

Laboratoire D@NTE

Blockchain, propriété intellectuelle et mode



Marie Malaurie-Vignal, professeure à l'Université de Versailles Saint-Quentin-en-Yvelines (Paris-Saclay, sous l'égide du Laboratoire D@NTE – Droit des Affaires et Nouvelles Technologies) a organisé le 17 mai dernier, avec le concours de l'Institut Droit Éthique et Patrimoine (Université Paris-Saclay) et l'Institut français de la mode, un colloque intitulé « Blockchain, propriété intellectuelle et mode ». Objectif : déterminer la réalité juridique des bienfaits apportés par la blockchain dans le milieu de la mode aujourd'hui. Présentation pratique et table ronde ont permis de mieux cerner les enjeux et défis suscités par cette nouvelle technologie.

« La blockchain connaît un engouement réel, notamment dans le domaine de la mode, car cette technologie pourrait faciliter la preuve de l'antériorité des droits, permettrait de prouver les droits sur leurs créations et assurerait la traçabilité des transactions et la réalisation de "smart contracts" », indique le laboratoire D@NTE dans un document de présentation du colloque. L'intérêt principal de cette technologie réside dans le fait que son modèle est ouvertement décentralisé, en-dehors de tout cadre légal général et de toute institution publique. Pour cette raison, elle suscite la peur chez certains juristes dont la plus grande crainte est que l'on ait plus besoin d'eux.

Afin de permettre aux professionnels du droit de comprendre davantage le fonctionnement de la blockchain, et de cerner ses atouts mais aussi ses inconvénients, la professeure Marie Malaurie-Vignal a organisé un grand débat réunissant experts en nouvelles technologies, avocats spécialistes en droit de la propriété intellectuelle, magistrats... Le colloque a consisté en une présentation pratique de cette technologie, et du *smart contract*. Se sont exprimés, outre le professeur Malaurie-Vignal, Arnaud Fontaine, directeur des opérations techniques chez Ubisoft ; Mélanie Clément-Fontaine, maître de conférences en droit privé et directrice du laboratoire D@NTE. S'est ensuivie une table ronde « *Preuve et blockchain* », présidée par Guy Canivet, Premier président honoraire de la Cour de Cassation, ancien membre du Conseil constitutionnel, et qui a réuni Sophie Canas, conseiller référendaire à la Cour de cassation ; Isabelle Gavanon, avocate associée du cabinet Fidal et spécialiste des nouvelles technologies ; Fabienne Jault-Seseke, professeure à l'Université de Versailles Saint-Quentin-en-Yvelines ; Laurence Joly, directrice de l'Observatoire de la propriété intellectuelle (INPI) ; Stéphanie Legrand, avocate associée du cabinet Legrand Lesage-Catek Gaultier ; et Véronique Magnier, professeure à l'Université Paris XI, directrice de l'Institut Droit Éthique et Patrimoine (IDEP). Le directeur général de l'Institut français de la mode, Dominique Jacomet, a procédé à la clôture des travaux.



Stéphanie Legrand, Fabienne Jault-Seseke, Véronique Magnier, Guy Canivet et Laurence Joly

LE FONCTIONNEMENT DE LA BLOCKCHAIN

Arnaud Fontaine, directeur des opérations techniques chez Ubisoft, s'est chargé dans son allocution d'expliquer concrètement, via une présentation pratique, le fonctionnement de la technologie blockchain dans ses grands principes.

Les travaux sur la blockchain ont débuté après la crise financière de 2008, a-t-il d'abord expliqué. Les premiers résultats sont apparus en 2009 et 2010. « On a utilisé un grand nombre d'éléments techniques, informatiques, et mathématiques qui étaient déjà très connus, et on en a fait quelque chose de très innovant ». De multiples technologies blockchain différentes ont surgi : le *bitcoin*, mais aussi une technologie disruptive comme Ethereum (2014), qui a notamment fait naître le *smart contract*.

En outre, d'autres types de technologies reposant sur le même principe de registre que Bitcoin et Ethereum ont été élaborées, mais sur la base de graphes. Deux exemples : *IoTa*, créé pour répondre à des problématiques concernant l'Internet des objets ; et *Hash Graph*.

« La blockchain est très attachée à une problématique liée à la monnaie », a poursuivi Arnaud Fontaine. Le but étant de trouver un moyen de pouvoir faire une transaction, de pair à pair, sans passer par un intermédiaire centralisé tel que la banque. Avec la blockchain, on se trouve devant un système

distribué où l'intégralité de la validation des transactions va être faite à base d'algorithmes et de consensus. « Et de manière générale, ça se fait de manière totalement transparente. L'activité est visible par tous. » a-t-il précisé.

En outre, une fois qu'une action a été inscrite, on ne peut plus l'effacer. La blockchain est totalement immuable.

Il existe plusieurs types de blockchains. Certaines sont dites publiques (Bitcoin, Ethereum, Ripple...). Le fonctionnement de ces dernières se fait de manière consensuelle. Ainsi, pour être inscrite dans ce type de blockchain, la transaction doit être validée par 51 % des mineurs. Certaines blockchains sont, elles, semi-privées. Elles sont utilisées dans des consortiums. Disney, par exemple, a créé une blockchain entre ses différents partenaires. Et enfin, il existe des blockchain complètement privées (utilisée au sein d'une entreprise).

Dans une blockchain, toutes les transactions arrivent dans un « *grand livre des comptes* », un registre distribué à tous les participants qui peuvent en avoir une copie. On parle alors de DLT (*Distributed Ledger Technology*), c'est-à-dire de technologie de registre distribué.

Le fonctionnement général de la blockchain est basé sur des transactions, et « il faut bien comprendre que le DLT est totalement aveugle au monde extérieur », a ajouté

Arnaud Fontaine. La transaction se fait entre deux adresses publiques au moyen de la cryptographie asymétrique. Chaque participant a un couple de clés, avec comme principe une clé privée qu'on garde chez soi, et une clé publique : « *ce qui est en crypté avec l'une, ne peut être décrypté qu'avec l'autre* ». Ainsi, n'importe qui peut utiliser une clé publique pour faire une transaction, envoyer quelque chose sur la blockchain, mais seule la clé privée peut l'ouvrir. Cependant, il faut bien comprendre qu'il n'est pas question « d'identité » ici. En effet, rien ne garantit que c'est la bonne personne qui ouvre la transaction, on sait juste que c'est elle qui détient la clé. « *On est tellement loin de l'identité, que sur les systèmes de blockchain DLT la plupart des utilisateurs ont des dizaines voire des centaines de comptes différents. Donc il est très difficile de faire le lien avec l'identité de la personne physique* ».

On va ensuite insérer ces transactions dans un bloc, et on va mettre en œuvre un certain nombre de stratégies différentes pour savoir quelle transaction dépend de l'autre. Ensuite, on va valider l'ensemble des transactions de ce bloc, et enfin certifier ce dernier. Il s'agit là du travail de minage (pour rappel, le minage est le procédé par lequel les transactions sont sécurisées. À cette fin, les mineurs effectuent avec leur matériel informatique des calculs mathématiques).

Une fois qu'on a certifié ce bloc de transactions valide, il existe un certain nombre d'autres techniques qui permettent de l'intégrer de manière définitive et immuable dans le registre. Si quelqu'un voulait modifier quelques transactions que ce soit, il va devoir reconstruire l'intégralité du registre, et faire accepter à tout le réseau, que ce nouveau registre est valide.

L'intervenant a ensuite fait un aparté sur la blockchain Ethereum. Cette blockchain apparue en 2014, et dont la monnaie est l'ether, a apporté deux avancées majeures. La principale étant le *smart contract*. Il s'agit d'un programme informatique conçu pour faire de l'auto-validation de transactions. « *Si telle transaction survient alors ça déclenchera telle autre transaction. Par exemple, si l'avion est en retard alors je serais automatiquement dédommagé* », a expliqué le directeur des opérations techniques chez Ubisoft.

« *La blockchain est totalement aveugle* », a-t-il poursuivi, « *elle ne connaît pas le monde extérieur, mais seulement les transactions, et les clés des comptes entre lesquels se font ces dernières* ». Or, avec les *smart contract*, il y a l'introduction de données extérieures. Par exemple, le fait que l'avion soit en retard ou non n'est pas contenu dans le programme. Dans le langage informatique, ces données

externes sont appelées « *oracles* ». En fonction de telle source de donnée extérieure, quelqu'un (une personne physique) devra évaluer et décider qu'il s'agit bien d'une source fiable.

Pour reprendre l'exemple de l'avion, dans le *smart contract*, les parties se mettent d'accord, par exemple, pour que la source de données extérieures à laquelle ils vont se référer soit le contrôle aérien (qui n'a aucune raison de tricher sur l'heure d'arrivée de l'avion).

Le deuxième apport d'Ethereum a été le « *token* » (ou jeton). Il s'agit d'une pseudo monnaie virtuelle « *au-dessus* » du bitcoin ou de l'ether. Elle est utilisée par les entreprises qui veulent financer leur développement ou projet et qui baptisent ces « *tokens* » de leur propre nom.

Cette nouveauté a fait surgir un système de *crowdfunding* d'un autre genre, qu'on a appelé ICO (*Initial Coin Offering* en allusion à l'IPO ou introduction en Bourse). Les sociétés émettent des « *tokens* » en déclarant qu'avec ces derniers, on peut consommer les services qu'elles proposent. Elles en pré vendent quelques-uns sur le Net à un tarif préférentiel. Ce mécanisme permet aux plus chanceuses de lever des fonds gigantesques en un temps record.

Dans la continuité des propos d'Arnaud Fontaine, Mélanie Clément-Fontaine, maître de conférences en droit privé et directrice du laboratoire D@NTE, a centré son propos sur la blockchain et le contrat, et notamment sur les spécificités du *smart contract*.

BLOCKCHAIN ET CONTRAT

« *Le smart contract est un programme autonome qui exécute automatiquement les conditions et les termes d'un contrat sans nécessiter l'intervention humaine, une fois que l'opération est démarrée* » a-t-elle débuté.

Par exemple, en ce qui concerne la propriété intellectuelle, le téléchargement d'un fichier contenant un dessin et modèle, va entraîner automatiquement le paiement.

Mais que dit le droit des contrats des *smart contracts* ?

Pour la professeure, il faut, au préalable, se poser deux questions : le *smart contract* est-il assimilable à un contrat ? Et quel effet juridique peut-on lui reconnaître ?

Concernant la première question, la réponse est non. En France, le « *contrat intelligent* » n'est pas un contrat au sens juridique du terme [cf. article 113 du Code civil], a-t-elle rappelé. Pourquoi ? Car la rencontre des consentements porte sur une opération, par exemple le paiement en contrepartie de l'accès à un fichier contenant un dessin et modèle. Le programme, lui, n'en est que la conséquence. Il n'est pas à l'origine de

l'accord, mais l'inverse. Le *smart contract* ne peut d'ailleurs être programmé que pour exécuter certaines clauses spécifiques du contrat. Les clauses déterminant l'usage qui peut être fait de ce dessin et modèle, l'étendue géographique, etc., ne seront pas nécessairement incrémentées dans le *smart contract*.

« *En réalité, il existe d'abord un contrat juridique, puis on utilise le smart contract comme modalité de mise en œuvre du contrat. Et en application de l'article 1128 du Code civil, le consentement est apprécié au niveau du contrat juridique et non du smart contract* », a-t-elle précisé. Ce qui signifie qu'il n'est pas nécessaire d'être expert en informatique pour comprendre à quoi on s'engage.

Le *smart contract* n'est donc pas un contrat. Il reste que pour la professeure, il y a de nombreux avantages à y avoir recours dans une blockchain pour la mise en œuvre d'obligations contractuelles. D'abord, la place du *smart contract* dans une blockchain offre la garantie que les termes du contrat ne pourront être modifiés. Ensuite, celui-ci permet de réduire les coûts de vérification d'exécution d'arbitrage et de fraude.

Quels effets juridiques peut-on ensuite reconnaître au *smart contract* ?

« *Le droit est muet sur ce point* », a reconnu Mélanie Clément-Fontaine. Certes, la blockchain a été introduite en droit français par l'ordonnance de 2016 relative aux bons de caisse, et celle de 2017 relative à un dispositif d'enregistrement électronique partagé pour la représentation et transaction de titres financiers, « *mais s'agissant du smart contract, beaucoup reste à faire* ».

De nombreuses difficultés restent en effet à résoudre.

D'abord, le *smart contract* n'est qu'un programme informatique qui n'interprète pas ce qui se passe dans le monde physique. Dans le domaine de la propriété intellectuelle, il ne permet pas ainsi de déterminer si l'auteur du dessin et modèle a bien rempli les exigences énoncées par son co-contractant. En effet, les conditions qui déclenchent l'exécution d'une obligation sont plus ou moins faciles à inscrire dans ce dernier. Le *smart contract*, on l'a dit, permet le déclenchement d'une transaction à partir de données extérieures (oracle). Ces informations venues de l'extérieur déclenchent l'opération. Mais que se passe-t-il si ces informations sont en réalité erronées ? Si le titre de propriété intellectuelle inscrit dans le fichier n'est pas valable par exemple ? Qui est alors responsable ? Est-ce l'oracle ? Faut-il accepter de toute façon la transaction même si la donnée extérieure est erronée ?, s'est interrogée

l'intervenante. « Dans tous les cas, que la donnée soit fausse ou vraie dans la vie réelle, l'opération se réalisera inexorablement. Par conséquent, cette situation ouvre-t-elle le droit à une action en responsabilité ? Et de qui ? »

Autre point à résoudre : le smart contract est déconnecté du droit des obligations. Cela a des incidences significatives. Par exemple, « la rétractation ne saura possible que si elle est incluse dans le programme, sinon cela ne sera pas possible, et ce, peu importe ce que dit la loi ».

En outre, a rappelé Mélanie Clément-Fontaine, la force majeure ou l'imprévision sont des concepts inconnus du smart contract. Sauf si on prévoit de multiples oracles sur les cas de forces majeures ou d'imprévision. Sinon « l'opération se déroulera comme prévu et l'inexécution d'une opération se transformera en inexécution forcée du débiteur ». Enfin, la résolution est un concept également inconnu du smart contract. En effet, juridiquement, la résolution annule rétroactivement un contrat, or le « smart contract, lui, ne peut disparaître de la blockchain puisque celle-ci est immuable ».

En conclusion, le smart contract pose à l'heure actuelle de nombreuses questions de droit non résolues. Cependant, si on est en présence d'une seule condition, d'une seule transaction, le smart contract permet de faciliter et de sécuriser l'exécution des contrats de propriété intellectuelle, en particulier dans un marché mondialisé. « Aussi il a tout son intérêt dans l'univers de la mode », a-t-elle conclu.

UTILISATION DE LA BLOCKCHAIN DANS LE MILIEU DE LA MODE

Marie Malaurie-Vignal, professeure à l'Université de Versailles Saint-Quentin-en-Yvelines a, elle, expliqué comment les professionnels font usage de cette technologie blockchain dans le milieu de la mode, mais également quels sont ses atouts et ses inconvénients.

« Un descriptif de l'œuvre (robe, modèle de vêtement) est hashé avec le Sha-256, puis l'empreinte va être inscrite sur la blockchain avec une transaction », a-t-elle expliqué. « Ce qui est enregistré dans la blockchain, ce n'est ni une donnée, ni un document original, mais l'empreinte haschée comportant une partie de l'empreinte numérique du bloc précédent. C'est la raison pour laquelle on parle de blocs de chaîne, car l'ensemble des transactions haschées s'inscrivent en blocs liés les uns aux autres ».

Puis, la transaction est ensuite partagée entre les « nœuds du réseau », pour être validée par des « mineurs ». Pour valider la transaction, ces derniers doivent résoudre des opérations mathématiques sur des ordinateurs très



puissants. Ce travail de résolution, via des algorithmes, est qualifié de « proof of work ». Le premier mineur qui réussit la résolution du problème mathématique est rémunéré en cryptomonnaie. Puis, il propose la validation aux autres mineurs.

A. ATOUTS DE LA BLOCKCHAIN ?

La blockchain permet de prouver qu'à l'atteinte de 51 % des mineurs, la transaction a été ancrée sur la blockchain. Cela joue donc un rôle d'horodatage.

La blockchain permet également de protéger le secret des créations. Car le hash est conçu pour être une fonction à sens unique. C'est-à-dire que c'est une fonction impossible à inverser. Si tout le monde peut avoir accès à une blockchain publique, « il est quasi impossible de reconstituer le document qui a été hashé et inscrit sur la blockchain, ce qui garantit le secret des informations inscrites ». Pour Marie Malaurie-Vignal, la blockchain permet aussi de prouver la titularité des droits sur une création. En cas de litiges devant un juge, celui qui revendique son droit aura en effet à refaire devant un expert le hashage du document qui contient sa création. Celui-ci sera comparé au hash qui a été inscrit dans la blockchain. Si le hashage correspond, alors on pourra présumer qu'il est l'auteur de la création. Cependant, et il s'agit d'une subtilité essentielle, celui qui inscrit une œuvre sur une blockchain, via une empreinte numérique, peut ne pas être l'auteur. De plus, la création inscrite sur la blockchain, peut être contrefaisante ; ou peut ne pas être originale. « La blockchain ne donne aucune indication sur la nature de l'œuvre, et n'assure aucune garantie, d'un droit de propriété intellectuelle sur l'œuvre revendiquée. »

Enfin, la blockchain facilite l'exécution automatique des contrats, en témoignent les fameux smart contract.

B. RISQUES ET INCERTITUDES LIÉS À LA BLOCKCHAIN ?

Concernant la traçabilité, les maisons de mode peuvent tout inscrire sur la blockchain, de la création jusqu'à l'achat final par le client. Celle-ci serait donc une sorte de passeport numérique garantissant l'authenticité du bien.

Cependant, pour le professeur Malaurie-Vignal, il y a toujours le risque qu'une transaction ne soit pas inscrite sur la blockchain pour une raison ou pour une autre. Si par exemple, le vêtement est vendu à un grossiste situé en Inde, puis revendu à un autre en Italie, puis ensuite vendu à un distributeur français... et qu'un des intermédiaires n'a pas accès ou de ne se réfère pas à la technologie blockchain, il ne va pas inscrire son opération. Il y aura donc rupture dans la chaîne des blocs. Or, « il est nécessaire que la tête de réseau puisse maîtriser tout son réseau pour que la blockchain puisse être ce vrai passeport numérique et garantir jusqu'à l'acte final d'achat l'authenticité du produit ».

Et qu'en est-il du coût ? La blockchain est présentée comme un outil qui « démocratiserait » le droit de la propriété intellectuelle, le coût d'inscription sur la blockchain étant modique. Le montant de rémunération des mineurs est en effet très faible à l'heure actuelle, mais cette rémunération s'évalue en fonction de l'offre et de la demande. Et le cours des bitcoins est extrêmement variable. En outre, on peut toujours envisager qu'advienne un jour où les mineurs s'entendent pour n'accepter de miner rapidement que les transactions bien rémunérées, et de miner avec beaucoup de retard celles qui ne le sont pas. Par conséquent, il n'est pas certain que le coût de la blockchain reste toujours modeste.

Cette technologie récente est-elle fiable ? Quid du piratage et de l'altération des données ?

Le risque de piratage, selon le professeur, n'est pas un vrai risque. Et pourtant, tout le monde a entendu parler de détournement de bitcoins. Mais, il ne servirait à rien de pirater des dessins ou des modèles, car le hash est une fonction à sens unique, donc impossible à inverser : « Il est donc

quasi impossible de reconstituer le document qui a été hashé et mis sur la blockchain ». Le vrai risque est donc celui de l'altération des données.

« La blockchain est réputée partout comme étant infalsifiable ». Car pour être inscrite dans la blockchain, la transaction doit être validée par 51 % des mineurs. « En conséquence, il est quasi impossible de modifier le contenu des blockchain publiques, car il faudrait détenir 51 % de la puissance de calcul du minage », a-t-elle argué. Cependant, cela suppose que le mineur qui valide et conserve les transactions soit toujours animé des meilleures intentions. Or, ce n'est pas toujours le cas... N'existe-t-il pas en effet un risque de collusion pour modifier le contenu de la blockchain ? Ainsi, en 2016, en raison d'un détournement d'Ethereum de cryptomonnaie, on a envisagé de revenir en arrière, en effaçant une journée de transactions. Finalement, on a réécrit une nouvelle blockchain.

En outre, a-t-elle expliqué, théoriquement dans le monde, n'importe qui peut être mineur, mais en réalité ces derniers sont géographiquement concentrés dans certains endroits de la planète, dans des États où l'électricité est peu chère (Islande, Chine, notamment). Ils sont regroupés dans d'immenses hangars de minage, constitués en coopératives (fermes de mineurs). Il faut en effet des ordinateurs très puissants pour faire du minage, « le risque de collusion ne relève donc pas que de la science-fiction ». Ainsi, en 2004, on a découvert qu'une ferme de mineurs qui concentrait 42 % de la puissance de calcul de réseau de bitcoin.

C. COMMENT RÉDUIRE CES RISQUES ?

Cependant, ces risques ne se sont pas encore survenus et peuvent même être amoindris. En effet, une attaque sur la blockchain par des mineurs pourrait faire chuter la valeur de la cryptomonnaie sur cette même blockchain. C'est pourquoi les mineurs n'ont aucun intérêt à attaquer cette dernière, sauf s'ils travaillent pour le compte d'entreprises concurrentes ou pour des États !

Pour réduire les risques liés à l'altération des données, d'autres systèmes de validation de la blockchain que le minage sont actuellement à l'étude. Plutôt que de passer par la « *proof of work* » on passerait par la « *proof of stake* », ou même par une validation par tirage au sort (pour éviter le risque de collusion des mineurs).

Quant à la pérennité de la blockchain, pour l'intervenante, il s'agit d'une technologie, or « *tout change, tout passe* ». On peut donc légitimement se demander si la blockchain sera pérenne. D'autant plus qu'il s'agit d'une technologie qui repose sur la confiance que les opérateurs ont dans ce système. Or, « *la confiance est fragile* », surtout si des failles informatiques surviennent. En outre, la blockchain est très énergivore, l'opération



de minage supposant des ordinateurs extrêmement puissants. Des scientifiques réfléchissent en ce moment à de nouvelles technologies plus respectueuses de la planète, fondées sur le mécanisme de la physique quantique. « *Celles-ci permettront une cryptographie quantique beaucoup moins gourmande en énergie* », a assuré Marie Malaurie-Vignal.

D. BLOCKCHAIN ET UBÉRISATION DE LA PROPRIÉTÉ INTELLECTUELLE

Malgré tous ces risques et incertitudes, la blockchain connaît un engouement réel, et ce, dans tous les domaines. Mais cette technologie suscite également des peurs chez les professionnels du droit, dont la plus grande crainte est celle d'être évincés, a-t-elle rappelé.

La blockchain repose en effet sur une communauté sans intermédiaires, le risque étant l'ubérisation de la profession : disparition des offices notariaux, de l'INPI, des tiers de confiance ? Marie Malaurie-Vignal s'est ainsi référée à la « *formule magique* » du professeur de droit américain Lawrence Lessig, « *Code is law* ». Une sentence qui signifie que les informations codées ont désormais force de loi, et qu'aucun cadre juridique n'est nécessaire.

Dans son article « *Code is law – On liberty in cyberspace* », Lawrence Lessig écrit en effet : « *Ce régulateur, c'est le code : le logiciel et le matériel qui font du cyberspace ce qu'il est. Ce code, ou cette architecture, définit la manière dont nous vivons le cyberspace. Il détermine s'il est facile ou non de protéger sa vie privée, ou de censurer la parole. Il détermine si l'accès à l'information est global ou sectorisé. Il a un impact sur qui peut voir quoi, ou sur ce qui est surveillé. Lorsqu'on commence à comprendre la nature de ce code, on se rend compte que, d'une myriade de manières, le code du cyberspace régule.* »

On pourrait croire que le professeur Lessig est un « *libertarien* », a expliqué l'intervenante. Or, en réalité ce n'est pas du tout le cas. Dans cet article, il a présenté cette absence de régulation, comme un simple état de fait, et a dénoncé le pouvoir des

cyber entreprises comme une menace pour les libertés individuelles. Il ne souhaite nullement une dérégulation, mais au contraire que les citoyens puissent avoir un rôle à jouer dans la façon dont est architecturé le cyberspace : « *Ce n'est pas entre régulation et absence de régulation que nous avons à choisir. Le code régule. Il implémente – ou non – un certain nombre de valeurs. Il garantit certaines libertés, ou les empêche. Il protège la vie privée, ou promeut la surveillance. Des gens décident comment le code va se comporter. Des gens l'écrivent. La question n'est donc pas de savoir qui décidera de la manière dont le cyberspace est régulé : ce seront les codeurs. La seule question est de savoir si nous aurons collectivement un rôle dans leur choix – et donc dans la manière dont ces valeurs sont garanties – ou si nous laisserons aux codeurs le soin de choisir nos valeurs à notre place.* », écrit-il en effet. « *Si nous ne le faisons pas, ou si nous n'apprenons pas à le faire, la pertinence de notre tradition constitutionnelle va décliner.* » conclut-il.

La crainte des juristes d'être supplantés doit être minimisée, car le droit a toute sa place dans l'écosystème moderne, ne serait-ce que pour garantir les libertés individuelles.

En outre, certains droits des pays nécessitent un enregistrement auprès d'offices physiques, « *donc tant que ces obligations sont dans les textes, il n'y aura pas de disparition de ces offices d'enregistrement* ». Quant aux offices notariaux, rappelons qu'en France, la preuve par blockchain n'est pas considérée comme une preuve authentique.

En conclusion, a déclaré le professeur Malaurie-Vignal, la caractéristique de toute innovation est d'être en constante évolution, « *et je ne doute pas qu'avec le temps, la technologie blockchain évoluera pour faire face aux défis énergétiques, technologiques qui l'attendent* ».

Maria-Angélica Bailly

2018-3912