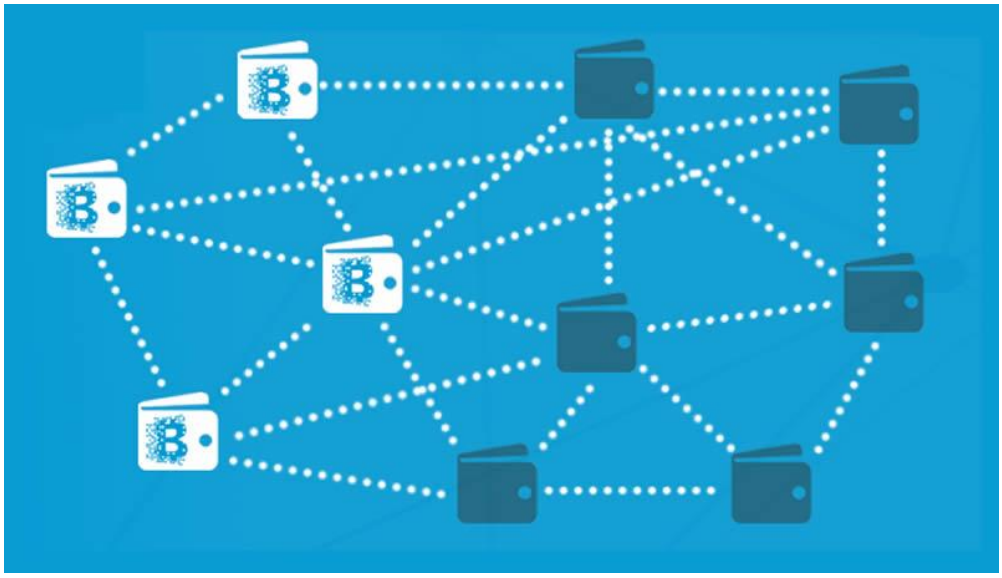
UNIVERSITÉ NATIONALE DU VIETNAM - HANOI (UNVH)

INSTITUT FRANCOPHONE INTERNATIONAL

Master en Systèmes Intelligents et Multimédia

Travaux personnels encadrés (TPE)

Blockchain et la gestion de certificats et diplômes



Présenté par : **Mongetro GOINT**

Encadrant : Dr. HO Tuong Vinh

03 octobre 2018

SOMMAIRE

Introduction

Depuis plusieurs années, la *blockchain* est apparue dans le monde technologique et se voit introduit dans plusieurs domaines.
La technologie *Blockchain* a été décrite comme la deuxième génération de l'Internet. La première génération d'Internet, lui, a complètement transformé la culture et l'industrie créative, en particulier en abaissant les coûts de distribution à presque gratuit. La blockchain (chaîne de blocs en français), est une liste sans cesse croissante d'enregistrements d'informations sur internet, appelés blocs, qui sont liés et sécurisés en utilisant la cryptographie. Chaque bloc contient généralement un hachage cryptographique du bloc précédent, un horodatage[1] et des données de transaction. Cette technologie constitue, en effet, un registre décentralisé et distribué qui enregistre les transactions sans avoir besoin d'un tiers de confiance ou intermédiaire.[2] De nos jours, la technologie *blockchain* commence à être utilisée à travers le monde dans plusieurs domaines, particulièrement dans la cryptomonnaie.

En effet, dans le cadre du cours de Travaux Personnels Encadrés (TPE), au master I en Système Intelligent et multimédia à [(l'Institut Francophone International (IFI)/ Université Nationale du Vietnam – Hanoi (UNVH)], il nous est recommandé de faire une étude sur la technologie *Blockchain*, de proposer un modèle d'application pour la gestion de certificats et diplômes (*plus précisément dans le contexte de la gestion des certificats et diplômes à l'Institut Francophone Internationale (IFI)*), et de développer un prototype.

D'abord, dans le premier chapitre du rapport de ce travail qui est l'*analyse du sujet*, nous aurons à regarder les existants concernant blockchain et la gestion certificats et diplômes ; la problématique ; définition des termes et outils employés, puis le résultat attendu.
Ensuite, dans le deuxième chapitre du rapport qui est la *recherche bibliographique*, nous tiendrons à présenter et analyser les solutions existantes pour la gestion des certificats et diplômes avec *blockchain*, notamment des plateformes comme : ***Digital Certificates Project, Blockcerts*** *et* ***Block.co.***

Enfin, dans le troisième chapitre du document, il s'agira de présenter la *solution proposée et le plan de travail.*

[1] L'**horodatage** (en anglais timestamping) est un mécanisme qui consiste à associer une date et une heure à un événement, une information ou une donnée informatique. Il a généralement pour but d'enregistrer l'instant auquel une opération a été effectuée.
[2] https://fr.wikipedia.org/wiki/Blockchain

CHAPITRE I

Analyse du sujet

A- Qu'est-ce qui existe déjà concernant blockchain et la gestion certificats et diplômes ?

Aujourd'hui, beaucoup de domaines, particulièrement les systèmes d'identification numérique tendent vers l'utilisation de la technologie *blockchain*, beaucoup d'outils et algorithme sont utilisés à cet effet.[3]

D'abord, ***Bitcoin*** (de l'anglais « *bit* » (unité d'information binaire) et « *coin* » (pièce de monnaie) est la première mise en œuvre de « *blockchain* » présentée par une personne (ou un groupe de personnes) sous le pseudonyme de ***Satoshi Nakamoto***, qui a annoncé son système en 2008 et publié le code source en 2009. En fait, il devient un peu difficile de dissocier la technologie *blockchain de Bitcoin.*[4]
EnEthereum, lancé en 2015, est une *blockchain* implémentation qui offre un script plus complexe (*'Turing complete'*) langage, et développe un mécanisme de consensus « preuve de l'enjeu » qui vise à résoudre le coût élevé et la centralisation potentielle de l'exploitation minière ***Bitcoin***.[5]

Pour la gestion de certificats et diplômes avec blockchain, d'abord, « **Digital Certificates Project »** est une initiative d'incubation par le « *Media Lab Community* » qui construit un écosystème pour la création, le partage et la vérification de certificats éducatifs basés sur la chaîne de blocs.[6]

Ensuite, il y a « **Blockcerts** » qui est une norme ouverte pour la création d'applications qui émettent et vérifient des enregistrements officiels basés sur des blockchains. Ceux-ci peuvent inclure des certificats pour les dossiers, les qualifications académiques, les permis professionnels, le développement de main d'œuvre, et plus.[7]

En plus, il y a **Block.co**, venant de l'Initiative Blockchain de l'*Université de Nicosie* (UNIC) en 2014, qui s'occupe aussi de la gestion de certificats avec *blockchain*. En particulier, l'objectif est d'aider les étudiants, les entreprises et les gouvernements à développer une vision sphérique des implications techniques, commerciales, légales et sociétales des technologies de crypto-monnaie et de *blockchain* afin de contribuer à construire un avenir meilleur.[8]

[3] http://www.mondedesgrandesecoles.fr/diplome-blockchain-avantages/
[4] https://fr.wikipedia.org/wiki/Bitcoin
[5] https://en.wikipedia.org/wiki/Ethereum
[6] https://medium.com/mit-media-lab/what-we-learned-from-designing-an-academic-certificates-system-on-the-blockchain-34ba5874f196
[7] https://www.blockcerts.org/guide/
[8] **https://block.co/who-we-are/**

B- La problématique

Alors que la technologie bat son plein, la majorité d'institutions utilisent encore le système traditionnel de gestion de documents de certification. Cependant, une minorité commence à s'approprier au nouvel ordre technologique mondial. Mais par ailleurs, un grand problème existe au niveau de la gestion (enregistrement, affichage et vérification) des informations d'identification numériques (certificats et diplômes) pour des institutions comme : universités, écoles…

Notamment, il existe des difficultés à prévoir dans les gestions à faire comme : l'adaptation des modèles de conception des certificats et des diplômes avec la technologie blockchain qui est relativement nouvelle, complexe et immuable.

C- Définition des termes et outils employés

- **Blockchain :** technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle (*définition de Blockchain France*).[9]
- **Bitcoin : M**onnaie virtuelle (ou crypto-monnaie) créée en 2009 par un ou plusieurs programmeurs informatiques utilisant le pseudonyme « *Satoshi Nakamoto*».[10]
- **Ethereum : P**late-forme (implémentation) informatique distribuée open-source, publique, basée sur la *blockchain* et un système d'exploitation doté de fonctionnalités de contrat intelligent (*scripting*).
- **Equihash :** Algorithme de preuve de travail axé sur la mémoire développé par le Centre interdisciplinaire de sécurité, de fiabilité et de confiance de l'Université du Luxembourg.[11]
- **Algorithme :** Un algorithme est un processus à effectuer pour répondre à un problème. [12]
- **Hachage :** Transformation d'une chaîne de caractères en valeur ou en clé de longueur fixe, généralement plus courte, représentant la chaîne d'origine.[13]

Dans le cadre de ce travail, les principaux sites de référence sont :
blockcerts.org
bitcoin.org/fr ;
en.wikipedia.org ;

[9] https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/
[10] https://en.wikipedia.org/wiki/Bitcoin
[11] https://www.science.lu/fr/nouvel-algorithme-equihash/vers-un-acces-egal-aux-monnaies-numeriques
[12] http://glossaire.infowebmaster.fr/algorithme/
[13] https://www.lemagit.fr/definition/Hachage

google.com ;
google.fr ;
medium.com ;
science.lu/fr ;
blockchainfrance.net

A propos de blockchain et la gestion de certificats et diplômes, des groupes de recherche et entreprises ont déjà travaillées dessus, notamment « ***Media Lab et Learning Machine*** » du Massachussetts Institute of Technology (MIT).

Dans le cadre de ce travail, nous aurons non seulement à travailler sur la technologie blockchain comme un domaine informatique, mais aussi sur la gestion académique puisque le sujet est implicitement lié à celle-ci. En fait, le travail consiste à proposer un modèle avec la technologie *blockchain*, pouvant faire : une meilleure gestion de l'identification numérique (la création, l'émission, l'affichage et la vérification des certificats basés sur la chaîne de blocs).

D- Résultat attendu

La finalité du projet consiste à permettre une vague d'innovation qui donne aux individus la capacité de posséder et de partager leurs propres documents officiels via « *blockchain* ».

D'abord, théoriquement, le travail doit offrir une possibilité d'information sur la technologie « *blockchain* », particulièrement relatif à la gestion des certificats et diplômes ;

Ensuite, sur le plan technique et pratique, le projet doit :

1- Permettre à un émetteur de signer un certificat numérique bien structuré et stocker son hachage dans une transaction blockchain. **Ex** : *Un responsable à l'Institut Francophone Internationale (IFI) pourra signer un certificat pour un étudiant ayant été diplômé au programme de master en informatique* ;
2- Faciliter l'affectation d'une sortie de transaction (affichage) d'un certificat ou d'un diplôme à un destinataire ;
3- Autoriser également aux utilisateurs de demander des certificats ou des diplômes ; et de lui générer une nouvelle identité de l'enregistrement de l'émetteur.

CHAPITRE II

Recherche bibliographique (Etat de l'art)

Dans cette partie du travail qui est la *recherche bibliographique*, nous tenons à présenter et analyser les solutions existantes pour la gestion des certificats et diplômes avec « *blockchain* ». En d'autres termes, je tiens à faire un état de l'art et proposer des idées nouvelles, utiles pour notre travail; et en plus présenter une liste de références des auteurs de ces différents travaux déjà réalisés. Comme mentionné dans la première partie du travail[14], plusieurs groupes de recherche ont déjà proposé des solutions pour la gestion des certificats et diplômes avec « *blockchain* » :

A- Digital Certificates Project

« **Digital Certificates Project**[15] **»** est une initiative d'incubation par le « *Media Lab Community* » qui construit un écosystème pour la création, le partage et la vérification de certificats éducatifs basés sur la chaîne de blocs. Dans un article publié sur le site de MIT MEDIA LAB en juin 2016[16], la version 1 du code source sous la licence MIT de ce projet open-source, basé sur la chaîne de blocs Bitcoin serait déjà disponible pour permettre aux autres de commencer à expérimenter des idées similaires.

Les initiateurs de MIT MEDIA LAB ont choisi la « *blockchain Bitcoin* » au lieu de Ethereum, juste parce que celui-là a été la blockchain la plus testée et la plus fiable à ce moment; de plus, les intérêts financiers relativement robustes des mineurs et l'investissement financier réalisé dans Bitcoin (et dans les sociétés liées à Bitcoin) font qu'il est probable qu'il restera encore longtemps, selon l'avis des initiateurs.

Sur la plateforme, la conception globale de l'architecture de certification se fait de manière à ce qu'un émetteur de certificat puisse signer un certificat numérique bien structuré et stocker son hachage dans une transaction « blockchain ». Ensuite, une sortie de transaction est affectée au destinataire.

1- Fonctionnement de la plateforme « Digital Certificates Project ».

Dans la conception d'un certificat, plusieurs aspects sont à considérer : d'une part, la section **Cert-schema** détaille comment créer un certificat numérique, qui lui-même est un fichier JSON[17] avec les champs nécessaires pour que le code **Cert-issuer** le place sur la « blockchain ».

[14] Voir l'Analyse à la page 3.
[15] https://medium.com/mit-media-lab/what-we-learned-from-designing-an-academic-certificates-system-on-the-blockchain-34ba5874f196
[16] https://medium.com/mit-media-lab/what-we-learned-from-designing-an-academic-certificates-system-on-the-blockchain-34ba5874f196
[17] JavaScript Object Notation (**JSON**) est un format de données textuelles dérivé de la notation des objets du langage JavaScript. Il permet de représenter de l'information structurée comme le permet XML par exemple.

D’autre part, la section **Cert-issuer** est utilisée pour prendre les certificats JSON et les émettre en créant une transaction entre l’émetteur et le destinataire sur la blockchain « bitcoin » qui inclut le hachage du certificat lui-même.

En plus, il y a la section « **Cert-Viewer »** qui est utilisée pour afficher et vérifier les certificats après avoir été émis, et pour permettre aux destinataires de demander un certificat et de générer leur propre identité « bitcoin » nécessaire pour le processus de création de certificat. En termes clairs, on crée un fichier numérique qui contient des informations de base telles que le nom du destinataire, le nom de l'émetteur (Institut Francophone pour l’Innovation (IFI) par exemple), une date d'émission, etc. On signe ensuite le contenu du certificat en utilisant une clé privée à laquelle seul l’IFI a accès, et on ajoute cette signature au certificat lui-même. Ensuite, on crée un hachage, qui est une chaîne courte qui peut être utilisée pour vérifier que personne n'a altéré le contenu du certificat. Et enfin, on utilise à nouveau la clé privée pour créer un enregistrement sur la « *blockchain* Bitcoin » qui stipule qu’on a émis un certain certificat à une certaine personne, notamment à une certaine date. Le système permet de vérifier à qui un certificat a été délivré, par qui, et de valider le contenu du certificat lui-même.

2- Avantages

L’un des avantages qu’offre « **Digital Certificates Project »**, est premièrement la solution qu’il apporte aux différents problèmes concernant les certificats, y compris celui des certificats frauduleux. Deuxièmement, la possibilité, à des réfugiés particulièrement, de fournir un certificat d'études à n’importe quel moment, à n’importe endroit où il est. Troisièmement, Pour la gestion des certificats, la révocation dans le système reste un avantage important pour son fonctionnement. Cette astuce est un indicateur que l'émetteur ou le destinataire peut définir pour signaler qu'il ne reconnait pas le certificat à être validé.

3- *Inconvénients*

Alors que ce projet présente tout un ensemble d’avantages, il n’est pas alors sans inconvénients. D’abord, l’un d’entre eux demeure autour de cette question : *« Les types d’institutions (émetteurs) en qui on doit avoir confiance pour la signature des certificats* ? » ; Pourtant, la fraude par diplôme reste un vrai problème à travers le monde aujourd’hui. Ensuite, le coté législateur des transactions relatives à un certificat sur la blockchain (s’il y a un bug par exemple), ce qui peut être considéré aussi pour toutes les transactions des autres systèmes de blockchain, reste jusqu’à maintenant un peu flou. En plus, la convivialité pour les utilisateurs non techniques n’est pas encore définie. En d’autres termes, toutes les briques technologiques sont jusqu’à maintenant construites coté algorithme, mais reste un peu complexe, ce qui paraît un peu contraire à ce que l’utilisateur final va voir. Par ailleurs, les certificats générés par la section **Cert-Viewer** pour être imprimés par les destinataires pourraient apparaitre plus esthétiques.

B- **Blockcerts**

« **Blockcerts**[18] » est une norme ouverte pour la création d'applications qui émettent et vérifient des enregistrements officiels basés sur des « blockchains », (bitcoin notamment). Ceux-ci peuvent inclure des certificats pour les qualifications académiques, les permis professionnels, le développement de main d'œuvre, et plus. La conception initiale et le développement dans le cadre de ce projet ont été menés par Media Lab et Learning Machine du MIT. Développée en langage Python, Blockcerts s'engage à l'identité auto-souveraine de tous les participants et permet aux destinataires de contrôler ses réclamations grâce à des outils faciles à utiliser tels que le portefeuille de certificats (application mobile).

1- Fonctionnement de la plateforme « Blockcerts ».[19]

Un peu similaire à **Digital Certificates Project,** dans **Blockcerts,** il y a la section « **Cert-issuer »,** qui permet à un émetteur de créer, de signer et d'émettre des certificats ; Ensuite, la section « **Cert-Viewer »** permet au destinataire d'afficher le certificat émis par l'émetteur ; Et enfin il y a « **Cert-Verifier »** qui permet de faire la vérification du certificat. Dans une procédure d'enchainement, la figure ci-dessous traduit les différentes étapes pour finaliser un certificat.

[18] https://www.blockcerts.org/
[19] https://www.blockcerts.org/

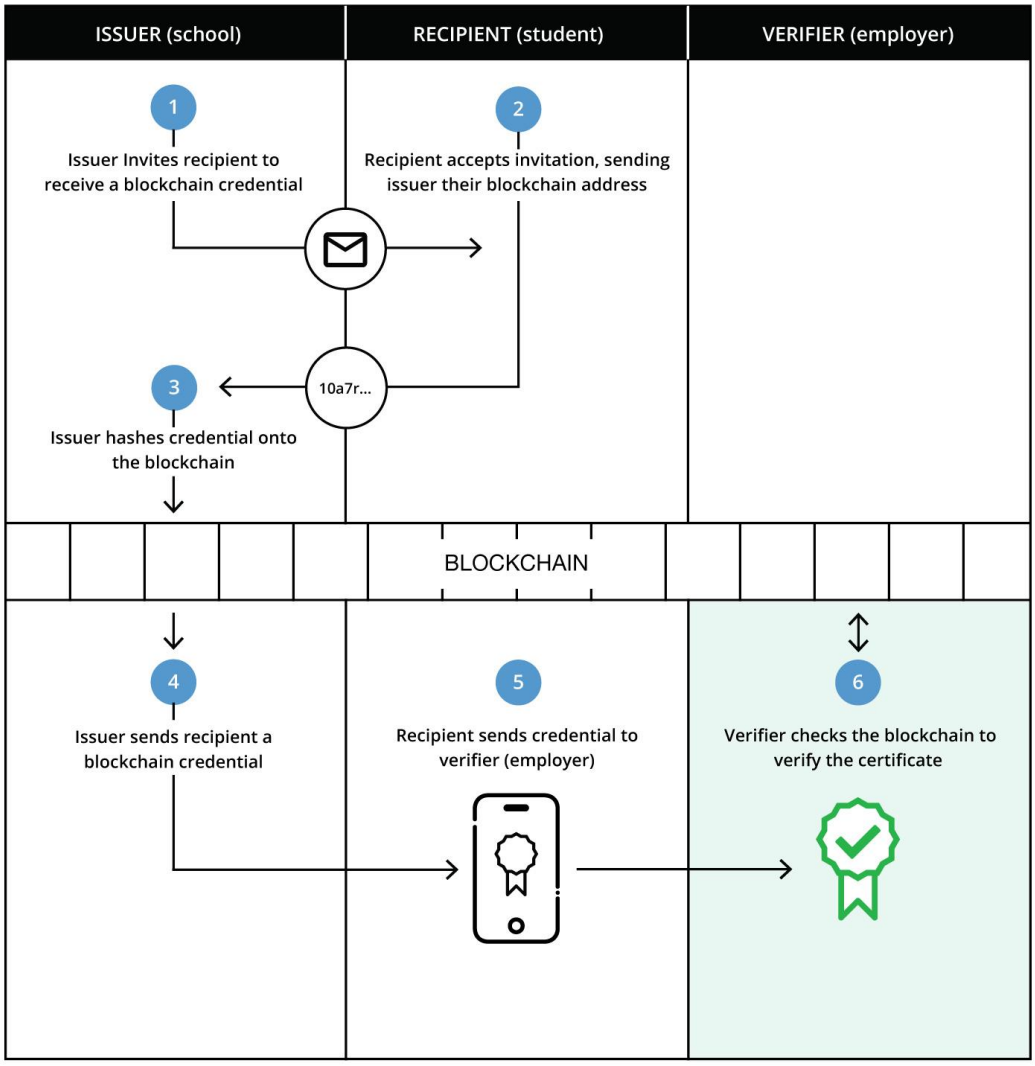


Figure 1 : Illustration des différentes étapes pour finaliser un certificat dans Blockcerts.

2- Avantages

Parmi les différents avantages intéressants qu'offre le **BlockCert,** on note fait qu'il utilise la blockchain bitcoin qui restreint la disponibilité des informations concernant les certificats. Ce qui est censé stocker sur la blockchain est un « **hash »**[20] à 1 voie. Cela ne le rend utile que pour la vérification ; c'est-à-dire que vous pouvez hacher un certificat et le comparer à ce qui se trouve sur la blockchain. Et compte tenu de ce qui est sur la blockchain, les données d'origine ne peuvent pas être récupérées de manière viable. Cela permet à un destinataire de révéler un certificat uniquement à des tierces parties. Ensuite, Le service de vérification qui valide la

[20] Transformation d'une chaîne de caractères en valeur ou en clé de longueur fixe, généralement plus courte, représentant la chaîne d'origine.

signature de l'émetteur et les données des certificats demeure un avantage clé dans la gestion de ces derniers; Il s'assure également que le statut du certificat n'a pas expiré ou a été révoqué.
En plus, l'immuabilité des certificats empêchant leur mise est aussi un avantage intéressant. Un émetteur peut révoquer les certificats qui ont des erreurs, ou, s'ils ont simplement exclu un destinataire admissible, l'émetteur peut émettre un autre lot.

3- Inconvénients

Au coté des avantages qu'offre **BlockCert**, il a y aussi des inconvénients : Comme on l'a si bien mentionné dessus pour **Digital Certificates Project**, « *Les types d'institutions (émetteurs) en qui on doit avoir confiance pour la signature des certificats* », reste aussi une inquiétude dans le cas de **BlockCert**. Et, du côté législatif des transactions relatives à un certificat sur la blockchain (s'il y a un bug par exemple), reste encore un peu flou.

C- Block.co

Après **Digital Certificates Project** et **BlockCert**, il y a aussi la plateforme **Block.co**[21], venant de l'Initiative Blockchain de l'*Université de Nicosie* (UNIC), et nous l'avons bien mentionné dans la première partie du document. Dans un esprit créatif, l'UNIC a constamment innové dans le milieu universitaire, étant la première université au monde à délivrer des certificats académiques sur la blockchain Bitcoin, en utilisant sa propre plate-forme logicielle interne (septembre 2014) pour la première cohorte du premier MOOC (cours en ligne ouvert massif) en crypto-monnaies dans le monde, et chacune des six cohortes depuis.

1- Fonctionnement de la plateforme Block.co.[22]

Un peu différent du fonctionnement des deux premières plateformes vues précédemment, deux aspects importants sont pris en compte au niveau de la gestion des certificats sur **Block.co** : D'abord *« Issuing Certificates* » (Emission des certificats), en suite **«** *Validating Certificates* » (Validation des certificats).

[21] https://block.co/who-we-are/
[22] https://block.co/who-we-are/

L’image ci-dessous illustre un peu le fonctionnement du système Block.co.

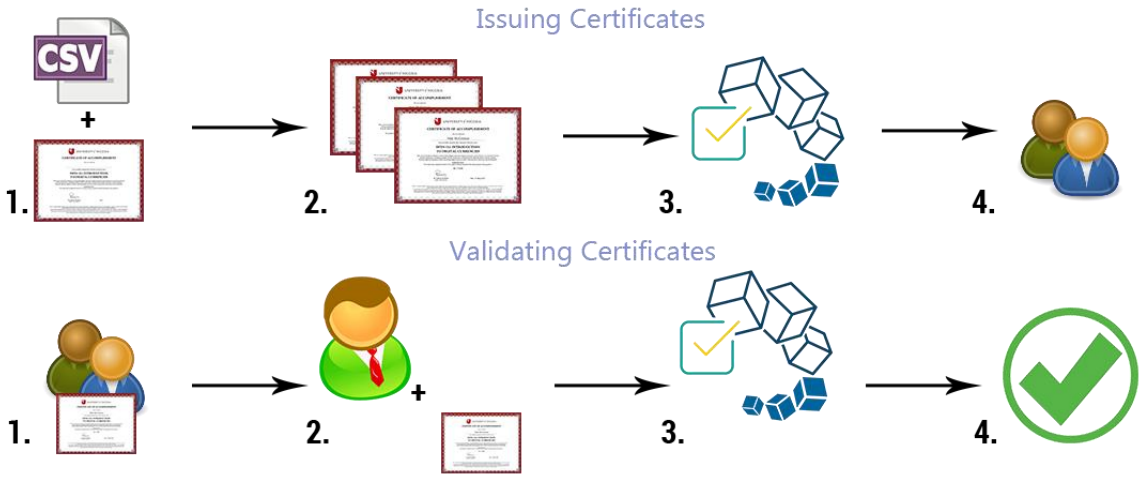


Figure 2 : Illustration du fonctionnement du système Block.co.

➢ Pour la partie « ***Issuing Certificates*** » :

1. Une liste CSV avec les informations des diplômés plus un modèle PDF sont nécessaires ;
2. Le logiciel remplit le modèle PDF avec les informations du diplômé et crée les certificats finaux ;
3. Une empreinte des certificats est ensuite publiée dans la blockchain ;
4. Chaque certificat est ensuite diffusé à son utilisateur respectif.

➢ Dans la deuxième partie « ***Issuing Certificates*** » :

1. Un utilisateur qui veut prouver qu'il possède un certificat envoie simplement son certificat PDF à un employeur ;
2. L'employeur utilise un validateur en ligne (qui utilise le logiciel) et télécharge le PDF qu'il a reçu ;
3. Le validateur vérifie que l'empreinte PDF est dans la blockchain comme prévu ;
4. Renvoie avec une confirmation (ou pas) que le certificat est bien valide.

2- Avantages

Y compris les différents avantages mentionnés pour les deux autres initiatives ciblées précédemment (**Digital Certificates Project** et **BlockCert**), il est à ajouter qu’avec **Block.co**, les certificats sont un peu plus faciles à émettre, valider et vérifier, et faciles à communiquer comparativement aux deux autres.

3- Inconvénients

Les inconvénients demeurent les mêmes que ceux des deux autres plates-formes citées précédemment.

Tableau de synthèse des travaux existants sur la gestion de certificats et diplômes avec blockchain.

	Présentation en synthèse
Digital Certificates Project[23]	**Digital Certificates Project** est une initiative offrant un écosystème de partage et de vérification de certificats éducatifs, développée par le « MIT MEDIA LAB» en juin 2016 et, basée sur la « blockchain » bitcoin. Sur cette plateforme, la conception globale de l'architecture de certification se fait de manière à ce qu'un émetteur de certificat puisse signer un certificat numérique bien structuré et stocker son hachage dans une transaction blockchain. Ensuite, une sortie de transaction est affectée au destinataire.
Blockcerts[24]	**Blockcerts** est une norme ouverte pour la création d'applications qui émettent et vérifient des enregistrements officiels basés sur des blockchains (bitcoin notamment). Ceux-ci peuvent inclure des certificats, des diplômes et autres. Etant un projet dont la conception initiale et le développement ont été menés par Media Lab et Learning Machine du MIT, Blockcerts s'engage à l'identité auto-souveraine de tous les participants et permet au destinataire de contrôler ses réclamations grâce à des outils faciles à utiliser tels que le portefeuille de certificats (application mobile). La **figure 1** illustre de façon claire le fonctionnement de la plateforme.
Block.co[25]	**Block.co** est une plateforme résultant de l'Initiative Blockchain de l'*Université de Nicosie* (UNIC), en 2104, qui s'occupe de la gestion de certificats avec blockchain. Le but de la plateforme est, d'une manière générale, de permettre de développer une vision sphérique des implications techniques, commerciales, légales et sociétales des technologies de crypto-monnaie et de blockchain. La **figure 2** illustre de façon claire le fonctionnement de la plateforme.

Tableau 1 : synthèse des travaux existants sur la gestion des certificats et diplômes avec blockchain

Analyse critique :

Pour toutes les plateformes ciblées dans le cadre de notre travail, il est à considérer que la gestion des certificats reste un peu compliquée pour les utilisateurs non-techniques. Alors, le mieux serait de développer les plates-formes d'une manière plus conviviale (avec des interfaces graphiques par exemple) pour faciliter la tâche aux utilisateurs non techniques.

Ensuite, pour la **BlockCert**, la version du certificat affichée en ligne peut changer visuellement, en fonction de l'appareil qui l'affiche. Par exemple, il peut apparaître d'une manière dans une application mobile et un peu différemment dans un navigateur Web, bien que les données

[23] https://medium.com/mit-media-lab/what-we-learned-from-designing-an-academic-certificates-system-on-the-blockchain-34ba5874f196
[24] https://www.blockcerts.org/
[25] **https://block.co/who-we-are/**

contenues dans le certificat ne puissent pas être modifiées. Dans ce cas, il serait bon de développer des applications mobiles (comme le fait facebook par exemple) afin d'adapter aussi la vue des certificats à n'importe quel appareil utilisé.

En somme, une synthèse des différents travaux ciblés, nous permettra de réaliser un travail intéressant dans le cadre de la gestion des certificats et diplômes à l'Institut Francophone Internationale (IFI), contexte dans lequel se place notre sujet de TPE.

CHAPITRE III

Solution proposée et plan de travail

Dans les parties précédentes, nous avons pris soin d'étudier et d'analyser les travaux connexes existants dans le cadre de mon sujet. Et, nous avons souligné les avantages et les inconvénients de ces derniers, ce qui nous a permis de mieux connaitre notre sujet pour y agir. En effet, il est donc temps de présenter la séquence la plus déterminante de notre travail qui est la *solution proposée et le plan de travail*.

À travers cette séquence, il s'agira donc de définir exactement le travail à réaliser (*la solution proposée*) ; de le justifier tout en identifiant et en détaillant les différents composants ; de dire comment le travail sera réalisé, et aussi quand on va réaliser chaque séquence de celui-ci.

A- Identification claire et précise du travail à réaliser

Le projet à réaliser consiste à implémenter une application en ligne, basé sur la technologie blockchain, permettant de faire la gestion des certificats et diplômes, spécifiquement à l'IFI :
En termes clairs, l'application doit :

a) Permettre à un émetteur de signer un certificat numérique bien structuré et stocker son hachage dans une transaction blockchain. **Ex** : *Un responsable à l'Institut Francophone Internationale (IFI) pourra signer un certificat pour un étudiant ayant été diplômé au programme de master en informatique* ;
b) Faciliter l'affectation d'une sortie de transaction (affichage) d'un certificat ou d'un diplôme à un destinataire ;
c) Permettre également aux utilisateurs de recevoir ou de générer une nouvelle identité de l'enregistrement de l'émetteur.

Connaissant qu'il existe déjà plein d'autres plate-formes qui font la gestion de certificats et diplômes avec « blockchain », nous n'allons pas réinventer la roue. Par contre, notre travail consiste à implémenter un prototype adapté au contexte de notre sujet, à savoir le système de gestion de certificats et diplômes à l'IFI.

✓ **Architecture générale du système**

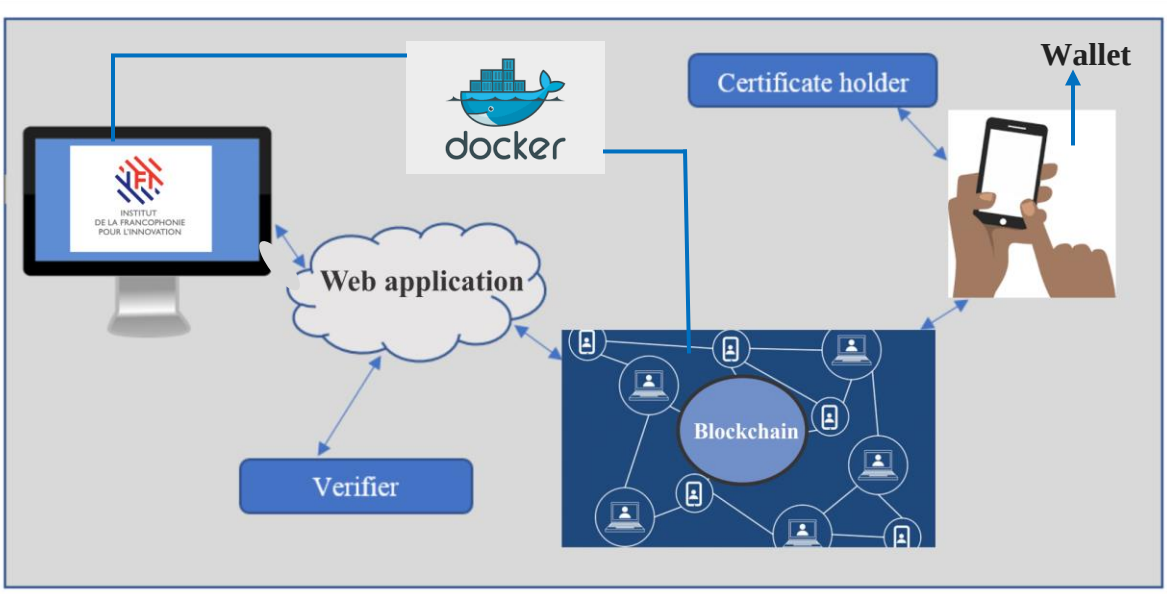


Figure 3 : Architecture générale du système

✓ **Les composants de l'application**

L'application sera composée de plusieurs sections :

D'abord, il y aura la partie **Cert-Emission :**

Dans cette section, un responsable de l'IFI, qui préalablement a été enregistré sur la plate-forme pourra signer et émettre un certificat à un destinataire (étudiant) ayant été diplômé de l'institution.

1- Etant connecté sur la plate-forme, l'émetteur pourra envoyer une demande à un destinateur, qui, lui-même a été enregistré sur la plate-forme pour lui proposer de recevoir un certificat.

2- Après que le destinataire ait accepté la demande, le responsable publie le certificat (scanné préalablement) dans la blockchain, qui elle-même lui génère une empreinte (*hachage*).

3- L'émetteur envoie l'empreinte (*hachage*) du certificat au destinataire.

Ensuite il y aura la section **Cert-Visualisation :**

Cette partie permettra au destinataire d'afficher et de publier (s'il le veut) le certificat émis par l'émetteur ;

1- Etant connecté sur la plate-forme, dans la section **Cert-Visualisation,** le destinataire entre l'empreinte (*hachage*) du certificat.

2- **Cert-Visualisation,** affiche le certificat, et offre la possibilité au destinataire de le publier sur des réseaux comme facebook, tweeter…

Il est à noter que le destinataire pourra visualiser ses certificats soit sur l'application web ou à l'aide d'une application mobile (« android wallet »).

Enfin, il y aura la section **Cert-Vérification :**

Cette dernière partie permettra à un tiers, détenteur de l'empreinte d'un certificat de la part de son possesseur de vérifier sa validité.

1- Le tiers (responsable d'une entreprise par exemple) entre l'empreinte du certificat dans l'espace réservée à cet effet dans la section **Cert-Vérification** et fait une demande d'authentification de celui-là.

2- **Cert-Vérification** confirme ou non, via la « blockchain », l'authentification du certificat sur la « blockchain ».

✓ **Fonctionnement de la plateforme**

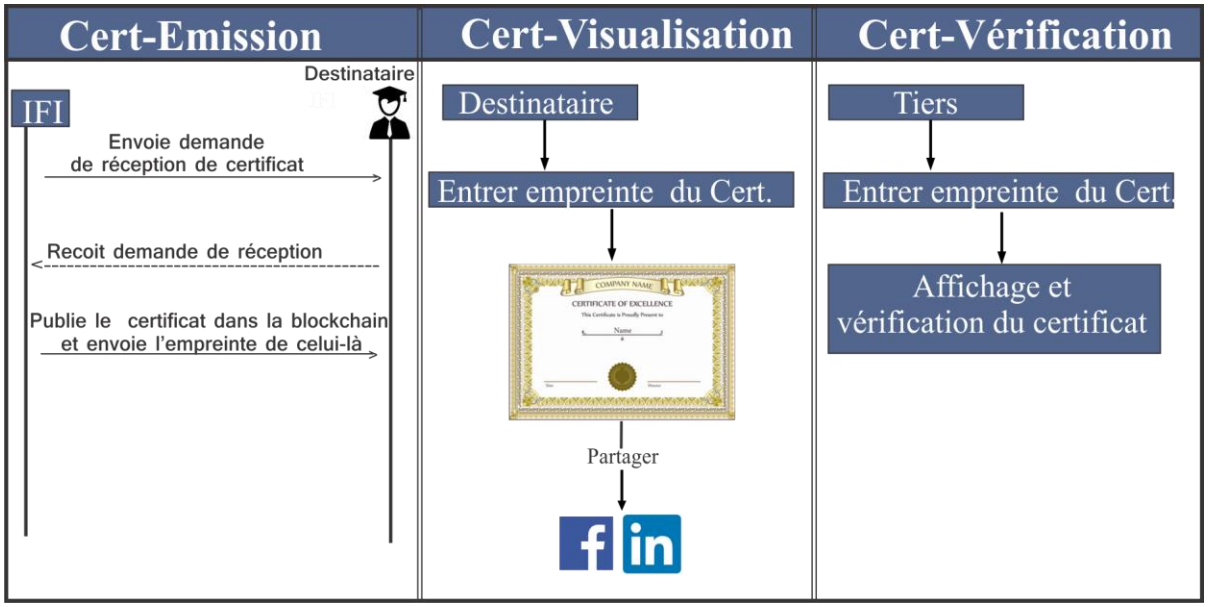


Figure 4 : Illustration de la solution proposée

B- Limites du travail

Normalement, dans le cadre d'un tel travail nous devrions non seulement réaliser les différentes parties mentionnées dessus dans la section « Les composants de l'application », mais aussi élever le niveau. Par exemple avec un module Cert-Révocation**,** qui permettrait aux responsables de l'IFI de révoquer le certificat d'un étudiant pour une raison quelconque. Alors, compte tenu des différentes contraintes, notamment celles liées au temps, il s'agira donc d'un prototype adapté au contexte de la gestion des certificats faite à l'IFI, qui prendra en compte les spécificités les plus pertinentes liées à l'émission, la visualisation et la vérification d'un certificat.

C- Comment le travail sera-t-il réalisé ?

La réalisation de ce travail sera assujettie à plusieurs paramètres :

- ✓ **Données nécessaires**

Etant donné que nous allons travailler sur la gestion de certificats et diplômes avec blockchain, qui devra être applicable au contexte de la gestion faite à l'administration de l'IFI, il nous sera donc nécessaire d'avoir des informations sur le modèle conceptuel des certificats délivrés par ladite institution.

- ✓ **Données disponibles**

En ce qui à trait aux données disponibles pour la réalisation du travail, il nous est disposé plusieurs sources : d'abord, il y a les informations concernant les plates-formes de gestion de certificats et diplômes déjà existantes comme celles ciblées dans le cadre de notre travail (« Digital Certificates Project », « Blockcerts et Block.co »), qui nous serviront de piste pour notre solution proposée. Ces informations se rapportant surtout sur le modèle conceptuel d'un certificat sur la blockchain et aussi sur la gestion des transactions entre les émetteurs et les destinataires de celui-là. Ces données nous permettront d'avoir une meilleure vision sur la conception de mon prototype à présenter. Ensuite, il y a les codes sources de l'initiative *Digital Certificates Project* de *Media Lab Community*, publiés sous la licence MIT open-source, *qui* sont disponibles pour l'expérimentation de notre travail.

En plus, il y a aussi certaines des réflexions sur la conception, ainsi que certaines des questions intéressantes sur la gestion des réputations numériques à poursuivre par l'initiative de Digital Certificates Project qui sont disponibles sur ***http://certificates.media.mit.edu.***

- ✓ **Outils disponibles**

Plusieurs outils nous serviront dans le cadre de notre travail : étant donné que nous allons travailler avec la technologie blockchain, la chaine de bloc Bitcoin qui, lui-même est à l'origine de cette technologie ; en plus qui est celle la plus testée et, qui a été aussi expérimentée par plusieurs plates-formes de gestion de certificats et diplômes, nous permettra de faire une meilleure expérience.

En plus, pour l'implémentation, nous allons utiliser **Python** qui est un langage de programmation objet, multiparadigme et multiplateformes. Le choix de ce langage dans le cadre de notre travail est du fait qu'il est conçu pour optimiser la productivité des programmeurs en offrant des outils de haut niveau et une syntaxe simple à utiliser. Outre, plusieurs plates-formes ciblées dans le cadre de notre sujet d'étude qui ont déjà travaillé sur un sujet similaire ont utilisé eux aussi python. Par ailleurs, nous aurons à utiliser docker[26] pour déployer l'application.

[26] https://en.wikipedia.org/wiki/Docker_(software)

✓ **Estimation des difficultés de réalisation**

Au cours de la réalisation de ce travail, nous avons déjà prévu un ensemble de difficultés :

- *Difficultés d'adaptation avec la technologie blockchain*

Dans le cadre de notre sujet, nous travaillons sur la **blockchain** qui est une technologie relativement nouvelle, et sa complexité et son immuabilité font qu'il est encore plus important d'examiner attentivement les effets à long terme des décisions de conception.

- *Difficultés liées aux outils et au langage de programmation à utiliser*

Pour le développement de l'application, **python** qui est un langage de programmation avec lequel nous allons nous familiariser pour la première fois. Donc, cela nous exigera un temps d'apprentissage important. Outre, nous aurons à déployer l'application des conteneurs docker, une technologie que nous allons expérimenter aussi pour la première fois.

- *Difficultés liées au temps*

En plus des difficultés susmentionnées, la surcharge des travaux à faire à l'IFI sera aussi une contrainte qui aura des répercussions sur la durée normale de la réalisation du travail. Donc, nous serons obligés d'établir un plan de travail avec une durée plus flexible et plus longue que la normale.

D- Plan de travail

✓ **Estimation du temps nécessaire pour réussir le travail**

Tenant compte des différentes difficultés mentionnées ci-dessus, nous allons présenter à travers le tableau ci-dessus, un plan de travail avec les durées nécessaires pour la réalisation de chaque séquence du travail.

Séquences	**Durée en semaine**
Familiarisation avec les outils de développement	3
Itération I(**Cert-Emission**)	4
Itération II (**Cert-Emission + Cert-Réception**)	4
Itération III (**Cert-Emission+Cert-Réception+Cert-Vérification**)	3
Test du prototype	1

Tableau 2 : Plan de travail

CHAPITRE IV

Implémentation

Pour l'implémentation de la solution proposée, nous nous sommes basés sur le projet Blockcert[27] de MIT Media Lab, qui lui-même est une initiative de gestion de certificats et diplôme.
D'abord, nous présentons dans le tableau ci-dessous les attributs concernant un certificat (présenté sous format JSON) et qui va être soumis à l'aide de la partie Cert-Emission.

Attribut	Type	Description
IdCert	String	Id du certificat
IssuedDate	Date	Date d'émission du certificat
RecipientName	String	Le récipiendaire auquel le certificat sera délivré
RecipEmail	String	Email du récipiendaire auquel
IssuerEmail	String	Email de l'émetteur du certificat
IssuerName	String	Nom de l'institution émettrice du certificat
PublicKey	String	Clé publique du recipiendaire
Hashed	Booléen	Etat d'ashage du certificat
CertType	String	Type du certificat
Signature	String	Signature de l'émetteur

Tableau 3 : Attributs concernant un certificat

Présentation d'un modèle de certificat JSON avant l'émission

Figure 5 : Modèle de certificat JSON avant l'émission

[27] https://www.blockcerts.org/

Pour l'émission d'un certificat, le processus est le suivant :

1- Cloner le référentiel et accéder au répertoire dans docker
2- Créer le conteneur docker
3- Executer l'application dans docker
4- Créer une adresse d'émission
5- Ajouter le certificat à publier dans le répertoire docker
6- Emettre le certificat sur la blockchain

N.B : Il est à noter que pour émettre un certificat, il faut avoir suffisamment de « bitcoin ». Par contre, en mode test il y a la possibilité de générer de faux « bitcoins » à l'aide de la commande « *bitcoin-cli generate 101* » afin d'émettre le certificat sur la blockchain.

CHAPITRE V

Expérimentations et résultats

Présentation d'un modèle de certificat JSON après l'émission

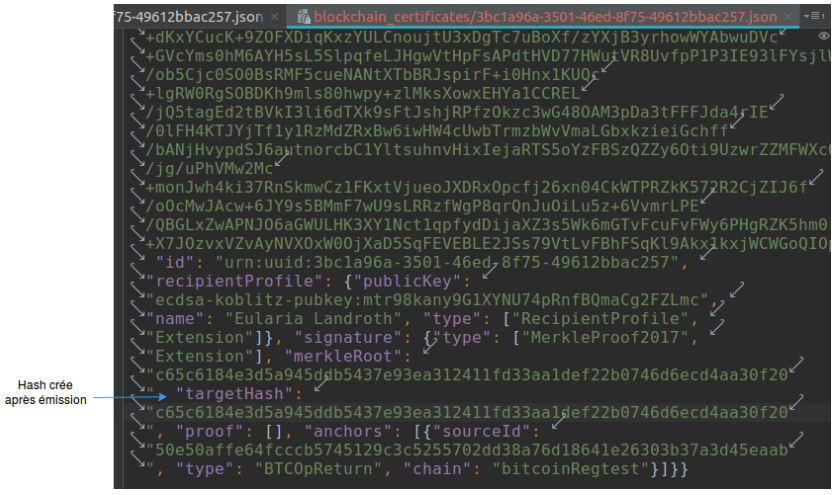


Figure 6 : Modèle de certificat JSON après l'émission

Après l'émission d'un certificat su la blockchain, on peut copier le certificat émis ver la machine locale, et celui-là se présente ainsi avec un « hash » cryptographique comme indiqué dans l'image ci-dessus (**voir Figure 6)**, ce qui explique que le certificat à été crypté et émis sur la blockchain.

Présentation d'un modèle de certificat après l'émission

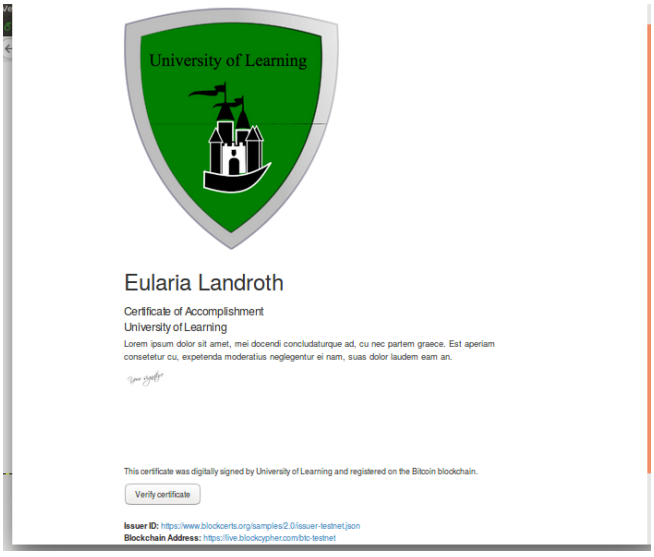


Figure 7 : Modèle de certificat après l'émission

Après l'émission sur la blockchain, le certificat peut être vu comme le montre l'image ci-dessus (**voir Figure 7)** avec un bouton de vérification.

Présentation d'un modèle de certificat vérifié après l'émission

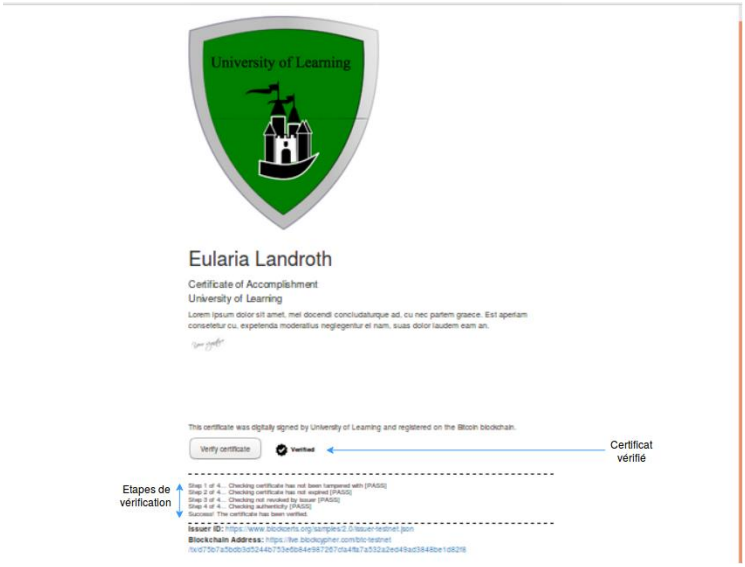


Figure 8 : Modèle de certificat vérifié après l'émission

Pour la vérification d'un certificat, il suffit de cliquer sur le bouton « Verify cettificate ». Si tout se passe bien, c'est-à-dire que le certificat soit authentique, non falsifié, non révoqué et non expiré, on aura un message de confirmation comme le montre la figure ci-dessus (**voir Figure 8**).

Présentation d'un modèle de certificat vérifié après l'émission

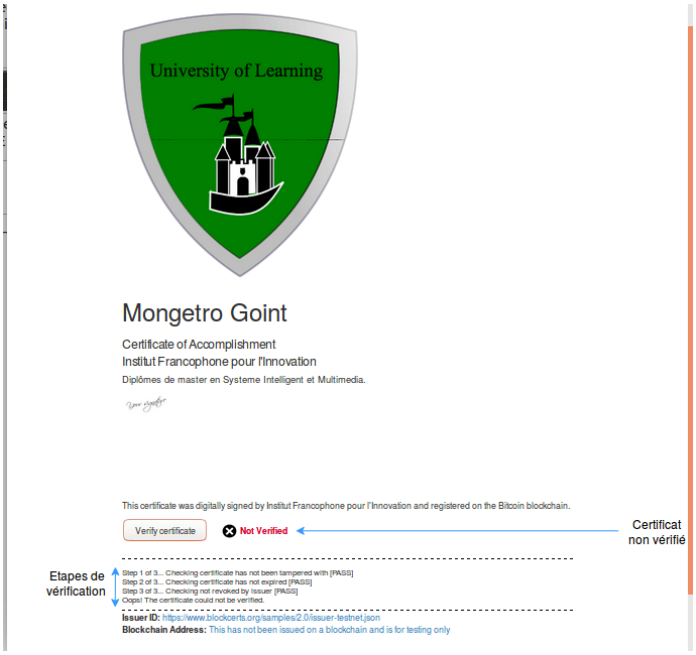


Figure 9 : Modèle de certificat non vérifié après l'émission

Dans le cas où le certificat ne respecte pas toutes les conditions mentionnées pour la **figure 8,** on aura un message d'erreur indiquant que le certificat n'a pas été vérifié (**voir Figure 9**).

Conclusion et perspectives

En somme, dans le cadre de ce Travail Personnel Encadré qui consistait à faire une étude sur la technologie *Blockchain*, de proposer un modèle d'application pour la gestion de certificats et diplômes et de développer un prototype, nous avons pu atteindre l'objectif avec les différents résultats montrés à travers le contenu précédent de ce rapport.

D'abord, nous avons pu faire une étude sur la « blockchain » en tant que nouvelle technologie en émergence, tout soulignant les différentes « blockchains » existantes et les algorithmes utilisés par cette technologie. Ensuite, nous avons fait une présentation et une analyse sur les solutions existantes pour la gestion des certificats et diplômes avec « *blockchain* », notamment des plateformes comme *Digital Certificates Project, Blockcerts et Block.co.* En plus, nous avons proposé un prototype puis présenté les résultats obtenus de ce dernier après les expérimentations.

En effet, ce travail nous a permis de prendre connaissances sur la technologie « blockchain », particulièrement son utilisation dans la gestion d'identité numérique, outre de disposer les résultats à tous ceux voulant travailler sur un sujet similaire.

Comme perspectives à notre cas d'étude (blockchain et la gestion de certificats et diplômes), nous proposons le développement d'interfaces graphiques et conviviales dans la partie Cert-Emission, ce qui permettra à des utilisateurs non avisés de pouvoir émettre des certificats avec plus de facilité.

Références bibliographiques / Webographie

1- Dai, Fangfang, et al. "*From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues*." Systems and Informatics (ICSAI), 2017 4th International Conference on. IEEE, 2017.

2- Bitcoin.org, « *À propos de bitcoin.org* », https://bitcoin.org/fr/a-propos-de-nous , consulté le 10-03-2018.

3- Block.co, « *The first team globally to put academic certificates on the blockchain*», https://block.co/who-we-are/ , consulté le 13-04-2018.

4- BLOCKCERTS, «*The open Standard for Blockchain Credentials*», https://www.blockcerts.org/guide/ , consulté le 26-03-2018.

5- Honoré, Hounwanou. *Premiers pas avec Python*, 2017

6- MIT MEDIA LAB, « *What we learned from designing an academic certificates system on the blockchain* », https://medium.com/mit-media-lab/what-we-learned-from-designing-an-academic-certificates-system-on-the-blockchain-34ba5874f196 , consulté le 26-03-2018.

7- Science.lu, « *Nouvel algorithme " Equihash" : Vers un accès égal aux monnaies numériques* », http://www.science.lu/fr/content/nouvel-algorithme-«-equihash-»-vers-un-accès-égal-aux-monnaies-numériques , consulté le 11-03-2018.

8- SCHMIDT Philipp, « *Certificates, Reputation, and the Blockchain*», https://medium.com/mit-media-lab/certificates-reputation-and-the-blockchain-aee03622426f, consulté le 09-04-2018.