672

La blockchain ou la confiance dans une technologie

La blockchain est une technologie susceptible de révolutionner de nombreux usages économiques et sociaux avec des applications variées (banques, assurances, gouvernements, …). Elle repose sur les principes d'architecture décentralisée avec un registre numérique partagé, sécurisé grâce aux procédés cryptographiques et d'échanges *peer-to-peer* (P2P). Dépendante des règles de droit des différents systèmes juridiques, la blockchain suscite de multiples interrogations juridiques, spécialement quant à la gouvernance, la régulation du système, la preuve, l'imputabilité des transactions et les responsabilités.

Éric A. Caprioli, avocat à la Cour de Paris, docteur en droit, membre de la délégation française aux Nations Unies, vice-président de la Fédération des tiers de confiance (FNTC) et du Club des experts de la sécurité de l'information et du numérique (CESIN)

Qu'est-ce que la blockchain ?

La Blockchain (ou chaîne de blocs) est une technologie de stockage et de transmission d'informations et qui fonctionne sans administrateur central qui contrôle l'ensemble. Elle vise à faire communiquer des serveurs entre eux sans pour autant utiliser un serveur central, les serveurs étant choisis de façon aléatoire en fonction de leurs capacités de calcul ; les « mineurs » valident les blocks contre rémunération par ex. *bitcoin*.

Pour les échanges, cette technologie se fonde sur l'utilisation de clés cryptographiques asymétriques et d'algorithmes de hachage. Ces procédés permettent d'assurer l'intégrité et l'authentification des transactions. En effet, c'est avec la clé publique correspondant à la clé privée ayant servi à signer la transaction que l'on vérifie la fiabilité de l'opération. Ainsi, chaque utilisateur peut vérifier la validité des transactions sur un registre numérique public, anonyme et sécurisé qui contient une base de données distribuée et hébergé dans un réseau de relais informatique sécurisés (un relais est un *full-node*). L'historique de tous les échanges est conservé dans cette base et partagé par les utilisateurs. La traçabilité des transactions est assurée par des procédés d'horodatage électronique. Chaque bloc contenant un ensemble de transactions est lié à un autre bloc ; chaque transaction est vérifiée de façon chronologique puis elle est intégrée dans la version N+1 du bloc suivant.

On doit distinguer LA blockchain qui correspond à la technologie (ou un protocole) et UNE blockchain pour une application spécifique liée à des usages.

La blockchain se fonde sur des logiciels *open source*, auditables, d'où sa transparence. Cependant, comme la sécurité du système repose sur des moyens cryptographiques, il est impératif de disposer de moyens d'un niveau de fiabilité adéquat. À défaut, la sécurité d'une blockchain pourrait être remise en cause.

En outre, la blockchain contient plusieurs *smart contracts*, à savoir des programmes interagissant entre eux, accessibles et auditables par toutes les parties autorisées, dont l'exécution est contrôlée et vérifiable, conçus pour exécuter les termes d'un contrat de façon automatique lorsque certaines conditions sont réunies.

Quelle différence entre bitcoin et blockchain ?

Il est important de ne pas confondre blockchain et bitcoin. La première blockchain est apparue avec la monnaie virtuelle ou crypto-monnaie appelée Bitcoin. Elle a été créée en 2009 sous le pseudonyme « Satoshi Nakamoto ». Même si la blockchain et le bitcoin sont nés ensemble, la plupart des acteurs privés et publics envisagent d'utiliser la blockchain pour d'autres usages que celui d'une crypto-monnaie. En réalité, les bitcoins utilisent la technologie blockchain et à ce titre, on peut dire qu'ils sont une blockchain. La Blockchain constitue l'architecture sous-jacente du Bitcoin. Le système est identique à la blockchain : échanges P2P, hachage (SHA-256 et RIPEMD-160) et signatures numériques (cryptographie à courbes elliptiques, ECDSA), enregistrement des transactions dans un registre public, vérifications des transactions par des nœuds du réseau. Pour une transaction, il faut envoyer un certain montant à partir d'une adresse bitcoin vers une autre adresse. Pour ce faire, les transactions réalisées s'effectuent de façon quasi-anonyme sous pseudonyme, de sorte qu'il sera très difficile d'établir le lien entre une opération réalisée en bitcoins et la personne qui la génère puisque la blockchain du bitcoin n'enregistre pas les auteurs, mais seulement les transactions. Sa valeur en mai 2016 était d'environ 400 euros par unité (plus de 6 milliards d'euros au total). Alors que les bitcoins sont de plus en plus acceptés par les entreprises, il n'en demeure pas moins que leur réputation est sulfureuse. En effet, la plupart des transactions réalisées sur le *dark web* : achats d'armes, drogues, organes et trafics en tous genres ou encore opérations illicites comme le *ransomware* sont payées à l'aide de bitcoins ou d'autres crypto-monnaies.

Un exemple de création d'une Blockchain ?

Fonctionnant sur la base de la blockchain Ethereum, indépendante de bitcoin, une organisation autonome décentralisée (*the DAO*, http://daohub.org) utilise un programme informatique qui fixe et publie dans une blockchain les règles de gouvernance de l'organisation. Cette blockchain collecte des fonds (*crowfunding*) afin de financer des projets (réalisés par des prestataires) en relation avec l'internet des objets (IOT ou une voiture électrique autonome). La décision de financement s'opère en fonction du vote des détenteurs de jetons de la DAO (les investisseurs).

Existent-ils différents types de blockchains ?

Il existe trois types de blockchains : publique, privée et hybride. Or, les tenants de l'orthodoxie blockchain pensent que cette technologie ne peut être privatisée puisqu'elle a été conçue comme étant ouverte, gratuite et partagée.

Les blockchains publiques (ex : bitcoin) sont ouvertes à tout le monde et gratuitement, alors que dans les blockchains privées l'accès et l'utilisation sont réservés à certains acteurs ; la validation des transactions est réalisée par un nombre limité de nœuds, lesquels permettent l'accès aux informations.

Lorsque la blockchain est hybride, on se trouve dans une situation où elle est sous le contrôle d'un ensemble d'organisations au sein desquelles le droit d'accès peut être ouvert à tous ou limité à certains utilisateurs. La création et la vérification des transactions peuvent s'effectuer avec une API dédiée.

Les règles de gouvernance de chaque blockchain déterminent leurs usages et les limites d'utilisation.

Quelles sont ses applications, et pour quels usages ?

Selon de nombreux spécialistes, on serait en présence d'une

technologie disruptive (de rupture). Elle favoriserait l'innovation dans de nombreuses activités, dans la sphère privée (banque, finance, assurance, art ou santé) et dans la sphère publique (ex : collecte d'impôts et taxes, vote, registre des titres fonciers, état civil.- V. rapport du UK Government Chief Scientific Adviser, déc. 2015 : https://fr.scribd.com/doc/295987915/Distributed-Ledger-Technology-beyond-block-chain).

On peut distinguer trois catégories d'usages des blockchains : des applications de registre pour assurer la traçabilité de biens et des actifs ; des applications de transferts d'actifs (monnaie, titres, actions, …) ; des applications de contrats intelligents (*smart contracts*) qui exécutent les conditions contractuelles automatiquement.

Exemple d'application financière : BNP Paribas securities services a signé un partenariat avec la plate-forme de *crowdfunding SmartAngels*. Son objectif est de permettre aux entreprises non cotées d'émettre des titres sur le marché primaire en s'appuyant sur la blockchain.

Exemple d'application administrative : le Honduras a en projet d'utiliser le registre décentralisé de la blockchain pour y inscrire l'achat et la vente de terrains dans le pays ; ces transactions devraient être enregistrées courant 2016 sur ce registre numérique, partagé en réseau. L'un des obstacles à résoudre a été d'identifier chaque membre de la communauté du réseau.

Quelles sont les règles de droit applicables ?

Lorsqu'on parle de blockchain, de nombreuses questions juridiques se posent, on pense ici notamment à la gouvernance, à la régulation et à la preuve.

Gouvernance : l'objectif est de créer une organisation avec une gestion à la fois décentralisée et collaborative, encadrée juridiquement par des règles de fonctionnement inscrites dans la blockchain (pouvoirs de décision, de modification des règles, accès, dépôts et vérifications des transactions, sécurité, garanties, preuves, contrats, …). Pour conserver une gouvernance décentralisée, le système doit être adapté à la technologie d'où l'apparition de blockchains privées. Les organisations sont gérées par les logiciels, sans intervention humaine.

En terme de **régulation**, la blockchain est souvent vue comme une technologie capable d'échapper aux règles de droit en vigueur et à la domination des États. Encore plus que sur Internet (V. la déclaration d'indépendance du cyberespace de John Perry Barlow), le code fait désormais effet de loi (*Code is law* selon L. Lessig, http://harvardmagazine.com/2000/01/code-is-law-htm). Le droit commun pourrait faire obstacle au développement de cette technologie. Avec l'autorégulation, on peut créer de nouveaux cadres contractuels. Mais la question centrale demeure : le code informatique est-il plus apte à réguler que le droit ? Ou encore, faut-il un nouveau cadre juridique ? À vrai dire force est de constater que l'on applique le droit commun et cela même si la blockchain possède des spécificités. Avec la blockchain la difficulté consiste à concilier toutes les règles juridiques existantes. Cette question pourrait dépendre de pratiques d'autorégulation du réseau d'un type de blockchain ou au contraire de la réglementation étatique. Par ex., l'ordonnance n° 2016-520 du 28 avril 2016 relative aux bons de caisse énonce que seuls des « *établissements de crédit ou des personnes physiques et sociétés qui exercent en qualité de commerçant et ont établi le bilan de leur troisième exercice commercial* » (*CMF, art. L. 223-2*) peuvent émettre des minibons. Ce texte définit ainsi la blockchain : « *un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations* ».

Sur le plan **probatoire**, il est souvent fait état de preuves techniques :

Preuve de travail : méthode exigeant de la puissance de calcul de chaque Mineur pour résoudre un problème plus ou moins difficile ;

Preuve de détention : méthode adaptant la difficulté du travail en fonction de chacun des Mineurs.

Mais finalement, la question n'est pas purement technique et il conviendra de vérifier la preuve juridique d'un bloc de blockchain et des transactions qu'il contient en vertu du respect des exigences (identification de l'auteur, manifestation de volonté, intégrité) applicables aux actes juridiques à l'aune notamment du Règlement européen eIDAS et du Code civil.

> « Avec la blockchain, la confiance se fonde exclusivement sur la technologie. »

Quelle responsabilité de l'organisation en cas de vol ou de fraude ?

Concernant la responsabilité, on doit en effet s'interroger sur certains points. On peut imaginer l'hypothèse où une organisation serait utilisée à des fins illicites ? En cas de préjudice, vers qui va-t-on se retourner pour les faits d'une organisation qui n'a pas d'administrateur ? De même, si l'on parvient à identifier les responsables, cela ne permettrait pas de bloquer les opérations de ces organisations puisque celles-ci agissent de façon complètement autonome sur la blockchain. Est-ce que l'éditeur de logiciel peut voir sa responsabilité engagée ? La problématique est complexe étant donné que les applications sont en général construites sur la base de logiciels libres avec des développeurs souvent anonymes. Comment mettre en cause la responsabilité du créateur d'applications, fut-il identifié ? Devant quel tribunal agir pour la mise en jeu de la responsabilité et ensuite pour l'exécution de la décision ? Les réponses pourront être trouvées au cas par cas, en fonction des éléments de l'espèce (ex : règles de la blockchain).

Blockchain et confiance vont-ils de pair ?

Selon ses promoteurs, la blockchain permet d'éliminer la question de la confiance séculaire fondée sur des intermédiaires. L'idée sous-jacente consiste à penser que les tiers de confiance actuels, intermédiaires fonctionnant en mode centralisé (ex : banques ou notaires) pourraient être remplacés par des blockchains fondées sur des systèmes distribués et partagés par les utilisateurs. Avec la blockchain, la confiance se fonde exclusivement sur la technologie. En définitive, on peut estimer que la confiance ne peut exister sans garantie et si la mise en jeu des responsabilités associées aux actes des utilisateurs (anonymes) et des organisations en cause reste floue. En matière de blockchain, bien maladroit celui qui fait fi du droit ! ■

Pour aller plus loin

- M. Bali, Les crypto-monnaies, une application des blockchains technologies à la monnaie : RD bancaire et fin. 2016, comm. 8
- EBA, *Opinion on virtual currencies*, 4 juill. 2014 : http://www.eba.europa.eu
- E. A. Caprioli, Ordonnance du 28 avril 2016 relative aux bons de caisse : Comm. com. électr. 2016, comm. 58
- Plateforme de transformation digitale, Comprendre la Blockchain, Livre blanc, janv. 2016.