactions et aussi à s'authentifier au prêt du serveur d'Alliance. Cette infrastructure comporte un service d'enregistrement des demandes de certificats, un service de certification, un service contrôle de l'état des certificats des clients. Le flux des messages échangés entre l'infrastructure et les clients a été modélisé à l'aide des diagrammes d'UML, de sorte à faciliter l'implémentation de la PKI. Le deuxième module quant à lui est la blokchain. Ce deuxième module comprend une base de données distribuée entre les nœuds du réseau, dont les principales fonctionnalités sont : valider les transactions, diffuser les transactions, regrouper les transactions dans un même bloc, miner le bloc, insérer le nouveau bloc dans la chaine. Ces fonctionnalités ont été explicitement décrites à l'aide des diagrammes d'UML. Enfin nous avons conclus pas l'architecture finale du nouveau système d'information d'Alliance suivi de quelques spécifications techniques.

CHAPITRE 3: Présentation des résultats et commentaires

Dans ce chapitre, nous présenterons dans un premier temps l'application « DirectCash », ensuite nous ferons intervenir la signature numérique dans l'application. Aussi, suivra une présentation de l'application web assurant la gestion des certificats clients d'Alliance Financial et enfin nous présenterons l'application blockchain. La présentation de chaque module sera suivie de commentaires afin de vérifier si l'architecture finale avec tous ses composants respectent les exigences du cahier de charge.

3.1 Présentation de l'application "DirectCash"

3.1.1 Architecture de l'application

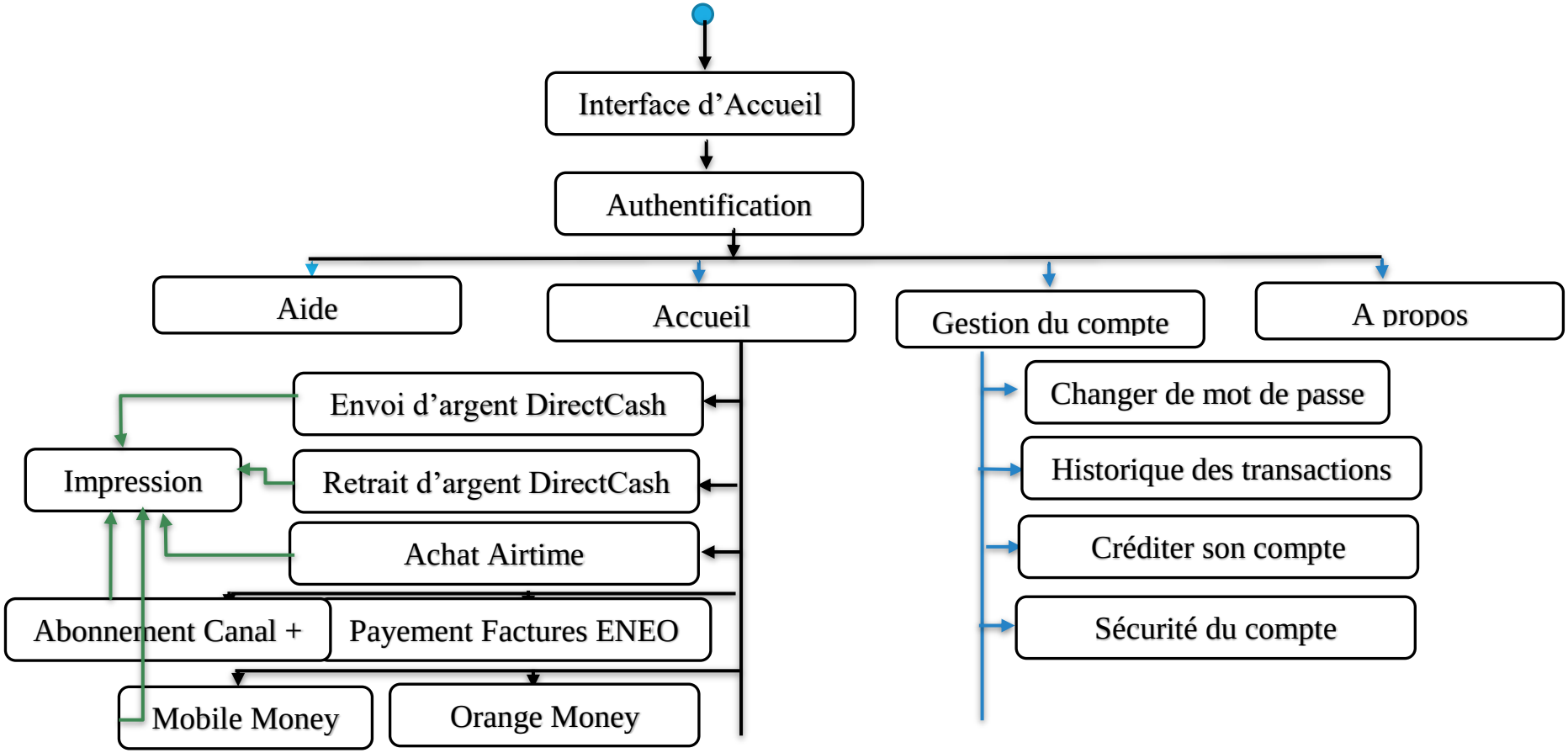


Figure 31: Architecture de l'application DirectCash

3.1.2 Présentation des interfaces

3.1.2.1 Interface d'authentification.

Une fois l'application téléchargée et installée depuis Play store, vous appuyer sur l'icône pour ouvrir.

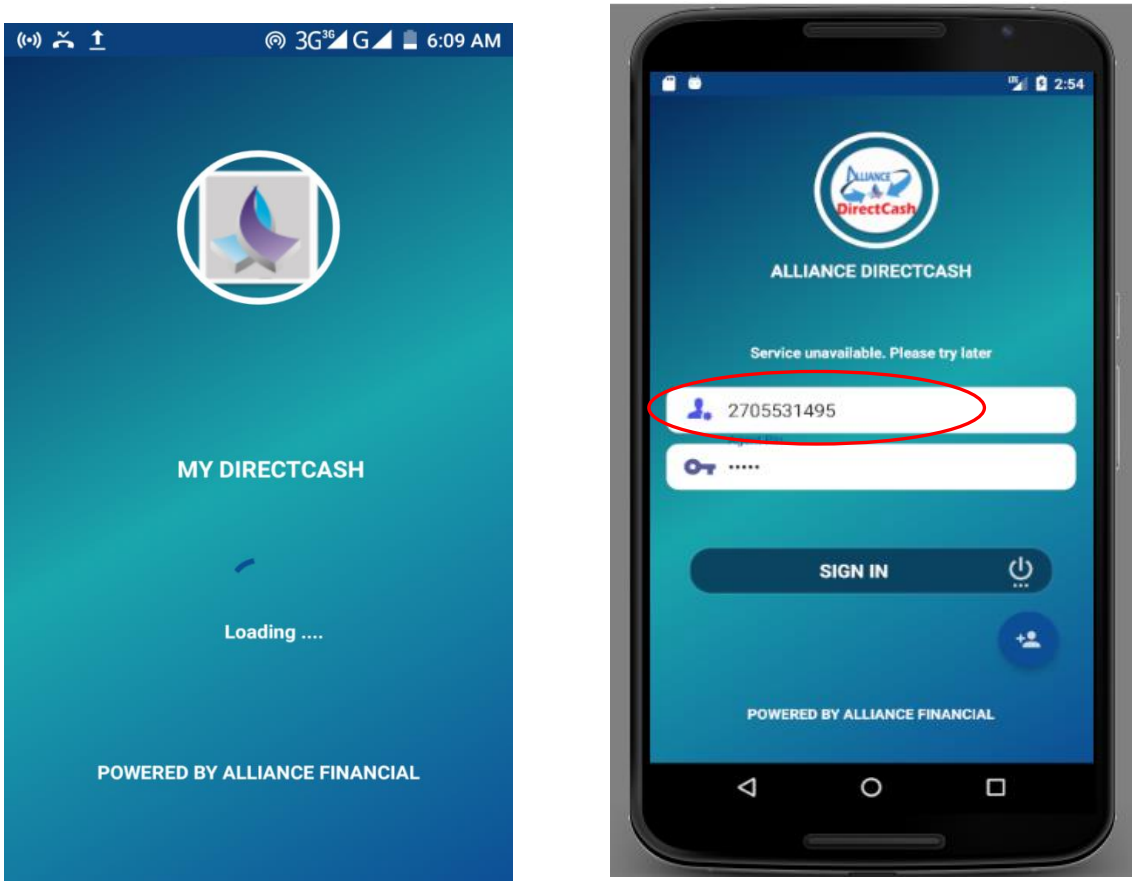


Figure 32: Interface de Connexion de "DirectCash"

A ce niveau, l'application demande les paramètres de connexion du client à savoir l'identifiant et le mot de passe. Ces paramètres doivent être renseignés correctement pour permettre au client de se connecter à l'application. Lorsque le client clique sur « SIGN IN », l'application vérifie si le client a déjà été enregistré auprès de l'infrastructure à clé publique. Si ce n'est pas le cas, l'application exécute un processus en arrière-plan pour créer le couple de clefs pour le client en question et le sauvegarde dans la mémoire du téléphone. La clé privée du client est chiffrée avec l'IMEI du téléphone mobile utilisé.

3.1.2.2 Demande et installation du certificat SSL

Notre application « DirectCash » contrôle la mémoire de stockage du téléphone à la recherche d'un certificat SSL.

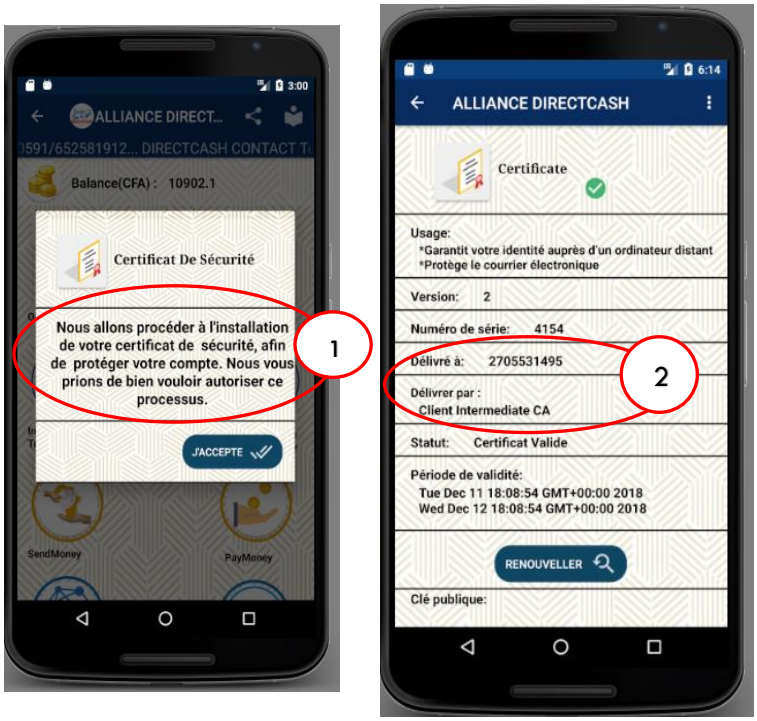


Figure 33: Interface de contrôle puis de présentations des certoficats Clients dans l'application "DirectCash"

Nous allons ensuite vérifie si ce certificat est provient bien de notre PKI,

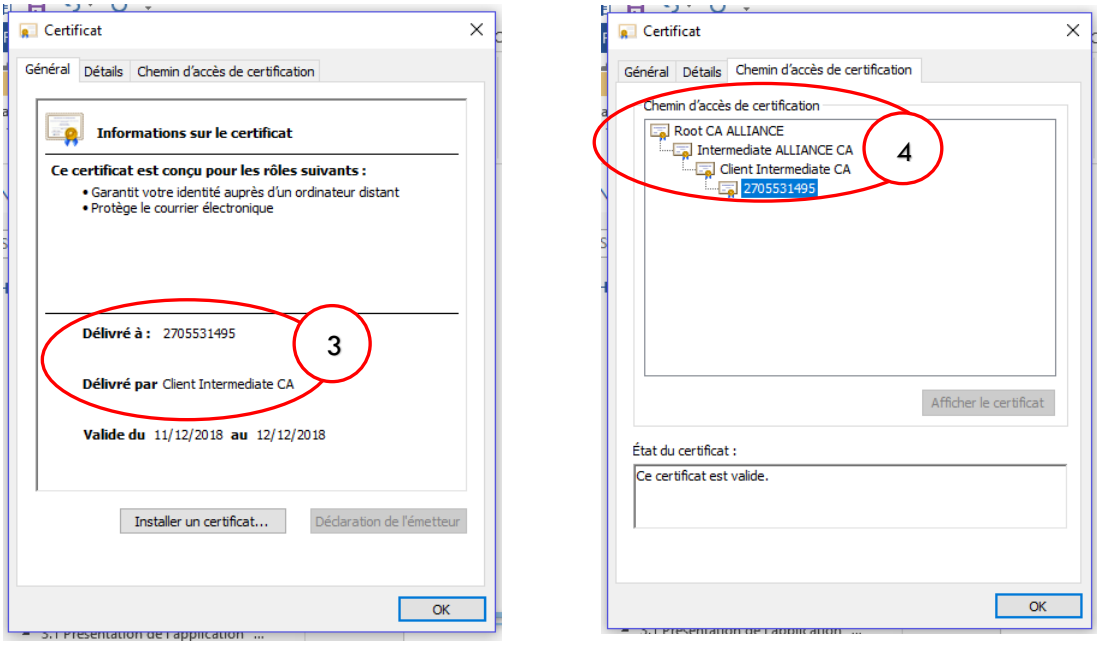


Figure 34: Présentation du certificat SSL du client 2705531495

4 : Ici, nous remarquons que le certificat du client « 2705531495 » nouvellement créé, fait intervenir une autorité racine « Root CA ALLIANCE » et deux autorités intermédiaires : « Intermediate ALLIANCE CA » et « Client Intermediate CA », qui ont toutes été enregistrées au niveau de la PKI.

Le client « 2705531495 » possède donc une paire de clé privée et publique pour garantir son identité après des serveurs d'Alliance Financial.

3.1.2.3 Présentation de l'interface d'accueil.

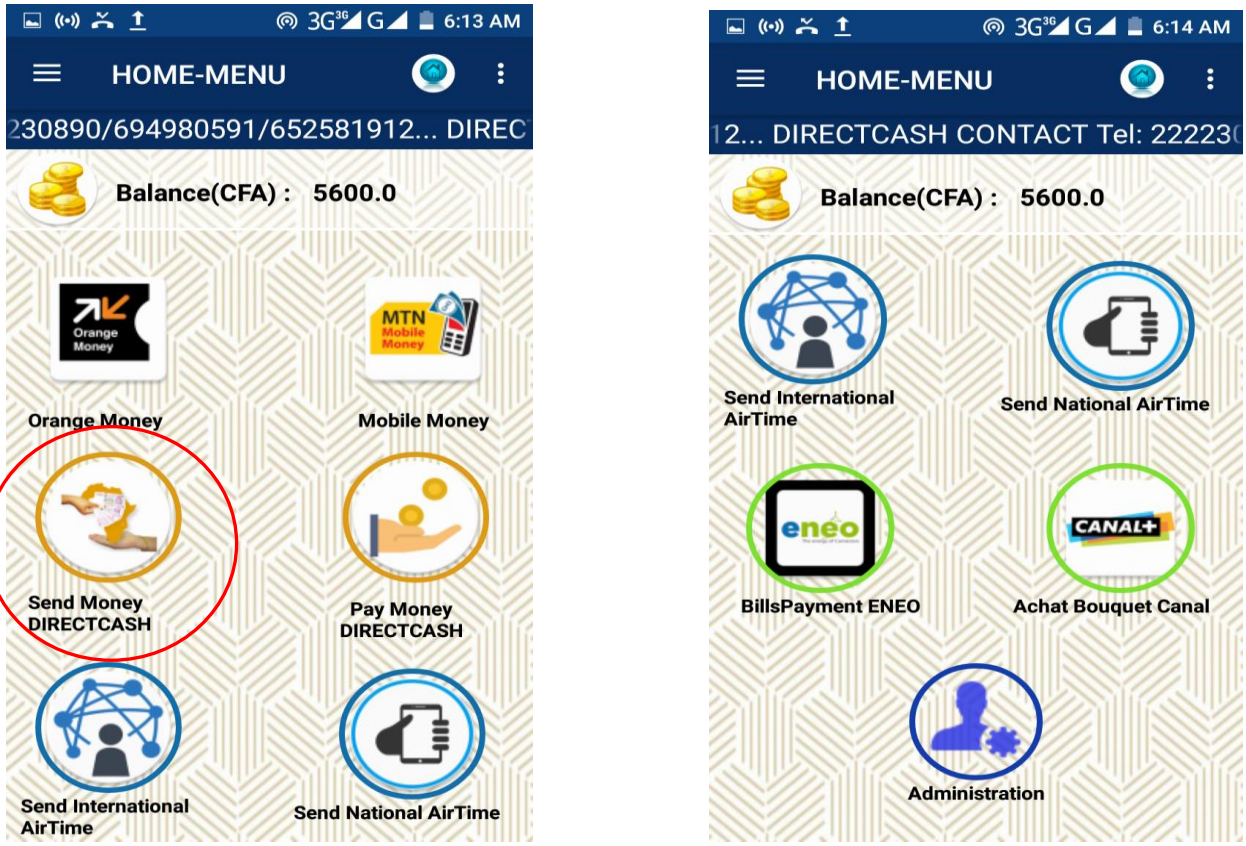


Figure 35: Interface présentant les services de l'application DirectCash

Comme vous pouvez remarquer, cette fenêtre présente les services fournis dans l'application. Ces services sont entre autres :

- l'envoi d'argent « DirectCash » ;
- le retrait d'argent « DirectCash » ;
- le payement des factures d'électricité ENEO ;
- le réabonnement Canal + ;
- l'achat du crédit de communication Orange, MTN, NextTel, CAMTEL, Yoomee ;
- l'achat du crédit de communication au niveau international à travers plus 412 opérateurs téléphoniques.

Le solde du client est mentionné plus haut et les transactions sont effectuées à hauteur de ce montant. Pour la suite, nous allons présenter uniquement deux services, l'envoi d'argent « DirectCash » et le retrait d'argent « DirectCash ».

3.1.2.4 Présentation du service d'envoi d'argent.

Le service d'envoi d'argent s'opère en trois étapes : la première étape consiste à renseigner les informations suivantes :

- Le numéro de téléphone du bénéficiaire,
- Le numéro de téléphone de l'expéditeur,
- Le montant de la transaction,
- Le numéro de CNI de l'expéditeur,

Pour la simulation, nous allons effectuer un envoi d'argent (1000 FCFA) du numéro « 690975410 » au numéro « 698184760 »

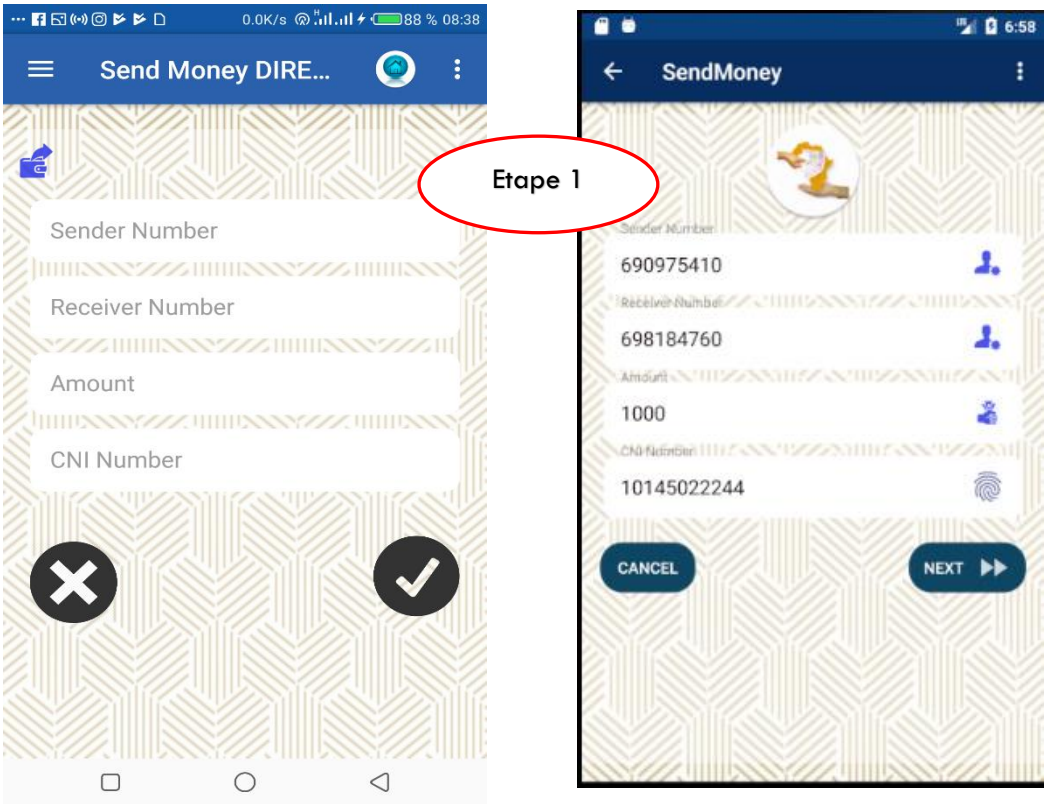


Figure 36: Illustration du service d'envoi d'argent "DirectCash" étape 1

La deuxième étape présente les détails de la transaction avec les frais de service inclus.

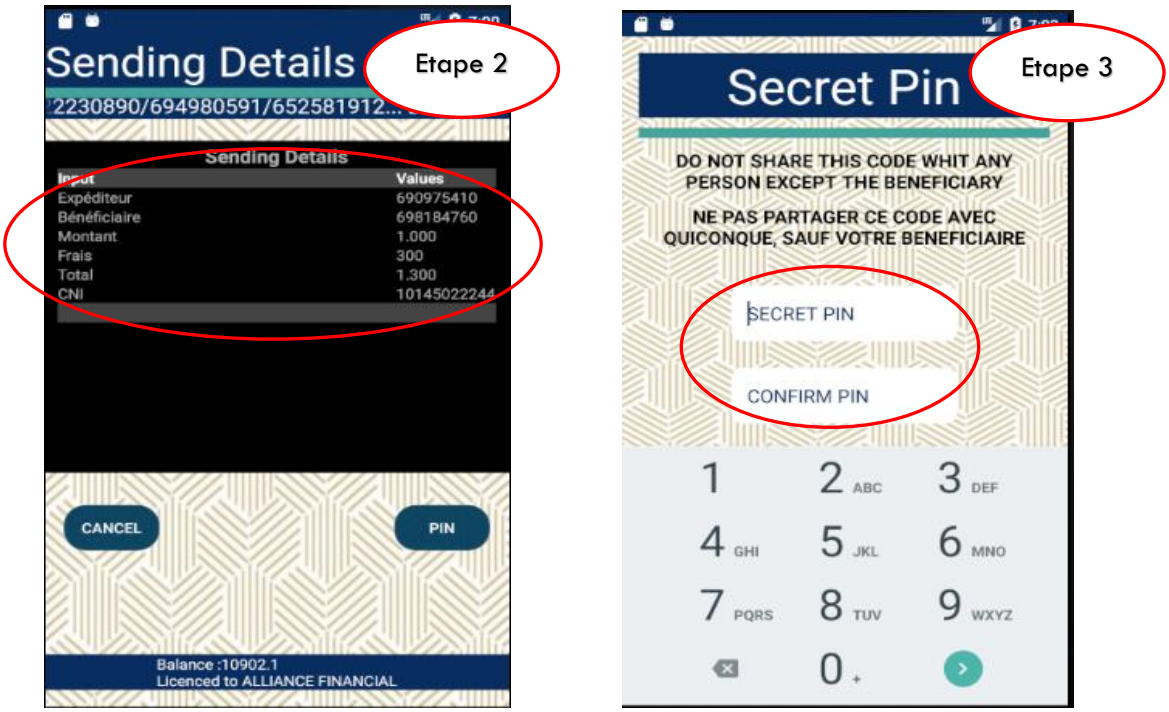


Figure 37: Illustration du service d'envoi d'argent "DirectCash" étape 2

Comme vous pouvez le voir, les frais de transactions figurent sur la facture.

La troisième étape consiste à entrer le mot de passe de la transaction. Ce mot de passe sera partagé entre l'expéditeur et le bénéficiaire. Il permettra au bénéficiaire de retirer son argent. L'expéditeur et le bénéficiaire sont ensuite informés par SMS par rapport à la transaction.

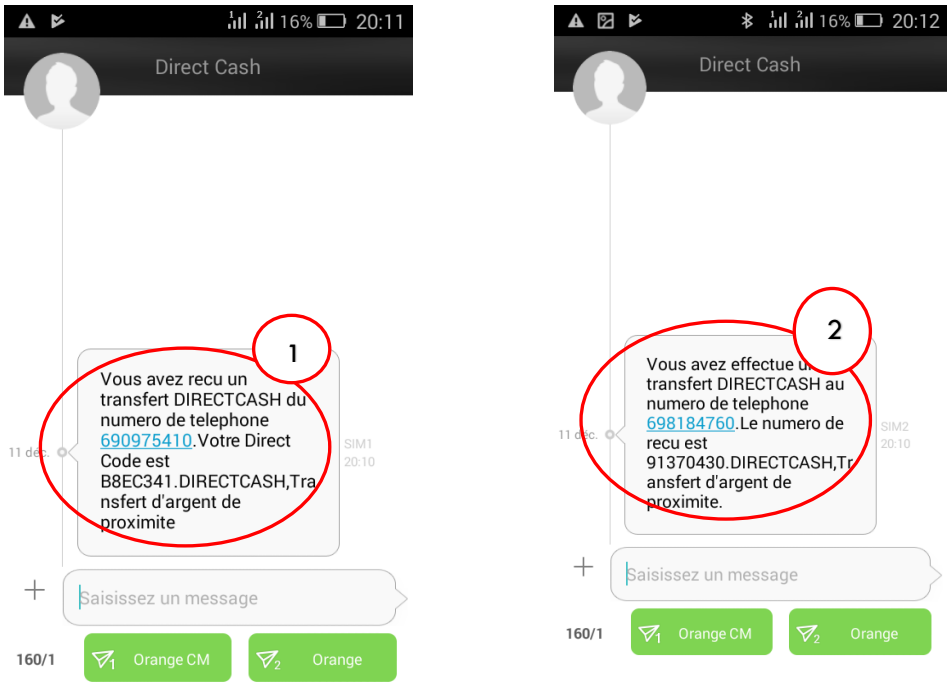


Figure 38: Message de notification de la transaction

Comme vous pouvez le voir sur la figure ci-dessus :

2 ✓ Le SMS reçu par l'expéditeur contient le numéro de la transaction. Ce numéro sera utilisé pour annuler la transaction en cas de problème majeur.

1 ✓ Par contre le SMS reçu par le bénéficiaire contient un « DirectCode ». Ce « DirectCode » sera utilisé par le bénéficiaire pour le retrait de son argent.

La dernière étape est facultative. Elle donne tout juste la possibilité au client d'imprimer la facture associée à la transaction.

Figure 39: Reçu de la transaction

3 Comme vous pouvez le remarqué, sur la facture (figure 39), apparait un QR-Code. Ce code contient le hash de la transaction effectuée. Ce hash est aussi contenu dans la base de données blockchain. Celui-ci permet d'assurer l'authenticité de la facture imprimée.

Pour la suite, nous allons vérifier si cette transaction a bien été signée puis enregistrée dans la blockchain.

3.2 Présentation de l'application blockchain

3.2.1 Architecture de l'application

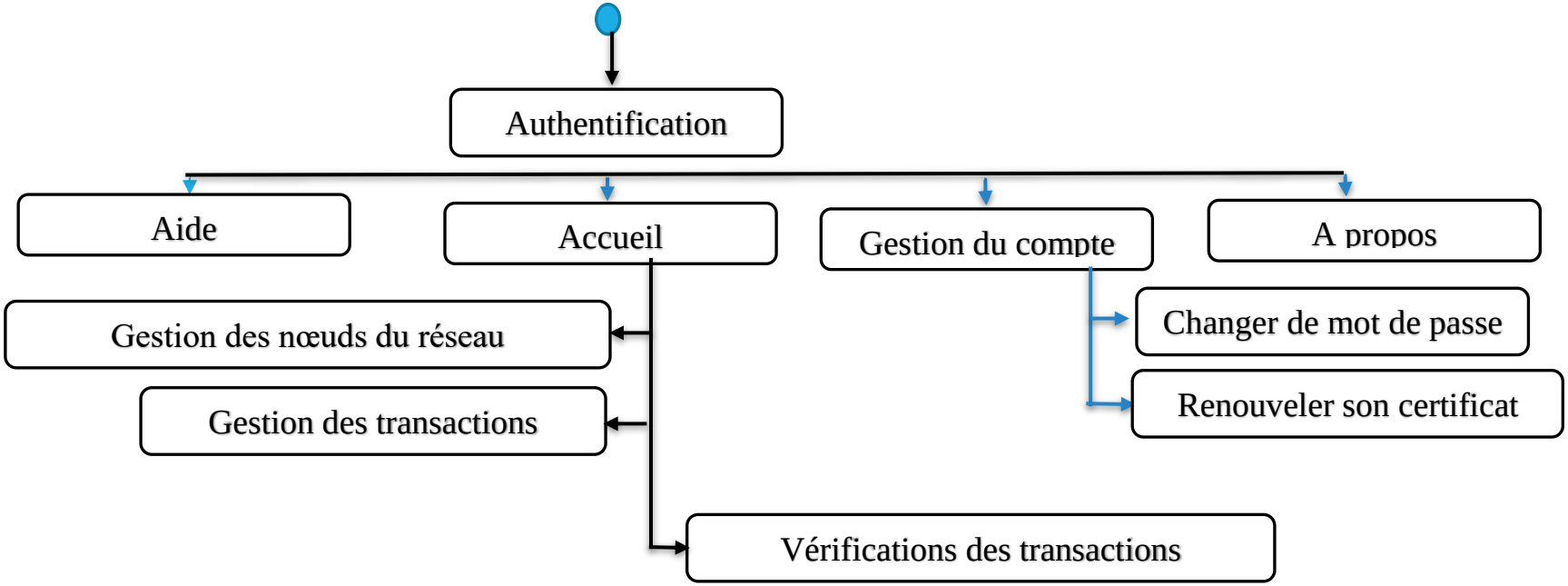
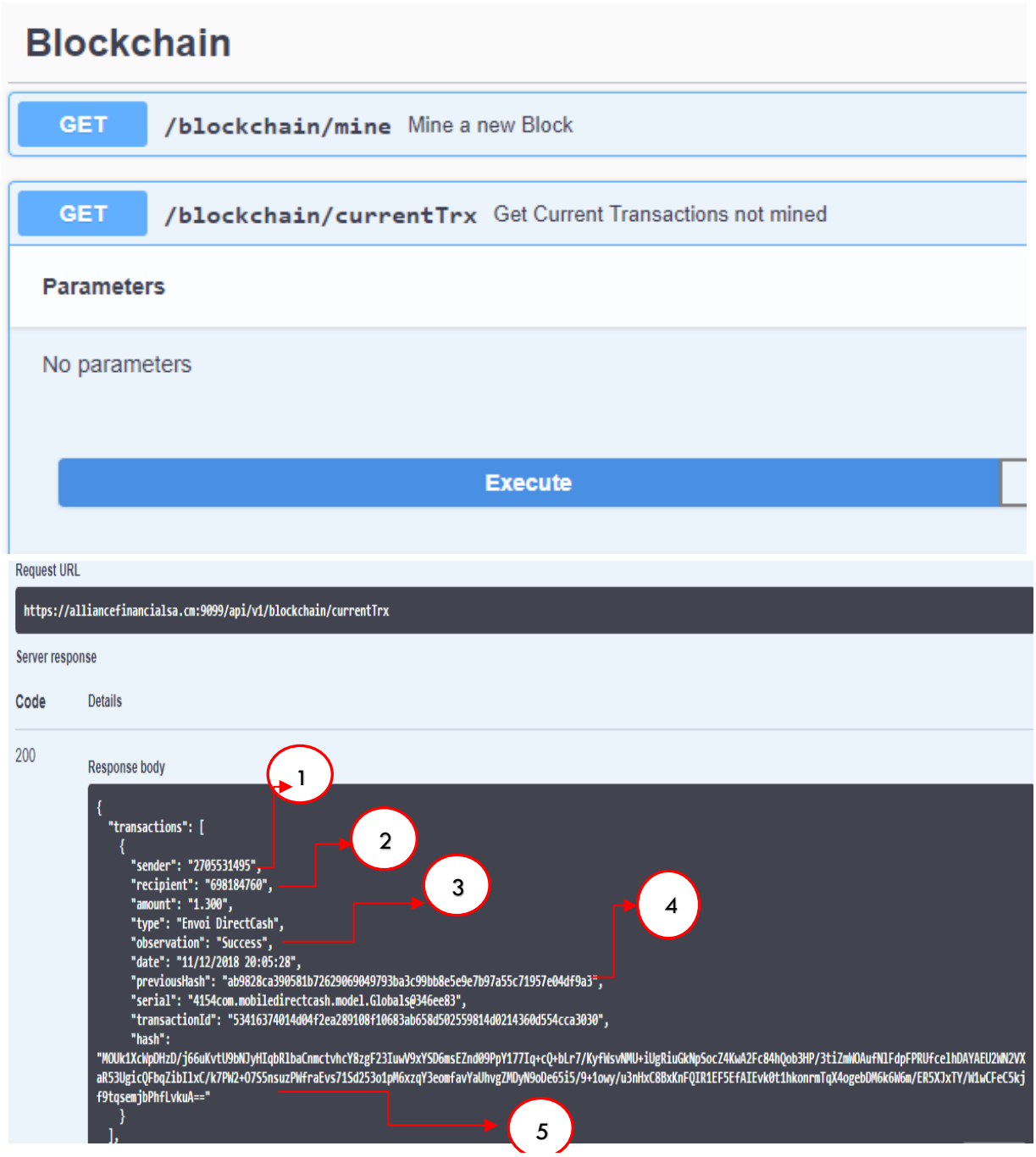


Figure 40: Architecture du module de gestion de la blockchain

3.2.2 Présentation la base données des transactions

Nous allons revenir sur la transaction présentée au paragraphe **3.1.2.4.** Rappelons qu'il s'agissait d'un envoi d'argent « DirectCash » avec comme expéditeur le numéro de téléphone « 690975410 » et comme bénéficiaire le numéro de téléphone « 698184760 » et le montant envoyé est de 1300Fcfa (1000Fcfa montant net+ 300Fcfa frais de service). Nous allons interroger un des nœuds de notre blockchain pour avoir la liste des transactions qui n'ont pas encore été minées.




```
{
  "transactions": [
    {
      "sender": "2705531495",
      "recipient": "698184760",
      "amount": "1.300",
      "type": "Envoi DirectCash",
      "observation": "Success",
      "date": "11/12/2018 20:05:28",
      "previousHash": "ab9828ca390581b72629069049793ba3c99bb8e5e9e7b97a55c71957e04df9a3",
      "serial": "4154com.mobiledirectcash.model.Globals@346ee83",
      "transactionId": "53416374014d04f2ea289108f10683ab658d502559814d0214360d554cca3030",
      "hash":
"MOUk1XcWpDHzD/j66uKvtU9bNJyHIqbRlbaCnmctvhcY8zgF23IuwV9xYSD6msEZnd09PpY177Iq+cQ+bLr7/KyfWsvNMU+iUgRiuGkNpSocZ4KwA2Fc84hQob3HP/3tiZmWOAufNlFdpFPRUfcelhDAYAEU2WN2VX
aR53UgicQFbqZibIlxC/k7PW2+O7S5nsuzPWfraEvs715d253o1pM6xzqY3eomfavYaUhvgZMDyN9oDe65i5/9+1owy/u3nHxC8BxKnFQIR1EF5EfAIEvk0t1hkonrmTqX4ogebDM6k6W6m/ER5XJxTY/W1wCFeC5kj
f9tqsemjbPhfLvkuA=="
    }
  ],
```


Figure 41: Contenu d'une d'une transaction

1 : Représente l'identifiant du client qui a effectué la transaction. Nous pouvons remarquer qu'il s'agit bien du client « 2705531495 » mentionné plus haut.

2 : Représente le bénéficiaire de la transaction. Il s'agit bien du numéro de téléphone « 698184760 ».

3 : Représente le statut de transaction. Il vaut « Success », ce qui indique que notre transaction n'a rencontré aucun problème au niveau du nœud de la blockchain.

4 : Représente la signature de la précédente transaction (n'oublions pas que les transactions sont aussi chainées entre-elles).

5 : Représente la signature de notre transaction.

Dans notre cahier de charge, nous avons convenu d'avoir un système qui permet l'horodatage des transactions. Ce que nous venons de vous présenter est la preuve que nos transactions sont bien horodatées.

Nous avons donc au niveau de ce nœud, un bloc contenant une transaction. Il ne nous reste plus qu'à miner ce bloc.

Voici la liste des blocs contenant chacun les transactions financières des clients d'Alliance Financial.

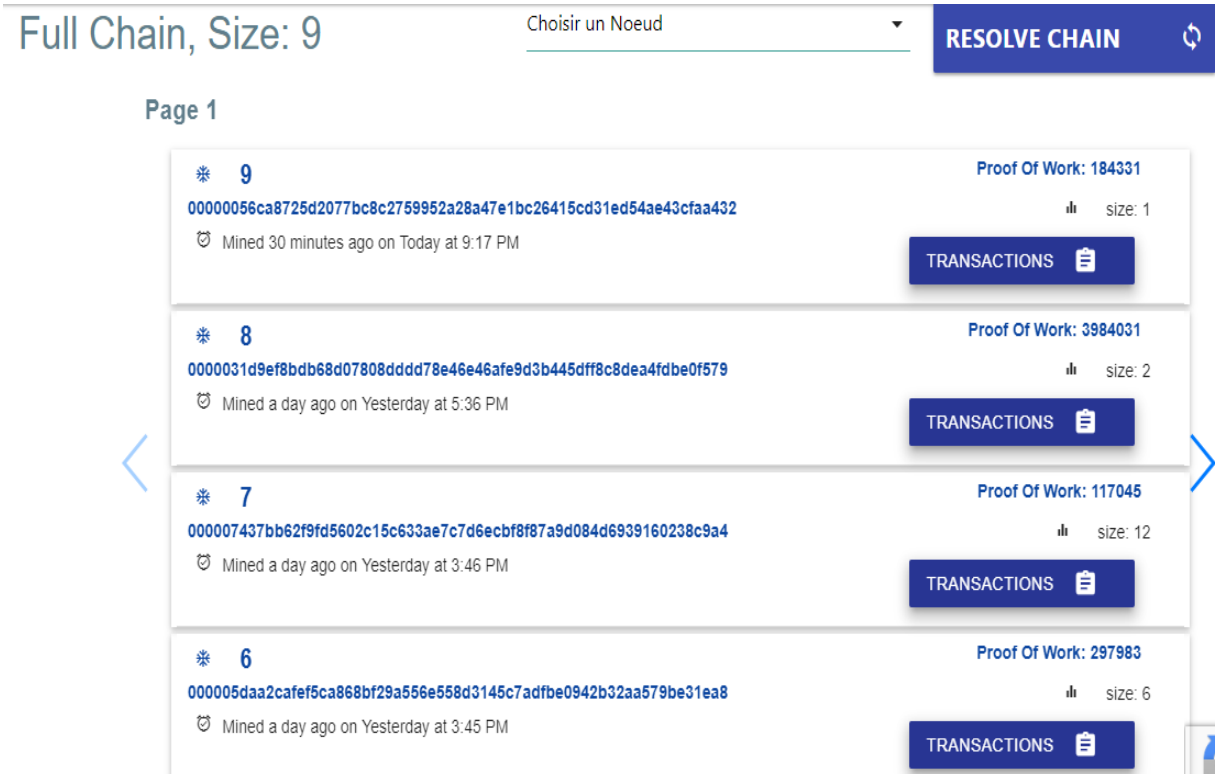


Figure 42: Interface de la base de données des transactions financières.

Nous allons nous intéresser uniquement au bloc 9 car c'est celui que nous venons de générer.

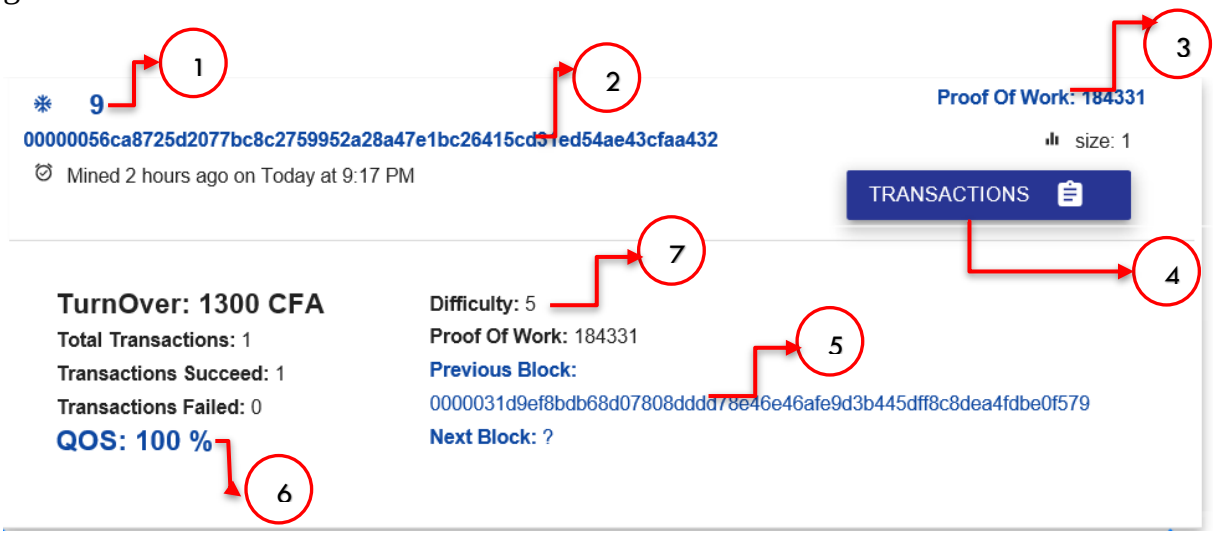


Figure 43: Visualisation d'un bloc de transactions

1 : Représente l'index du bloc courant.

2 : Représente la signature du block (encore appelé le hash), qui est en réalité le condensé de toutes les transactions se trouvant dans le bloc.

3 : Représente « la preuve de travail », qui est en réalité le nombre « i » mentionné au paragraphe **2.2.2.2 d,** qui a permis de sceller le bloc. C'est aussi la preuve que le nœud a effectué 184331 itérations afin de trouver le nonce cryptographique permettant de sceller le bloc.

4 : Permet d'accéder aux transactions contenues dans le bloc.

5 : Représente la signature du bloc précédent (car dans la blockchain, les blocs sont chainés entre eux).

6 : Représente le taux de transactions ayant abouties dans le bloc.

7 : Représente la difficulté de l'équation de minage. Comme prévu dans le cahier de charge, cette difficulté a été fixée à 5 par rapport à la puissance de calcul du nœud qui est d'environ 4 millions de hash par seconde.

Nous allons jeter un coup d'œil sur les transactions contenues dans ce bloc.

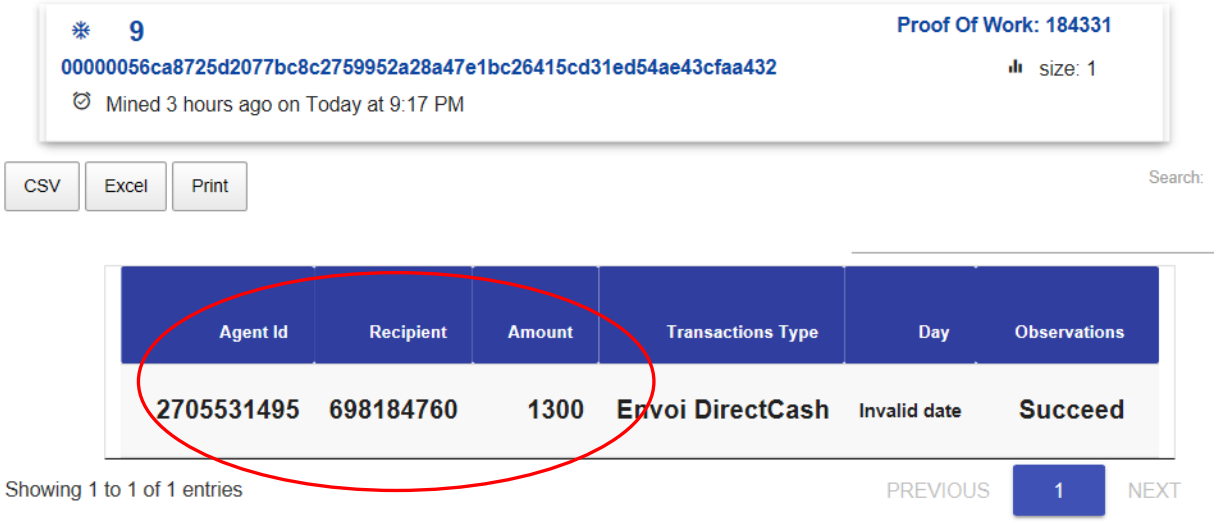


Figure 44: Visualisation des transactions dans un bloc

Nous remarquons que ce bloc contient une seule transaction : c'est celle que nous venons d'effectuer.

La procédure que nous venons de décrire est celle qui est opérée par chaque nœud du réseau afin d'insérer de manière sécurisée les transactions dans le grand livre des transactions : la blockchain.

3.3 Présentation de l'application pour la gestion de la PKI

3.3.1 Architecture de l'application

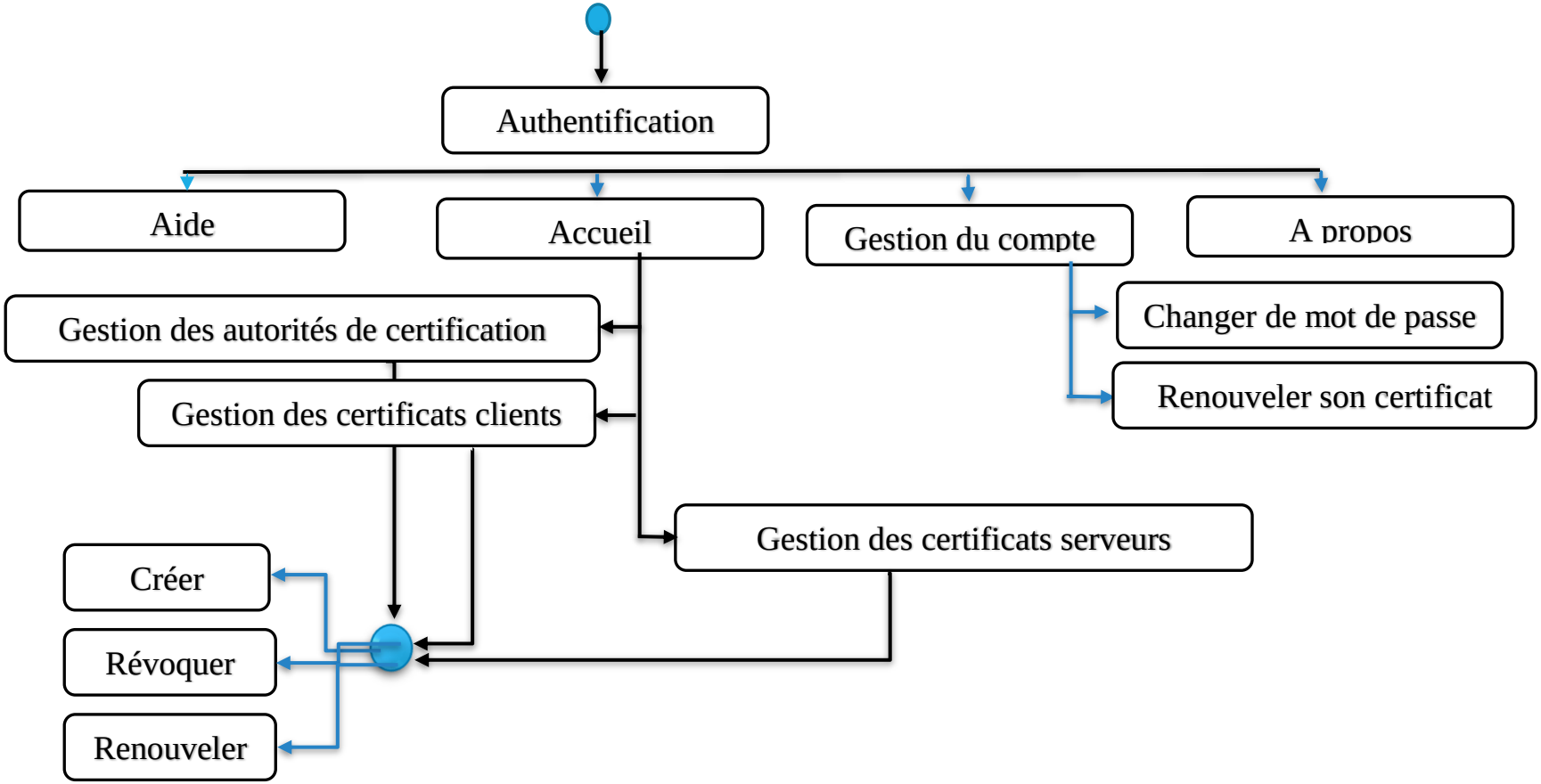


Figure 45: Architecture du module de gestion de la PKI

3.3.2 Présentation de l'interface de programmation (API) pour les services de la PKI.

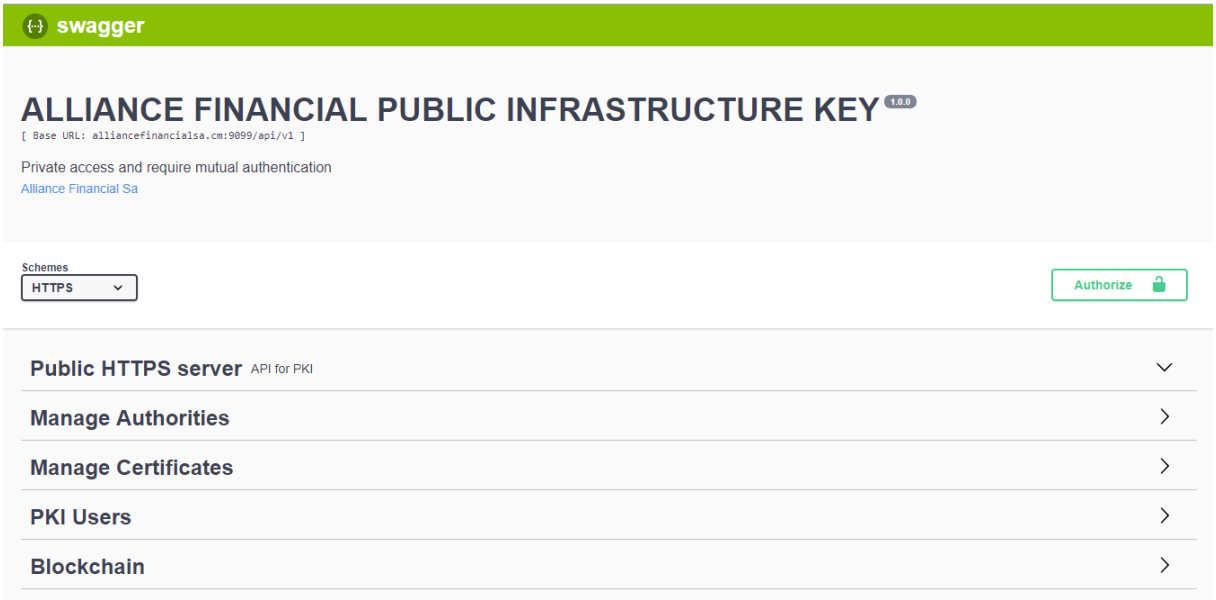


Figure 46: Serveur HTTPS, pour la gestion des fonctionnalités de la PKI.

Sur cette interface, nous avons quatre modules. Le module de gestion des autorités de la PKI (Manage Authorities), le module de gestion des certificats (Manage Certificates), le module de gestion des utilisateurs de la PKI (PKI Users) et le module de gestion de la blockchain (Blockchan).

- Présentation de l'interface de gestion des autorités de la PKI

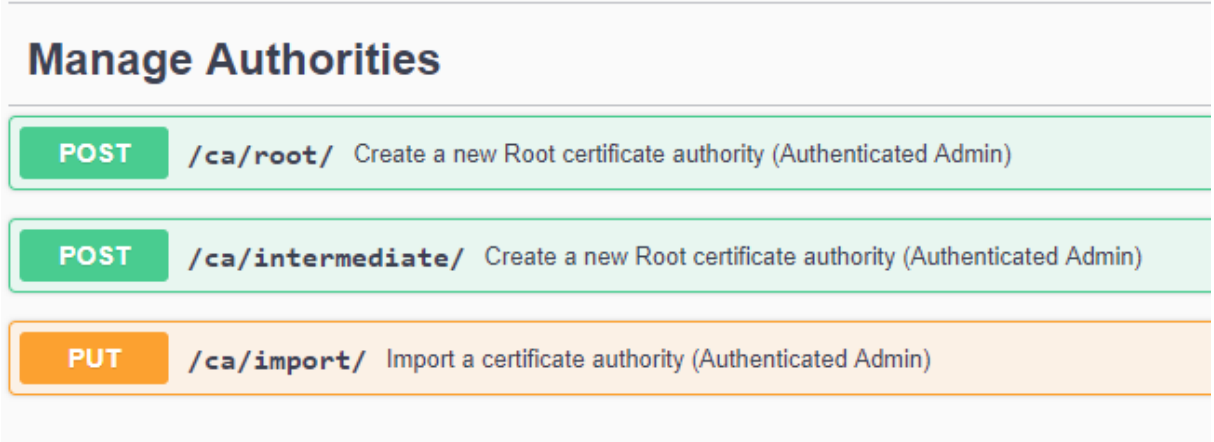


Figure 47: Fonctionnalités pour la gestion des autorités de certification

Cette interface présente des liens https (POST et PUT) permettant d'ajouter ou d'importer (clé privée et clé publique) une autorité racine ou une autorité intermédiaire dans la PKI. Pour ajouter par exemple une nouvelle autorité racine, voici les champs requis :

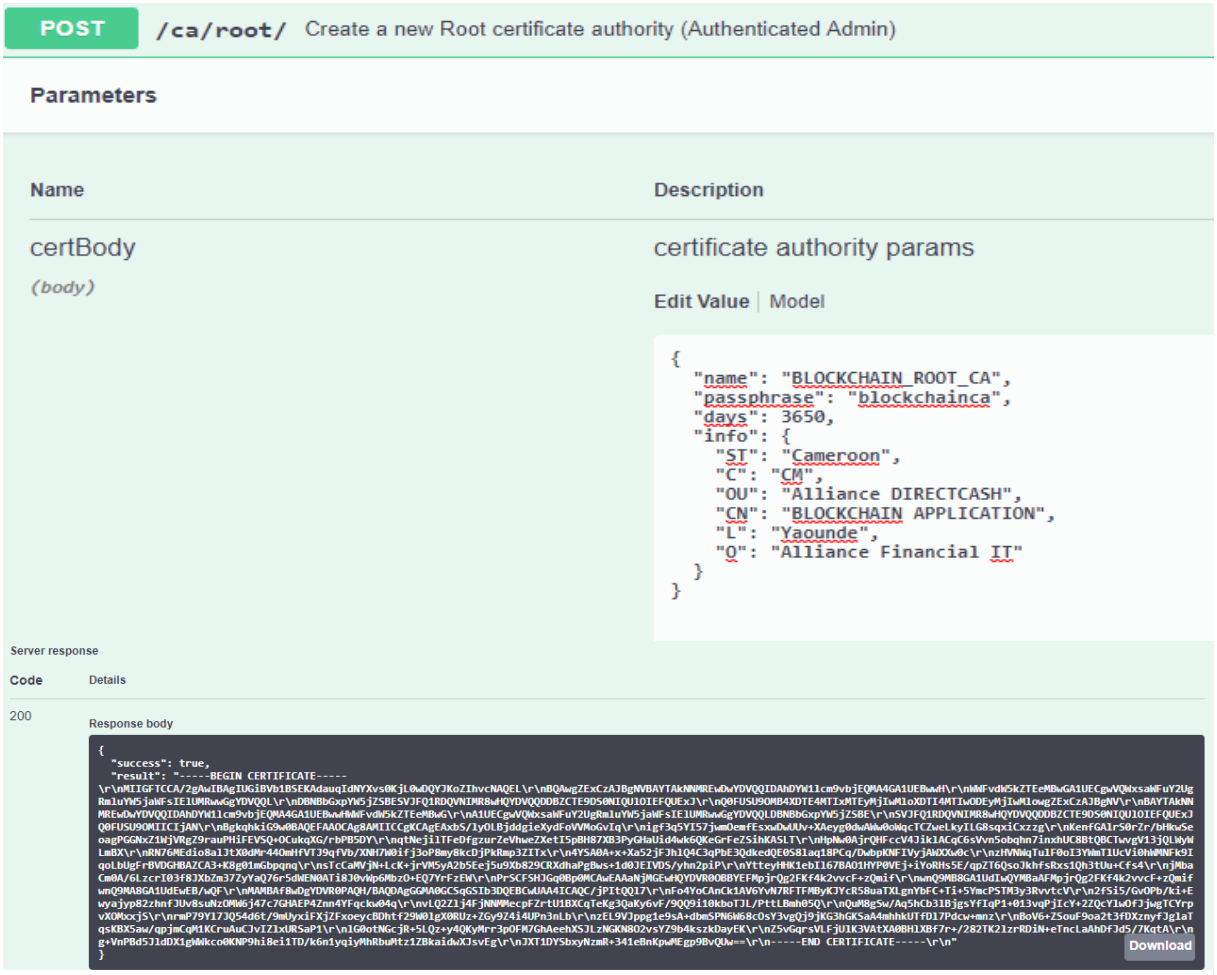


Figure 48: Interface de création d'une nouvelle autorité de certification

Commentaires:

Nous venons de créer une autorité racine dans notre PKI, avec les paramètres suivants :

- **Nom (name)** : BLOCKCHAIN_ROOT_CA,
- **Mot de passe pour la protection de la clè privée (passphrase):** blockhainca
- **Durée de vie du certificat de l'autorité (days)** : 3650 jours soient 10 ans,
- **Pays (info.ST)** : Cameroon,
- **Code du pays (info.C)** : CM,
- **Unité d'organisation (info.OU)** : Alliance DIRECTCASH,
- **Nom commun (info**.CN) : BLOCKCHAIN APPLICATION
- **Ville (info.L):** Yaounde,
- **Organisation (info.O)** : Alliance Financial IT

La reponse du serveur HTPPS est le certificat de d'autorité créée plus haut. Ce certificat se présente comme suit :

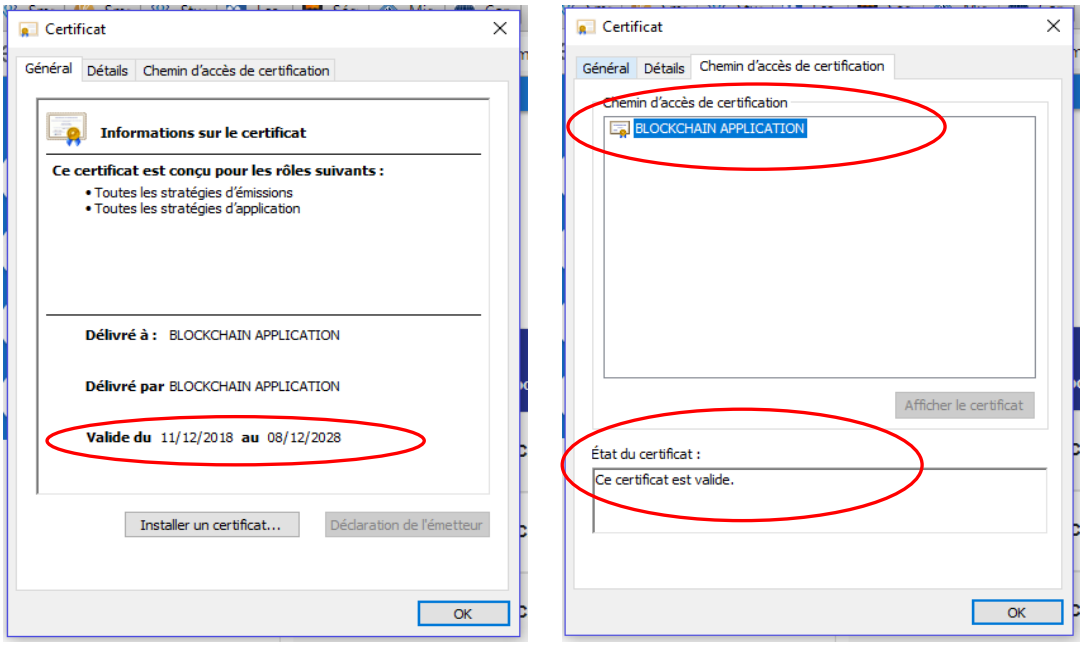


Figure 49: Présentation du certificat de l'autorité racine « BLOCKCHAIN APPLICATION »

Nous avons aussi procédé de la même maniére pour enregistrer une autotité de certificat intermediate avec comme nom « CA BLOCKCHAIN INTERMEDIATE ». Le serveur a répondu à la requête d'enregistrement et nous a retourner le certificat de cette autorité .

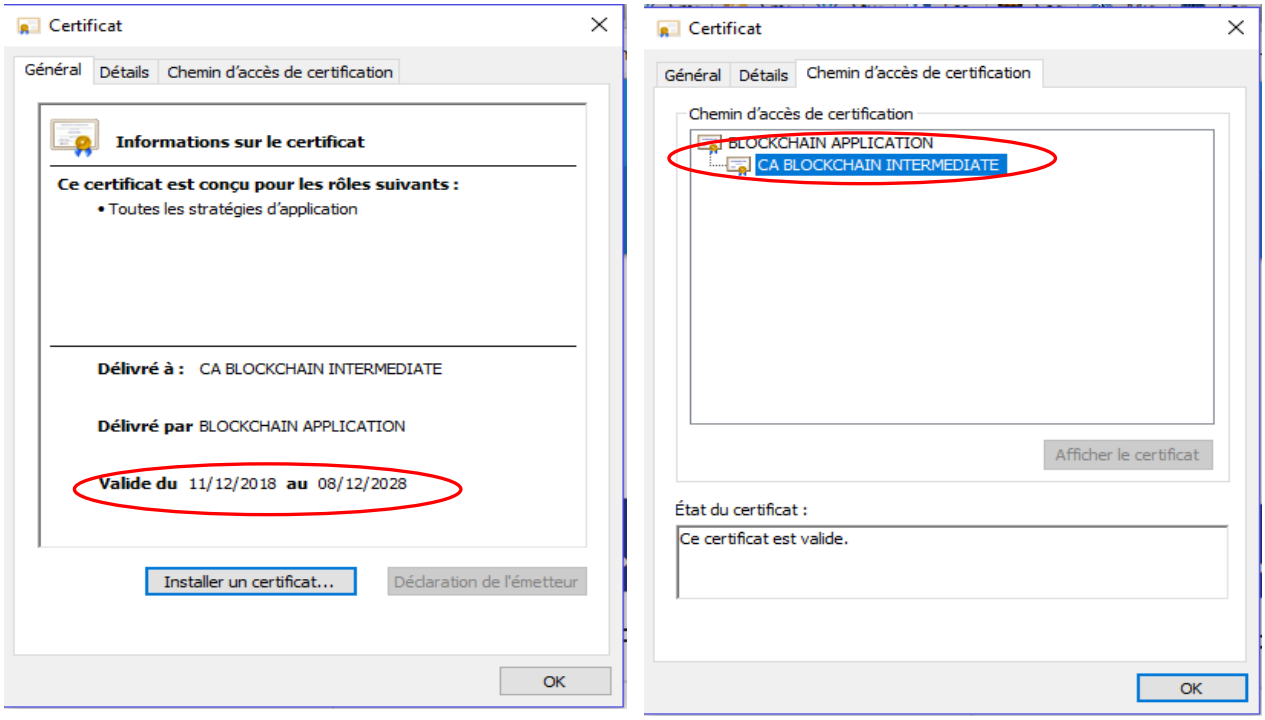


Figure 50: Présentation du certificat de l'autorité intermédiaire "CA BLOCKCHAIN INTERMEDIATE"

Nous pouvons bien observer sur le certificat de l'autorité intermediat « CA INTERMEDIATE BLOCKCHAIN » la chaine de confiance établie avec l'autorité racine.

- Présentation de l'interface de gestion certificats de la PKI

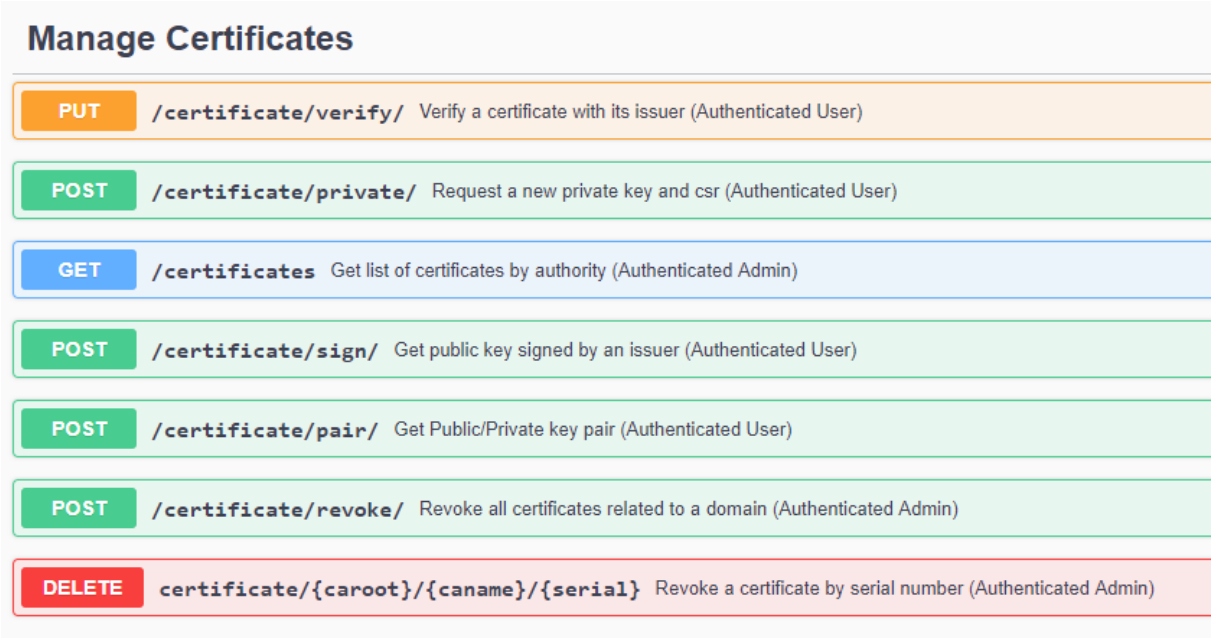


Figure 51: Présentations de liens disponibles pour la gestion des certificats

Sur cette interface, figurent les liens (PUT, POST, GET, et DELETE) permettant d'accomplir les fonctionnalités suivantes:

- Vérifier si un certificat a bien été généré par une autorité de la PKI (PUT/certificate/verify),
- Générer une nouvelle clé privée (POST/certificate/private),
- Avoir la liste des certificats (GET/certificate),
- Signer une demande de certificat (POST/certificate/sign),
- Générer une paire de clés publique et privée (POST/certificate/pair),
- Révoquer les certificats attachés à un même domaine (POST/certificate/revoke),
- Révoquer une certificat (/certificate/{caroot}/{caname}/{serial}.

Ces fonctionnalités correspondent bien aux attendes de notre cahier de charge. Pour les exploiter, il convient d'utiliser des clients HTTPS et dont nous avons implémenté une application Web.

3.3.3 Application Web pour la gestion de la PKI

3.3.3.1 Interface d'authentification

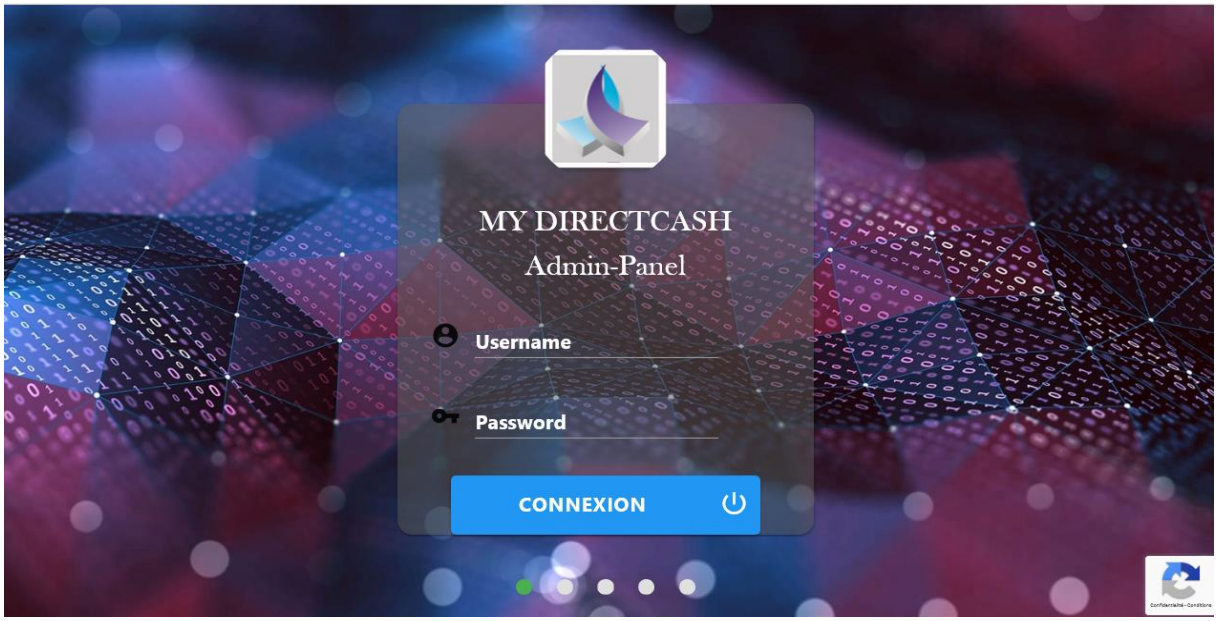


Figure 52: Interface de connexion pour l'application web client permettant de gérer la blockchain

Cette interface est accessible à travers le lien: https://localhost/directcash. Les paramètres de connexion sont alors requis pour permettre à l'administrateur de la plateforme d'accéder aux fonctionnalités de l'application.

3.3.3.2 Interface d'administration de la PKI

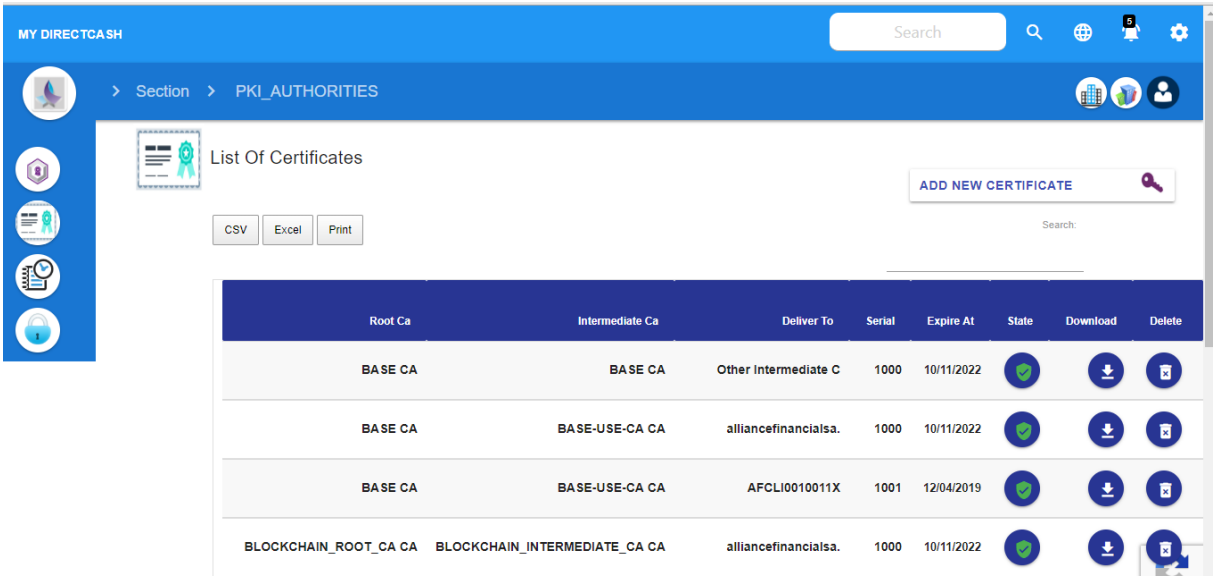
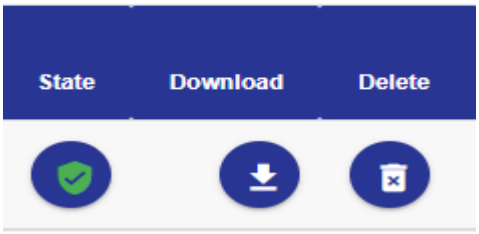


Figure 53: Liste des certificats de la PKI

Sur cette interface, nous avons la liste de tous les certificats générés par la PKI et un autre bouton pour en créer un autre. Aussi, dans la liste des certificats, deux fonctionnalités sont disponibles : celle qui permet de télécharger le certificat et celle qui permet de le révoquer.



Le formulaire utilisé pour générer un nouveau certificat se présente comme suit :

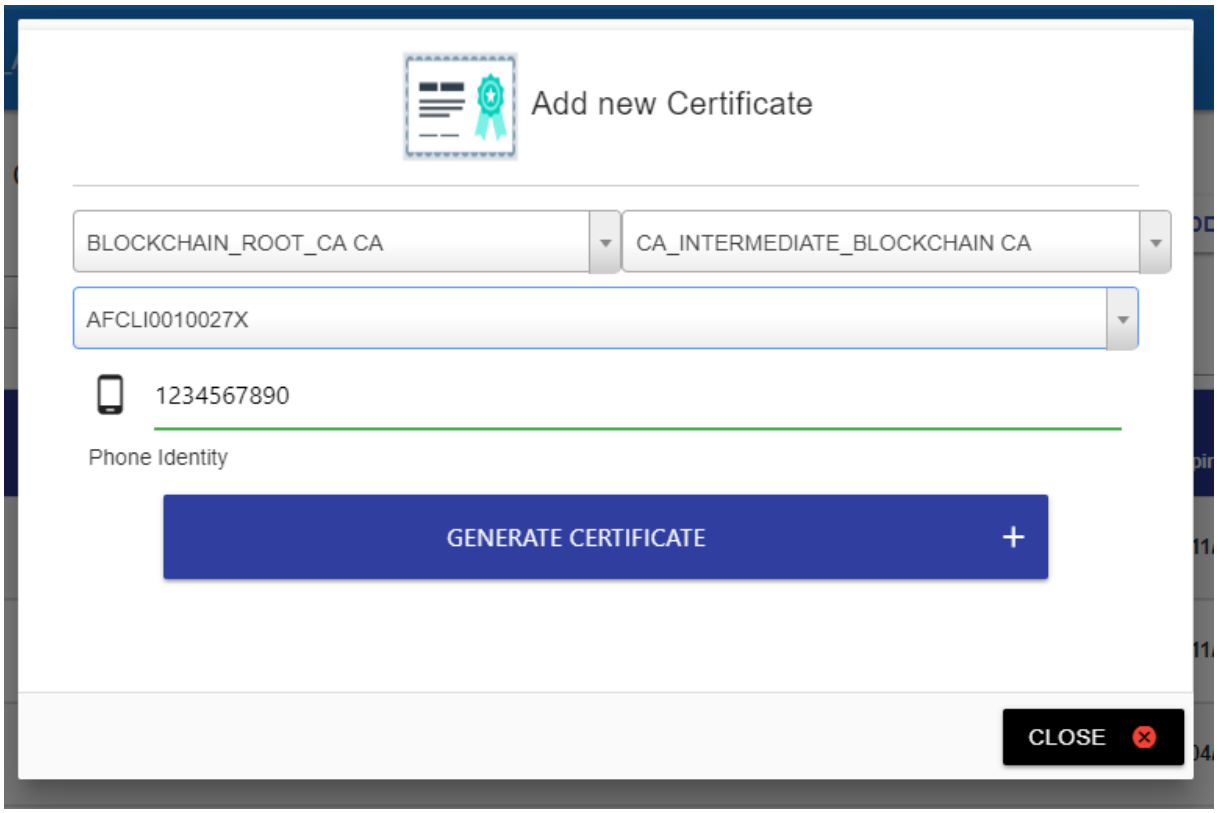


Figure 54: Interface d'ajout d'un nouveau certificat

Nous voulons en réalité générer un certificat pour le client dont l'ID est « AFCLI0010027X » et les autorités qui vont intervenir pour signer son certificat sont :

- l'autorité racine « BLOCKCHAIN_ROOT_CA »
- l'autorité intermédiaire « CA_INTERMEDIATE_BLOCKCHAIN »

En en effet il s'agit des deux autorités de certifications précédemment créées.

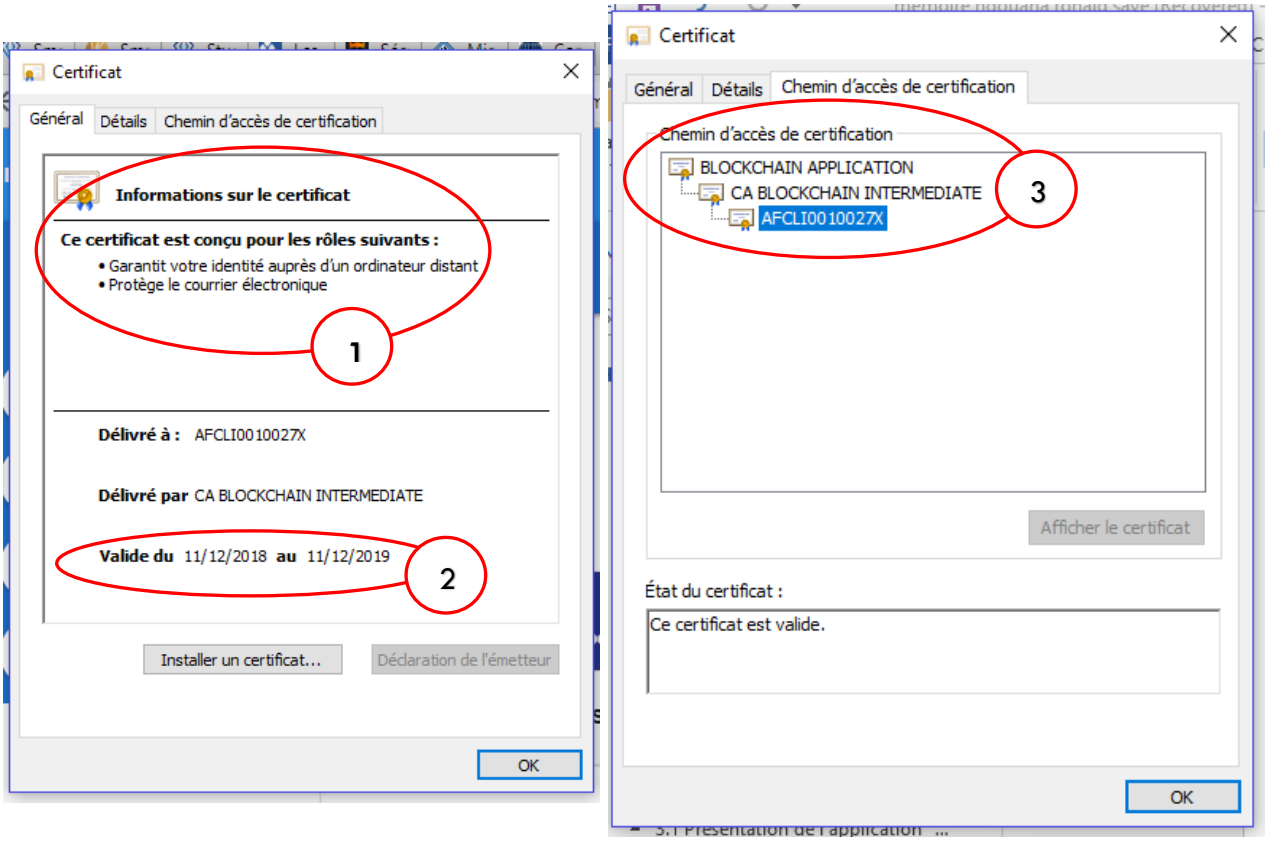


Figure 55: Présentation du certificat du client AFCLI00100027X

1 : Représente les rôles du certificat. Ce certificat a dont deux rôles :

- ✓ Garantir l'identité du client « AFLCI00100027X » auprès des serveurs de l'entreprise.
- ✓ Chiffrer les transactions financières du client « AFLCI00100027X ».

2 : Représente la durée de validité du certificat du client « AFLCI00100027X ». Cette durée est d'une année.

3 : Représente la chaine de confiance caractérisée par l'autorité racine « BLOCKCHAIN APPLICATION CA », l'autorité intermédiaire « CA BLOCKHAIN INTERMEDIATE » et puis le client « AFLCI00100027X ».

Ceci est bien la preuve que l'infrastructure à clé publique remplir les fonctionnalités prévues dans notre cahier de charge.

3.4 Conclusion du chapitre

Dans ce chapitre nous avons présenté les différentes applications qui entrent dans le processus de sécurité et de traçabilité des transactions financières des clients d'Alliance Financial. Dans un premier temps, nous avons présenté l'application mobile « DirectCash » utilisée par les clients pour effectuer leurs transactions. Nous avons ensuite simulé une opération d'envoi d'argent pour vérifier si tous les mécanismes prévus pour garantir la sécurité et la traçabilité de la transaction ont bien été implémentés. Ensuite nous avons présenté l'application web contenant l'historique des transactions financières. En parcourant cette application, nous avons constaté que la transaction financière effectuée avait bien été signée, horodatée, puis sceller dans un bloc par un nœud du réseau : ce qui témoigne que nous avons bien atteint les objectifs prévus dans notre cahier de charge. Enfin, nous avons présenté notre infrastructure à clé publique. Dans ce module, nous avons créé des autorités de certification (racine et intermédiaire), nous avons généré un certificat SSL pour un client et nous l'avons fait signer par l'une des autorités de certification. Nous avons ensuite vérifié si la chaine de confiance entre les certificats était bien respectée. Dans cette infrastructure à clé publique, étaient aussi présentes les fonctionnalités pour télécharger et révoquer un certificat.

Conclusion Générale

Face aux problèmes de sécurité et de traçabilité que nous avons pu déceler au sein du système d'information d'Alliance Financial, précisément au niveau de ses services financiers ouverts en ligne, nous avons mené une démarche scientifique afin de juguler ces problèmes. Nous rappelons que dans le processus d'analyse de ces problèmes, un audit de sécurité a été fait afin de justifier la pertinence de la mise en place de notre solution. L'objectif général visé par cette étude est d'implémenter un système d'information semblable à celui de la blockchain Bitcoin pour les services financiers d'Alliance Financial. Ce système regroupe des entités qui assurent d'une part la sécurité des transactions financières et d'autre part assurent leur traçabilité.

Dans un premier temps, il convenait d'abord d'étudier la blockchain Bitcoin, qui en réalité est un grand livre regroupant des transactions financières. Ce grand livre est partagé par les nœuds du réseau dont les principales fonctionnalités sont : valider les transactions financières, ajouter les transactions financières dans ce grand livre, et assurer son intégrité au moyen de procédés cryptographiques qui demandent une puissance de calcul très élevée pour chaque nœud. L'opération qui permet d'assurer l'intégrité des transactions est le « minage » (relativement aux mineurs d'or). Cette opération conduit à la création d'une crypto-monnaie appelée « Bitcoin », attribuée aux mineurs en signe de récompense pour l'énergie et les ressources matérielles mises en place pour sceller les transactions financiers dans des blocs. L'ensemble des blocs contenant les transactions constitue la « blockchain ». Nous nous sommes appuyés sur ce mécanisme pour concevoir une solution semblable à celle-ci, car la blockchain reste jusqu'à présent, une des solutions les plus sécurisées pour garantir la sécurité et la traçabilité de toute information qui peut être numérisée. Les limites que nous avons évoquées pour cette technologie sont principalement liées à une consommation d'énergie très élevée pouvant atteindre la consommation électrique annuelle de tout un pays, et une mauvaise gestion des clés des comptes clients conduisant automatique à la perte de leur fonds en Bitcoin sachant qu'une seule unité de Bitcoin vaut entre deux millions et quatre millions de Fcfa.

L'analyse de la solution existante nous a permis d'évaluer le niveau de complexité de la solution à mettre en place. En d'autres termes, nous avons convenu de mettre en place un système semblable au niveau des procédés utilisés pour sécuriser et tracer les transactions, mais plutôt optimal au niveau de la consommation d'énergie et des clefs de protections des comptes clients. Ceci a conduit à la modélisation d'une infrastructure à clef publique capable d'assurer l'ensemble des fonctions suivantes : enregistrement de demande de clefs, signature des clefs, publication des clefs, livraison

des clefs, contrôle du statut des clefs, révocation des clefs et recouvrement des clefs. Les clefs fournies par notre infrastructure garantissent d'une part leur identité auprès des services d'Alliance Financial, et d'autre part cryptent leurs transactions financières de manière à ce que seul le serveur d'Alliance Financial soit à mesure de les décrypter. Nous avons ensuite utilisé cette infrastructure comme l'un des composants des entités requises dans le processus de traçabilité des transactions financières. La deuxième partie de notre méthodologie était consacrée à la modélisation de la blockchain. Nous avons opté pour une architecture décentralisée comportant deux nœuds (serveurs), une infrastructure à clé publique et plusieurs clients. Un client d'Alliance communique au moins avec l'un de ces nœuds afin d'effectuer une transaction. Chaque nœud à la possibilité de valider, de diffuser et de sceller de nouvelles transactions. Tous les nœuds ont en temps réel une trace de l'ensemble des transactions du réseau. Chaque nœud participe à intervalle de temps régulier à un consensus dont la finalité est de s'accorder sur une chaine de transactions intègre et la plus longue procédée par au moins 51% des nœuds.

La modélisation de l'infrastructure à clef publique et de la blockchain au moyen des diagrammes d'UML a conduit à l'implémentation de deux applications web client et d'un serveur http au niveau de chaque nœud. Nous avons ainsi présenté toutes les étapes entrant dans le processus de sécurité et de traçabilité d'une transaction financière que nous avons simulée. Nous avons illustré comment se fait le processus de demande puis d'installation des clefs pour un client. Nous avons présenté la base de données des transactions financières en se rassurant que ces transactions étaient bien signées et horodatées. Nous avons terminé par la présentation de l'infrastructure à clef publique en créant des autorités de certification racine et intermédiaire, puis des certificats SSL client.

Au vu des spécifications du cahier de charges et des résultats obtenus, nous pouvons dire que nous avons un système fonctionnel présentant les fonctionnalités requises. Il y a adéquation entre les résultats attendus et les résultats obtenus. Les objectifs sont donc atteints. Mais nous tenons quand même à signaler quelques limites au niveau des résultats obtenus. Tout abord la technologie blockchain que nous avons implémenté est une technologie orientée pour les réseaux à grande échelle afin d'empêcher l'attaque 51%. En effet cette attaque consiste à corrompre 51% des nœuds du réseau. Donc plus le réseau est dense, plus il est difficile de corrompe les nœuds. Or dans notre cas, nous avons uniquement deux nœuds. Aussi, nous n'avons pas pu entrer en possession des mineurs (machines très puissances). Nous nous sommes contentés des serveurs ordinaires avec une puissance de calcul de 4 Millions de hash/s au lieu de 4 Téra de hash/s comme prévu dans les spécifications techniques (Soit un rapport d'un Million).

Ce travail nous a été très bénéfique dans la mesure où nous avons embrassé l'une des technologies les plus sécurisées dans tout le monde entier qui est la blockchain. C'est

vrai que nous n'avons pas pu toucher à tous ses aspects, mais nous nous réjouissons déjà d'avoir osé et d'avoir construit un système fiable capable de garantir la sécurité et la traçabilité des transactions financières des clients d'Alliance Financial Cameroun.

Perspectives

Nous projetons étendre notre solution dans plusieurs autres secteurs d'activités, puisque, comme nous le disons tantôt, la blockchain est capable d'assurer la traçabilité de toute information ou donnée jugée confidentielle et pouvant être numérisée. Le premier secteur visé est le secteur bancaire où nous aurons la possibilité de tracer les transactions financières des clients des banques. Le deuxième secteur visé est celui de l'agro-alimentaire, où nous aurons la possibilité de suivre toute une chaine de production en insérant à chaque fois dans la blockchain toutes les informations importantes, manipulées lors de la création d'un nouveau produit. Le troisième et dernier secteur visé est celui de la santé, où nous aurons la possibilité de suivre un patient au sein d'un hôpital durant toute sa vie (opérations subies, maladies traitées, médicaments prescrits, etc).

Références

[1]. Bitcoin: A peer-to-peer electronic cash system. Nakamoto, S.2008.

[2]. Satoshi Nakamoto. Bitcoin.fr. [En ligne] https://bitcoin.fr/satoshi-nakamoto/.

[3]. Total Electricity Net Consumption. U.S. Energy Information Administration (EIA). [En ligne] https://www.eia.gov/beta/international/data/browser/#/?pa=0000002&c=ruvvvvvfvtvnvv1urvvvvfvvvvvvfvvvou20evvvvvvvvvnvvuvo&ct=0&tl_id=2-A&vs=INTL.2-2-AFGBKWH.A&vo=0&v=H&start=2013&end=2014

[4] Coinfox. [En ligne] http://www.coinfox.info/news/reviews/6417-proof-of-work-vs-proof-ofstake-merits-and-disadvantages, consulté le 20 Novembre, 2018.

[5] Hash Rate. [En ligne] https://www.blockchain.com/fr/charts/hash-rate, consulté le 20 Novembre, 2018.

[6] Livre d'ALEXANDRE FERNANDEZ-TORO Management de la sécurité de l'information « Mise en place d'un SMSI et audit de certification 2e Edition Implémentation ISO 27001 ».

[7] Livre de sécurité informatique Ethical hacking « Apprendre l'attaque pour mieux se défendre », par Sébastien LASSON, en 2009

[8] Audit de Sécurité des systèmes d'information. [En ligne]

https://www.antic.cm/index.php/fr/component/k2/item/315-security-audit.html; publié le 07, Août 2017 ; consulté le 20 Novembre 2018

[9] **« The Heartbleed Bug »** [archive], sur *Heartbleed* (publié le 9 avril 2014, consulté le 27 Septembre 2018)

[10] John Viega**,** Matt Messier et Pravir Chandra**, *Network Security with OpenSSL*,** Sebastopol, CA, O'Reilly, 15 juin 2002**,**

[11] David GABAY et Joseph GABAY, UML 2 analyse et conception, Paris: DUNOD, 2008**,**

[12] Livre blanc édité en Janvier 2016 par U • uchange.co. [En ligne]

https://www.finyear.com/attachment/648901/

[13] Infrastructures à Clés Publiques : Aspects Techniques et organisationnels présenté par Dr. Y. Challal, Maître de conférences Université de Technologie de Compiègne [En ligne]

https://www.itu.int/ITU-D/arb/ARO/2009/E-Cert/Documents/Doc14-Dr.Challal.pdf

[14] Public Key Infrastructure (PKI). Publié en Janvier 2010, consulté le 4 Novembre 2018 [En ligne]

http://igm.univ-mlv.fr/~dr/XPOSE2007/vma_PKI/pki.html

[15] Histoire de l'internet. Publié en Janvier 2010, consulté le 4 Novembre 2018 [En ligne]

https://www.universalis.fr/encyclopedie/internet-histoire/6-securite/

[16] Firewalls et applications Web : architecture et sécurisation, publié en 2012, consulté le 4 Septembre 2018 [En ligne]

http://www.chambet.com/publications/sec-web-apps/

Table des matières

Annexe 1

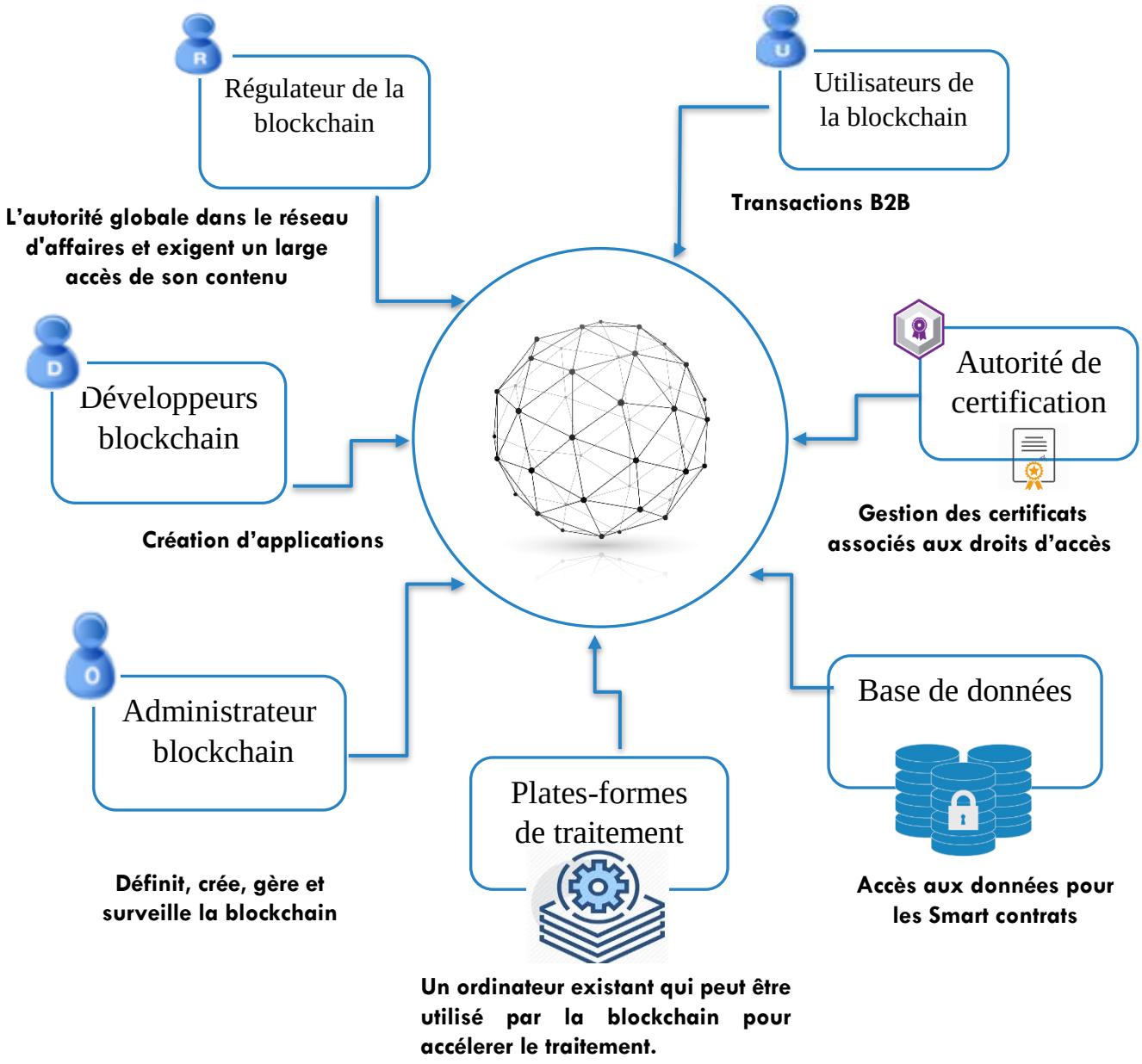
Extraits norme ISO 27001.

Table A.1 *(continued)*

A.12.1.3	Capacity management	*Control* The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.
A.12.1.4	Separation of development, testing and operational environments	*Control* Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.
A.12.2 Protection from malware		
Objective: To ensure that information and information processing facilities are protected against malware.		
A.12.2.1	Controls against malware	*Control* Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.
A.12.3 Backup		
Objective: To protect against loss of data.		
A.12.3.1	Information backup	*Control* Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.
A.14 System acquisition, development and maintenance		
A.14.1 Security requirements of information systems		
Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.		
A.14.1.1	Information security requirements analysis and specification	*Control* The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.
A.14.1.2	Securing application services on public networks	*Control* Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.
A.14.1.3	Protecting application services transactions	*Control* Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

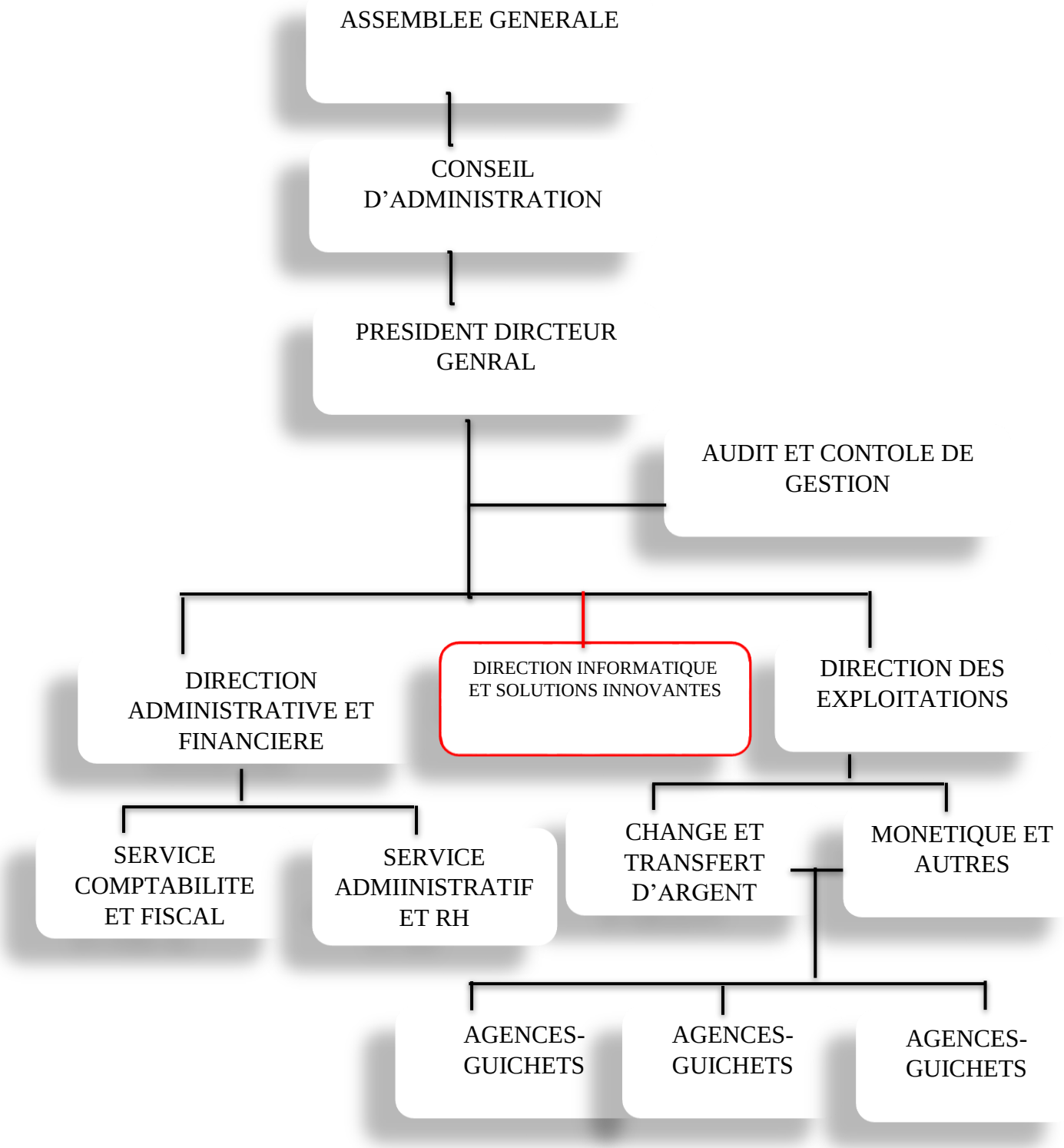
Annexe 2

Architecture des composants d'une blockchain



Annexe 3

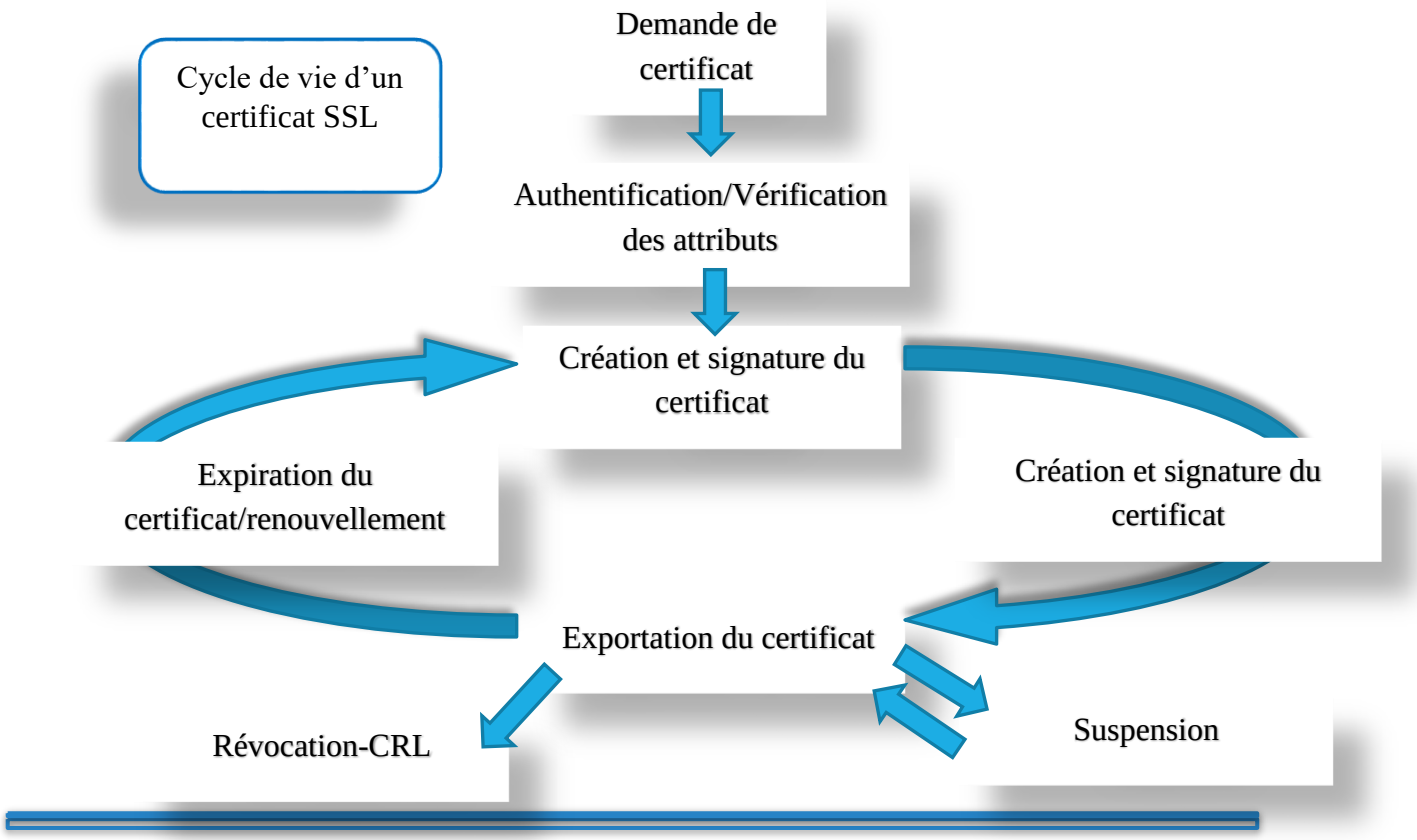
Organigramme d'Alliance Financial.



Annexe 4

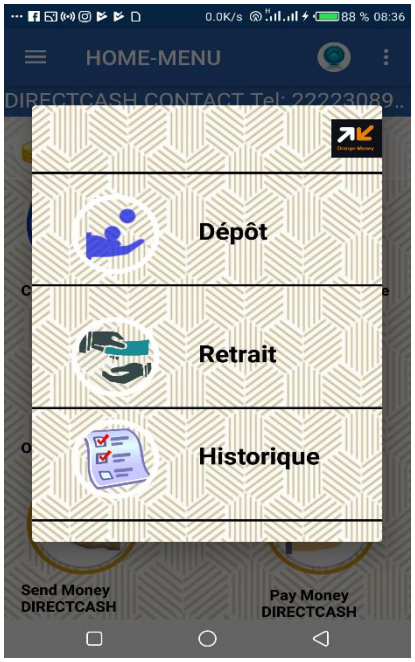
Format des certificats SSL adopté :

- Version
- Numéro de série
- Algorithme de signature du certificat
- DN (*Distinguished Name*) du délivreur (autorité de certification)
- Validité (dates limites)
  - Pas avant
  - Pas après
- DN de l'objet du certificat
- Informations sur la clé publique
  - Algorithme de la clé publique
  - Clé publique proprement dite
- Identifiant unique du signataire (optionnel, X.509v3)
- Identifiant unique du détenteur du certificat (optionnel, X.509v3)
- Extensions (optionnel, à partir de X.509v3)
  - Liste des extensions
- Signature des informations ci-dessus par l'autorité de



Annexe 5

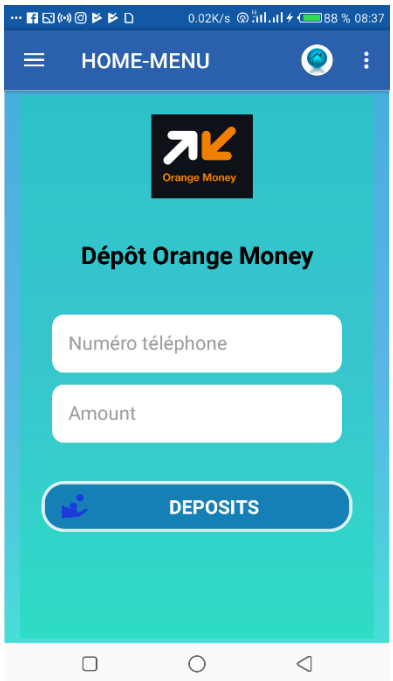
Autres services de l'application DirectCash : Dépôt/Retrait Orange Money

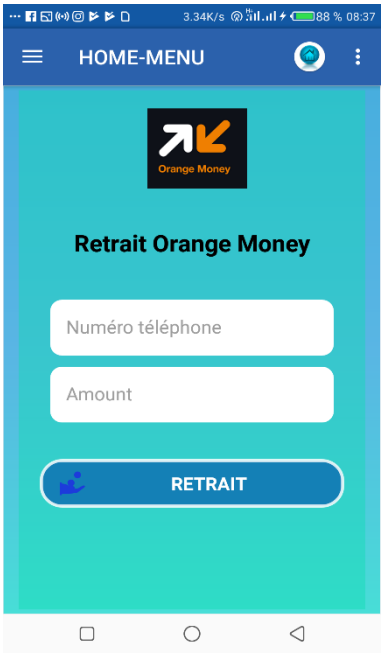


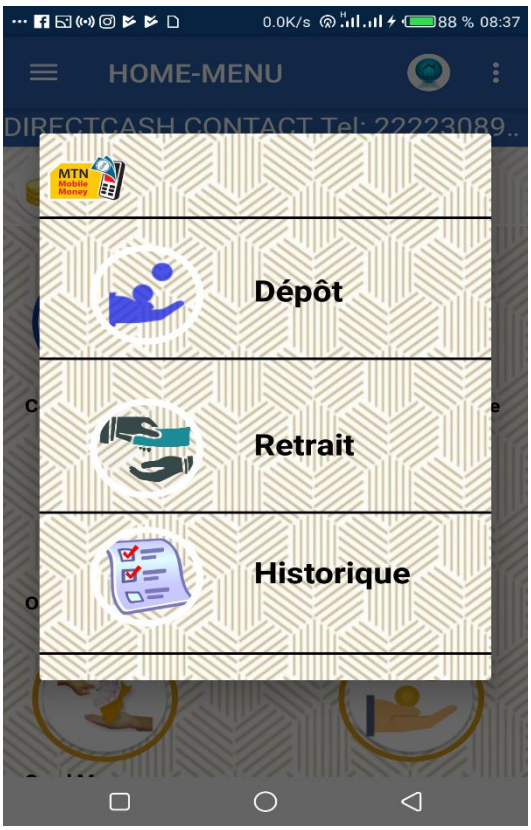
MODULE DE DEPOT/RETRAIT ORANGE MONEY :

Les champs à renseigner :

- N° Tel bénéficiaire,
- Montant,





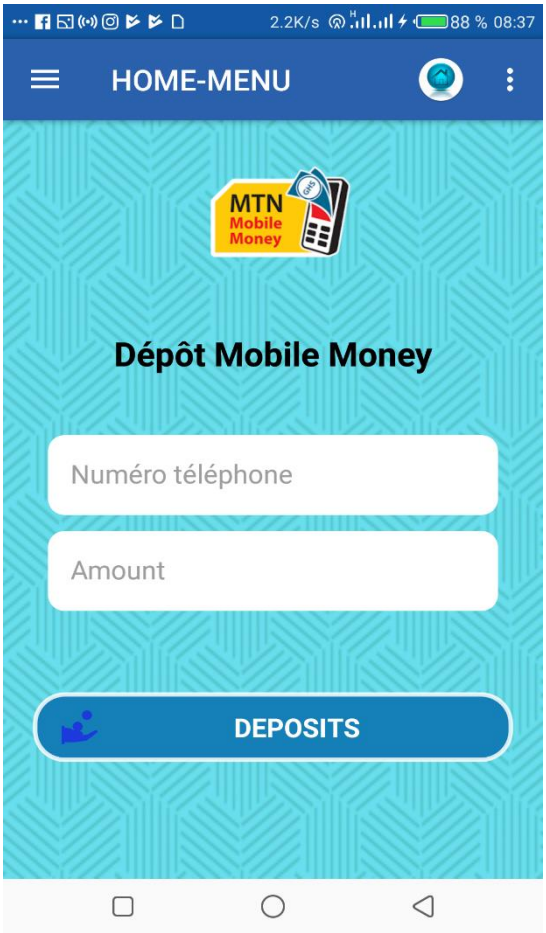


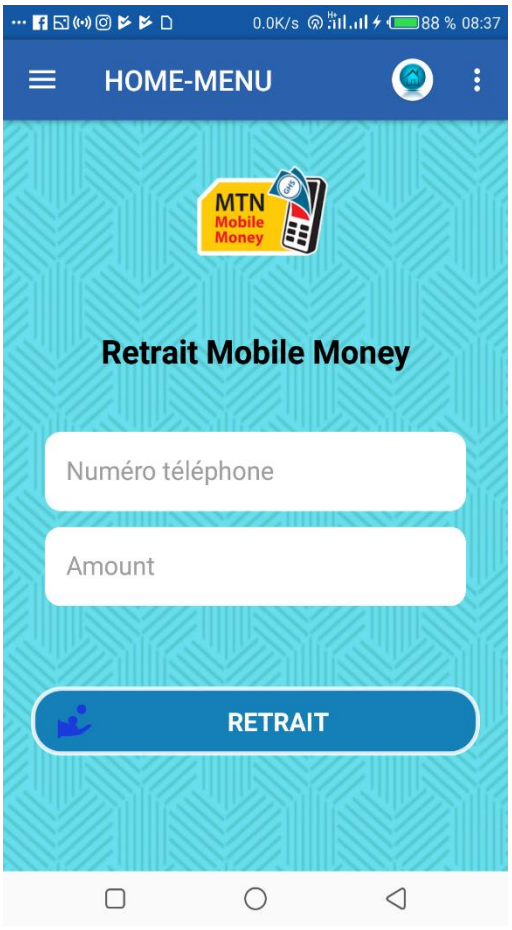
MODULE DE DEPOT/RETRAIT MOBILE MONEY :

Les champs à renseigner :

- N° Tel bénéficiaire,
- Montant,

MODULE DE DEPOT /RETRAIT





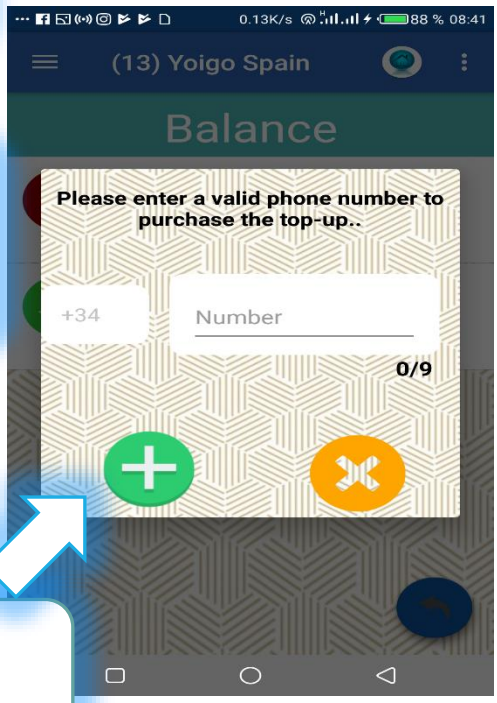
ETAPE 1 :

CHOIX DU PAYS

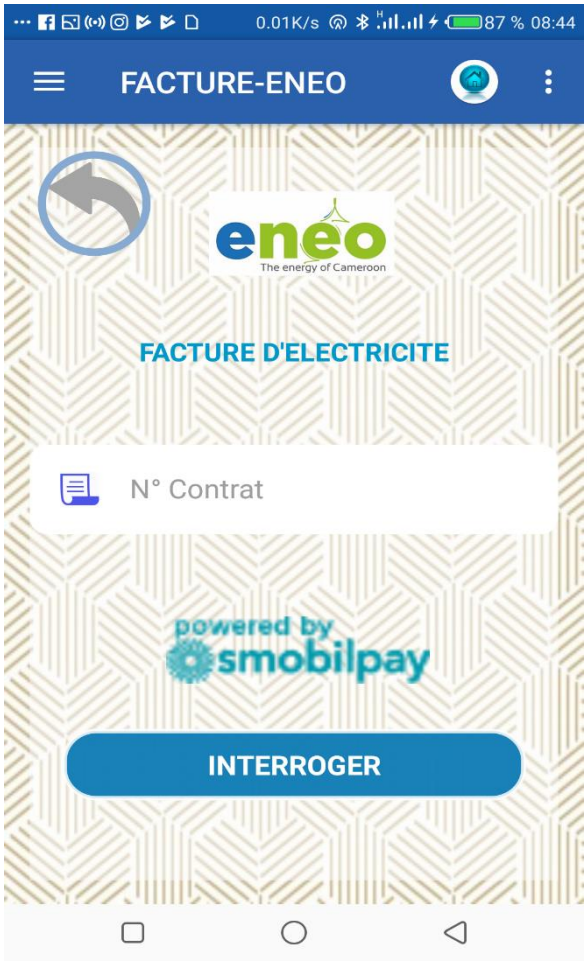
ETAPE 2: CHOIX DE L'OPERATEUR

MODULE D'ACHAT DU CREDIT DE COMMUNICATION AU NIVEAU INTERNATIONAL

ETAPE 3: CHOIX DU MONTANT DE LA RECHAGE



ETAPE 4: N° Tel bénéficiaire



MODULE DE PAIEMENT DE FACTURES D'ELECTRICITE:

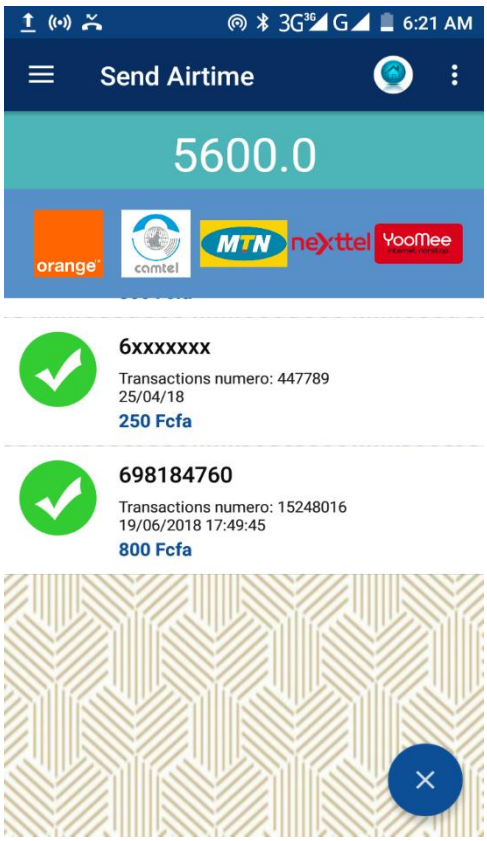
Les champs à renseigner :

- N° Contrat du client d'ENEO,

MODULE DE REABONNEMENT AUX BOUQUETS CANAL +:

Les champs à renseigner :

- N° DE LA CARTE CANAL+,



MODULE D'ACHAT DU CREDIT DE COMMUNICATION:

Les champs à renseigner :

- N° Tel bénéficiaire,
- Montant,
- Mot de passe de l'agent