Chapitre 3 : Blockchain dans la Certification numérique

3.1 Qu'est-ce que la certification ?

D'une manière générale, la certification décrit tout processus par lequel un certificat est délivré en tant que vérification d'une réclamation. [17]

En éducation, la certification est utilisée dans de nombreux scénarios par exemple, comme preuve de :

- Réalisation des résultats d'apprentissage, quelle que soit la forme d'apprentissage ;
- La compétence d'un enseignant ;
- Un processus d'apprentissage entrepris par un apprenant, quelle que soit la forme d'apprentissage ;
- Une organisation éducative ou un cours répondant à certains critères de qualité ;

3.1.1 Composants d'une certification

La certification, dans sa forme la plus essentielle, consiste en une déclaration d'une partie à une autre selon laquelle certains faits sont vrais. Ainsi, toute certification comporte les éléments suivants [17] :

- L'affirmation selon laquelle « cet ensemble de faits est vrai ». Exemples dans un contexte éducatif peut inclure, « un apprenant a acquis une compétence », « un enseignant a suffisamment de connaissances pour enseigner » ou « un élève a terminé un travail ».
- Un émetteur : un organe qui a vérifié et validé les faits et qui certifie que la demande est vraie.
- Preuve à l'appui de la réclamation, comprenant généralement la procédure de vérification de la réclamation et des informations supplémentaires sur la réclamation.
- Un destinataire : la personne à laquelle la demande s'adresse, l'apprenant qui acquiert les compétences, l'enseignant qui a suffisamment de connaissances pour enseigner ou l'étudiant qui a terminé un travail
- Un certificat : un document qui atteste l'identité de l'émetteur, l'identité du destinataire, la réclamation et fait référence aux éléments de preuve si nécessaire.
- Un certificat comportera une signature qui est un symbole, un tampon, une image ou un code unique, qui ne peut être apposée que par l'émetteur, confirmant ainsi leur identité.

3.1.2 Processus impliqués dans la certification

La certification implique trois processus distincts :

- Délivrance : il s'agit du processus d'enregistrement de la demande, de l'émetteur, de la preuve, du destinataire et de la signature sur un certificat.
- Vérification : il s'agit du processus par lequel un tiers vérifie l'authenticité du certificat. Il y a deux modalités pour cela :
    1) Vérification à l'aide de fonctions de sécurité intégrées au certificat lui-même : cela peut inclure des mesures telles que la vérification de l'authenticité du papier de sécurité spécial, de la signature, etc.
    2) Vérification du certificat auprès de l'émetteur d'origine, le tiers contactant l'émetteur d'origine pour lui demander s'il a réellement délivré le certificat. (Dans ce cas, l'émetteur initial peut consulter sa base de données centralisée des revendications ou vérifier les fonctions de sécurité intégrées au certificat) ;
- Partage : il s'agit du processus par lequel le destinataire d'un certificat partage ce certificat avec un tiers.

3.2 Acteurs pour un système de certification fiable

Bien que toute personne puisse délivrer un certificat à toute autre personne, attestant de quoi que ce soit, l'objectif d'un système de certification est que les certificats soient largement acceptés par des tiers. Cela nécessite que les tiers fassent largement confiance au système et à ses processus. [17]

La confiance dans le contexte de la certification est créée par les méthodes et processus suivants :

3.2.1 Méthode de vérification de l'identité

Cela implique de créer un climat de confiance en vérifiant qui est impliqué dans la transaction. Dans la mesure où un certificat implique l'émission d'une déclaration d'une partie à une autre, il est important de pouvoir vérifier l'identité de l'émetteur et du détenteur du certificat. L'identité est généralement vérifiée à l'aide de documents d'identité, qui sont eux-mêmes des certificats attestant l'identité d'une personne.

Lorsque la vérification des documents d'identité peut être complexe, des tiers sont souvent impliqués pour vérifier l'identité de l'une ou l'autre des parties.

3.2.2 Processus normalisés pour la délivrance et la certification

Le seul fait de connaître l'identité des parties à une transaction signifierait que les tiers devraient avoir une confiance totale en la première. Étant donné que ces circonstances se produisent rarement, il est également nécessaire d'avoir confiance dans la manière dont les

certificats sont délivrés, en indiquant notamment la méthode par laquelle l'émetteur est parvenu à la conclusion énoncée dans la demande.

Il est également nécessaire de veiller à ce que tous les certificats d'un système soient délivrés de manière prévisible et équitable, c'est-à-dire qu'un certificat sera délivré à toute personne qui répond à un certain ensemble de critères et ce, uniquement si elle répond à cet ensemble de critères.

3.2.3 Fonctions de sécurité

Un tiers qui souhaite vérifier l'authenticité d'une revendication dans un certificat doit pouvoir s'assurer que ce certificat n'est pas falsifié. Il existe deux moyens d'éviter de tels faux :

- Par le biais de mécanismes physiques anti-contrefaçon tels que les signatures, les filigranes, les dessins spéciaux incorporés dans le certificat lui-même, qui garantissent que seul l'émetteur aurait pu créer ce certificat spécifique ;
- Via une base de données de créances émises, détenue soit par l'émetteur, soit dans une base de données centralisée appelée registre, permettant à un tiers de vérifier que la réclamation a bien été émise.

3.3 Utilisations de la certification en éducation

Utilisation des certificats délivrés aux apprenants

Les certificats sont largement utilisés tout au long de l'enseignement, à diverses fins.

- L'achèvement d'une expérience d'apprentissage spécifique. Des exemples de ceci pourraient inclure un certificat de fin d'études dans l'éducation formelle ;
- La totalité des apprentissages réalisés dans un domaine spécifique, par exemple pour un certificat attestant de l'attribution d'un diplôme ;
- Des expériences spécifiques qui contribuent à l'apprentissage, telles que des certificats attestant l'achèvement d'un apprentissage ou d'un autre type d'expérience professionnelle ;

- L'acquisition de compétences spécifiques, telles que les certificats délivrés dans le cadre de procédures de reconnaissance des acquis ;
- La réalisation de certains critères d'excellence, par exemple en remportant certains prix d'excellence ou en obtenant le diplôme « avec mention » ;
- Le niveau de compétence spécifique atteint dans des domaines spécifiques, grâce à la délivrance d'attestations d'examen ou de cartes de notes.

3.4 Limitations des Certificats

La plupart des enregistrements sont toujours publiés sur papier ou sur d'autres supports physiques, bien que les gouvernements et les industries déploient des efforts de numérisation dans le monde entier. Il n'existe pas de « format parfait » pour les certificats. De nombreux pays utilisent des certificats hybrides grâce auxquels les certificats papier sont sauvegardés par des bases de données numériques.
Cependant, les limitations importantes de chaque système montrent clairement le besoin d'une technologie de certification meilleure et plus robuste.

3.4.1 Limitations des certificats papier

Les certificats papier sont encore souvent considérés comme la forme de certification la plus sûre, car ils sont :

- Difficile à falsifier en raison de fonctions de sécurité intégrées aux certificats eux-mêmes ;
- (Généralement) détenus directement par le destinataire, qui a donc tout le contrôle sur Certificat ;
- Relativement facile à stocker en toute sécurité pendant de longues périodes, par ex. en les gardant dans un coffre-fort ;
- Ils peuvent être présentés par le destinataire n'importe où, à n'importe qui, pour n'importe quel but.

- Cependant, les certificats papier présentent également des inconvénients importants :

- Bien qu'il soit difficile à falsifier, aucun certificat n'est à l'abri du risque de falsification. Ainsi, l'émetteur est tenu de conserver un registre central des certificats délivrés pouvant servir à vérifier l'authenticité des certificats ;
- Les registres de certificats sont des points uniques d'échec : bien que les certificats puissent rester valables, leur capacité à les vérifier est perdue ;
- Tenir un tel registre des réclamations et répondre aux questions concernant la validité des certificats est un processus manuel qui nécessite d'importantes ressources humaines ;
- Les caractéristiques de sécurité du certificat physique découlent exclusivement du niveau de difficulté et de l'expertise requise pour créer le document. Plus le certificat est sécurisé, plus il est coûteux à produire.
- La capacité de l'émetteur à indiquer de manière frauduleuse l'horodatage ou d'autres détails du certificat n'est soumise à aucune restriction ;

- Une fois délivré, il n'y a aucun moyen de révoquer un certificat sans que le propriétaire en abandonne le contrôle ;
- Si un tiers doit utiliser les certificats, par exemple pour vérifier les revendications dans le CV, ils doivent lire et vérifier chaque certificat individuellement et manuellement, ce qui prend beaucoup de temps.

3.4.2 Limitations des certificats numériques (non-blockchain)

Les certificats numériques présentent de nombreux avantages par rapport aux certificats papier :

- Ils ont besoin de beaucoup moins de ressources pour émettre, maintenir et utiliser, car :
    1) La véracité des certificats peut être vérifiée automatiquement par rapport au registre, sans intervention humaine ;
    2) Lorsqu'un tiers doit utiliser les certificats, ceux-ci peuvent être automatiquement rassemblés, vérifiés et même résumés s'ils sont émis dans un format normalisé ;
    3) La sécurité du certificat découle de la sécurité des protocoles cryptographiques, qui garantissent que le certificat est peu coûteux à produire mais extrêmement coûteux à reproduire par quiconque à l'exception de l'émetteur ;

- Les certificats peuvent être révoqués par l'émetteur ;

- Certains types de fraude par l'émetteur, tels que la modification de l'horodatage ou le certificat de série, peut être rendu impossible en fonction de la conception du système.

Cependant, les certificats numériques présentent également des inconvénients importants, à savoir que :

- Sans l'utilisation de signatures numériques, il est extrêmement facile de les falsifier ;
- Lorsque des signatures numériques sont utilisées, elles nécessitent la participation de fournisseurs de certificats tiers pour garantir l'intégrité de la transaction - ces tiers ont un contrôle important sur tous les aspects du processus de certification et de vérification, qui peuvent faire l'objet d'abus ;
- Il est plus facile de détruire des enregistrements électroniques. Pour les conserver en sécurité, vous devez disposer de systèmes de sauvegarde sophistiqués à plusieurs niveaux, sujets à l'échec.

- En cas d'échec du registre, les certificats eux-mêmes perdent leur valeur car, contrairement aux certificats papier, ils n'ont aucune valeur intrinsèque sans le registre ;

3.5 Certificats numériques utilisant la technologie Blockchain

La technologie Blockchain est idéale en tant que nouvelle infrastructure pour sécuriser, partager et vérifier les acquis de l'apprentissage. Dans le cas des certifications, une blockchain peut conserver une liste des émetteurs et destinataires de chaque certificat, ainsi que la signature du document (hash) dans une base de données publique (la blockchain), stockée de manière identique sur des milliers d'ordinateurs du monde entier. Les certificats numériques ainsi sécurisés sur une blockchain présentent des avantages importants par rapport aux certificats numériques « ordinaires », en ce sens que :

- Ils ne peuvent pas être falsifiés- il est possible de vérifier avec certitude que le certificat a été initialement délivré et reçu par les mêmes personnes indiquées dans le certificat ;
- La vérification du certificat peut être effectuée par toute personne ayant accès à la blockchain, avec un logiciel open source facilement disponible - aucune partie intermédiaire n'est nécessaire ;
- Étant donné qu'aucune partie intermédiaire n'est tenue de valider le certificat, celui-ci peut toujours être validé même si l'organisation qui l'a délivré n'existe plus ou n'a plus accès au document délivré ;
- Le registre des certificats émis et reçus sur une blockchain ne peut être détruit que si chaque copie de chaque ordinateur du monde hébergeant le logiciel est détruite ;
- Le hachage est simplement un moyen de créer un "lien" avec le document original, qui est détenu par l'utilisateur. Cela signifie que le mécanisme ci-dessus permet de publier un document sans avoir à le publier lui-même, préservant ainsi la confidentialité des documents.

3.5.1 Caractéristiques idéales pour le destinataire

Les Blockchains répondent aux exigences idéales suivantes pour un certificat du point de vue du destinataire :

- Indépendance : le destinataire est en possession du justificatif d'identité et n'exige pas que l'émetteur ou le tiers vérificateur soit impliqué après la réception du justificatif ;
- Propriété : le destinataire peut prouver qu'il est propriétaire du justificatif d'identité ;
- Contrôle : le destinataire contrôle la manière dont il gère les informations d'identification qu'il possède. Ils peuvent choisir d'associer des informations d'identification à un profil établi qu'ils possèdent ou non ;
- Vérifiabilité : le justificatif d'identité est vérifiable par des tiers, tels que des employeurs, des comités d'admission et des organisations de vérification ;
- Permanence : le justificatif d'identité est un enregistrement permanent

3.5.2 Caractéristiques idéales pour l'émetteur

Les Blockchains répondent aux exigences idéales suivantes pour un certificat du point de vue de l'émetteur :

- L'émetteur peut prouver qu'il a délivré le justificatif d'identité ;
- L'émetteur peut définir un délai d'expiration pour les informations d'identification ;
- L'émetteur peut révoquer le justificatif d'identité ;
- Le système d'accréditation est sécurisé et n'impose une charge permanente minimale que pour le rester.

3.5.3 Autres caractéristiques

Pour qu'un justificatif d'identité ait un sens et une utilité, un vérificateur tiers, tel qu'une institution recevant le justificatif d'identité dans le cadre d'une application, doit être convaincu de la véracité d'un certificat. Les éléments suivants sont des exigences standard :

- Intégrité : le contenu n'a pas été altéré ; c'est-à-dire qu'il correspond à ce que l'émetteur avait initialement prévu.
- Authenticité : confiance que l'émetteur est le destinataire du certificat et qu'il n'a pas été falsifié.

3.6 Certifier l'identité à l'aide d'une blockchain

D'un point de vue technique, l'identité d'une personne est constituée de la somme de toutes ses informations personnellement identifiables.

Lorsqu'une personne souhaite confirmer son identité à une autre personne ou institution, elle partage une grande partie de ces informations personnellement identifiables.
Ainsi, par exemple, un étudiant potentiel pourrait confirmer son identité au bureau de l'admission d'une université en fournissant son nom, son adresse, son numéro d'identification gouvernemental, son sexe et ses grades. En règle générale, le bureau des admissions conservera toutes ces données dans une base de données centralisée, ce qui obligera l'utilisateur à se fier à lui pour veiller à la sécurité de ses données. Toutefois, en raison de la valeur de ces données, elles sont extrêmement exposées aux risques tels que les abus, la fraude et le vol, comme en témoigne la récente vague de vols de données volumineux de grande envergure perpétrés par des gouvernements et des entreprises du monde entier. [17]

Actuellement, chaque fois qu'une personne doit effectuer une transaction avec une nouvelle personne ou organisation, elle doit à nouveau transmettre ses données et donner à une autre personne le contrôle sur la manière dont ces données sont sauvegardées et sauvegardées.

La technologie Blockchain permet un nouveau concept d'identité autonome, selon lequel un utilisateur stocke ses propres informations personnellement identifiables sur un appareil personnel, tel qu'un smartphone, et ne les partage qu'avec des tiers, le cas échéant. C'est l'équivalent numérique de conserver vos certificats papier dans un coffre chez vous et de les afficher à un tiers pour prouver votre identité, tout en gardant le contrôle sur le fait de savoir si ces tiers peuvent copier ces documents ou non. La technologie Blockchain permet en outre à l'utilisateur de certifier son identité sans avoir à partager les données sous-jacentes constituant cette identité.

3.6.1 Utiliser une identité souveraine certifiée

Une fois qu'une personne a une identité totalement autonome :

- Leurs données personnelles sont stockées numériquement sur un appareil auquel ils ont uniquement accès et qu'ils contrôlent, tel qu'un portefeuille au niveau de l'appareil ;
- Un hachage de ces données, qu'il s'agisse de revendications ou de documents numériques, peut être stocké dans la blockchain ;
- La véracité de ces données est certifiée par des tiers, tels qu'un établissement émetteur ou vérificateur dont les certificats sont également :

1. Stockées sur le périphérique sécurisé avec les autres données de la personne ;
2. Haché sur une blockchain ;

- Avec ces éléments, une personne peut s'identifier de manière sécurisée auprès de toute partie qui fait également confiance à l'institution de vérification, simplement en prouvant qu'elle est le propriétaire de la clé publique associée à la demande de certificat et sans qu'il soit nécessaire de partager un élément personnellement identifiable.

3.7 Délivrance de diplôme directement à l'aide d'une blockchain

Chaque fois qu'un diplôme peut avoir une valeur mesurable, il peut être représenté sous forme de jeton et échangé directement sur une blockchain personnalisée. Ainsi, par exemple sur une blockchain pour un diplôme de fin d'études, un seul certificat peut être considéré comme un seul jeton ;
Les diplômes pourraient être transférés d'une personne à une autre, simplement en transférant un jeton sur la blockchain.
Ainsi, il est possible de concevoir une base de données dans laquelle certaines informations seraient privées et détenues par l'utilisateur, tandis que d'autres informations seraient conservées publiquement sur une blockchain. L'avantage d'émettre des certificats directement sur une blockchain est que les certificats eux-mêmes, plutôt que la simple preuve de leur signature, deviennent immuables et permanents.

L'inconvénient est que toute chaîne de blocs à usage général utilisée de cette manière augmenterait considérablement, ce qui entraînerait une perte de performances et une utilisation élevée des ressources. Ainsi, un tel modèle ne pourrait être implémenté qu'en tant que blockchain privée / autorisée.

De manière pragmatique, un diplôme ne contient que très peu d'informations. Il contient la date, l'institution d'attribution, le boursier et le titre du diplôme. Ainsi, on pourrait lire que l'Université Cheikh Anta Diop a délivré un diplôme en sciences (avec mention) à Nicolas le 18 JUILLET 2018. C'est une quantité infime d'informations qui se prête bien au stockage dans un grand livre et prendrait peu de place. Ainsi, il pourrait être publié sur une blockchain soit :

- En clair, s'il s'agit de créer une base de données publique sur les diplômes décernés ;
- Comme hachage du certificat (en utilisant un système tel que Blockcerts) si le but est de sécuriser le certificat numérique attribué à l'étudiant.

Ces informations peuvent contenir plusieurs pages. Bien qu'elles soient bien adaptées au stockage dans une base de données, elles le sont moins au stockage dans un grand livre. En outre, il serait extrêmement coûteux de stocker ce niveau d'informations directement sur une blockchain. Par conséquent, les diplômes et leur supplément au diplôme pourraient être publiés sur une chaîne de blocs.