BITCOIN ET BLOCKCHAINS : RÉFLEXIONS TERMINOLOGIQUES ET IDENTITAIRES

Réflexions terminologiques à propos du Bitcoin et des systèmes d'échanges décentralisés types blockchains et tentative de définition d'un nouveau paradigme d'identité et de certification.

L'objectif de la présente proposition de contribution est la mise en place d'un lexique précis autour des termes de la sphère Bitcoin et blockchains ainsi que la mise en place d'une réflexion sur les enjeux identitaires de ces nouveaux systèmes.

Le premier axe de réflexion est celui d'une définition claire des termes ayant trait à l'écosystème Bitcoin[1]. En effet le lexique employé découlant principalement des utilisateurs au fur et à mesure du temps, il s'avère que ce lexique n'est pas forcément limpide et similaire pour toutes les parties. Or il est essentiel de se mettre d'accord sur une terminologie précise pour pouvoir échanger entre les différents acteurs des secteurs pouvant être concernés par cet écosystème : l'informatique, le droit, la finance, etc.

L'objectif serait ici de réussir à élaborer un lexique commun avec le moins de décalages analogiques possibles ou du moins de réfléchir à leur pertinence. (mineur, portefeuille, compte, contrat, etc.) Cela permettra aussi de réfléchir par la même occasion à des normes techniques. Dans quelle mesure telle ou telle blockchain[2] pourrait-elle être considérée comme fiable ? Dans quelle mesure les jetons d'une blockchains pourraient-ils représenter des actifs ? Toutes ces questions peuvent être totalement résolues ou partiellement résolues à l'aide d'un lexique commun et d'une définition commune de ce qu'est une blockchain. En effet, dans l'optique, d'un jour peut-être, conférer une valeur probante[3] aux enregistrements dans les blockchains, il est essentiel de savoir lesquelles sont considérées comme telles et selon quels critères.

---

[1] Bitcoin : Système d'échanges décentralisé né en 2009 suite à la publication d'un livre blanc : *Bitcoin a peer-to-peer electronic cash system* de l'anonyme Satoshi Nakamoto. Ce protocole permet la production et l'échange d'actifs numériques non reproductibles (des bitcoins) à l'aide notamment d'un livre de compte dans lequel il est possible d'ajouter des données horodatées de manière fiable et infalsifiable.

[2] Blockchain (ou chaîne de blocs) : Registre de transactions décentralisé, c'est un des rouages permettant le bon fonctionnement des systèmes d'échanges décentralisés. Cependant chaque protocole ayant des spécificités différentes, il est impossible d'employer ce terme de manière défini au singulier sans l'accompagner du protocole qui définit ladite blockchain.

[3] La député Madame Laure de La Raudière a proposé un amendement en ce sens : http://www.la-raudiere.com/lng_FR_srub_39_iart_1327-je-presente-un-amendement-a-propos-du-blockchain-a-l-assemblee-nationale-pour-que-la-f.html

Une telle contribution n'est possible qu'avec la collaboration des acteurs des différents secteurs et de ce fait, l'évènement semble être très approprié pour cela.

Le deuxième axe de réflexion, fortement lié au premier, est celui de la valeur (juridique, économique) qu'il est possible de porter aux écritures au sein d'une blockchain comme celle de Bitcoin. Ce nouveau type de registres décentralisés de transactions permet la constitution d'une identité numérique bien plus fiable que celle des bases de données centralisées. (en raison de leur faiblesse aux attaques et du fait qu'elles impliquent de déléguer son identité à un tiers.) Dans une logique d'anticipation, serait-il possible par exemple de signer un document avec une adresse bitcoin ?

Là où un compte Facebook ou Google appartient à la firme qui propose le service, (en ce sens qu'il est dans ses serveurs et qu'il n'est possible à l'utilisateur de faire des changement qu'à l'aide d'une interaction avec l'entreprise) une adresse sur le réseau Bitcoin appartient totalement à la personne concernée. (en ce sens qu'elle est la seule à connaître sa clef privée.) Ce changement paradigmatique inclut dès lors une remise en question de l'identité numérique qui, dépourvue de toute possession extérieure, se rapproche de plus en plus d'une identité physique (je suis seul détenteur de mes empreintes.) , même si paradoxalement elle n'est délivrée par aucun tiers. (l'état se sert de mes empreintes pour m'identifier.) Cependant la constitution d'une identité claire dans ce territoire à part entière qu'est le cyberespace semble un enjeu capital autant d'un point de vue citoyen (possibilité de vote électronique sans faille.) que d'un point de vue judiciaire. (contrôle d'identité en ligne sans pour autant souffrir d'une atteinte à la vie privée.)

Et cela va de pair avec la certification sur les réseaux décentralisés. Il est possible de considérer que l'empreinte d'un document dans la blockchain Bitcoin est horodatée, fiable et infalsifiable dans le temps. *De facto* nous pensons à de nombreux cas pratiques comme celui de la « preuve d'antériorité ». Dans quelle mesure, l'envoi de l'empreinte d'un document dans la blockchain pourrait être considéré comme ayant la même fiabilité et la même valeur qu'une enveloppe Soleau délivrée par l'INPI ? De la même manière, il est essentiel que l'état puisse « marquer » des adresses pour jouer son rôle de tiers. Ainsi il serait possible d'avoir son âge et son sexe liés à son identité numérique sans pour autant la confier à un tiers. (ici l'état) Toutes ces questions doivent être étudiées car elles constituent une étape intermédiaire et obligatoire pour permettre la création d'une identité numérique respectant les droits fondamentaux du citoyen.

ADLI TAKKAL BATAILLE
Étudiant en master recherche de linguistique / Entrepreneur et représentant associatif dans le numérique