Étude comparative de solution d'authenticité

Le trafic des faux diplômes est d'envergure mondiale. Désormais, il est facile de se procurer un diplôme pour 150 euros sur Internet, comme sur le site fauxdiplômes.org. Ce site vous promet en 48 heures un diplôme « qualité d'origine certifié », discrétion garantie. [16]

Figure 11 : Site pour les faux diplômes [I11]

4.1 Ampleur du phénomène

Une façon simple de définir les faux diplômes serait de procéder par exclusion, en les définissant comme tous les prétendus diplômes ne satisfaisant pas aux conditions de définition des vrais diplômes.

Malgré son caractère englobant, une telle définition ne permet pas d'approfondir l'analyse, d'où la nécessité de la dépasser. Les faux diplômes peuvent être classés en deux grands types, à savoir, la contrefaçon pure et simple d'un vrai diplôme et la création ex nihilo d'un document écrit attestant un titre ou un grade, délivré par une institution souvent virtuelle et non habilitée. [16]

Dans le premier cas, le faux diplôme en question porte des signes distinctifs cherchant à imiter le vrai diplôme, comme le nom ou le logo de l'institution dument habilitée à le délivrer. Une telle falsification est relativement similaire, au moins sur le plan analytique, aux faux billets ou aux fausses pièces d'identité.

Dans le deuxième cas, qui retiendra la majeure partie de notre attention, le faux diplôme est un document délivré (ou plutôt vendu) par une institution non reconnue, et ne répondant pas aux critères minimaux (personnel qualifie, cours, examens, etc.) permettant de délivrer le titre concerné. La notion de faux diplômes est étroitement liée a celles d'<< usines à diplômes >>, c'est-à-dire d'institution non habilitées ou bénéficiant d'habilitation douteuses. Ces habilitations douteuses peuvent correspondre à une large variété de stratégies, comme l'habilitation par des organismes eux-mêmes non habilites à le faire, des << usines a accréditions >> ou le mensonge pur et simple en affichant une contrefaite d'un organisme réellement accrédité. [5]

Aujourd'hui tout le monde se met en valeur sur son CV, et c'est tout à fait normal. En revanche, si gonfler son expérience sur certains sujets pose rarement un problème, mentir sur ses diplômes est un vrai danger. Certains présentent des diplômes d'écoles prestigieuses alors qu'ils n'ont fait que suivre un programme en partenariat avec l'école par exemple. Mais ça peut aller plus loin, et d'autres peuvent parfois inventer complètement des diplômes ou les acheter de manière illégale. Au final, il s'agit un marché de plusieurs milliards dans le monde et une véritable plaie pour les services des ressources humaines.

Délivrance de diplômes à l'UCAD

Depuis que l'Université Cheikh Anta Diop existe, on ne nous délivre pas de diplômes qui sanctionne la fin d'un cycle. Les étudiants n'obtiennent que des attestations et des relevés de note à leur place.

Imaginons que le recteur décide de délivrer des diplômes à la place de ces attestations. Le travail deviendra fastidieux, cela nécessitera de signer tous les diplômes papiers, ce qui devient obsolète, vu le nombre croissant d'étudiants.
Pour l'authenticité de ces derniers, il faut que le diplôme que l'on nous fournit qu'on est la certitude que sa provient de l'UCAD et que les données ne sont pas altérées.

Jusqu'ici, sauf à présenter des diplômes originaux la meilleure solution d'apporter la confiance sur l'obtention d'un diplôme était d'en demander une copie certifiée conforme à l'émetteur pour s'inscrire à une université étrangère par exemple. Mais c'est un processus fastidieux et chronophage de chacune des parties.

La blockchain est récemment devenue un sujet de prédilection, en particulier pour les crypto-monnaie. Quelqu'un dit que cela redéfinit la confiance, car en utilisant la blockchain, il n'est plus nécessaire de faire confiance à quiconque sauf à l'algorithme.

Utiliser la blockchain pour les diplômes revient à certifier ces derniers.

4.3 Travaux Connexes

De nos jours certains universités ont appliqué la technologie Blockchain à l'éducation, et la plupart d'entre elle l'utilise pour soutenir la gestion des diplômes universitaires.
L'Université de Nicosie a été le premier établissement d'enseignement supérieur à stocker des certificats académiques sur la blockchain de Bitcoin. [18]

4.3.1 Cas de BCDiplôma

BCDiplôma a été fondé en 2017 par Luc Jarry-Lacombe et Vincent Langard, experts dans les domaines de l'enseignement et de la blockchain, c'est un projet français, lancé par une ICO (Initial Coin Offering) qui est une méthode de distribution de tokens via une levée de fond en début 2018.

BCDiplôma repose sur la technologie Ethereum (une plateforme basée sur la technologie blockchain qui permet aux développeurs de réaliser et de déployer des applications décentralisées).

4.3.1.1 Objectifs

L'objectif de BCDiplôma est simple : faciliter et automatiser la vérification et l'authenticité des diplômes. [19]
Le principe est le suivant :

- L'école partenaire déploie simplement les diplômes de ses étudiants sur le service proposé.
- Ensuite, chaque détenteur de diplôme pourra alors partager un lien vers ce dernier, en utilisant un code QR ou une URL.
- Les recruteurs n'auront plus qu'à suivre le lien pour vérifier le diplôme en question.

Il s'agit d'un grand gain de temps par rapport aux recherches de plusieurs heures qui sont d'usage actuellement. Un autre avantage apporté par le stockage des diplômes sur la blockchain est qu'ils ne peuvent plus être perdus ou détruits.

Les outils sont open-source et ils proposent une API dédiée au service.

Cela permet notamment de conserver un accès aux diplômes en cas d'arrêt du service. Il y a une donc une garantie d'accessibilité dans le temps aux diplômes, tant pour les établissements que pour les étudiants.

Au niveau de la tarification du service, les frais sont payés en utilisant le token BCDT, ou en monnaie fiat. Les frais sont fixes et payés uniquement lors du déploiement des diplômes sur la blockchain (il n'y a pas d'abonnement).

Le token BCDT de type applicatif a été distribué lors d'une ICO entre décembre 2017 et février 2018. Le paiement des services de mise sur le réseau des diplômes se fait en utilisant ce token. Les établissements peuvent également directement payer un certain nombre de diplômes déployés par le biais de monnaies traditionnelles.

4.3.1.2 Architecture de fonctionnement de BCDiplôma

Figure 12 : Architecture de fonctionnement de BCDiplôma

Le processus d'utilisation se déroule en trois étapes :

- Les écoles et universités enregistrent les diplômes sur la blockchain
- Les élèves reçoivent les liens sous diverses formes qu'ils peuvent partager à leur guise
- Le recruteur reçoit le lien vers le diplôme et peut vérifier instantanément son origine

Techniquement, l'établissement délivrant le diplôme insère toutes les informations nécessaires sur l'interface dédiée.

C'est donc un système de smart-contracts qui est mis en place pour sauvegarder et retrouver les diplômes**.**

Techniquement, l'établissement délivrant le diplôme insère toutes les informations nécessaires sur l'interface dédiée, informations telles que la civilité de l'étudiant et les détails de son parcours scolaire. C'est donc avec une simple application que les établissements doivent interagir, et les informations peuvent être envoyées avec un fichier Excel par exemple. Ils peuvent également personnaliser l'apparence des diplômes, de façon à ce qu'ils soient identiques aux existants.

Une fois les diplômes déployés sur le service, et donc sur la blockchain Ethereum, le système délivre automatiquement les liens aux étudiants. Ces liens sécurisés peuvent être donc uniquement partagés par l'étudiant, et redirigent directement vers un site aux couleurs de l'école.

4.3.1.3 Sécurité et droit des données

Les établissements ont besoin de saisir de nombreuses données personnelles concernant les diplômés. Tout d'abord l'identité de ces derniers, mais également les détails de leurs scolarités, comme leurs notes ou certains commentaires.
Toutes ces données seront utilisées pour publier les diplômes sur la blockchain Ethereum. Elles seront donc en théorie accessibles à tous et ne pourront pas être retirées du système. Cela peut donc poser des questions quant à la sécurité et la protection de ces données.

BCDiplôma a décidé d'apporter une réponse cryptographique à la question << comment concilier le droit à la protection des données personnelles avec la blockchain ? >>
En outre, il permet de :

- Rendre le diplômé responsable du partage de son diplôme ;
- Rendre possible le droit à l'oubli ;
- Respecter le RGPD ;
- Assurer le plus haut niveau de sécurité possible.

BCDiplôma stocke les données sur la blockchain Ethereum avec un haut niveau de cryptographie. Chaque diplôme est crypté avec un haut niveau de cryptographie. Il utilise trois clés pour crypter chaque diplôme :

- La clé du diplôme ;
- La clé de persistance ;
- La clé permanente de l'école.

L'algorithme de BCDiplôma garantit la maitrise de l'accès à la donnée (clé du diplômé) et le droit à l'effacement (clé de persistance), en accord avec le RGPD, règlement européen entrant en vigueur en mai 2018, et dont la portée légale s'étend au monde entier. La sécurité est maximale : ce n'est que grâce à la possession des trois clés que la donnée encryptée peut être lue, grâce à l'algorithme AES_256_GCM considéré comme un mode de chiffrement intègre, aussi appelé mode combiné, offrant simultanément chiffrement et intégrité.

4.3.2 Cas de Blockcert

Le MIT et le Learning Machine ont conjointement créé l'open standard Blockcert. Il associe un diplôme qui contient des images, du texte et une signature avec l'identifiant unique des étudiants diplômés. Ces données sont cryptées, grâce à une clé privée, et stocké dans la blockchain. Les jeunes diplômés peuvent ensuite transmettre leurs diplômes aux recruteurs, qui peuvent vérifier l'authenticité des informations sur credntials.mit.edu. [20]

C'est un standard ouvert pour la création d'applications qui émettent et vérifient les enregistrements officiels basés sur la blockchain. Ceux-ci incluent les certificats pour les diplômes universitaires.

Elle est composée de bibliothèques, d'outils et d'applications mobiles open source permettant un écosystème décentralisé, basé sur des normes et centré sur le destinataire, permettant une vérification sans confiance grâce aux technologies de la chaîne de blocs.

Ces référentiels sont open source et peuvent être utilisés par d'autres projets de recherche. Il contient des composants pour créer, émettre, afficher et vérifier des certificats sur n'importe quelle blockchain. Ces composants forment toutes les pièces nécessaires à un écosystème complet.

4.3.2.1 Objectifs

L'objectif est de fournir aux individus la capacité de posséder et de partager leurs propres records officiels de réussite.
La pierre angulaire du projet Blockcerts est la conviction que les gens devraient pouvoir posséder et prouver la propriété de leurs importants documents numériques.

Caractéristiques idéales pour le destinataire

Pour qu'un certificat valablement délivré soit utile à un destinataire, les caractéristiques suivantes sont nécessaires :

- Indépendance : le destinataire possède les informations d'identification et n'exige pas que l'émetteur ou le tiers soient impliqués après avoir reçu les informations d'identification
- Propriété : le destinataire peut prouver la propriété des informations d'identification
- Contrôle : le destinataire a le contrôle sur la façon dont il conserve les informations d'identification qu'il possède. Ils peuvent choisir d'associer ou non les informations d'identification à un profil établi dont ils sont propriétaires.
- Vérifiabilité : les informations d'identification doivent être vérifiables par des tiers
- Permanence : les informations d'identification doivent être un enregistrement permanent (voir limitations à la fin)

Caractéristiques idéales pour l'émetteur

Pour qu'un système d'accréditation soit utile à un émetteur, les caractéristiques suivantes sont nécessaires :

- L'émetteur peut prouver qu'il a délivré les informations d'identification
- L'émetteur peut définir une heure d'expiration sur les informations d'identification
- L'émetteur peut révoquer les informations d'identification

Le système d'accréditation est sécurisé et impose une charge continue minimale pour conserver cette caractéristique

4.3.2.2 Architecture et fonctionnement

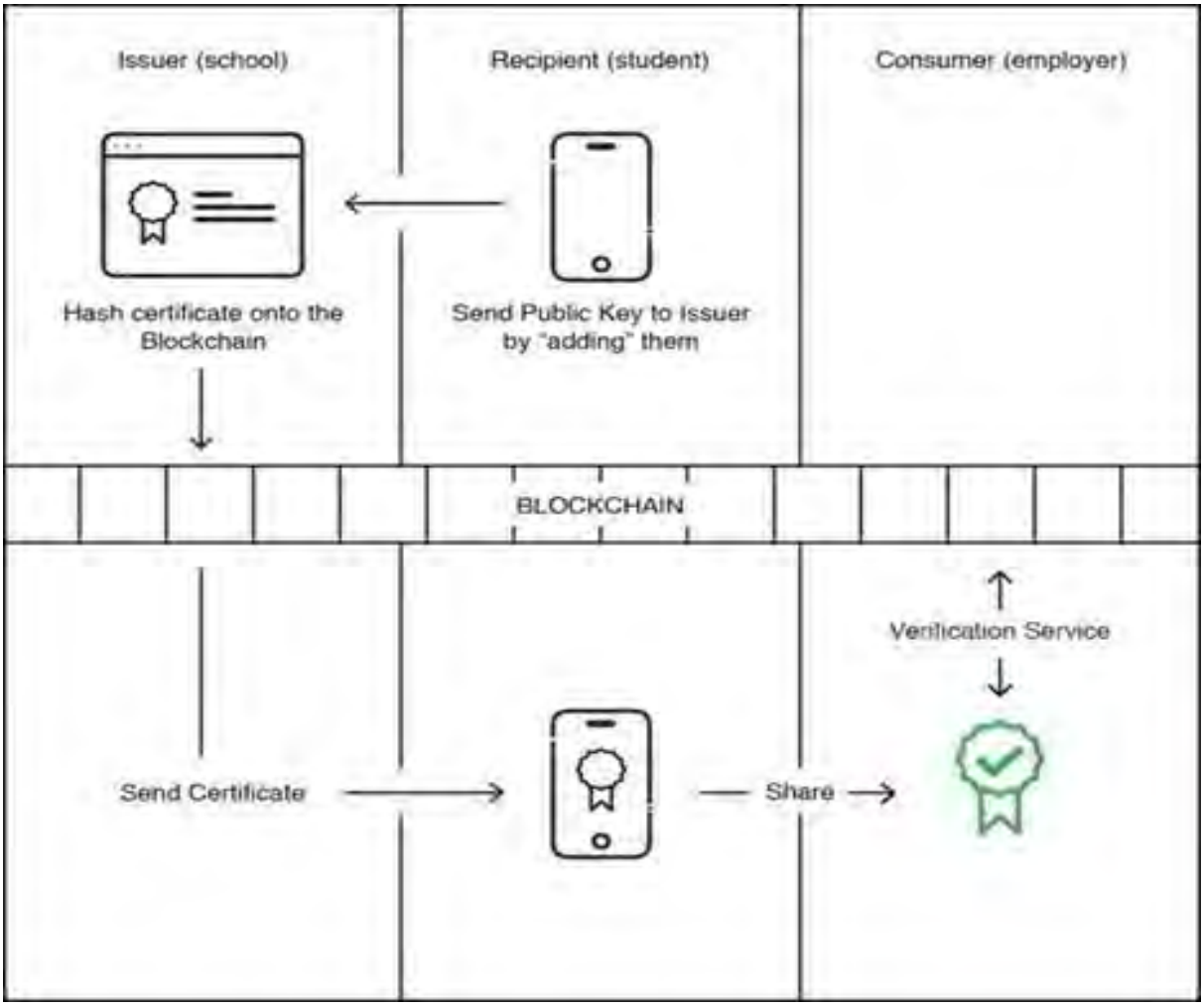

Figure 13 : Architecture de Blockcert [I13]

- Émetteur invite l'étudiant par (email, QR code, etc.)
- L'étudiant ajoute l'émetteur dans l'application en transmettant l'adresse de la chaine de bloc
- Un identifiant est créé par le destinataire ajoutant son adresse a l'intérieur des identifiants. Les informations d'identification sont ainsi hachées
- Le destinataire reçoit les informations d'identification (lien, fichier JSON)
- Le destinataire peut ainsi envoyer à un vérificateur
- Le vérificateur vérifie à l'aide de vérificateurs à code source

Pour assurer la sécurité du diplôme, le pilote utilise la même technologie de blockchain qui alimente la monnaie numérique Bitcoin. Et même si les compétences numériques ne sont pas nouvelles, le projet pilote du MIT est révolutionnaire car il donne aux étudiants une autonomie sur leurs propres dossiers.

L'idée est de permettre aux étudiants d'être les conservateurs de leur propre titre de compétences. Ce projet leur permettra d'avoir la propriété sur leur dossier et de pouvoir les partager de façon sécurisée avec qui ils veulent.

4.3.3 Tableau comparatif

Tableau 5 : Tableau comparatif entre Blockcert et BCDiplôma

Critères de comparaison	BCDIPLOMA	Blockcert
Ecosystème	Evidenz	Blockcert
Type de blockchain	Publique	Publique
Type de crypto-monnaie	Ethereum	Bitcoin
Smart contract	OUI	NON
Moyen de prouver l'authenticité	URL	URL
Stockage de données	Cryptée sur la chaine	Basée sur le hachage

Plus loin, notre choix se portera sur l'architecture de MIT qui utilise l'écosystème Blockcert On fera une étude plus détaillée de notre choix dans le chapitre mise en œuvre de la solution.