



La blockchain, terra incognita juridique ?

publié le **13/06/2016**, vu **8027 fois**, Auteur : [Maître Matthieu Pacaud](#)

La blockchain va provoquer l'apparition de nouveaux modèles économiques, qui devront être encadrés juridiquement. Quelques exemples d'applications à réguler.

Au détour d'un achat sur internet, vous avez sans doute déjà remarqué une possibilité de régler le magasin en ligne en Bitcoin. Le nom vous est certainement familier, mais quid de sa technologie sous-jacente, la blockchain ?

Le fonctionnement de ces outils reste encore nébuleux pour la majorité du public. Leurs aspects juridiques le sont encore plus, y compris pour les praticiens.

Le Bitcoin est un usage intéressant de ce procédé, mais son application reste limitée. Les usages envisageables ne sont en réalité limités que par l'imagination : smart contracts, gestion de sinistre par les assureurs, collecte des impôts à la source, authentification, vote, dossiers médicaux, internet des objets...

Ce nouveau système, qui se veut révolutionnaire, pourrait avoir un impact sociétal au moins équivalent à l'avènement du web collaboratif il y a une dizaine d'années. Comme tout nouvel outil, celui-ci ne va pas sans soulever de nombreuses problématiques juridiques quant à sa nature et régulation (gouvernance, valeur probatoire, confidentialité et anonymat des échanges, opacité liée à sa décentralisation, problématiques de conflit de droit...).

Le fonctionnement technique de la blockchain

La blockchain est une base de données chronologique de transactions, distribuée et cryptée, dont l'intégrité est assurée par chaque utilisateur, qui dispose de l'intégralité des opérations réalisées depuis sa création. Le fonctionnement est, dans sa logique, assez proche d'un registre de comptabilité : la blockchain a vocation à enregistrer des événements, et à les rendre inaltérables.

Il est en conséquence possible pour toute personne utilisant la blockchain d'en vérifier l'intégrité.

Chaque transaction est entièrement cryptée, et consiste en un bloc qui s'inscrit sur un registre des échanges. Chaque nouveau bloc est vérifié par les utilisateurs, qui participent ainsi à la sécurisation des échanges. En effet, seuls les blocs validés par plusieurs utilisateurs sont considérés comme sécurisés. Une fois validé, le bloc est synchronisé sur l'intégralité de la blockchain et ne peut être effacé.

La blockchain est publique lorsque n'importe qui peut en devenir utilisateur, et privée si elle est limitée à des utilisateurs spécifiques.

La blockchain privée est particulièrement intéressante dans le cadre des assurances, des banques, et d'une manière générale, à l'intérieur d'un réseau, dès lors qu'il est ainsi possible d'être certain de l'identité de tous les utilisateurs et de limiter les risques liés à l'anonymat.

Elle participe à un mouvement général de sécurisation des échanges, dont l'utilité est indéniable avec la montée en puissance du cloud et de l'internet of things (internet des objets).

Grâce à la blockchain, les utilisateurs n'ont plus besoin de connaître leurs interlocuteurs dès lors que la blockchain s'assure automatiquement de la réalité des informations fournies (par exemple, en matière financière, la transaction sera impossible si les conditions ne sont pas remplies – les fonds suffisants sur le compte du débiteur). La confiance n'est ainsi plus liée à l'identité et la réputation d'une entité (qu'il s'agisse d'une entreprise ou d'une personne physique), mais plutôt à l'ouverture du code informatique. Il s'agit d'un changement total de paradigme juridique.

Toute base de donnée peut potentiellement être sécurisée au moyen de la blockchain.

Quelles sont les questions juridiques soulevées par la blockchain ?

Il est pour le moment particulièrement difficile de fournir une définition juridique de la blockchain, et d'entrevoir l'étendue de son impact.

Le législateur a toutefois tenté de fournir une première ébauche de définition, qui peut s'appliquer à la blockchain, dans une [ordonnance sur les bons de caisse du 28 avril dernier](#). La blockchain n'est pas mentionnée in extenso mais le rapport initial de l'ordonnance utilisait ce terme. Elle est définie de la manière suivante :

« un dispositif d'enregistrement électronique partagé permettant l'authentification d'opérations ».

Cette définition reste assez vague mais les notions essentielles de partage et d'authentification d'opérations paraissent pertinentes. Ces notions nous semblent suffisamment générales pour pouvoir être réutilisées pour réguler les futures utilisations de la blockchain.

Des [discussions ont par ailleurs commencé à l'Assemblée Nationale](#) pour tenter d'élargir cette définition et permettre au gouvernement de légiférer sur le sujet par voie d'ordonnance. Cette fois, la notion de blockchain a été utilisée.

La régulation est toutefois opposée à l'esprit de la blockchain, qui se veut totalement décentralisée et à l'abri de tout contrôle externe. Un idéal qui se rapproche de l'objectif d'internet à l'origine : un outil hors du contrôle des états, sans gouvernance.

L'exemple du Bitcoin est frappant à ce titre : la monnaie est un outil régalien, entièrement contrôlé par les états. A l'inverse, la monnaie numérique existe hors de tout contrôle étatique et est un outil uniquement influencé par le marché.

Il sera donc nécessaire de trouver un moyen de rapprocher ces philosophies opposées.

Il est également possible de rapprocher les possibilités de certification apportées par la blockchain de la notion de tiers de confiance. En effet, le processus est identique, mais totalement automatisé. La blockchain pourrait donc potentiellement entrer dans le cadre de notions juridiques existantes. La seule différence est qu'il est impossible d'engager la responsabilité du certificateur.

Le caractère anonyme de la blockchain est en effet un véritable problème : qui est responsable en cas de préjudice causé à un utilisateur ? Les développeurs ? L'utilisateur ayant causé le préjudice ? Le système étant opaque, il est impossible de les identifier, sauf en cas d'utilisation d'une blockchain privée. Cette dernière est probablement également une solution aux problématiques de gouvernance mais ne sera pas adaptée à toutes les situations.

Quels sont les applications pratiques de la blockchain et comment les encadrer juridiquement ?

Qu'il s'agisse de prouver ou d'authentifier une transaction, la technologie de la blockchain permet d'écartier toute possibilité d'erreur et de falsification.

En l'état actuel, il convient de noter que les inscriptions sur la blockchain ne disposent pas de valeur légale. Elles pourraient avoir la valeur d'un écrit ou d'un acte authentique, mais rien n'a été consacré par le législateur pour le moment.

D'une manière générale, les transactions ayant vocation à s'intégrer dans une chaîne en tireront un avantage dès lors qu'elles pourront être automatisées de manière sécurisée, ce qui assure le contrôle de la chaîne et l'impossibilité de fraude.

[Certains ont déjà envisagé des services d'authentification d'œuvres d'art](#), ce qui est pertinent dès lors que le droit d'auteur fonctionne sans dépôt. Il est ainsi fréquent de voir devant les tribunaux des contentieux portant sur l'identité du créateur. Il en va de même pour le contrôle des reproductions : seuls ceux qui ont le droit de la reproduire le pourront.

L'usage en tant que smart contracts (contrats intelligents) est également particulièrement intrigant. L'idée est la suivante : les parties peuvent confirmer qu'un événement figurant au contrat a eu lieu (comme un événement déclencheur de paiement – dans le domaine des contrats informatiques, une VABF par exemple) ou qu'une condition est remplie (comme l'obtention d'un prêt pour une acquisition immobilière), ce qui va permettre de réaliser un second événement de manière automatique.

L'intérêt du smart contract est de fluidifier la gestion contractuelle : le lien logique entre les différentes clauses est effectué sans intervention humaine, et de manière entièrement sécurisée. Le système lui-même garantit l'exécution des clauses du contrat. Des start-ups comme Ethereum se sont d'ores et déjà placées sur ce marché et fournissent un langage de programmation de smart contracts intégré à la blockchain.

En outre, en matière de contrats internationaux, les difficultés d'interprétation de clauses liées au droit local seraient limitées. En effet, les conditions seraient interprétées de manière automatique sur la base du langage informatique. De là à y voir une création d'un droit nouveau (l'expression « *code is law* » a même été consacrée par un juriste éminent américain, Lawrence Lessig) applicable à un nouveau territoire, il n'y a qu'un pas. Si nouveau langage du droit il y a, il conviendra toutefois de créer une pierre de Rosette adaptée.

Les applications en matière d'impôts, de suivi bancaire et d'assurances sont également conséquentes. Un impôt comme la taxe sur la valeur ajoutée serait particulièrement adapté à cette technologie : la collecte de la TVA par une partie entraîne automatiquement une déduction chez une autre partie. Le fait d'intégrer ces calculs à la blockchain, au moyen de logiciels de comptabilité par exemple, pourrait avoir pour effet d'anéantir la fraude carrousel. Il en va de même pour la fraude aux assurances.

On peut même imaginer un système de vote, où chaque citoyen représente un nœud et sécurise les urnes numériques. Un bon moyen d'empêcher le bourrage des urnes, en particulier dans les pays peu développés, le coût d'un tel système étant a priori modique.

Ces applications ne sont qu'une infime partie de ce que le marché va inventer pour profiter de ce nouveau système. Nul doute que le droit va devoir s'adapter rapidement.

Les résistances ont déjà commencé, mais l'exemple de l'uberisation et de la généralisation du digital montre qu'il est préférable d'accompagner le mouvement plutôt que d'y mettre un frein et de se retrouver dépassé.

Matthieu PACAUD

Avocat au Barreau de Paris

<http://www.pacaud-avocat.fr>

?