Louis de Méneval
Simon Polrot

La blockchain, un nouveau paradigme pour le numérique

La blockchain, registre partagé de transactions enregistrées, garantit le caractère immuable, infalsifiable et non duplicable des inscriptions. Cette technologie encore émergente permet également la création d'actifs numériques. Révolution ou évolution ? Pour comprendre les enjeux de la blockchain et les problématiques juridiques qu'elle soulève, nous nous sommes adressés à deux juristes : Louis de Méneval, responsable des contrats corporate et du contentieux d'AXA Investment Managers et Simon Polrot, avocat au cabinet Fieldfisher, le premier s'intéressant plus particulièrement à la blockchain privée et le second à la blockchain publique. Au cours de cet entretien croisé, nous avons notamment évoqué les questions d'identité numérique, de création d'actifs numériques uniques, de propriété intellectuelle, de responsabilité, de la difficulté de l'immutabilité des actifs pour les acteurs privés, de la nécessité de l'intervention d'un régulateur, d'un besoin d'une régulation souple, des smart contracts.

Sylvie Rozenfeld : Louis de Méneval, vous êtes responsable des contrats corporate et du contentieux d'AXA Investment Managers, au sein d'un groupe qui s'intéresse à la blockchain privée, et Simon Polrot, vous êtes avocat, au cabinet Fieldfisher vous vous êtes plus particulièrement penché sur la blockchain publique.
J'ai souhaité vous rencontrer pour y voir un peu plus clair dans cette technologie qui a fait le buzz de l'année 2016. Contrairement aux algorithmes qui ont été l'autre thème tendance de l'année, la blockchain est un concept complexe, difficile d'accès aux néophytes. Sans nous perdre dans les explications techniques, on peut dire que la blockchain est une technologie qui permet de transférer la tenue d'un registre vers des acteurs répartis sur le web, sans qu'aucun n'ait la possibilité de falsifier les transactions du registre.
Avant d'aborder les problématiques liées à la blockchain, cette définition vous semble-t-elle suffisante pour en appréhender ses caractéristiques et envisager les problèmes juridiques ? Ou celle du code monétaire, introduite en 2016 à l'occasion de la réglementation sur les minibons : « *un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations* » serait une bonne définition juridique de la blockchain ?

Simon Polrot : Il s'agit effectivement d'un registre partagé de transactions enregistrées. J'ajouterais une particularité de la blockchain liée à son fonctionnement, à savoir le consensus entre les différents acteurs. La façon dont les acteurs se mettent d'accord sur le contenu de ce registre permet de sécuriser ce qui y est inscrit et d'éviter l'altération du registre. L'intérêt principal de la blockchain est donc d'avoir un registre infalsifiable. Ceux qui vont y accéder seront ainsi certains qu'il n'a pas été modifié et que les inscriptions qui y figurent sont celles d'origine.

« En réalité, ce principe d'une totale immutabilité n'est pas atteignable. »

Pensez-vous que nous sommes face à une technologie révolutionnaire qui va impacter toute la société ou bien va-t-elle seulement se développer dans des domaines nécessitant le recours à un registre ?

Louis de Méneval : A mon sens, il est difficile de parler d'une seule blockchain. On peut imaginer à terme qu'il y aura une révolution grâce à une blockchain publique, mais à court terme, nous verrons plutôt des applications sectorielles, dans des domaines où il y a beaucoup d'intermédiaires et de tiers de confiance, comme la finance. Elles seront sans doute moins révolutionnaires que dans une blockchain publique.

Simon Polrot : Toutes les utilisations ont un aspect « *révolutionnaire* », à mon sens, avec une différence d'échelle entre les deux types de blockchain, celle publique et celle privée. En plus du caractère infalsifiable du registre et de l'impossibilité de dupliquer les inscriptions, cette technologie permet surtout de faire apparaître des actifs numériques. Cela n'existait pas jusqu'à présent.

Pouvez-vous préciser ce que vous entendez par « *faire apparaître des actifs numériques* » ?

Simon Polrot : Si je vous donne une bouteille d'eau, j'en suis dépossédé. Au niveau numérique, si je transmets un fichier, je continue d'en disposer. C'est la classique dichotomie entre un bien physique et un bien numérique. Ce qui est nouveau avec la blockchain, c'est le fait que les inscriptions sont rattachées à un compte. Si je donne mon inscription, ma clé virtuelle à un autre compte, je n'en dispose plus. En fait, on reconstruit au niveau numérique la propriété matérielle. On peut ainsi donner à des inscriptions numériques les caractéristiques d'un bien physique. Le fonctionnement de la blockchain interdit les doubles dépenses, les doubles inscriptions. C'est la raison pour laquelle elle s'est d'abord développée avec les crypto-monnaies. Dans le domaine de la monnaie, il est essentiel d'avoir un actif unique. La création d'actifs numériques a commencé avec les bitcoins et elle se répand aujourd'hui dans différents usages tels que le cadastre. Dans ce dernier cas, il est important que l'inscription de la maison soit unique et non duplicable. Il s'agit de la création d'actifs numériques uniques qui possèdent certaines caractéristiques proches des biens physiques pour qu'on puisse y appliquer des raisonnements similaires : des droits de propriété, des transferts, des dons, des réceptions, etc. Cela existe aussi bien dans les blockchains publiques que privées. Pour moi, la blockchain représente un changement de paradigme de la façon d'appréhender le numérique. Medium de transmission de l'information, le numérique peut devenir un medium de transmission d'actifs. Un autre usage est celui de la preuve d'un document.

Vous avez évoqué l'existence de blockchains publiques et privées. Peut-on encore parler blockchain avec la blockchain privée, dans la mesure où on réintroduit de la centralité et une autorité, l'oracle ?

Louis de Méneval : Selon moi, la blockchain privée se distingue de celle publique au niveau du consensus. Celui-ci opère sur un réseau privé, avec une personne qui joue le rôle de gestionnaire ou d'administrateur qui définit et sélectionne

les participants à sa blockchain. On peut imaginer une certaine qualité du réseau car il y a moins de nœuds, une transmission plus rapide des informations. Une autre caractéristique de la blockchain en général qui fait l'objet de discussions est celle de l'immutabilité. C'est une notion que l'on met en avant pour définir la blockchain publique alors qu'elle peut poser problème dans le cadre privé. Si une erreur est enregistrée au départ, on ne peut pas la corriger, la supprimer à l'avenir. Pour les sociétés du secteur privé, il est difficile d'imaginer qu'on ne puisse pas revenir sur ce qui a été écrit.

Comment résoudre la difficulté du caractère immuable d'un enregistrement qui peut être une erreur d'origine ?

Louis de Méneval : Comme certaines sociétés le font déjà, on peut imaginer des protocoles de blockchain où existerait la possibilité de modifier un enregistrement.

Simon Polrot : La blockchain publique a été prévue à l'origine pour être accessible à tous, de manière à fonctionner avec le plus d'utilisateurs possible pour la sécuriser au maximum, avec l'application du principe de l'immuabilité des inscriptions, la confiance reposant sur ce principe. En réalité, ce principe d'une totale immutabilité n'est pas atteignable. En pratique, on a vu que le consensus de l'ensemble des participants à une blockchain peut changer. Dans la plupart des cas, les blockchains sont immuables, mais il y a des exceptions. L'absence complète d'immutabilité retirerait tout intérêt à la blockchain. Il y a un équilibre à trouver.

« On peut imaginer que pour la blockchain privée, le régulateur édictera des règles pour que l'identité des personnes participantes soient certifiées d'une manière ou d'une autre. »

Quel avantage possède la blockchain privée par rapport au recours à un tiers de confiance ?

Louis de Méneval : Elle apporte de la rapidité et de la sécurité. Je ne parlerais donc pas de révolution car les schémas technologiques sont assez proches de systèmes qui existent aujourd'hui. Si on prend l'exemple de l'achat d'actions, le trading, le settlement ou le post-settlement – un processus qui peut aujourd'hui être assez long -, on peut imaginer que le processus d'achat durera quelques instants avec la blockchain : vérification de l'heure de l'achat, confirmation de la contrepartie, etc. Aujourd'hui des intermédiaires prennent beaucoup plus de temps pour toutes ces vérifications.

Simon Polrot : L'intérêt de la blockchain privée réside dans la traçabilité et la conservation de toutes les opérations. Les utilisateurs gagnent du temps en se passant des intermédiaires ; ils n'ont pas besoin de rapprocher des bases de données différentes pour vérifier que la personne qui vend un bien le possède effectivement et que le vendeur dispose des fonds.
Mais tout ce qui est permis dans une blockchain publique n'est pas possible dans le schéma privé car on est entre acteurs connus.

Louis de Méneval : Sur cette notion d'acteurs connus, la question de l'identité est très importante. L'anonymat caractérise la blockchain publique. On peut imaginer que pour la blockchain privée, le régulateur édictera des règles pour que l'identité des personnes participantes soit certifiée d'une manière ou d'une autre.

Quelles sont les applications de blockchains privées chez AXA ?

Louis de Méneval : AXA est un grand groupe. AXA Next, l'entité Innovation du Groupe AXA qui étudie les nouvelles tendances, se penche notamment sur les smart contracts liés à l'assurance. Il y a un projet, en coordination avec d'autres acteurs de l'assurance dans le cadre du consortium LabChain (sur l'assurance en cas de décès). Ce serait une utilisation de la blockchain pour pouvoir rapidement débloquer les fonds d'une assurance après un décès. La question se pose de savoir qui donne l'impulsion en certifiant qu'une personne est bien décédée, qui est l'oracle ?

Au niveau d'AXA Investment Managers, société de gestion pour laquelle je travaille, nous avons des réflexions sur la manière dont la blockchain peut être utilisée dans la chaîne de traitement d'une transaction et comment mettre en place une relation commerciale avec un client du début jusqu'à la fin d'une transaction.

Aujourd'hui, il est intéressant d'observer la façon dont s'organisent les différents acteurs du marché. On voit des consortiums de banques, notamment R3, qui travaillent ensemble sur un projet. On constate que chaque acteur a du mal à partager et à collaborer ensemble. Deux tendances peuvent se dégager à l'avenir. Une tendance où les acteurs d'un même secteur réussissent à se mettre d'accord, par exemple, l'AFG, l'Association Française de Gestion, a publié un document dans lequel elle incite les acteurs du secteur de la gestion à travailler ensemble sur ce sujet. Une autre tendance se dessine où chaque banque développe son propre protocole, sa propre blockchain, dans la perspective d'imposer son standard et de faire payer un ticket d'entrée aux autres.

Simon Polrot : Les consortiums ont peut-être été créés trop tôt. La technologie blockchain est très récente, la première date de 2009, mais on commence à s'y intéresser depuis 2013/2014. Ils se sont d'abord créés avec pour objectif d'observer le phénomène. Mais ils sont très vite passés à l'étape suivante, à savoir développer un protocole de consensus particulier, c'est le cas de R3 avec Corda. Certains membres du consortium ont considéré que cela allait trop vite alors qu'ils étaient loin de comprendre comment cela fonctionne. D'où l'idée que chacun explore de son côté, plutôt que de se lancer dans un projet qu'on ne maîtrise pas. Ainsi chaque banque développe son propre projet, en explorant ce qui existe déjà, en étudiant par exemple la blockchain Bitcoin ou Ethereum, afin de ne pas avoir à tout écrire de zéro. Cela explique en grande partie le foisonnement actuel de projets dans les secteurs de la banque et de l'assurance. Cette technologie n'est pas encore stabilisée. Même les blockchains publiques les plus anciennes comme Bitcoin et Ethereum ont encore du chemin devant elles pour arriver à remplir leurs promesses.

« Même les blockchains publiques les plus anciennes comme Bitcoin et Ethereum ont encore du chemin devant elles pour arriver à remplir leurs promesses. »

Quid de la propriété intellectuelle de la blockchain ?

Louis de Méneval : La propriété intellectuelle sur le protocole représente un enjeu important. Qu'elle devienne un standard ou pas, est-ce une technologie propriétaire ? Des brevets ont déjà été déposés sur le sujet.

Simon Polrot : Il y a eu un brevet qui porte notamment sur la modification du contenu de la blockchain, ce qui a provoqué une levée de bouclier des défenseurs de la technologie. Accenture a déposé un brevet, Bank of America aussi.

Louis de Méneval : Le sujet sur lequel je me penche plus particulièrement est celui de la notion de technologie propriétaire ou non sur la blockchain privée. Si un acteur réussit à imposer son standard, peut-être via un régulateur qui pourrait préconiser une technologie jugée plus sécurisée que d'autres, cela pourrait poser un problème de propriété intellectuelle en matière de réutilisation, de blocage à l'entrée, d'exigence de paiement, etc.

Quelles autres applications sont-elles envisagées ?

Louis de Méneval : Le KYC, know your customer. Cela fait partie de la Compliance. Les institutions financières doivent vérifier qui investit. On évoque beaucoup la blockchain liée à la vérification de l'identité des personnes, application jugée relativement facile à mettre en place. Cela apporterait la preuve que la vérification KYC qui a été faite est inscrite sur la blockchain.

Simon Polrot : C'est un domaine très lié à celui de l'identité numérique ou la gestion de ses données personnelles en ligne. La brique technologique de la blockchain pourrait vraiment apporter quelque chose pour la validation de notre identité numérique et sur son usage. Pour le KYC comme dans les banques, si tout le monde avait une identité validée une fois pour toute, utilisée pour des transactions publiques ou privées, cela serait un grand pas en avant dans l'acquisition d'une véritable identité numérique.

Cette technologie permettrait-elle de certifier une identité ?

Louis de Méneval : Ce serait une base. Le KYC dans les banques est un processus qui prend du temps. Dans le cas d'un ordre d'achat ou de vente ou de création d'un compte, cette vérification peut prendre quelques heures, voire quelques jours. Avec la blockchain, cela pourrait devenir automatique. Dans beaucoup de projets de banques, ce point a été identifié comme un gain de temps. Chez AXA IM, je vois deux types d'expérimentation avec la blockchain : soit avec des banques soit avec des start up qui développent des technologies utiles pour nous.

Nous avons évoqué le concept de smart contracts. Est-ce un contrat ?

Louis de Méneval : On peut en discuter longtemps. Ce serait un contrat qui s'auto-exécuterait si une donnée externe remplissait certaines conditions prédéfinies.

Simon Polrot : Un smart contract, c'est du code, une instruction qui s'exécute, une fois qu'on la déclenche sur la blockchain. Dans ce code, on peut introduire ce qu'on veut. On a assimilé le smart contract à un contrat dans la mesure où on peut exécuter des instructions qui peuvent être des échanges, des obligations.

Comme dans l'assurance dont le paiement de la prime est déclenché si une condition est remplie.

Louis de Méneval : Et bien dans ce cas, l'oracle est la personne qui va certifier que l'événement s'est produit.

Simon Polrot : Dans ce cas, le smart contract est assimilable à un contrat. Aujourd'hui, leur utilisation en est à un stade préliminaire. Il n'existe pas encore de services ouverts au public. Nous voyons des expérimentations sur les blockchains publiques

et privées. Pour les premières, les smart contracts sont vraiment réservés à un public averti. Par exemple, sur Ethereum, il existe une plateforme sur laquelle vous pouvez échanger des actifs virtuels de manière automatisée. Un autre smart contract, InsurEth, est un contrat d'assurance complètement décentralisé sur les retards de vols. C'est un domaine où les données sont disponibles et vérifiables.

Si, par exemple, je souscrits pour 3 Ethers (la crypto-monnaie d'Ethereum), j'en récupère 20 en cas de retard. Le contrat va s'exécuter automatiquement si la condition du retard est remplie, sans qu'un acteur gère le paiement. La vérification de la condition se fait par consultation d'une base de données externe. Ce smart contract existe mais il est encore réservé à un public restreint car c'est techniquement difficile d'y accéder. Mais cela préfigure ce qu'il sera possible de faire à l'avenir.

Et pour les blockchains privées ?

Louis de Méneval : C'est un sujet qui est étudié. On identifie tout ce qui pourrait être proposé sous forme de smart contracts, à partir du moment où on a un processus en chaîne avec différents événements et un paiement au bout. En fonction des domaines, ce n'est pas forcément simple à mettre en place.

A priori pour des applications simples ?

Louis de Méneval : Avec des événements qui impliquent que certaines conditions prédéfinies se remplissent.

Simon Polrot : Les premières applications vont se porter sur des cas très simples.

Cela ne pose-t-il pas de difficultés par rapport à la manifestation de la volonté ? de la formation du consentement ?

Louis de Méneval : Non, si le smart contract a été codé de façon à ce que le consentement soit exprimé et que la condition est remplie. Le contrat n'est pas formé au moment de la construction du smart contract lui-même mais au moment où la condition se réalise, celui de son auto-exécution.

« En termes de responsabilité, le fait de participer à une blockchain induit l'acceptation qu'il n'y ait pas de responsabilité d'un autre acteur. »

Simon Polrot : Peut-on considérer qu'il s'agit d'un vrai contrat qui nécessite une offre et son acceptation, le lien entre l'identité de la personne et celle qui signe, si ces éléments ne sont pas faciles à retrouver tels quels dans la blockchain ? La question reste ouverte. Mais on ne peut pas nier que cela génère des obligations..

Louis de Méneval : Ce qui va être important, ce sont les règles du jeu de chaque blockchain. On peut imaginer que pour participer à une blockchain privée, on ait un contrat à signer qui en définit les modalités. Va se poser la question de la responsabilité liée au développement du code, de l'oracle en cas de problème, etc. Cela risque de générer des discussions entre de futurs participants et l'initiateur d'une blockchain qui n'accepte par exemple aucune responsabilité.

La blockchain a été conçue au départ pour fonctionner de manière autonome, sans désignation d'un responsable. N'y-a-t-il pas une sorte de déresponsabilisation collective ?

Simon Polrot : Ce serait plutôt l'inverse.

Louis de Méneval : Plutôt un univers où tout le monde est responsable et accepte une part de responsabilité. On l'a vu quand est intervenu le problème sur Ethereum.

Simon Polrot : Sur la blockchain publique, qui est libertarienne dans l'esprit, on est responsable de ce qu'on fait, on est présumé comprendre son fonctionnement et si on se trompe, tant pis.

Et quand il y a un bug dans la blockchain, comme ce qui s'est passé avec Ethereum ?

Simon Polrot : Ce qui s'est passé a été considéré comme une « *infraction* » au principe de la blockchain par de nombreuses personnes.

C'était une fraude ou un bug ?

S. P. C'était un hack car le code a été exploité de manière non prévue. Donc il n'avait pas été suffisamment sécurisé.

Pouvez-vous résumer l'incident qui a eu lieu sur Ethereum ?

Simon Polrot : Ethereum est une blockchain publique comme Bitcoin. Sur cette plate-forme a été créée une structure, une sorte de fond d'investissement, avec des smart contracts comportant des règles codées. Par exemple : si j'envoie 100 à cette structure, je reçois 100 parts sociales, avec un droit de vote qui équivaut à 100. Tout le monde pouvait adhérer à cette structure qui n'avait pas d'existence légale. Il s'agissait d'une organisation décentralisée autonome. Cette expérience unique a connu un très vif succès, 150 millions de dollars ont été versés dans ce fond. Or, il y avait une faille informatique qui a permis

à un hackeur de détourner 3 ou 4 millions d'ethers, ce qui correspondait à l'époque à près de 50 millions de dollars. Cet événement a soulevé un grand débat au sein de la communauté Ethereum sur ce qu'il devait être fait. Doit-on considérer que le code fait loi, même s'il y a une faille ? Dans ce cas, on en assume les conséquences et chacun perd ce qu'il avait investi. Chacun est responsable, ce qui correspond à la philosophie de la blockchain. Ou bien estime-t-on qu'on est en présence d'un événement hors norme ? Rappelons qu'à cette époque, beaucoup de gens avaient acheté des ethers sans bien en comprendre le fonctionnement. Je gère un site sur la blockchain Ethereum et j'avais reçu beaucoup de messages de personnes intéressées qui n'y connaissaient rien. Beaucoup d'investisseurs non informés sur un domaine non réglementé se sont lancés dans l'aventure sans être conscients des risques. Suite à ce piratage, il a été décidé de dupliquer la blockchain et d'en créer une nouvelle. Elle est la suite de l'ancienne qu'on abandonne. On ne revient pas en arrière mais on efface les conséquences du hack pour l'avenir. Les fonds ont donc été rendus à tous les investisseurs initiaux. Cette solution a été décidée plus ou moins par consensus. Je dis plus ou moins car tous les processus de consensus étant décentralisés, il est difficile de savoir qui dit quoi. L'impulsion est venue de la fondation Ethereum qui gère le développement.

Les fonds ont été rendus, mais n'avaient-ils pas été dérobés ?

Simon Polrot : On a décidé d'abandonner la blockchain d'origine et d'en créer une identique en tous points, sauf pour le compte du hacker qu'on a vidé. Il y a donc eu intervention. On a cassé l'immutabilité puisqu'on a attaqué le compte d'une personne et on a transféré son contenu dans un contrat de redistribution. Tous ceux qui avaient des parts ont pu récupérer leur investissement initial.

On peut donc dire que la communauté a agi ensemble.

Louis de Méneval : On en revient à la notion de consensus. Il y a eu un accord pour modifier la chaîne et pour effacer les conséquences de ce hacking.

Simon Polrot : La difficulté réside dans le fait qu'il faut un accord de 100 % des participants. En pratique, ce taux n'a pas été atteint. 85 % de ceux qui avaient créé cette blockchain étaient d'accord. Les 15% restant ont continué à fonctionner avec l'ancienne. Maintenant, il existe deux chaînes : Ethereum est la nouvelle chaîne suivie par la majorité et Ethereum Classic est celle de ceux qui restent fidèles aux « *vrais* » principes de la blockchain, comme l'immutabilité, à tout prix.

Pour en revenir à la question de la responsabilité, vous disiez que tout le monde est responsable.

Simon Polrot : Dans la branche classique, chacun est responsable.

Louis de Méneval : On pourrait aussi dire, qu'en termes de responsabilité, le fait de participer à une blockchain induit l'acceptation qu'il n'y ait pas de responsabilité d'un autre acteur. J'imagine que la fondation derrière Ethereum ou Bitcoin ne prend pas de responsabilité en tant que telle sur le sujet.

« Une des clés du développement futur de la blockchain privée passe par la question du rôle des régulateurs et de leur compréhension du sujet. »

Simon Polrot : J'ajouterais que ce n'est pas parce qu'on dit qu'on n'a pas de responsabilité qu'on n'en a pas. La question de la responsabilité d'Ethereum se pose encore aujourd'hui. En fait, cet événement a été révélateur de beaucoup de difficultés non résolues. Est-il possible d'avoir une blockchain vraiment immuable ? Par l'exemple, on a montré qu'une blockchain n'était pas immuable. Cet incident a également permis de prendre conscience des problématiques de sécurité. D'où la nécessité de sécuriser les smart contracts qui comportent des règles beaucoup trop complexes et pas assez vérifiées.

Louis de Méneval : J'imagine qu'en matière de blockchains privées, les régulateurs vont probablement avoir un rôle à jouer.

Une gouvernance doit être mise en place.

Louis de Méneval : Une des clés du développement futur de la blockchain privée passe par la question du rôle des régulateurs et de leur compréhension du sujet. On voit bien qu'aux Etats-Unis, la SEC, la Securities Exchange Commission, s'intéresse de près au sujet : elle a créé un groupe de travail, elle envoie des questionnaires à certains secteurs d'activité sur des sujets comme les agents de transferts. En Europe, on y réfléchit aussi. Nous attendons beaucoup des régulateurs pour instaurer un cadre et permettre le développement de la blockchain. En gros, pour trouver un bon équilibre.

La question de confidentialité ne pose-t-elle pas problème ?

Louis de Méneval : La confidentialité est une question très sensible pour le secteur financier. On en revient à la notion de sécurité sur laquelle le secteur attend

d'être complètement rassuré. On se demande si les systèmes déjà en place sont complètement sécurisés, même s'il est difficile d'imaginer un système sans faille. Je pense que les régulateurs vont s'intéresser notamment aux protocoles de sécurité. Aujourd'hui, le secteur ne va pas se lancer si un régulateur ou une référence n'apporte pas des garanties.

L'immutabilité pose également le problème du droit à l'oubli.

Louis de Méneval : C'est toute la problématique des purges du système de blockchain qui est un registre qui conserve l'information. Effectivement, la réglementation européenne sur la protection des données personnelles veut obliger les systèmes à pouvoir oublier ou être purgés. C'est un vrai problème car l'enregistrement d'une information sur la blockchain n'est pas effaçable.

Simon Polrot : Ce problème ne se pose pas de façon aussi forte qu'on l'imagine car la blockchain est surtout un support d'enregistrement de preuves d'existence d'actifs virtuels et de représentation virtuelle d'un actif réel, plus qu'un support d'information.

Son objet n'est pas d'y enregistrer des informations mais davantage d'être un support qui garantisse la fiabilité d'une information. Tout cela n'est pas forcément lié à une identité, dans le sens où c'est lié à un compte qui ne désigne pas nécessairement une personne mais plutôt un pseudonyme. L'information en tant que telle n'est pas enregistrée dans la blockchain.

Louis de Méneval : Sur le KYC, on peut imaginer qu'il y aura quand même des informations, mais ce sera surtout des garanties que la personne a bien communiqué ses données qui ne circuleront pas nécessairement.

Simon Polrot : Il me semble aussi qu'on aurait davantage des comptes certifiés par des acteurs externes qui valideraient le fait que les informations ont bien été communiquées. La personne concernée va juste faire valider ses documents qui ne figurent pas sur la blockchain. Ce que permettent les technologies cryptographiques : dans une suite de caractères, on a la référence au document, la certification mais pas le document lui-même.

Y-a-t-il une question juridique spécifique à la blockchain ?

Simon Polrot : Je pense à la question du statut des actifs numériques. Qu'est-ce qu'un Bitcoin ? Au niveau juridique, c'est encore très flou. Fiscalement, c'est plus ou moins considéré comme un bien meuble. Mais les définitions sont différentes en fonction des pays. Selon une jurisprudence européenne, la vente de Bitcoins contre des euros est assimilable à une transaction financière et donc exonérée de TVA. C'est donc un meuble financier, un domaine qui n'existe pas. De façon générale, le statut d'une inscription dans une blockchain n'est pas encore clair.

Est-il encore trop tôt pour réguler, encadrer ?

Louis de Méneval : Oui et non. Il est important de lancer les chantiers de réflexion. Sur ces sujets, il ne faut pas non plus se retrouver dans un « *corner* » quant à l'obligation de choisir une seule solution blockchain. Par exemple, si une plateforme de blockchain est mise en place et semble incontournable, il faut bien en comprendre les conditions de participation, les responsabilités des différents acteurs.

Simon Polrot : Il y a deux pièges à éviter. D'une part, l'absence de réglementation est problématique car les acteurs se retrouvent face à un vide juridique qui les empêche d'avancer. D'autre part, trop de réglementation ou un encadrement mal pensé peut bloquer les usages et l'innovation. Ce dernier cas s'est produit avec la signature électronique pour laquelle on avait prévu un cadre trop restrictif, trop compliqué, trop coûteux dont personne se sert.

« De façon générale, le statut juridique d'une inscription dans une blockchain n'est pas encore clair. »

Pour le numérique, on exige trop de sécurité alors qu'on n'en demande pas autant pour le papier, comme pour la signature manuscrite. Il ne faut pas commettre cette erreur avec la blockchain en imposant un cadre trop précis. Il faut se garder d'imposer des garanties inatteignables.

Propos recueillis par Sylvie ROZENFELD