Les blockchains et le droit

Boris Barraud

Les blockchains et le droit

Boris Barraud

Docteur en droit, Laboratoire interdisciplinaire droit, médias et mutations sociales (LID2MS), Université d'Aix-Marseille

Revue Lamy droit de l'immatériel (Wolters Kluwer), n° 147, avr. 2018, p. 48-62

Une blockchain est une base de données décentralisée et sans intermédiaire qui permet d'automatiser une transaction, de l'authentifier et de l'horodater, tout en garantissant son immuabilité et son inviolabilité. Elle peut aussi assurer la confidentialité des données grâce au cryptage. Cette technologie, que certains imaginent aussi révolutionnaire que l'internet — elle serait aux transferts de valeurs ce que l'internet a été aux échanges d'informations —, interroge le droit à plus d'un titre. Elle pourrait contribuer à remplacer ou, du moins, renouveller le droit, notamment en lui permettant de se passer d'État et, plus généralement, de tiers de confiance. Les blockchains possèdent un potentiel disruptif à l'égard de la production et de la pratique du droit dont il faut prendre conscience afin de ne pas se laisser surprendre par les bouleversements qu'elles provoquent. Elles remettent en cause des modèles de génération et de garantie de la confiance qui existent depuis des siècles : droit, État, banques, notaires etc. Les blockchains sont le meilleur témoin du grand mouvement de technologisation des sociétés : les hommes s'en remettent de moins en moins à autrui et de plus en plus à la technologie. Et cela concernerait y compris le monde juridique. Le futur que les blockchains rendent possible est un monde plus horizontal. Le nouveau droit qu'elles forgent serait par conséquent un droit plus horizontal, se passant d'organes de tutelle et de contrôle.

La technologie des blockchains est l'objet d'un intérêt fort et croissant de la part des banquiers et des assureurs. Mais les systèmes bancaires et assurantiels ne sont pas les seuls touchés et les systèmes juridiques et politiques pourraient être eux-aussi profondément remodelés par les « chaînes de blocs ». C'est pourquoi les pouvoirs publics et les juristes, qu'ils soient notaires, huissiers de justice, avocats, juristes d'entreprise, mais aussi enseignants-chercheurs ou étudiants, sont invités à consacrer un peu de leur temps à ce qui pourrait constituer, pour une part au moins, l'avenir du droit. Leurs rôles et leurs travaux respectifs sont susceptibles d'évoluer assez radicalement. Notamment, ils devraient être en mesure de proposer une nouvelle expertise : une expertise technologique, en matière de code informatique. L'heure des « juristes-codeurs » pourrait bientôt sonner.

Les enjeux liés à la relation entre blockchains et droit sont majeurs, en termes de blockchains saisies par le droit, mais aussi et surtout en termes de droit saisi par les blockchains. En particulier, la gouvernance des blockchains et la force juridique des opérations réalisées au moyen de cette

technologie posent question ; et les réponses commencent seulement à se stabiliser. Les blockchains obligent à réinventer les métiers de légiste et de juriste, tandis que les codeurs sont appelés à faire du droit — plus ou moins consciemment. Dans un futur qu'il n'est pas nécessaire d'imaginer lointain, les *legal start-up* spécialisées dans la technologie blockchain pourraient produire et/ou appliquer beaucoup de normes, complétant ou concurrençant le droit « classique ». Les professionnels du droit devraient alors collaborer avec les développeurs afin de créer les outils juridiques de demain.

Profitant de l'essor des nouvelles technologies numériques, les blockchains seraient à l'origine d'un phénomène de remplacement rapide d'un modèle par un autre ; et cela impacterait jusqu'au droit et à l'État. Elles pourraient être l'élément déterminant dans le processus menant du droit moderne au droit postmoderne et de l'État moderne à l'État postmoderne — à moins qu'il faille davantage y voir la source d'un paradroit, une forme de régulation sans droit et sans État. Au-delà, l'économie, la finance et la structure et le fonctionnement de la société dans son ensemble pourraient être profondément changés, avec la grande mutation des mécanismes de transaction et de certification. Serait notamment remise en cause l'utilité des plateformes jouant un rôle d'intermédiation.

Ces promesses s'accompagnent forcément de défis et de menaces, qui touchent y compris le droit et qui l'obligent à réagir. Les États pourraient être lourdement impactés, interrogés dans nombre de leurs missions dites « régaliennes », qu'ils ne seraient plus seuls en mesure d'accomplir. Le rêve libertarien et crypto-anarchiste serait proche de devenir réalité : en profitant des opportunités offertes par les nouvelles technologies de communication, se passer d'État — si ce n'est pour assurer par la force le respect des conventions privées.

D'un point de vue historique, les blockchains sont intimement liées au bitcoin, première forme de monnaie électronique privée. En 2008, cette technologie a été inventée en même temps que le bitcoin par un (ou des) inconnu(s) empruntant le pseudonyme de Satoshi Nakamoto, dans un contexte qui n'est pas anodin : celui de la plus grande crise financière que le monde ait connu depuis 1929, une crise suscitant la défiance envers les habituels tiers de confiance que sont les États ou les banques. Depuis, d'autres acteurs l'ont utilisée afin de développer de nouvelles applications, au-delà de la création de cryptomonnaies.

Reste que, si « blockchain » est un des grands « buzzword » du moment, définir une blockchain n'est pas chose aisée. Or, pour mesurer l'impact éventuel de cette technologie sur les mondes politique et juridique, il est important d'en comprendre la mécanique, le fonctionnement, ainsi que les implications et les conséquences concrètes. Le danger dont il faut se prémunir est de brandir les blockchains telle la révolution ultime sans maîtriser les tenants et les aboutissants de cette révolution supposée. C'est pourquoi il convient, avant toute autre chose, de préciser aussi finement que possible ce qu'est une chaîne de blocs.

Concrètement, il existe diverses blockchains particulières, parfois très différentes les unes des autres[1]. La blockchain bitcoin en est une, par exemple. Pour recourir à une métaphore assez simple, une blockchain est un grand livre comptable ouvert et infalsifiable, que chacun peut consulter et où l'on peut écrire sous le contrôle de tous, sachant que ce qui est écrit ne peut pas être effacé par la suite. Une page du livre correspond à un bloc, tandis que sa reliure est la chaîne. Le terme « blockchain » provient du fait que les transactions enregistrées sont groupées en blocs, tous les blocs étant liés entre eux par une signature numérique permettant de construire une chaîne de blocs d'informations. Une blockchain garantit de la sorte l'horodatage, l'immutabilité et l'intégrité du registre, car tout ajout, retrait ou modification d'une transaction invalide l'empreinte cryptographique de la chaîne tout entière.

[1] On peut parler « des blockchains » en général ou de « la blockchain » afin de désigner la technologie blockchain.

Une blockchain associe de manière originale deux technologies déjà connues. La première consiste en la sécurisation de blocs de données par cryptages successifs rendant impossible la falsification de l'un de ces blocs, tous étant comme « encastrés », avec leurs dates, dans une série d'autres blocs. La seconde est l'exploitation d'un réseau distribué pour exécuter une application informatique. En d'autres termes, une blockchain est une base de données, un registre qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Et cette base de données est distribuée, transparente, décentralisée et sécurisée. En informatique, une base de données distribuée est traitée par un réseau d'ordinateurs interconnectés dont chacun stocke les données en cause. Ensuite, on enchaîne les blocs d'informations les uns aux autres grâce à des hashs, des empreintes numériques uniques pour chacun[2]. L'intérêt du hashage est de ne s'appliquer que dans un sens : il n'est pas possible, à partir d'un hash donné, de remonter au contenu d'origine ; en revanche, il suffit de hasher à nouveau ce contenu pour vérifier que les hashs sont identiques et donc qu'aucune modification du contenu en question n'a été opérée. La blockchain est ainsi protégée contre les risques de falsification par les nœuds de stockage, tout le monde pouvant vérifier la validité d'une information en consultant la base de données.

Et sa grande caractéristique est bien de fonctionner sans organe central de contrôle, sans intermédiaire, sans serveur principal. L'inaltérabilité est garantie par un réseau de pairs indépendants. Chaque ordinateur possédant une copie de la blockchain constitue un « nœud » s'assurant en permanence de son intégrité. C'est pourquoi la technologie blockchain est extrêmement solide : ce n'est pas un tiers de confiance éventuellement corruptible ou partial qui valide les opérations. Chaque bloc comporte une marque numérique qui l'associe au bloc précédent et le certifie ; et cette opération de marquage est assurée par des utilisateurs volontaires, appelés « mineurs »[3]. Ces derniers mettent à disposition la puissance de calcul de leurs ordinateurs pour administrer la blockchain contre rémunération — ce qui a donné naissance au phénomène du « cryptojacking », consistant à introduire un script qui, lors de l'utilisation d'un service en ligne, déclenche des calculs de « minage », monopolisant ainsi le processeur de l'utilisateur sans son consentement[4].

Pour porter atteinte à une blockchain, il faudrait parvenir à corrompre 51 % des « mineurs » afin qu'ils en viennent à valider collectivement une information erronée, chose quasi-impossible étant donnée leur disparité — ils se trouvent généralement aux quatre coins du monde et ne se connaissent pas entre eux. Et plus une blockchain comporte de nœuds, plus le risque d'être corrompue devient négligeable, si bien que la sécurité des blockchains les plus importantes est extrêmement élevée.

Il importe, en outre, de se prémunir contre d'éventuelles usurpations d'identité — d'autant plus que de nombreux utilisateurs des blockchains opèrent derrière des pseudonymes, notamment dans le système bitcoin. Pour ce faire, on recourt à une cryptographie dite « asymétrique » : deux clés différentes (une privée et une publique) sont nécessaires afin de réaliser une opération sur une

[2] Le hash est une fonction mathématique qui transforme n'importe quel contenu en un nombre hexadécimal.

[3] À chaque transaction, tous les ordinateurs vérifient sa validité en tentant de résoudre une énigme cryptomathématique très complexe et qui constitue une forme de péage qu'on appelle la « preuve de travail ». Cela permet de s'assurer que celui qui intervient sur la blockchain est un ordinateur et non une personne humaine. Une fois l'énigme résolue — ce qui peut prendre une dizaine de minutes —, l'information est inscrite dans un bloc. Et quand ce bloc est rempli, il est horodaté et on lui attribue une empreinte numérique qui est reprise par le bloc suivant, si bien que l'un et l'autre se retrouvent enchaînés de manière irrévocable. Une fois ajouté à la chaîne, un bloc ne peut plus être ni modifié ni supprimé, ce qui garantit l'authenticité et la sécurité du réseau. Autrement dit, une partie du bloc précédent est intégrée dans le nouveau bloc, de telle sorte que si un bloc antérieur se trouvait modifié, toute la blockchain s'écroulerait. Plus le temps passe, plus une blockchain se renforce et devient inviolable.

[4] La puissance de calcul libre des ordinateurs est mise à profit par ces scripts afin de « miner » des transactions, au bénéfice non pas de l'utilisateur mais du fournisseur de service. C'est ainsi que plusieurs services en ligne ont vu dans le « minage » un nouveau moyen de se rémunérer grâce à leurs visiteurs. Il s'agit pour eux d'une alternative à la publicité envahissante.

blockchain. La clé publique est comme une boîte aux lettres et la clé privée, connue seulement de son utilisateur, est comme une signature ou un mot de passe — très complexe puisque comprenant une soixantaine de caractères alphanumériques. L'une et l'autre sont indispensables afin de réaliser des transactions.

Par ailleurs, doivent être distinguées les blockchains publiques et les blockchains privées. Les blockchains publiques sont ouvertes à tous ; n'importe quel utilisateur peut enregistrer des opérations sur les chaînes de blocs ou participer à la validation des opérations. À l'inverse, l'accès aux blockchains privées et leur utilisation sont restreints à certains acteurs précisément identifiés et sont sous le contrôle d'un organisme particulier qui maîtrise le processus d'approbation. Avec la chaîne de blocs privée, une seule et même organisation peut limiter les autorisations d'entrée, de lecture et d'écriture, de telle sorte qu'un tiers de confiance apparaît et que la décentralisation est très imparfaite, ce qui, pour beaucoup de spécialistes, va à l'encontre de l'esprit originel de la technologie blockchain — « blockchain privée » serait un oxymore. Une blockchain privée peut aussi reposer sur des procédés de cooptation ou de consortium, les contrôles étant alors effectués par un ensemble présélectionné de nœuds.

Toujours est-il que, malgré ses limites certaines[5], beaucoup d'observateurs voient dans la technologie blockchain une révolution comparable à celle de l'internet[6]. Blockchain serait au transfert de valeurs ce qu'internet est à l'échange d'informations, une invention aussi importante que celle du protocole TCP/IP, au potentiel disruptif analogue. En 2030 ou 2040, peut-être fera-t-on ses courses sur des blockchains, paiera-t-on avec des cryptomonnaies, s'acquittera-t-on des impôts et taxes au moyen de blockchains, contractera-t-on un prêt sur une blockchain, signera-t-on son contrat de travail ou de bail grâce à une blockchain, enregistrera-t-on ses travaux et ses diplômes dans des blockchains, se mariera-t-on dans les blockchains etc.

Pour l'heure, la technologie blockchain souffre toutefois de la complexité de son protocole, qui la rend peu accessible. Elle en serait au même niveau que le protocole TCP/IP avant l'invention du World Wide Web, au temps d'Arpanet, ancêtre de l'internet actuel. À bien des égards, la situation actuelle ressemble à celle de l'internet dans les années 1980 — les attentes, parfois exagérées, côtoient le scepticisme, parfois également exagéré, mais le potentiel de la technologie est certain. Le développement des usages que les blockchains permettent dépendra des améliorations qui leur seront

[5] Certes, financièrement, créer l'architecture d'une blockchain est bien moins coûteux que créer un réseau centralisé : une blockchain nécessite peu de machines et de supports physiques en raison de son caractère distribué. Et, comme les données y sont inaltérables, il n'est pas nécessaire de recourir à d'importantes équipes de contrôle qualité. En même temps, peu d'informations circulent, pour l'instant, sur les blockchains : les identités numériques de l'acheteur et du vendeur, le montant payé et le bien acheté. Or, en droit étatique-officiel, pour effectuer une transaction bancaire légale, près de cent champs différents doivent être remplis. En outre, il s'agit d'une technologie récente qui connaît de nombreuses limites en termes de performances. Un système reposant sur une blockchain peut gérer moins d'une dizaine de transactions par seconde, loin des dizaines de milliers d'un réseau tel que Visa — sachant que les transactions ne peuvent pas être en temps réel puisqu'il faut attendre que les « mineurs » valident les opérations, ce qui peut prendre de longues minutes. Et puis une blockchain enregistre continuellement de nouvelles informations sans jamais rien supprimer ; se pose donc le problème du stockage exponentiel des informations, lequel n'est *a priori* pas viable à long terme. Mais c'est peut-être surtout le coût énergétique des blockchains qui pose — et surtout posera — problème. Par exemple, les « mineurs » des bitcoins réalisent 450 000 trillions d'opérations par seconde afin de résoudre les problèmes et obtenir les preuves de travail, si bien qu'il n'est pas rare que le coût en électricité de ces opérations soit supérieur à leur rentabilité en bitcoins. En l'état, les besoins en puissance de calcul des blockchains sont gigantesques, rendant leur coût énergétique considérable. D'aucuns n'hésitent pas à parler de « gouffres énergétiques », notamment en raison des « fermes » construites afin de concentrer des milliers d'ordinateurs, fermes appartenant à des sociétés dont la plupart sont implantées en Chine.

[6] Des journaux ont pu titrer : « Blockchain : l'invention la plus importante depuis internet » (*La Tribune*, 5 févr. 2016).

apportées ou non, de leur capacité à se démocratiser à mesure qu'elles connaîtront de nouvelles versions moins austères et absconses[7].

Pour l'instant, il n'existe pas encore de véritable écosystème des blockchains. Très peu de start-up s'y intéressant dégagent des bénéfices. L'heure est toujours à l'exploration. Pour autant, des sociétés multinationales commencent à investir dans cette technologie, conscientes que leurs secteurs d'activité pourraient être bientôt « blockchainisés ». L'engouement suscité par les blockchains et par leurs promesses a un effet d'entraînement et un cercle vertueux s'enclenche, laissant supposer que les blockchains seraient en mesure de conquérir le monde comme l'internet l'a fait.

Or cette technologie pourrait engendrer des conséquences importantes à l'égard du système juridique et des habitudes des juristes. Les blockchains concurrencent le droit (*I*) et le remodèlent sur de nouvelles bases, donnant lieu à des formes originales de production et d'application des normes (*II*). Cela interroge les États, qui peuvent y voir une menace à redouter autant qu'une opportunité à saisir (*III*). Et cela pose la question de la gouvernance des blockchains, donc du droit des blockchains (*IV*). En somme, il semble que les blockchains soient un défi pour le droit bien plus que le droit est un défi pour les blockchains.

I. Les blockchains concurrencent le droit

Les blockchains, nouvelles garantes des transferts de valeurs

Chose inédite, la Landesbank Baden-Württemberg et le constructeur automobile Daimler AG ont annoncé, le 28 juin 2017, avoir mis en œuvre la technologie blockchain afin d'exécuter une transaction financière. Il pourrait s'agir de la première pierre posée d'un édifice ô combien innovant. Pour beaucoup de spécialistes des liens entre technologie et économie, les blockchains seraient le futur ; elles seraient appelées à devenir le support privilégié de réalisation des transactions économiques. Or, jusqu'à présent, c'était au droit qu'il revenait d'instaurer la confiance nécessaire à la prospérité et au bon déroulement des relations économiques. Plus globalement, il incombait au droit de garantir la bonne tenue des relations entre les hommes, des relations sociales. Les blockchains pourraient donc remplacer le droit.

Leur potentiel disruptif s'explique par leur capacité à bouleverser les habitudes en matière d'échanges, au détriment du droit tel qu'on le conçoit habituellement. Si l'internet a constitué une révolution de l'information et de la communication, les blockchains pourraient entraîner une révolution des transactions et des relations ; et cela ne serait pas sans conséquences sur le droit, son utilité et sa consistance. C'est pourquoi l'invention des blockchains, pouvant concerner potentiellement tout ce qui présente une quelconque valeur, pourrait impacter le droit bien plus profondément que ne l'a fait l'invention de l'internet.

En effet, la grande différence entre l'internet (TCP/IP) et les blockchains est la suivante : lorsqu'on envoie une chose sous forme de données en utilisant un réseau pair-à-pair classique ou le

[7] Contrairement au protocole TCP/IP universel de l'internet, il n'existe pas de normes internationales ni d'interopérabilité entre les blockchains. Cela constitue une autre limite. L'Organisation internationale de normalisation (ISO), et l'AFNOR en France, commencent néanmoins à réfléchir à une nouvelle norme « ISO/TC 307 Technologies des chaînes de blocs et technologies de registre distribué ». Ainsi cette limite n'en sera-t-elle peut-être plus une demain, dès lors que des standards mondiaux auront été adoptés.

web, cette chose n'est qu'une copie et l'envoyeur conserve l'original ; il y a toujours accès. Il lui est donc possible de transférer librement autant de copies que souhaité. Le bien est non rival, sa possession n'est pas exclusive : transférer l'information ne conduit pas à priver l'émetteur de sa jouissance. L'internet, sans blockchains, est par conséquent inutile pour transférer des choses qui ont de la valeur comme des titres ou des actions. Il permet seulement des partages. Pour le dire très caricaturalement, quand A envoie de l'argent à B, il est important que A n'y ait plus accès après son envoi, donc qu'il n'en conserve pas une copie ou l'original. Jusqu'à présent, on recourait à des intermédiaires comme les banques ou les États[8]. Pour la première fois dans l'histoire de l'informatique, « le protocole bitcoin a réussi à créer un bien numérique non reproductible »[9]. La propriété d'un bien numérique peut être transférée sans être dupliquée. C'est pourquoi les blockchains pourraient devenir à terme la nouvelle infrastructure des échanges, fonctionnant sur une base décentralisée, sans banque ni État. Le droit deviendrait tout simplement inutile, la technologie s'y substituant ; à moins que cette technologie ne soit le nouveau droit ou la nouvelle source du droit.

Les « smart contracts » ou « contrats intelligents », applications permettant d'échanger toutes sortes de biens ou de services grâce aux blockchains et fonctionnant de manière autonome, seraient au cœur de cette nouvelle mécanique. Ensuite, il reviendrait aux théoriciens du droit de les caractériser ou non telles des normes juridiques ou telles des sources de normes juridiques.

Reste qu'il devient possible de transmettre, par un réseau informatique et au-delà de la cryptomonnaie, de l'argent, des titres, des obligations, des actions, des droits de vote, des autorisations administratives, des places de concert, des droits d'auteur, mais aussi des biens mobiliers ou immobiliers (en réalité leurs titres de propriété) tels que des voitures ou des appartements ou encore, par exemple, des quotas de gaz à effets de serre. C'est la blockchain qui devient la garante de ces transactions.

Ces évolutions technologiques et les nouvelles voies qu'elles ouvrent en matière de transactions constitueraient avant tout une réponse à la défiance qui vise les tiers de confiance en général et les États en particulier, lesquels sont les sources du droit moderne. Elles accompagnent, et pas nécessairement de manière fortuite, un mouvement de rejet de plus en plus massif des élites et des formes de régulation verticales. Cela rejaillit forcément sur le droit qui, alors qu'il a vocation à susciter la confiance, est désormais regardé avec suspicion et méfiance. Dans ce contexte, les concurrents du droit officiel-étatique tels que les blockchains peuvent prospérer, offrant une transparence totale et une désintermédiation permettant de ne plus s'appuyer sur des tiers de confiance. Le pouvoir appartient désormais aux utilisateurs et aux consommateurs, qui profitent de processus simplifiés et d'une haute qualité de l'information fournie. Cela est favorable à la stabilité et à la sécurité des transactions.

Ordinairement, la confiance est la croyance ou la foi dans la fiabilité d'une personne ou d'un système. Cette confiance reposait jusqu'à présent sur l'association de la technique, de l'organisation et du droit. Avec les blockchains, on s'en remet entièrement à la technologie. C'est ainsi que les « smart contracts » permettent à deux partenaires de nouer une relation commerciale sans se connaître et sans tutelle d'une autorité centrale. Le système en lui-même garantit la validité et l'honnêteté de la transaction. La confiance ne dépend plus des hommes mais des machines — « The Trust Machine », comme l'a titré *The Economist*[10] au sujet des blockchains.

La crise de confiance actuelle touche en particulier le secteur bancaire et il n'est guère étonnant que le bitcoin et l'ether, qui sont des cryptomonnaies reposant sur la technologie blockchain,

[8] Et cela n'est pas sans risque. Par exemple, en 2013, en raison de la crise de la dette publique de Chypre, les banques endettées ont décidé arbitrairement de prélever 10 % sur les comptes en banque des chypriotes.
[9] A. T. Bataille, J. Favier, *Bitcoin, la monnaie acéphale*, CNRS Éditions, 2017, p. 1.
[10] La une de *The Economist* du 31 octobre 2015 était : « La machine à confiance – Comment la blockchain pourrait changer le monde ».

donnent lieu à de véritables systèmes monétaires indépendants et parallèles par rapport aux systèmes monétaires étatiques et bancaires. Pareilles cryptomonnaies semblent capables de générer cette confiance qui, de plus en plus, fait défaut dans le monde hérité du XX^{e} s.[11]. Et toutes les activités requérant des procédés d'authentification et de certification, c'est-à-dire de confiance, sont potentiellement concernées par cette nouvelle technologie. C'est pourquoi il faudrait soit prendre acte du retrait progressif du droit, soit accepter que le droit connaisse quelques mutations.

Décentralisation, désintermédiation, désuberisation

La philosophie des blockchains est claire : reprenant à leur compte l'idéologie originelle du cyberespace « *no borders, no banks* », il s'agit d'une doctrine libérale et même parfois libertaire visant à se passer des intermédiaires historiques et, en premier lieu, des États — et de leur droit. Certaines plateformes numériques ont déjà montré que les hommes peuvent préférer le réseau à la pyramide. Avec Airbnb ou Uber, les utilisateurs font confiance au réseau, sans toutefois s'émanciper de toute forme d'autorité. Le droit aussi pourrait passer « de la pyramide au réseau »[12] ; et les blockchains pourraient contribuer à ce mouvement.

Il y a vingt ans, on se risquait rarement à dormir chez un inconnu ou à monter dans la première voiture venue ; de même, on était méfiant à l'égard des formes non étatiques de régulation. Mais les choses changent. Ce nouveau protocole de transaction qu'est la blockchain contribue au passage d'un modèle de confiance basé sur les entreprises et sur les institutions à un modèle de confiance reposant sur un système et une communauté décentralisés. Toutes les opérations nécessitant une confiance totale dans l'information fournie sont possiblement concernées : contrôles d'identité, élections, comptabilité, certification, traçabilité agro-alimentaire, transactions immobilières, assurance, commerce international, industrie pharmaceutique, protection de la propriété intellectuelle etc.[13].

Une blockchain s'appuie sur une approche communautaire du processus d'échange qui permet de créer un consensus entre les utilisateurs. La confiance est placée dans le pouvoir de la multitude. En l'absence de consensus, aucune transaction n'est possible. Cela incite donc les utilisateurs à faire confiance à la technologie et à la communauté tout entière ; et cela génère en outre un cercle vertueux dans lequel la confiance est source de consensus, lui-même encourageant la confiance des utilisateurs. En cette mécanique réside toute la force des chaînes de blocs. Les individualités se trouvent dépassées et la technologie suscite une forme de lien social permettant à la confiance de s'appliquer à un corps social plutôt qu'à une autorité centrale ou à un tiers de confiance privé. Pour procéder à une transaction, il suffit de faire confiance à un tiers universel qui est la somme de l'ensemble des parties prenantes du système de transaction. Les blockchains permettraient ainsi de reconstruire sur de

[11] Cela même si certains économistes et autres banquiers centraux formulent des avertissements, prévoyant la création d'une bulle spéculative sur les cryptomonnaies en l'absence de tout contrôle financier au niveau international. D'ailleurs, après avoir pris de la valeur de manière continue depuis mi-novembre 2017, le bitcoin a perdu plus de 25 % de sa valeur entre le 15 et le 22 décembre 2017. Certains commentateurs n'ont pas hésité à parler de « krach » du bitcoin.

[12] Réf. à F. Ost, M. van de Kerchove, *De la pyramide au réseau ? Pour une théorie dialectique du droit*, Publications des Facultés universitaires Saint-Louis, 2003.

[13] Le marché du transfert d'argent est un excellent exemple. La Banque mondiale estime que ce marché représente 636 milliards de dollars en 2017. Les opérateurs prélèvent en général quelques 10 % de commission sur chaque transfert, de telle sorte que l'Afrique perdrait, selon l'ONG Overseas Development Institute, près de deux milliards de dollars chaque année. Les transactions via blockchains permettent de se passer de ces intermédiaires et, donc, de ne plus devoir leur verser des commissions exorbitantes.

nouvelles bases les sociétés, le collectif, les interindividualités, suivant le modèle d'une société décentralisée, horizontalisée[14].

Les blockchains pourraient réussir là où l'internet a échoué : le réseau informatique mondial n'est jamais parvenu à se passer entièrement des tiers de confiance. Or, en raison de son architecture décentralisée et distribuée, telle est justement la finalité d'une blockchain. Et il faudrait se réjouir de cette technologisation de la confiance puisqu'une autorité centrale supervisée par des humains serait par nature fragile dès lors que les hommes sont corruptibles et susceptibles de commettre des erreurs, donc potentiellement défaillants. Ce sont jusqu'aux tiers de confiance de l'économie collaborative qui peuvent être touchés par les applications des blockchains (Uber, Airbnb, eBay, Paypal etc.). Aussi les blockchains pourraient-elles bouleverser la nature même de l'organisation des sociétés actuelles, ce que n'ont pas fait Uber et ses semblables — qui se sont finalement contentés de remplacer des prédateurs capitalistes par d'autres prédateurs capitalistes.

La décentralisation de la diffusion de l'information a donné naissance à de nouveaux centres névralgiques. C'est ainsi que les moteurs de recherche du web — et surtout Google — sont devenus les principaux détenteurs du pouvoir dans le monde actuel, leurs algorithmes étant une source essentielle de normativité qui a notamment droit de vie et de mort sur de nombreuses entreprises et qui modèle les comportements des individus à travers des « suggestions » qui sont très souvent suivies. Ils s'appuient sur la multitude pour créer et concentrer la valeur. Dans un monde en interconnexion permanente, l'effet réseau favorise la constitution de nouvelles entités gargantuesques à visée monopolistique. La décentralisation n'est donc que partielle, parfois seulement de façade. Mais les blockchains pourraient permettre à cette décentralisation de connaître de nouveaux et profonds développements, ce qui se traduit, dans la littérature récente, par l'idée de « désuberisation ». Le Conseil d'État relève ainsi, dans sa dernière étude annuelle, que « cette technologie peut être regardée comme un aboutissement du processus de désintermédiation »[15].

La fortune des plateformes dominantes du web s'est construite à partir de leur capacité à certifier la validité de certaines informations essentielles au fonctionnement d'un réseau donné, donc leur capacité à se présenter tels des tiers de confiance. Les blockchains remettent ce rôle — dont Uber est le meilleur symbole — en cause. Elles sont un moyen technique de générer un consensus autour des informations utiles au bon fonctionnement du réseau. Le bitcoin, pour reprendre cet exemple, permet à des paiements d'être envoyés directement d'une partie à une autre sans avoir besoin de passer par une institution financière. Pour de nombreux acteurs économiques, l'émergence de la blockchain est donc un danger davantage qu'une opportunité. Les intermédiaires tels qu'Uber risquent de devenir inutiles[16].

Là où les plateformes de l'économie collaborative ont engendré un déplacement de la valeur de la production du produit ou du service vers la fonction d'intermédiation, les blockchains permettent une meilleure redistribution de la valeur entre ceux qui en sont les sources véritables. Cette transformation correspond aux principes de l'« holacratie », ce système organisationnel qui tranche avec les logiques pyramidales des sociétés modernes. Or c'est notamment le système juridique, institutionnel et politique qui préfère classiquement la verticalité et la hiérarchisation à l'horizontalité et à la collaboration. Les blockchains pourraient favoriser l'avènement d'un nouveau modèle touchant y

[14] *Cf.,* not., J. Rifkin, *La troisième révolution industrielle – Comment le pouvoir latéral va transformer l'énergie, l'économie et le monde,* Les liens qui libèrent, 2011.

[15] Conseil d'État, *Puissance publique et plateformes numériques : accompagner l'« ubérisation »,* La documentation française, 2017, p. 13.

[16] Par exemple, Ujo Music propose un service visant à rendre aux artistes la pleine propriété de leurs productions. Cela pourrait mettre à mal les plateformes qui cannibalisent une partie de la valeur créée. Pour ce qui est du transport par automobile, des projets tels que La Zooz ou Arcade City ont pour finalité de donner lieu à des Formes d'Uber sans Uber et, donc, sans prélèvement de commissions en échange de la confiance garantie.

compris les modes d'organisation publique et la régulation juridique. Il s'agirait de se libérer, grâce à la technologie, de l'emprise des pouvoirs institués, de la tutelle des firmes et des États.

L'une des activités stratégiques des plateformes est l'élaboration du code du réseau et du logiciel permettant de gérer les membres et leurs interactions. Les grands projets open source ont montré qu'une logique de coopération ouverte et libre peut donner des résultats très satisfaisants en termes de productivité, d'efficacité et de créativité. Les blockchains permettent de pousser ce processus encore plus loin, d'établir des réseaux auto-gérés, auto-opérés et auto-régulés, à base de gouvernance décentralisée[17]. Cela concerne toutefois les blockchains publiques mais non les blockchains privées. Ces dernières présentent des caractéristiques qui les rapprochent des systèmes transactionnels traditionnels contrôlés par un ou plusieurs acteurs précisément identifié(s)[18].

La mutation socio-économique provoquée par la technologie reste dans tous les cas porteuse de risques. Sont notamment redoutés des biais induits par les traitements algorithmiques. Si la technologie est neutre en soi, son usage par les hommes ne l'est pas. Les possibilités de détournement sont bien connues dans l'histoire du numérique : elles ont touché de près l'évolution de l'internet, avec une exploitation du potentiel d'innovation détournée de sa finalité initiale, passant d'un espace libre de partage et d'échange pensé sur un modèle décentralisé à une monétisation de cet espace réintermédié sous le couvert des grands principes originels. Concernant les blockchains, un même processus est à craindre en raison de la volonté de beaucoup d'acteurs de créer « leurs » blockchains privées. L'esprit libertarien qui a accompagné l'internet durant ses premières années a finalement été très vite rattrapé par des enjeux économiques et politiques. De même, l'idéologie de rupture au fondement du bitcoin est déjà en train d'être remodelée par de puissants acteurs financiers. Des dizaines de brevets sont déposés afin de s'approprier la technologie blockchain, parasitant son développement au service du bien commun et de l'intérêt général.

Une profession juridique menacée par les blockchains : le notariat

La dématérialisation et la désintermédiation des échanges obligent mécaniquement à améliorer la sécurité des transactions et la qualité de l'information des utilisateurs. Or, pour créer cette sécurité et cette qualité, les blockchains pourraient constituer le meilleur outil. Parmi les différentes professions juridiques, c'est en particulier celle de notaire que l'avènement des blockchains questionne — même si les avocats, les huissiers et les greffiers peuvent être aussi concernés. Cela explique pourquoi divers congrès, rencontres et autres journées d'étude ont récemment visé à interroger le potentiel disruptif de cette technologie à l'égard du notariat. Avec les blockchains, un nouveau genre d'organisations apparaît. Et, parmi ces organisations, l'opérateur central qui assiste les individus et prélève la valeur dégagée n'a plus lieu d'être. Désormais, ces individus collaborent directement, seule la technologie servant d'intermédiaire et de garant. C'est pourquoi les blockchains posent la question de la fin — ou

[17] Néanmoins, certaines garanties offertes par les plateformes, telles que des systèmes de recommandation ou des recours en cas d'inexécution de la prestation commandée, peuvent manquer dès lors qu'on se sert des blockchains. Or ces missions annexes peuvent jouer un rôle déterminant dans le succès d'un service, notamment dans les secteurs locatif et bancaire ou dans l'économie du partage.

[18] Le débat concernant les blockchains publiques et privées est dû à la volonté de certaines institutions financières, et même de certaines banques centrales, d'expérimenter des blockchains purement privées. La technologie blockchain pourrait dès lors conduire à de puissants phénomènes de réintermédiation dans beaucoup de secteurs et notamment en matière bancaire — c'est pourquoi les banques travaillent d'arrache-pied afin de mieux saisir et exploiter ses potentialités.

du moins du déclin — des intermédiaires et administrateurs ordinaires, au premier rang desquels figurent les notaires, chargés de certifier la valeur des actes authentiques.

Les blockchains permettent la conservation des données grâce à un système d'horodatage quasiment infaillible, chaque blockchain étant marquée par une empreinte numérique infalsifiable et reprise de bloc en bloc. Les informations sont ainsi irréversibles, immuables et intangibles. C'est pourquoi on s'interroge quant à l'avenir de l'acte notarié permettant de garantir une date certaine et une entière force probante. Dès lors qu'une opération est enregistrée dans une blockchain, chacun peut en vérifier la réalité et les données, sans recourir à aucun intermédiaire. La technologie est ainsi susceptible de subroger l'humain. À la place du notaire, il pourrait se trouver un simple prestataire technique qui recueille les empreintes numériques des données et crée le lien cryptographique entre ces empreintes et les transactions[19].

Cependant, la blockchain est une technologie de certification et non d'authentification. D'ailleurs, elle va souvent de pair avec l'anonymat de ses acteurs. Aussi les notaires peuvent-ils mettre en avant le fait que les blockchains permettent de conserver des empreintes numériques de documents donnés, mais sans contrôle de l'identité, de la capacité ou des pouvoirs en cause. Il faudrait donc que des blockchains allient certification et authentification pour véritablement concurrencer les notaires. En l'état, les blockchains permettraient de rendre des informations infalsifiables et de les sauvegarder, mais sans accomplir toutes les fonctions qui sont propres aux notaires. Par exemple, une blockchain ne permet pas de contrôle de l'équilibre de la convention ou de sa conformité à l'ordre public. Et aucune force exécutoire n'est donnée à l'acte. Mais cela vaut uniquement à l'égard de l'ordre juridique étatique[20]. Or, en même temps que les blockchains concurrencent les notaires, des ordres normatifs privés concurrencent l'ordre juridique étatique. Cependant, tant que le notaire apportera de la valeur ajoutée à ses actes et du conseil à ses clients, il perdurera sans doute — profitant en outre de l'inertie des usages juridiques.

Toujours est-il que les blockchains remettent en cause nombre de pans du droit, au moins potentiellement. Elles peuvent en particulier permettre de recourir à de nouvelles modalités de création et d'application du droit. Ainsi, pour en revenir au cas des notaires, ceux-ci pourraient profiter des blockchains pour construire des outils efficaces d'assistance à l'exécution des transactions par ce qu'on appelle les « smart contracts ».

[19] Par exemple, une vente immobilière contractée par acte sous seing privé ou par acte authentique possède la même valeur pour les parties, ainsi que pour les héritiers et ayants cause ; la principale différence réside dans le caractère certain de la date que l'acte authentique confère. Or une blockchain permet d'obtenir la même certitude s'agissant de l'horodatage et des parties à une transaction immobilière donnée, de même que pour la certification du titre de propriété du vendeur, la disponibilité des fonds pour l'acheteur, la conclusion de l'acte de vente ou la conservation et l'inviolabilité de cet acte. Il pourrait donc devenir possible de réaliser des opérations immobilières sans le concours d'un notaire. Cela d'autant plus que l'article 1366 du Code civil consacre la validité de l'acte authentique électronique.

[20] D'autres limites sont la lenteur des transactions et l'absence de conservation des documents dans les blockchains (seules leurs empreintes y sont conservées), tandis que les notaires ont l'obligation de représenter un acte authentique pendant 75 ans.

II. Les blockchains renouvellent le droit

La blockchainisation du droit

Les blockchains sont un défi pour le droit. Elles sont aussi sources de droit. Si ces nouvelles technologies sont des objets juridiques, le droit est également un objet de ces nouvelles technologies, qu'elles contribuent ainsi à remodeler. Sous cet angle, on ne se demande pas comment le droit saisit la technologie ou comment il l'influence mais, à l'inverse, comment la technologie saisit le droit et l'influence ; et comment la technologie fait le droit, devient source de normes juridiques véritables. Il ne s'agit pas d'observer comment le droit appréhende les nouvelles technologies de l'information et de la communication mais d'observer comment ces nouvelles technologies appréhendent le droit — et de réfléchir aux conséquences, limites, dangers, opportunités liés à ce phénomène.

Les trois grands apports de la blockchain au droit sont les transferts de valeur (évoqués précédemment), les contrats à exécution automatique (« smarts contracts ») et l'enregistrement de preuves. De plus, si des lois ou des règlements en bonne et due forme ne sauraient jaillir des blockchains, il ne fait aucun doute que celles-ci emportent des effets normatifs importants, en premier lieu à l'égard de leurs utilisateurs qui se trouvent contraints d'opérer dans un cadre technologique particulier. Or il est important de prendre conscience de cet impact technologique sur le droit. Le risque n'est-il pas de se retrouver un peu comme ces gens par trop conservateurs que Jean-Jacques Rousseau décrivait, « devenus pauvres sans avoir rien perdu, simplement parce que tout changeait autour d'eux et qu'eux n'avaient point changé »[21] ?

Les professionnels du droit sont sommés d'anticiper, de comprendre et de préparer le développement des blockchains. En particulier, les « smart contracts » devraient gagner du terrain de façon exponentielle. Au-delà, peut-être nombre de fondements traditionnels et de branches du droit seront-ils remis en question. La technologie pourrait impacter tous les pans du droit, toutes les activités des juristes. L'avocat, le notaire, le magistrat, mais aussi l'enseignant et l'étudiant devront adapter leurs façons d'enseigner, d'apprendre, de pratiquer et d'appliquer les règles de droit.

Les contrats à exécution automatique (« smart contracts »)

Les blockchains tendent à réinventer les procédés contractuels. En France, le droit des contrats, réformé en 2016[22], pourrait bien vite devoir s'adapter. C'est comme si la technologie, chaque jour un peu plus, obsolétisait le Code civil. Et ce sont en particulier les « smart contracts » qui bouleversent les habitudes contractuelles. Ils constituent l'un des aspects juridiquement les plus innovants des blockchains.

[21] J.-J. Rousseau, « Discours sur l'inégalité », in *Œuvres complètes*, Le Seuil, 1971, p. 228.
[22] Ord. n° 2016-131, 10 févr. 2016, *Portant réforme du droit des contrats et du régime général de la preuve des obligations*, entrée en vigueur le 1er octobre 2016.

Plutôt que des « contrats intelligents », il s'agit en réalité de contrats à exécution automatique. Plus encore, ce ne sont pas, au sens proprement juridique du terme, des contrats mais seulement des modalités de réalisation de contrats. Un « smart contract » consiste en un transfert automatisé de valeurs fondé sur un accord préalable entre deux personnes et qui s'exécute au moyen d'une blockchain. Il peut permettre, par exemple, le paiement automatique d'un colis dès sa bonne réception ou le transfert de gains au vainqueur d'un pari sportif une fois le match en cause terminé et son résultat enregistré. C'est un programme informatique qui, sur une blockchain, vérifie qu'une série de conditions d'exécution sont réunies et, lorsque tel est le cas, déclenche les actions objet de la convention. C'est pourquoi on parle de processus « if…, then… » (« si…, alors… »).

Les contrats à exécution automatique présentent des garanties de bonne exécution et de flexibilité, empêchant donc toute contestation au niveau de leur réalisation. Les conditions étant assurées par la technologie, il n'y a plus de place pour la confusion, les difficultés d'interprétation ou les différends[23]. Cela modifie radicalement le cadre juridique traditionnel puisque le recours au juge ne constitue plus la garantie ultime des accords contractuels. Les règles deviennent tout à la fois les termes de l'accord et les moyens d'en prévoir et assurer l'exécution. Outre l'effet dissuasif qui s'attache aux « smart contracts », le nombre de contentieux pourrait en conséquence diminuer, contribuant à désencombrer les tribunaux. Avec l'automaticité, il n'est plus nécessaire pour une partie de faire constater que son cocontractant n'a pas procédé au paiement puisque c'est la technologie qui constate le non-paiement et active la clause correspondante. Et cela peut s'appliquer en particulier aux contrats d'assurance prenant en charge les indemnités en cas de mauvaise exécution d'un contrat de transport, tel le retard d'un train ou d'un avion[24], ainsi qu'aux contrats d'assurance automobile, d'assurance antipollution ou d'assurance décès. L'usager pourrait obtenir son dédommagement sans même avoir à remplir de déclaration de sinistre[25]. L'automaticité de l'exécution du contrat garantit une pleine effectivité des droits — alors que, souvent, nombre de clients ne réclament pas ce qui leur est dû — et une lutte plus efficace contre les mauvais payeurs. Cela pourrait aussi concerner l'exécution d'un pacte entre actionnaires, la distribution de dividendes etc.

En outre, le caractère automatisé de la mise en œuvre du contrat permet à deux partenaires de nouer une relation commerciale sans qu'il soit nécessaire qu'ils se fassent confiance au préalable, sans autorité ou intervention centrale et en réduisant grandement les coûts. Car c'est le système lui-même, et non ses agents, qui garantit l'honnêteté de la transaction. Et, avec la technologie blockchain, les

[23] Les « smart contracts » pourraient notamment permettre la bonne exécution des décisions de justice et des décisions d'arbitrage, contrairement à ce qui se produit pour l'instant concernant les litiges relatifs au e-commerce. Ils pourraient aussi, autre exemple, assurer une meilleure gestion des droits d'auteur. C'est ainsi que Spotify, en avril 2017, a annoncé avoir acheté la start-up Mediachain Labs, laquelle propose des « contrats intelligents » dans la blockchain Ethereum afin de gérer précisément et efficacement les droits des artistes. Leur rétribution est rendue beaucoup plus transparente et, par suite, beaucoup plus juste. Les paiements se déclenchent automatiquement dès lors que les œuvres sont diffusées.

[24] Concernant les retards des vols, les contrats sont associés aux bases de données de Flightstats, recensant le trafic aérien mondial, et dès qu'un vol atteint un certain retard l'indemnisation est déclenchée automatiquement sans besoin d'effectuer une déclaration ou de procéder à une quelconque démarche. Autre exemple, la location d'un logement avec une serrure qui s'ouvre et se bloque automatiquement selon que le paiement a été effectué ou non, ainsi qu'au moment où le contrat arrive à échéance. Enfin, dernière illustration, promus par la Banque mondiale pour couvrir les agriculteurs des pays en voie de développement, des « smart contracts » assurantiels permettent d'enclencher les indemnisations automatiquement sitôt qu'une anomalie météorologique est constatée, par exemple dès lors qu'une période de sécheresse dure trente jours ou plus.

[25] Des sociétés réfléchissent à des applications, plus novatrices encore, reposant sur des assurances pair-à-pair, c'est-à-dire des coopératives d'assurés qui se couvrent mutuellement. Par exemple, une communauté pourrait s'autoassurer contre la perte d'emploi loin de toute compagnie d'assurances. Pour cela, elle créerait une cagnotte et, lorsqu'un membre se retrouverait sans emploi (l'information étant transmise par l'autorité habilitée à constater la perte d'emploi), une somme préalablement convenue lui serait versée, éventuellement proportionnelle au dernier salaire touché et à la durée de l'activité salariée antécédente. Tout se ferait au moyen d'un « smart contract ».

conventions sont rendues infalsifiables. Le contrat dit « intelligent » offre donc une grande sécurité aux parties, ainsi qu'une réduction importante des coûts de rédaction, de vérification et d'exécution du contrat, notamment grâce à la désintermédiation. Le fonctionnement du monde des affaires, qui dépend pour beaucoup de l'instrument contractuel, pourrait se trouver largement repensé en raison du recours aux « smart contracts »[26].

Les contrats à exécution automatique chamboulent les notions et régimes habituels du droit des contrats, notamment le consentement, la contrepartie, la bonne foi ou encore l'exécution forcée. Et les « smart contracts » ont tendance à standardiser les conventions, celles-ci devant être les plus simples possible afin de pouvoir être exécutées spontanément par des ordinateurs. Il faut donc écarter au maximum la négociation et l'interprétation. Aussi cette technologie s'oriente-t-elle vers l'utilisation de modèles-types contractuels.

Il est, en outre, impossible, sauf à l'avoir prévu dès le départ, de modifier une convention à exécution automatique, ce qui oblige à se montrer très vigilant durant la phase de conception de cette convention. Puisque les systèmes numériques sont déterministes, toutes les issues possibles liées au contrat, notamment sa rupture et la décision de soumettre les éventuels litiges à un arbitre, doivent être spécifiées initialement et explicitement.

Par ailleurs, le recours aux contrats à exécution automatique n'est pas envisageable, en droit officiel-étatique, lorsque diverses exigences procédurales doivent être accomplies (mise en demeure, notification préalable, délai raisonnable, mentions manuscrites, motivation *ad hoc* etc.)[27]. Et restent les problématiques juridiques classiques mais toujours fortes sous l'angle de ce droit officiel-étatique : quelle loi applicable à des « smart contracts » transnationaux ? quelle juridiction compétente ? quels responsables et quelles obligations en cas de faille du système ?

[26] Ensuite, et concrètement, les conditions d'exécution d'un contrat correspondent à deux hypothèses : soit elles dépendent d'autres écritures dans la blockchain ou bien renvoient à des conditions de temporalité et, dès lors que ces écritures existent ou une fois que la date prévue est atteinte, la convention est automatiquement exécutée ; soit ces conditions renvoient à des évènements potentiels et extérieurs à la blockchain — par exemple la réalisation d'une prestation prédéfinie — et il est dès lors indispensable qu'un tiers de confiance entre dans la blockchain l'information selon laquelle cet évènement s'est produit ou non. Ce dernier cas témoigne des limites des « smart contracts » qui ont souvent besoin d'« oracles ». Ces oracles ont pour mission d'enregistrer dans la blockchain l'information de façon fiable afin que le contrat puisse s'exécuter correctement. Par exemple, ils sont indispensables afin d'entrer dans la blockchain les horaires d'arrivée prévus et réels des avions en cas de « smart contract » visant à rembourser automatiquement les clients des compagnies aériennes dès que les retards des vols dépassent une certaine durée. Sinon, les « smart contracts » ne pourraient être utilisés qu'afin d'exécuter des opérations par nature indépendantes de tout aléa. Ensuite, l'oracle peut être :
- un tiers de confiance connu des deux parties et désigné préalablement ;
- une base de données externe et précisément identifiée que le « smart contract » consultera automatiquement (par exemple, dans le cas des paris sportifs, les résultats enregistrés par les fédérations nationales et internationales) ;
- un service *ad hoc* décentralisé, faisant appel à de nombreux participants qui valident les données de la blockchain ; c'est alors le consensus entre les participants qui aboutit au résultat permettant l'exécution du contrat.

[27] Il existe, dans ce droit officiel-étatique, deux types de transactions : celles qui ne supposent qu'un accord de volonté entre les parties, qui le formalisent et le conservent comme elles l'entendent, et celles qui, solennelles ou authentiques, sont encadrées par la loi, notamment en prescrivant des conditions de fond et de forme dans l'édiction, la réalisation et la conservation (transactions immobilières, création de sociétés, transactions portant sur des titres financiers etc.). Les contrats à exécution automatique peuvent à l'évidence s'épanouir davantage concernant les premières que concernant les secondes — d'autant plus que la loi reconnaît que le processus d'offre et d'acceptation d'une offre de contracter peut se réaliser par voie électronique.

Les preuves enregistrées dans les blockchains

Une blockchain permet d'enregistrer et de certifier des contrats formés en suivant les conditions ordinaires de conclusion des contrats. Il s'agit de traduire en langage informatique un accord de volonté né dans le monde physique. Le « smart contract » et la blockchain, profitant de ses possibilités en matière de certification décentralisée et de registre public sécurisé, immuable et fiable, permettent alors d'horodater la convention et d'apporter la preuve de son existence et de son contenu.

Il est envisageable d'ancrer tout type de document ou d'information sur une blockchain (texte, photo, son, vidéo etc.). Il suffit de posséder un format numérique pour créer un hash cryptographique s'y rapportant et horodater le document sur une blockchain en y inscrivant ce hash. On ne stocke donc pas le document sur la blockchain mais seulement son hash cryptographique, son empreinte numérique. Cela pourrait justifier d'abandonner, par exemple, le système de l'enveloppe Soleau. Et cela pourrait servir à tracer toutes sortes de produits et services[28].

Dès lors que la preuve est libre, la technologie blockchain semble ô combien prometteuse sous cet angle, au-delà du cas de l'enregistrement des contrats de manière sûre et certaine. Bien des choses, inscrites dans une blockchain, pourraient être ainsi protégées — d'autant plus que l'utilisation d'une chaîne de blocs à des fins de preuve peut être très opportune financièrement. La blockchain est une technologie très efficace pour se préconstituer une preuve parce que le certificateur n'est pas une entité donnée, éventuellement faillible, éventuellement corruptible, mais des milliers de personnes partout dans le monde[29].

En permettant de rapporter différemment la preuve de l'existence et de l'antériorité d'un droit subjectif comme un droit de propriété, la blockchain invite à repenser, par exemple, les registres cadastraux ou à créer de nouveaux instruments de gestion des droits de propriété intellectuelle. Aujourd'hui, la contrefaçon de musiques, images et vidéos s'est banalisée avec l'internet. Les créateurs sont littéralement spoliés de leurs droits. Or la technologie blockchain permet d'enregistrer de façon fiable et sécurisée les droits de propriété intellectuelle sur les œuvres et de contrôler leur diffusion. Le monde de la création artistique pourrait être à nouveau ébranlé par la technologie, mais cette fois positivement. En outre, des inventions, des marques, des dessins et modèles ou d'autres types de création peuvent être sauvegardés sur des blockchains. Ces applications devraient attirer l'attention des sociétés de gestion collective : pour elles, les blockchains constituent à la fois une forme de concurrence et une opportunité en permettant d'améliorer leur gestion des droits.

Les diplômes pourraient aussi être enregistrés dans des blockchains, cela afin de pouvoir vérifier aisément leur réalité quand, aujourd'hui, les recruteurs sont souvent contraints de croire en la bonne foi des curriculum vitae — et alors que les écoles et les entreprises dénoncent régulièrement les trop nombreuses usurpations de titres et autres qualifications[30]. Les registres dans les blockchains

[28] Ainsi l'organisme fédéral américain de contrôle des marchés financiers a-t-il déjà accepté d'utiliser une blockchain comme registre de la propriété des actions.

[29] La force probante dépend toutefois du nombre de « mineurs » qui sécurisent les transactions et est donc plus importante en matière de blockchains publiques qu'en matière de blockchains privées. Les acteurs d'une blockchain privée pourraient s'accorder afin de modifier l'historique des transactions et altérer une opération *in favorem*. L'ancrage des données dans une blockchain publique est en revanche très sécurisé, le risque de collusion entre les « mineurs » y étant nul.

[30] L'ESILV (École supérieure d'ingénieurs Léonard de Vinci) et la société Paymium, ainsi que l'École d'ingénieurs Holberton de San Francisco et la société Bitproof enregistrent les signatures de chaque diplôme dans une blockchain, tenant ainsi à jour et en libre accès le registre de leurs diplômés.

intéressent également les industries du luxe, des pierres précieuses et des objets d'art. En recensant les biens, leurs provenances et leurs propriétaires, et en assurant leur traçabilité, cela pourrait permettre de lutter contre la fraude dans ces secteurs d'activité[31]. Dans les domaines de la finance, de l'assurance, des transports, de l'alimentation et de l'énergie et du développement durable, on développe également des applications fondées sur les blockchains. Cette technologie permet surtout des progrès en termes de traçabilité, garantissant une bonne information quant à l'origine des produits, cela afin de redonner confiance au consommateur[32]. La blockchain devient de plus en plus une infrastructure sécurisée de dialogue et d'échange entre les différents acteurs des chaînes de production[33].

Toutefois, le déploiement de ces nouveaux modes de preuve technologique est freiné par le besoin de posséder des bitcoins ou une autre cryptomonnaie pour effectuer une transaction. Car l'empreinte, servant de preuve, doit être placée dans une transaction. Par ailleurs, la blockchain ne saurait être utilisée en matière de signature électronique puisqu'elle ne permet pas de créer un lien fiable entre la signature numérique et l'identité réelle des personnes.

Bien sûr, en droit officiel-étatique, l'utilité des blockchains comme nouveaux modes de preuve dépendra pour beaucoup d'éventuelles interventions du législateur afin de les consacrer — ou non[34]. Au-delà, dans une blockchain ouverte, les opérations effectuées ne sauraient revêtir d'autre force juridique que celle que les participants à la chaîne acceptent de leur donner. Concernant le bitcoin, par exemple, les transactions effectuées au moyen de cette cryptomonnaie n'ont pas de valeur légale mais seulement une valeur dans le système bitcoin. Devant un juge, elles ne peuvent pas être reconnues comme opposables. L'opposabilité aux tiers est ainsi un des grands enjeux de la preuve enregistrée dans une blockchain — des tiers qui, souvent, n'ont même jamais entendu parler de « blockchain ».

Tous ces changements potentiels attachés aux blockchains posent en filigrane la question de l'accueil que les États peuvent et/ou doivent réserver à cette technologie. Faut-il qu'ils se prémunissent contre ce qui serait un danger ou bien qu'ils exploitent au maximum ce qui serait une chance à saisir ?

---

[31] Everldger a développé une blockchain permettant de certifier l'origine de centaines de milliers de diamants. Désormais, cette start-up applique son modèle et sa technologie au marché des œuvres d'art.

[32] Nestlé, Unilever, Walmart et sept autres groupes agroalimentaires travaillent ainsi sur la traçabilité des denrées périssables à travers les blockchains. En cas de contamination alimentaire, la difficulté d'accès aux informations empêche d'agir efficacement afin de retirer des gondoles des supermarchés tous les produits touchés. Identifier l'origine et le lieu de la contamination peut prendre des semaines, ce qui entraîne des problèmes sanitaires, des pertes de marchandises et une baisse du chiffre d'affaires. Les acteurs des chaînes de production pourraient utiliser les blockchains afin de tracer les produits beaucoup plus efficacement.

[33] Par exemple, la start-up Provenance a créé un service permettant, au moyen d'une « *proof of concept* », de garantir la traçabilité du thon : une blockchain enregistre les différentes étapes de la vie des thons. Un autre exemple significatif se trouve dans les « *smart grids* ». Les grandes entreprises de l'énergie les expérimentent actuellement. Ces « *smart grids* » permettent de tracer l'énergie verte produite localement et de relier producteurs et consommateurs d'énergie d'un même quartier ou d'une même commune, cela tout en garantissant l'origine de la production. Une blockchain est utilisée pour ces échanges, permettant la création d'un réseau local décentralisé d'enregistrement et de contrôle des échanges d'énergie et une gestion fine des certificats garantissant l'origine.

[34] En cas de litige, la recevabilité des preuves par blockchain pose question. Faut-il appliquer les conditions relatives à la preuve d'un écrit électronique — *i.e.* les conditions d'intégrité et d'imputabilité du contenu posées par l'article 1366 du Code civil ? Par suite, comment assurer l'entière fiabilité de la blockchain ? Doit-elle être présumée ? Et si recevabilité de pareille preuve il y a, quelle en est la force ?

III. Les blockchains interrogent l'État

Des blockchains au service de l'État ?

Concernant les transactions dites « consensuelles », non soumises à un quelconque formalisme légal, l'utilisation de la technologie blockchain devrait progressivement s'imposer. Il serait dès lors peu satisfaisant, du point de vue des pouvoirs publics, que ces transactions, que le législateur n'a pas souhaité protéger par un formalisme particulier, profitent de plus de sécurité et d'efficacité que les démarches administratives légalement encadrées et reposant toujours sur des supports papiers conservés dans des salles d'archives. Mais il n'appartient qu'aux institutions publiques de se saisir de l'opportunité technologique que les blockchains constituent. Celles-ci pourraient servir à perfectionner le fonctionnement de certains services publics, ainsi que les rouages des institutions en général. Par exemple, le législateur pourrait harmoniser de nombreuses procédures en créant un grand registre unique et dématérialisé sur une blockchain. Il ne s'agirait pas nécessairement de remplacer les intermédiaires et dépositaires de registres divers déjà existants (greffe, cadastre, INPI etc.), mais de repenser leurs modes de fonctionnement afin d'améliorer l'efficience de leurs actions[35].

Les chaînes de blocs pourraient notamment être utiles afin de défendre le droit de propriété. Elles seraient alors utilisées en tant que registres décentralisés et sécurisés permettant d'inscrire les achats et ventes de terrains et d'immeubles. Un registre foncier inscrit dans une blockchain permettrait de se prémunir contre les risques de fraude ou de falsification en assurant la traçabilité des transactions. Sous cet angle, les blockchains pourraient être bienvenues dans les pays où la fraude est massive et les droits de propriété soumis à des autorités peu fiables[36]. Une fois inscrits dans la blockchain, les actes fonciers deviennent immuables sans un transfert de propriété en bonne et due forme.

Aux États-Unis, les pouvoirs publics utilisent les blockchains pour lutter contre la corruption et la fraude fiscale. Au Royaume-Uni, le gouvernement y recourt afin d'organiser le versement des prestations sociales. Apparaissent ainsi des blockchains officielles, institutionnalisées. Tel est aussi le cas en Chine, où le gouvernement a fait du recours aux blockchains une priorité[37].

[35] L'Estonie est souvent citée en exemple, elle qui enregistre déjà les mariages et de nombreuses autres données dans des blockchains.

[36] C'est ainsi qu'au Ghana, pays qui ne dispose pas de cadastre officiel, l'ONG Bitland a créé un registre de propriété transparent et infalsifiable. Et des projets de cadastre blockchainisés sont annoncés dans des pays tels que la Grèce, la Géorgie ou le Honduras où la propriété foncière est sujette à corruption et à manipulation.

[37] Dès 2016, la technologie blockchain a été intégrée au treizième plan quinquennal consacré à l'informatique. C'est ainsi que, désormais, la collecte des taxes sociales et l'émission des factures se font, en Chine, au moyen de chaînes de blocs. Et la banque populaire de Chine de tester sa propre cryptomonnaie. Plusieurs autorités locales ont également engagé des politiques visant à développer l'usage des blockchains, alors que des agences gouvernementales ont créé des équipes de recherche et développement *ad hoc*.

En France, les blockchains sont encore loin de préoccuper autant les autorités publiques[38]. Il faut pourtant gager qu'elles pourraient rendre beaucoup de services. Par exemple, des applications en matière de taxe sur la valeur ajoutée seraient tout spécialement adaptées : le prélèvement de la TVA par une partie provoquerait automatiquement une déduction chez une autre partie. Le fait d'intégrer ces calculs à une blockchain permettrait d'anéantir la fraude carrousel. En matière d'état civil aussi, les blockchains pourraient conduire à une profonde révision des pratiques administratives. Cet état civil, qui consiste en l'ensemble des données relatives aux naissances, reconnaissances d'enfants naturels, mariages et décès, pourrait être transporté dans une blockchain. Il serait dès lors aisé de produire un extrait d'acte de naissance précisant la date et le lieu de cette naissance afin de certifier une identité, une application blockchain, accessible immédiatement et de son domicile, comportant toutes ces informations. De même, de grandes simplifications sont concevables à l'égard des démarches à effectuer au moment d'un mariage ou d'un décès.

Les chaînes de blocs pourraient encore être utilisées en matière électorale, favorisant le bon fonctionnement de la mécanique démocratique. Des start-up ont ainsi créé des systèmes de vote sécurisés[39]. Mais les blockchains sont aussi — et peut-être surtout — un défi de taille pour les États.

Des blockchains à la place de l'État ?

Se pose jusqu'à la question de la subrogation des blockchains aux États, au moins concernant certaines de leurs missions traditionnelles. Dans nombre de situations, la technologie serait en mesure de faire mieux que les institutions publiques. Pour certains chercheurs, comme Primavera de Filippi[40], les souverainetés seraient appelées à disparaître et les États ne seraient plus guère que des archaïsmes à oublier. Dans leurs travaux, ils parlent d'ailleurs peu d'État ; et lorsqu'ils évoquent l'État, c'est en tant que vieille chose dépassée et en voie d'extinction. Aussi ces chercheurs ne se demandent-ils pas si l'État devrait s'intéresser aux blockchains car, pour eux, que tel soit le cas ou non ne présenterait que peu d'importance par rapport aux enjeux attachés aux forces privées de la société civile qui se déploient.

Mais si l'on continue à interroger l'État, considérant qu'il resterait un horizon indépassable dans les modes contemporains et à venir de régulation sociale, il semble alors que la technologie blockchain soit de nature à remodeler en profondeur l'ordonnancement étatique et le mode de

[38] Depuis quelques mois, les blockchains sont cependant au cœur de certaines réflexions des pouvoirs publics. Pour la première fois, leur utilisation a été juridiquement consacrée dans le secteur financier (concernant le financement participatif) par l'ordonnance n° 2016-520 du 28 avril 2016 *Relative aux bons de caisse*. Désormais, l'article L. 223-12 du Code monétaire et financier prévoit que « l'émission et la cession de minibons peuvent être inscrites dans un *dispositif d'enregistrement électronique partagé* permettant l'authentification de ces opérations, dans des conditions, notamment de sécurité, définies par décret en Conseil d'État ». Cela ressemble fort à une première consécration légale des blockchains. Et l'article L. 223-13 du même code de reconnaître les blockchains comme un outil d'enregistrement permettant l'authentification de transferts de propriété, rendant la cession de minibons sur une blockchain opposable aux tiers. En outre, la loi n° 2016-1691 du 9 décembre 2016 *Relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique*, dite « Sapin II », a autorisé le Gouvernement à légiférer par ordonnance afin d' « adapter le droit applicable aux titres financiers et aux valeurs mobilières pour permettre la représentation et la transmission, au moyen d'un dispositif d'enregistrement électronique partagé, des titres financiers qui ne sont pas admis aux opérations d'un dépositaire central ni livrés dans un système de règlement et de livraison d'instruments financiers ».

[39] En France, en 2017, LaPrimaire.org, initiative citoyenne libérée de tout parti politique traditionnel, a utilisé la blockchain Ethereum pour organiser la primaire permettant de choisir son candidat à l'élection présidentielle. Des scrutins plus officiels pourraient, à l'avenir, être dématérialisés en développant ce genre de technologie.

[40] Not., P. De Filippi, A. Wright, *Blockchain and the Law – The Rule of Code*, Harvard University Press, 2018.

gouvernement qui s'y attache. Et cela pourrait notamment s'expliquer, à l'ère de la grande défiance des citoyens à l'égard des élus et du personnel politique en général, par la préférence donnée au monde incorruptible des blockchains. Les constructions symboliques ancestrales qui hier permettaient à l'État de s'imposer, à base de territoire, de nation et de contrat social, ne semblent plus capables de produire leurs effets dans le cyberespace.

Par suite, si les fonctions que l'État est chargé de remplir du fait de sa souveraineté sont le contrôle d'un territoire, la maîtrise d'une monnaie, la levée des impôts ou encore le prononcé de la justice — en particulier afin de garantir les transactions —, toutes sont remises en cause par les blockchains. On peut considérer que les États devraient dès lors s'effacer. On peut aussi penser qu'ils devraient pleinement se tourner vers cette nouvelle technologie, celle-ci se présentant dès lors non telle une menace mais tel un allié précieux dans le monde actuel — celui de la globalisation, de l'internet, des multinationales anationales, des échanges transfrontières permanents, de l'évasion et de l'érosion fiscales. Car, si les États délaissaient les blockchains, s'ils les ignoraient, elles risqueraient fort de façonner un monde sans souveraineté s'apparentant à l'état de nature. Le droit n'en sortirait sans doute guère grandi.

C'est en particulier en matière monétaire que des questions se posent. Les cryptomonnaies sont l'application phare de la technologie blockchain. Le bitcoin est associé à la première (historiquement, qualitativement et quantitativement) des blockchains ; mais il en existe bien d'autres telles que l'ether correspondant à la blockchain Ethereum. Comment les États doivent-ils réagir ? Faut-il qu'ils luttent contre ces cryptomonnaies concurrentes des monnaies officielles ou qu'ils les accueillent à bras ouverts ? Par exemple, en matière de fraude fiscale, les blockchains pourraient rendre la tâche de l'administration fiscale très difficile, allant éventuellement jusqu'à la rendre impossible. En effet, comment prélever les impôts si les flux anonymes de cryptomonnaie venaient à se généraliser ? Les paiements étant effectués par les contribuables sur des systèmes parallèles, contrairement aux opérations courantes des banques, l'administration fiscale n'aurait pas accès à d'innombrables données et, par suite, serait dans l'incapacité de mener à bien sa mission.

Si des États sont intervenus afin de réguler les usages des blockchains, comme les États-Unis, la Chine ou la Corée du Sud, c'est souvent afin de limiter drastiquement ces usages et notamment d'interdire le recours aux cryptomonnaies. Au Japon, en Allemagne, en Finlande ou en Bielorussie, en revanche, le législateur a validé l'existence des cryptomonnaies[41]. Il est ainsi possible, dans ces pays, de vendre et acheter des biens au moyen de bitcoins ou d'ethers. Or les États ne sortent-ils pas gagnants de telles réformes ? Légaliser les transactions effectuées avec des cryptomonnaies leur permet en effet de les taxer. Certes, pour l'heure, les hommes recourent trop souvent aux cryptomonnaies à des fins illicites et même crapuleuses — le bitcoin sert notamment à acheter drogues, armes et autres contenus pédopornographiques dans le darknet. Mais il pourrait en aller différemment si tous les États validaient l'existence de monnaies privées non plus concurrentes mais complémentaires des monnaies publiques[42].

Si les États peuvent ou non voir dans les blockchains une technologie d'avenir, s'ils peuvent ou non consacrer d'importants moyens au développement de leurs usages dans les administrations et dans le corps social, toujours est-il que les chaînes de blocs sont aujourd'hui — et sans doute pour longtemps — des instruments principalement privés appelant une régulation privée, des normes privées, un droit privé. La question de la gouvernance des blockchains et du droit des blockchains ne se pose pas moins avec insistance.

[41] Le 1er avril 2017, le Japon a reconnu le bitcoin en tant qu'instrument de paiement, tout en régulant les places de marché ouvertes au public sur lesquelles s'effectue le change entre monnaies officielles et monnaies électroniques.
[42] En ce sens, il est remarquable qu'en Suisse, depuis 2014, il existe des distributeurs permettant d'échanger des francs suisses contre des bitcoins. En France, une expérience de ce genre est menée à Montpellier depuis 2016.

IV. Les blockchains sont l'objet d'un droit

La régulation technologique des blockchains

Les blockchains, ou du moins celles qui sont considérées telles de véritables blockchains — *i.e.* les blockchains publiques —, reposent sur une idéologie libertarienne selon laquelle elles devraient s'émanciper de toute régulation humaine. « *Code is Law* », célèbre maxime de Lawrence Lessig, trouve ici parfaitement à s'appliquer — tout comme l'idée de « *lex cryptographia* ». Les parties prenantes à une blockchain (développeurs, « mineurs », opérateurs d'*exchanges*, personnes effectuant des transactions etc.) interagissent dans le cadre et suivant les modalités dictés par le protocole informatique. Et il faudrait laisser la technologie entièrement libre de ses mouvements. Il serait donc inutile de poser la question de la gouvernance d'une technologie qui n'aurait guère de sens si elle était contrôlée d'une quelconque façon. Avec les blockchains, on parle de « confiance », de « décentralisation » et de « démocratie technologique », mais guère de « régulation » et encore moins de « droit ».

Seulement la réalité des blockchains n'est-elle pas tout à fait celle-là. La technologie est une construction humaine et, si « *Code is Law* », ce sont bien des hommes qui écrivent ce « *Code* ». Partant, ils décident des configurations des chaînes de blocs, de leurs visages. D'ailleurs, il existe des différences entre les blockchains qui s'expliquent par les volontés respectives de ceux qui les construisent — en premier lieu, les blockchains privées se démarquent fortement des blockchains publiques. Certes, le code informatique s'est imposé comme régulateur des blockchains. Ce sont toutefois des individus qui lui donnent ses orientations. Or programmer le code d'une blockchain revient à établir les règles du jeu à l'égard d'un écosystème tout entier. Ce n'est, en définitive, rien d'autre qu'un acte politique.

En même temps, puisque le code sert d'intermédiaire entre ces individus et les conséquences que les blockchains produisent, il devient difficile, si ce n'est impossible, de trouver des responsables en cas de faille dans un système. Mais ce serait justement cela, selon les crypto-anarchistes défenseurs de la seule régulation par le code, qui permettrait aux blockchains d'exprimer tout leur potentiel.

En conséquence, puisque les protocoles cryptographiques sont édictés par des humains, parfois anonymes, qui peuvent être animés par des desseins idéologiques ou autrement politiques, une blockchain fonctionne généralement d'une manière non neutre et non objective. Et les règles de fonctionnement d'une chaîne de blocs dépendent de son degré d'ouverture : plus la chaîne est ouverte, moins la gouvernance est forte, et inversement. Par suite, concernant les blockchains privées, la gouvernance dépend de l'institution qui gère chaque blockchain ; de véritables règlements peuvent déterminer les normes de fonctionnement. Dans une blockchain publique, à l'inverse, la technologie et le code se trouvent nécessairement au cœur du mode de gouvernance. Puisque l'accès est libre, il n'est pas possible, au contraire d'une blockchain privée, que toutes les parties impliquées soient identifiées et liées par un contrat préalable définissant les normes de fonctionnement de la blockchain. Partant, d'aucuns considéreront qu'on pourrait tout réguler dans une blockchain privée et rien dans une blockchain publique.

Cela pose problème, par exemple, concernant la blockchain bitcoin. En effet, dès l'élaboration du protocole, la limite du nombre de transactions par seconde a été fixée à sept. Or, pour faire évoluer cette limite, il faut aboutir à un consensus ; et celui-ci est difficile à obtenir en l'absence de règles de gouvernement claires et prédéfinies. Une limite touchant le bitcoin est donc que cette blockchain pourrait se retrouver bientôt saturée. Que les décisions doivent se prendre par consensus complique l'adoption des « réformes structurelles » nécessaires à l'adaptation du système.

Reste que le droit des blockchains marque une rupture avec le droit moderne tel qu'on l'édicte, l'applique, le pratique, l'enseigne et l'étudie depuis des décennies. Il est peut-être le parangon du « droit postmoderne » appelé à prendre demain le pouvoir. De ce point de vue, le cas des DAO (Decentralized Autonomous Organization, *i.e.* organisation décentralisée autonome) est significatif. L'idée d'autonomie exprime le fait que l'organisation est à elle-même sa propre norme (« auto-nomos »). Les DAO témoignent de la capacité des nouvelles technologies de communication de coordonner différentes parties sans recourir à une instance régulatrice centrale ou surplombante. Leurs règles sont transparentes et immuables puisqu'inscrites dans des blockchains. Le code informatique d'une DAO joue dès lors un double rôle : il exprime les règles de fonctionnement (les codifie) et est le moyen de les appliquer concrètement — grâce à la mise en œuvre programmée de ces règles sous la forme d'instructions logicielles.

Pareilles organisations horizontales et le droit qui les accompagne rompent radicalement avec les modes d'organisation habituels, attachés aux États modernes et supposant une logique verticale. Elles rompent aussi avec l'organisation propre aux sociétés issues de la révolution industrielle, également très verticales, avec à leurs sommets des dirigeants et des actionnaires mus uniquement par la quête de profits. De telles DAO pourraient façonner de nouveaux modèles sociaux, politiques et économiques plus libres, transparents et démocratiques. C'est ce qu'on appelle la « coopétition » (mélange de coopération et de compétition) : l'administration de ces nouvelles structures horizontales est le fait de l'ensemble de leurs membres qui interagissent sans direction et sans structure hiérarchique. Ainsi les nouvelles technologies de l'information ne permettraient-elles pas seulement l'automatisation et la substitution des robots aux humains, mais aussi la coordination entre les hommes et l'autogouvernement de groupes de plus en plus maîtres de leurs activités.

La première expérience en la matière est « The DAO », fonctionnant sur la blockchain Ethereum. Or celle-ci a connu récemment de graves dysfonctionnements qui posent les questions des responsabilités en cas de faille et, par suite, de la viabilité du droit des blockchains.

L'exemple de la gouvernance d'Ethereum et The DAO

The DAO[43] fonctionne sur la base d'un programme informatique qui détermine et publie automatiquement les règles de fonctionnement de l'organisation. Elle ne dispose pas d'organe central de contrôle et il est difficile d'identifier ses utilisateurs. Dans une telle structure, l'anonymat et la gouvernance technologique posent des difficultés qui n'existent guère en présence d'un tiers de confiance ou d'une blockchain privée. Faut-il pour autant laisser le code réguler les rapports entre les acteurs de la chaîne de blocs, donc s'y soumettre quelles qu'en soient les conséquences ? Que faire si une blockchain telle qu'Ethereum est utilisée à des fins illicites ? Vers qui les personnes subissant un

[43] The DAO est un fonds d'investissement décentralisé (fonctionnant avec la blockchain Ethereum et sa cryptomonnaie l'ether) visant à collecter des deniers (*crowfunding*) afin de financer des projets de développement d'objets connectés, notamment des voitures intelligentes. Pour ce faire, les projets soumis sont évalués par les membres de la communauté, qui décident collectivement de les financer ou non, les risques et bénéfices étant répartis entre les participants.

préjudice peuvent-elles se retourner dès lors qu'il n'y a pas d'administrateurs ? Les tribunaux ne sauraient condamner la technologie ni le programme informatique. D'ailleurs, à supposer qu'on identifie de quelconques responsables quelque part dans le monde, cela ne permettrait pas de bloquer les opérations frauduleuses dès lors que celles-ci sont automatisées. De toute manière, les applications sont pour la plupart élaborées à partir de logiciels libres et par des développeurs anonymes. De même, concernant la manipulation des données personnelles, aucune authentification d'un « responsable de traitement », au sens de la loi *Informatique et libertés* française, n'est possible puisque la blockchain est décentralisée et distribuée.

En droit officiel-étatique, un régime de responsabilité semblable à celui applicable aux intermédiaires techniques de l'internet (FAI et hébergeurs) pourrait être envisagé. Mais la question se pose aussi — et peut-être surtout — dans l'ordre juridique parallèle et privé propre à la blockchain. C'est sous cet angle que l'« affaire » ayant impliqué Ethereum et The DAO est lourde d'enseignements. En juin 2016, Ethereum a dû être « reboutée » après qu'un hacker a attaqué The DAO, prélevant 3,6 millions d'ethers investis par les membres de la communauté[44]. Cette attaque a été rendue possible par une erreur de codage : une faille dans le code du « smart contract » permettant à The DAO de fonctionner. La création d'un « nouvel » Ethereum, en procédant à un retour en arrière et à la construction d'un registre parallèle, a finalement permis de réattribuer les ethers détournés à leurs titulaires légitimes.

Mais cette manoeuvre a fait couler beaucoup d'encre : les crypto-anarchistes selon lesquels « *Code is Law* » même lorsque cela emporte des conséquences déplorables, et pour qui le code logiciel serait une loi qui ne saurait connaître d'exception y compris dans un cas extrême, s'opposent aux partisans d'une intervention humaine visant à rétablir la situation légitime en modifiant le code. D'ailleurs, certains utilisateurs d'Ethereum continuent aujourd'hui de recourir à l'ancienne chaîne de blocs qui, pour eux, serait la seule acceptable, quels que soient ses travers. Cela génère une grande confusion et une hypervolatilité de la cryptomonnaie. Et il est significatif que l'auteur de l'attaque a menacé de procès quiconque tenterait de récupérer les ethers dérobés, convaincu que, dans l'univers cryptographique des blockchains, les seules normes applicables aux relations humaines et sociales seraient celles générées par les logiciels et par les algorithmes. Il aurait donc agi en toute « légalité ».

À mille lieues du principe ancestral qui veut que quiconque cause un dommage à autrui est obligé de le réparer, les partisans du droit technologique estiment qu'il n'y aurait guère de vol dès lors que la porte d'entrée n'a pas été verrouillée. En effet, le hacker a respecté le code (informatique) de The DAO. Dans l'ordre normatif propre à cette technologie, il n'a donc commis aucune infraction et les ethers en sa possession sont devenus sa propriété. Telle est la position défendue par les promoteurs d'un code informatique tout puissant, y compris juridiquement.

En outre, le système étant décentralisé, il était difficile de réagir rapidement et efficacement. Aucun organe central n'était là pour décider dans l'urgence de la réponse à apporter à la situation. Il revenait aux « mineurs » de voter en faveur de la solution à appliquer. En décidant de modifier le code de la blockchain afin de recréer les ethers détournés, de procéder à un « fork », c'est-à-dire à une réécriture de la blockchain, ils ont enfreint les principes fondamentaux des chaînes de blocs que sont l'immuabilité du code et des données et l'application automatique des règles. Ils ont rétabli la situation légitime et empêché qu'une action dolosive de grande ampleur demeure sans réponse. Mais ils ont aussi instillé un climat d'insécurité juridique dans le monde des blockchains, car, dès lors que la réécriture des blocs a été permise une fois, on imagine que des communautés de « mineurs » pourraient réitérer cette opération, au détriment de ceux dont les transactions seraient annulées. Ainsi la confiance, pourtant au cœur du fonctionnement des blockchains, a-t-elle été grandement malmenée.

[44] Cela correspond à plus de 10 % du montant total de la cryptomonnaie en circulation, équivalents à 60 millions de dollars.

Mais l'aurait-elle moins été si les « mineurs » avaient décidé de laisser le hacker s'évaporer dans la nature avec les ethers subtilisés ?

Cet épisode, montrant que les blockchains ne sauraient être parfaitement fiables, que les risques de biais ou de failles de sécurité, notamment au niveau des règles de gouvernance du système, sont réels, a provoqué une crise profonde parmi la communauté blockchain — d'autant plus qu'il ne s'agit pas du seul cas de détournement de cryptomonnaie[45]. Il a placé la question de la gouvernance et du droit des chaînes de blocs au cœur des discussions. Peut-être la limite des blockchains réside-t-elle justement dans cette gouvernance et dans ce droit, de telle sorte que, bien que cela malmène l'esprit originel de la technologie, les chaînes de blocs privées présenteraient plus de garanties que les chaînes de blocs publiques. Les problèmes soulevés par l' « affaire » The DAO-Ethereum n'auraient pas existé dans le cas d'une blockchain privée puisque la sécurité, les contrôles et les décisions auraient été le fait d'un organe central engageant sa responsabilité et intervenant arbitrairement. En revanche, sans contrôle du code par un responsable précisément identifié et possédant un pouvoir normatif fort, clair et transparent, toute chaîne de blocs semble potentiellement vulnérable. Et, si cette vulnérabilité est plus juridique et politique que technologique, dans le cas d'une blockchain publique droit, politique et technologie se confondent, rendant la situation ô combien délicate à gérer.

L'autorégulation a donc montré ses limites, posant la question d'une régulation plus institutionnalisée et organisée *ex ante*. Le mode de gouvernance des blockchains publiques, à base d'immutabilité, de formalisme et d'automatisme, devient un obstacle dès lors que surgissent des imprévus et des circonstances complexes appelant des réponses adaptées et cliniques. Il semble dès lors nécessaire de réfléchir à de nouveaux moyens d'assurer la confiance des acteurs des blockchains au-delà des protocoles technologiques — des moyens plus « juridiques ». Mais sera-t-il possible d'éviter le conflit entre les partisans de la régulation par le code, par la « *RegTech* » (pour « *Regulatory Technology* »), et les promoteurs d'un droit des blockchains ouvert à la souplesse humaine et non abandonné à la rigidité technologique ?

Conclusion

Décentralisées et globalisées, sans centre et sans frontières, les blockchains posent des difficultés en termes de droit applicable aux transactions, de responsable en cas de faute et de légalité des pratiques. Il n'y a pas de blockchain hors la loi ; mais il faut déterminer la loi applicable, question qui se pose notamment concernant les blockchains publiques, lesquelles s'appuient sur un ensemble de « mineurs » pouvant se situer partout sur la planète. Il est difficile de contraindre juridiquement des développeurs informatiques et des fournisseurs de services situés aux quatre coins du monde. Seuls un cadre international et des normes à portée mondiale auraient du sens. Pourtant, les droits restent largement nationaux.

Sous l'angle du droit officiel-étatique, il n'existe guère, actuellement, de droit spécial des blockchains. Il est difficile pour les autorités législatives d'intervenir à l'égard d'une technologie naissante, en gestation, mouvante et dont les potentialités et les limites restent mal comprises. Aussi les

[45] Diverses ICO (*Initial Coin Offering*, des levées de fonds en cryptomonnaie afin de financer des projets) ont également été l'objet d'attaques pirates. Tel a été le cas, par exemple, de CoinDash, le 17 juillet 2017. Quelqu'un s'en est pris au site web de la société, au moment du lancement de l'ICO, parvenant à recueillir avec sa propre adresse Ethereum les fonds que les intéressés étaient censés verser sur l'adresse Ethereum de CoinDash. L'équivalent de huit millions de dollars ont ainsi été subtilisés.

institutions de l'Union européenne, si elles s'intéressent de près aux blockchains, préconisent-elles de ne pas les réglementer avant qu'émergent des modèles d'exploitation pérennes. Le danger serait en effet de légiférer trop vite et, parce que trop vite, de légiférer mal. Il semble important de connaître les principaux cas d'usage des blockchains avant d'intervenir, cela afin d'encadrer par le droit officiel-étatique ce qui mérite de l'être sans étouffer les marchés émergents — d'autant plus que, concernant des technologies transnationales, ces marchés sont nécessairement mondiaux, impliquant une concurrence féroce entre États, un dumping réglementaire sans merci. À trop vouloir réglementer et prévoir tous les risques et tous les cas de figure, le danger est d'en venir à décourager les entreprises blockchain à s'installer et/ou à se développer sur le territoire national. Les chaînes de blocs devraient constituer un important facteur de compétitivité des économies nationales durant les prochaines années. C'est pourquoi il importe, en France par exemple, de donner la possibilité aux start-up les maîtrisant de prendre de l'avance dans la compétition mondiale qui débute.

Toutefois, le flou juridique est aussi un frein pour nombre de start-up qui n'osent pas lancer de services originaux tant que le cadre réglementaire appelé à s'y appliquer n'est pas précisément arrêté. Notamment dans le secteur financier, des entrepreneurs hésitent à développer leurs *business models* parce qu'ils ne savent pas si ceux-ci seront ou non jugés illégaux par les autorités compétentes.

Face à ces enjeux — n'intervenir ni trop en amont ni trop en aval —, une solution réside dans les « bacs à sable réglementaires » (« *regulatory sandbox* »). Ceux-ci permettent aux entreprises souhaitant offrir des services liés aux blockchains d'être protégés contre tout risque de contrevenir à la loi en vigueur ou à venir. Les start-up et les acteurs de la société civile peuvent ainsi innover dans un climat de confiance propice au déploiement des blockchains — cela au service d'intérêts particuliers mais aussi de l'intérêt général et même parfois d'une meilleure protection de certains droits et libertés fondamentaux. En renforçant la sécurité juridique, ces « bacs à sable réglementaires » donnent à l'innovation sa chance tout en auditant en parallèle les ressources et travers du droit positif existant[46]. Ils permettent d'éviter de légiférer trop tôt à l'égard de technologies très évolutives et de prendre le pouls des projets en cours, de leurs éventuels défauts à corriger par le droit et de leurs potentiels apports à soutenir par le droit — ou par l'absence de droit. S'ouvre ainsi la voie, y compris dans l'ordre étatique, des modes de régulation plus ouverts et collaboratifs, plus horizontaux et moins verticaux que les blockchains appellent.

[46] En juin 2015, l'État de New York a lancé BitLicense, un système de licence bancaire particulier pour les utilisateurs des blockchains. Or cette licence a eu pour effet indésirable d'entraîner le départ hors de l'État de nombreuses entreprises innovantes, beaucoup s'installant en Suisse. Sur la vingtaine d'entreprises qui ont accepté de se soumettre à cette licence, une seule pour l'instant l'a obtenue. Les autres se retrouvent dans une situation d'incertitude juridique générant d'importants coûts financiers liés aux frais d'avocats. Au Royaume-Uni, à l'inverse, la Financial Conduct Authority a créé un « bac à sable réglementaire » où les start-up souhaitant proposer des services liés aux cryptomonnaies peuvent les tester sans risquer de commettre des infractions.