

La pérennité des preuves *blockchain* et ses implications dans le domaine de la propriété intellectuelle

The endurance of blockchain evidence and its implications in the field of intellectual property

Fernanda Sabrinni-Chatelard¹, Erika Dewald², Laurence Joly³

¹ Laboratoire ESPI2R, Groupe ESPI, France, f.chatelard@groupe-espi.fr

² Cabinet LPA-CGR avocats, France, edewald@lpacgr.com

³ Diag n'Grow et la Fabrique du futur, France, laurence.joly@diagngrow.com

RÉSUMÉ. La question de la pérennité de la preuve est particulièrement importante dans le domaine de la propriété intellectuelle. La *blockchain* avec toutes ses évolutions aurait un rôle à jouer dans ce domaine mais à condition de l'encadrer techniquement et juridiquement. Dans ce sens, plusieurs questions se posent comme celle de la sécurité, la transparence, la traçabilité, la confidentialité. Sur tous ces points, il convient de rappeler le rôle fondamental des tiers de confiance. En France la *blockchain* est actuellement reconnue, au même titre que toutes les autres preuves numériques, comme un commencement de preuve par écrit. En revanche dans d'autres endroits du Monde elle fait l'objet d'une reconnaissance plus avancée.

ABSTRACT. Endurance of evidence is particularly important in the field of intellectual property. Blockchain, with all its evolutions, could have a role to play in this field, but only if it is technically and legally regulated. In this sense, several concerns arise such as that of security, transparency, traceability and confidentiality. When it comes to all of these concerns, it is important to remember the fundamental function of trusted third parties. In France, blockchain is recognized, like all other digital proofs, as *prima facie* evidence in writing. In other parts of the world however, it is even more widely recognized.

MOTS-CLÉS. *Blockchain*, Droit d'auteur, Fiabilité, Gouvernance, NFT, Pérennité, Preuve, Propriété intellectuelle, Sécurité, Tiers de confiance.

KEYWORDS. Blockchain, Copyright, Trust, Governance, NFT, Endurance, Evidence, Intellectual property, Security, Trusted third party.

1. Introduction : définition et atouts de la preuve *blockchain*

Une *blockchain* est une technologie de stockage décentralisé des données dans des blocs reliés les uns aux autres et visible par tous les utilisateurs [GUR 18]. Par extension, on désigne également par *blockchain*, 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. Les *blockchains* possèdent un potentiel disruptif qui pourrait contribuer à renouveler le droit, notamment certains droits spécifiques, tout particulièrement la propriété intellectuelle.

Il faut distinguer les *blockchains* publiques des *blockchains* privées [SIX 21]. Selon [BAR 18], « 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 ».

A une époque où la preuve n'a jamais été aussi fragile alors que les moyens de l'apporter ne cessent de se multiplier, on pourrait ainsi se demander si la *blockchain* pourrait être un outil à son service, permettant de la renforcer. En effet, la *blockchain* semble tout d'abord un outil parfaitement adapté au droit commun de la preuve car l'un des apports de la *blockchain* c'est l'enregistrement des données.

L'article 1366 du code civil dispose qu'un écrit électronique a la même force probante qu'un écrit "papier" sous deux conditions : premièrement, permettre l'identification des parties et, deuxièmement, que la preuve soit conservée dans son intégralité. Or la *blockchain* peut remplir ces deux conditions avec, par exemple, la mise en place d'une certification des identités. De plus, il s'agit d'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 ("mineurs") qui valident par consensus.

La pierre angulaire de la *blockchain*, créée sur une rupture de confiance, c'est son caractère inaltérable de par le consensus sur lequel elle repose. Il faut également évoquer d'autres avantages de la preuve *blockchain* telles que : la confidentialité, la traçabilité et la transparence. La confidentialité est garantie grâce au cryptage des informations enregistrées sur la *blockchain*. Le cryptage des informations est assuré grâce à un hash (one-way hash function) qui est une fonction à sens unique impossible à inverser. Ce qui veut dire que même si tout le monde peut avoir accès à la *blockchain* (*blockchain* publique), les données « hashées » qu'elle contient sont quasiment non reconstituables [BAR 19]. « Ainsi la *blockchain* permet de protéger le secret des créations, qu'elles soient ou non protégées par un droit de propriété intellectuelle (par ex., un savoir-faire) » [MAL 18]. Plusieurs rapports ont d'ailleurs été publiés sur le sujet [MIN 16].

L'ADN de la *blockchain* c'est la traçabilité de l'information. L'horodatage va par exemple se montrer très utile en matière de propriété intellectuelle en permettant de suivre de manière très précise les différentes étapes d'un processus de création. Elle « permet de prouver qu'à la date où les mineurs ont validé la transaction, un document y a été ancré » [MAL 18]. L'inscription sur la *blockchain* permet de prouver la date à laquelle les "mineurs" ont validé la transaction ainsi que le contenu de la création, grâce au rapprochement entre le document la décrivant et son empreinte. Par exemple, en cas de litige, l'auteur pourra produire en justice l'original de sa création (un fichier photo) et le hash inscrit sur la *blockchain* et le comparer avec l'empreinte « hashée » sur la *blockchain*. Cependant, la création inscrite sur la *blockchain* peut être contrefaisante ou peut ne pas être originale. La *blockchain* ne donne donc aucune indication sur la nature de l'œuvre et aucune garantie d'un droit de propriété intellectuelle sur la création revendiquée.

Par son immutabilité, la *blockchain* est certes un espoir de pallier le problème de fragilité de la preuve mais, comme nous venons de le voir, cette technologie trouve quand même ses limites et il ne faudrait pas non plus que celle-ci la fragilise encore plus. Il semble donc indispensable de continuer à optimiser cette technologie et de l'encadrer juridiquement.

2. La question de la sécurité et de la fiabilité de la preuve *blockchain* et de la titularité des droits et de l'évolution du tiers de confiance

La question de la sécurité est cruciale concernant la *blockchain*. Nous commencerons ainsi par aborder la question de la sécurité et la fiabilité de la preuve *blockchain* (2.1). Puis nous envisagerons celle de la titularité des droits et de l'évolution du tiers de confiance (2.2).

2.1. Question de la sécurité et de la fiabilité de la preuve blockchain

La *blockchain* représente une technologie de rupture sur le point de la sécurisation des données : elle repose sur la combinaison d'algorithmes cryptographiques associée à un stockage redondé d'informations sur un réseau informatique.

L'authentification des transactions de la *blockchain* repose sur le principe de cryptographie asymétrique. Ce système utilise des doublets de clés, l'une privée qui doit être conservée absolument secrète par l'utilisateur, et l'autre publique qui doit être communiquée ouvertement. Un message encrypté avec la clé privée ne peut être décodé qu'avec la clé publique et réciproquement. Les *blockchains* fonctionnent sur le principe de systèmes distribués et ne dépendent pas d'une autorité centrale pour valider les opérations. La technologie utilise une logique de consensus : selon les règles de gouvernance établies, une opération n'est validée que lorsqu'un nombre suffisant d'ordinateurs indépendants les uns des autres ont validé cette opération. Ce principe de consensus rend les registres de *blockchain* infalsifiables puisqu'il faudrait réussir à obtenir un consensus identique pour falsifier des données.

Pour autant, les niveaux de sécurité sont variables selon le type de *blockchain* mise en œuvre et au cours des dernières années, des incidents de piratage ont eu lieu. Les piratages ne portent pas forcément sur la *blockchain* elle-même. Ainsi, le spécialiste français de la *blockchain* Ledger a subi en 2020 un piratage des données personnelles de ses clients à la suite d'une erreur de l'un de ses prestataires sur un module de commerce en ligne.

Une utilisation de la *blockchain* dans un dispositif de preuve juridique nécessite de pouvoir identifier formellement les identités des participants et non sur la base du pseudonyme. La principale solution mise en place est alors de recourir à un tiers de confiance qui agit comme autorité de certification de l'identité (assurant qu'à une clef publique définie, correspond bien une identité). Cette gestion des identités se fait en dehors de la *blockchain* et présente des niveaux de risques et de sécurité variables selon le tiers de confiance.

Enfin, lorsque la *blockchain* est utilisée pour archiver ou horodater des informations plus complexes que des transactions financières, il peut se poser un problème de validation des informations entrées dans la *blockchain*. La *blockchain* ne permet pas, par elle-même, de préjuger de la validité de cette information (authenticité d'une pièce, ...). Là encore, il est nécessaire de trouver d'autres mécanismes pour assurer la validité des informations soit en réinstituant des tiers de confiance chargés d'assurer la validité des informations au moment de leur inscription initiale dans la *blockchain* (qui pourra ensuite être utilisé comme système de transaction et d'horodatage), soit au moyen de solutions spécifiques au cas d'usage.

2.2. Preuve de la titularité des droits et évolution du tiers de confiance

Dans le domaine de la propriété intellectuelle, la question de la titularité des droits sur une œuvre ou une création est cruciale mais souvent très compliquée à rapporter d'où la nécessité de faire appel à des tiers de confiance ou tiers extérieurs (sociétés de gestion de droits d'auteur, ...) [JOL 18]. En permettant de rapporter différemment la preuve de l'existence et de l'antériorité d'un droit subjectif comme celui de propriété, la *blockchain* pourrait être un nouvel instrument de gestion des droits de propriété intellectuelle. En effet, la technologie *blockchain*, en enregistrant de manière fiable et sécurisée les droits de propriété intellectuelle sur les œuvres et contrôlant la diffusion de celles-ci, pourrait devenir un moyen efficace de lutter contre la contrefaçon qui s'est généralisée depuis l'explosion d'internet. Un autre atout de la technologie *blockchain* serait aussi de permettre une sauvegarde fiable et immuable des inventions, des marques, des dessins et modèles ou d'autres types de créations et d'ainsi améliorer la gestion de leurs droits afférents.

En revanche, l'empreinte *blockchain* reprend les caractéristiques d'une œuvre mais non pas l'œuvre elle-même. Elle ne peut donc pas être considérée comme une divulgation au sens de l'article L. 113-1

du code de la propriété intellectuelle qui dispose que “la qualité d'auteur appartient, sauf preuve contraire, à celui ou à ceux sous le nom de qui l'œuvre est divulguée”. Ainsi, à supposer que l'œuvre tout entière soit téléchargée (« uploadée ») sur la *blockchain*, celle-ci n'est pas divulguée au public, car il n'est pas possible d'en reconstituer l'empreinte. De plus, l'empreinte inscrite sur la *blockchain* ne mentionne pas l'identité de l'auteur, celle-ci ne permettra donc pas non plus de prouver la titularité du droit.

Alors que la technologie *blockchain* est née de la remise en cause d'une autorité centrale, l'adoption d'un système totalement décentralisé se heurte à la question de la confiance [TOU 19]. Avec la mise en œuvre de services reposant sur la *blockchain* au-delà des cryptomonnaies, la désignation et le rôle des tiers de confiance est omniprésente. Cette question de confiance repose sur l'établissement de règles de gouvernance et de fonctionnement des *blockchains* privées ou semi-privées. Ces règles peuvent porter sur le niveau de sécurité mais également sur l'organisation et le choix des personnes ou organismes en charge de valider les informations inscrites.

Dans ce sens, nous pouvons évoquer Logion qui est une initiative assez unique en Europe¹. C'est une approche différente de d'habitude car on n'a pas une seule *blockchain* mais une multitude de *blockchains* connectées les unes aux autres (technologie Polkadot). La particularité de Logion c'est qu'elle est gérée par des officiers publics et ministériels européens, qui participent au processus de validation des informations contenues par cette *blockchain*. On devrait plutôt dire des officiers judiciaires car ce sont souvent des juristes exerçant une partie de l'imperium public et qui, par ce fait, sont tenus par un cadre légal et déontologique extrêmement stricte. Ce qui est extrêmement important, c'est que l'on a décidé d'utiliser les compétences que ces personnes ont de par la loi ou par leurs statuts pour offrir des services spécifiques. Logion va donc embarquer une partie de cette puissance publique dans son système et c'est justement là une part de sa pérennité. C'est par tout le statut lui-même qu'il embarque cette pérennisation car c'est quelque chose qui est réglementairement reconnu et identifié au sein de notre société comme un îlot de sécurisation. Donc c'est d'abord par le comment ? que l'on rentre dans cette pérennisation et ensuite, c'est par la qualification de la chose elle-même et par sa reconnaissance et sa sécurisation juridique avec le droit classique.

La *blockchain* est très souvent au service d'une application. Or Logion est au service de toutes les applications possibles car il est au service du droit. Il a donc adopté une approche transversale, qui ne s'intéresse pas uniquement à la chaîne mais également à tout ce qu'il y a autour, et c'est là que nous pouvons trouver des éléments pour la pérennité de la preuve. Logion vient donc combler le vide juridique qui existe actuellement s'agissant de l'utilisation juridique ou contractuelle de la *blockchain*.

Ici, il ne s'agit pas de recentraliser mais d'utiliser les tiers de confiance de façon totalement décentralisée. Ils travailleront les uns avec les autres en toute transparence mais dans un univers décentralisé. Pour le moment, c'est une association qui gouverne la chaîne Logion (avec tous les acteurs) mais le but c'est de faire glisser progressivement la gouvernance sur la chaîne, d'après des règles établies par les validateurs. Il n'existe qu'une seule barrière à l'entrée : pour être validateur, il faut être officier ministériel européen. Les validateurs doivent être irréprochables. C'est pour cela que Logion a commencé avec 10 validateurs auxquels il a demandé d'établir leurs propres règles, qui correspondent plus ou moins à leurs règles déontologiques. L'intégration des validateurs se fera progressivement car c'est plus facile de commencer avec des pays qui ont un socle juridique commun (ex : la notion même d'officier judiciaire). Ici, l'apport de l'Union internationale des officiers judiciaires est essentiel car c'est elle qui, à chaque fois, est capable d'aller chercher les meilleurs interlocuteurs.

Il existe une initiative identique aux Etats-Unis : système POA network. Ce système a été développé avec des notaires mais aux USA, les notaires ne sont pas des officiers ministériels donc leur champ de

¹ Les informations sur Logion ont été recueillies lors d'un entretien réalisé le 28 mai 2021, avec David Schmitz et Maître Casey Joly.
© 2022 ISTE OpenScience – Published by ISTE Ltd. London, UK – openscience.fr

compétences va être plus limité. Mais l'approche est identique à celle de Logion : on a des nœuds de confiance.

La preuve de la titularité des droits est très souvent apportée *a posteriori* et la *blockchain* aurait l'avantage de couvrir la période de l'avant-brevet. Ainsi, la sécurité du brevet serait assurée de sa conception à sa concrétisation [BIN 20] : ce qui permettrait d'asseoir ce projet sur des bases solides et protectrices et ainsi d'augmenter la confiance des investisseurs. Pour une application dans le domaine de la propriété intellectuelle, la preuve *blockchain* offrirait donc de nombreux et importants avantages car la *blockchain* est clairement un outil majeur de datation/authenticité/certification.

3. La question de la reconnaissance de sa valeur probatoire par les juges

Après avoir étudié les nombreuses potentialités offertes par la preuve *blockchain*, en particulier pour les droits de la propriété intellectuelle, envisageons maintenant la manière dont celle-ci a été reçue par le juge. Nous commencerons par examiner sa réception par le juge français (3.1) puis la manière dont celle-ci a été accueillie dans d'autres endroits du Monde (3.2).

3.1. Etat des lieux de la reconnaissance de sa force probatoire par le juge français

Une première tentative d'encadrement juridique de la preuve électronique a eu lieu avec le règlement européen (eIDAS) du 23/07/2014².

Applicable en France depuis le 1er juillet 2016, ce règlement octroie à la signature qualifiée la même force probante qu'un écrit « papier ». Concrètement, cela se traduit en pratique par l'utilisation d'un certificat électronique délivré en personne par des prestataires de services de confiance qualifiés (sociétés privées faisant l'objet d'une qualification par l'ANSSI et d'un contrôle régulier).

La qualification d'un prestataire de service atteste de sa conformité aux exigences de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Légalement, c'est la même chose pour l'horodatage (la technologie qui assigne une date et heure certaine à un fichier). Ainsi, à ce jour, seul « l'horodatage qualifié » a une réelle force probante présumée, tant sur la date que sur l'intégrité des données auxquelles elle se rapporte, dès lors qu'il est bien délivré par les prestataires susmentionnés.

Comme l'indique clairement le rapport parlementaire sur les usages de la *blockchain* présenté ce mercredi 12 décembre 2018, « aucun texte ne détermine la portée juridique des éléments inscrits sur un protocole technique. Dès lors qu'il ne fait pas partie des moyens de preuve actuellement reconnus au plan juridique (les signatures et horodatages qualifiés), il appartient au juge de déterminer leur valeur probatoire, au vu des circonstances de l'espèce. ». Les rapporteurs relèvent tout de même qu'« en raison de la traçabilité garantie par la fonction d'horodatage et l'immuabilité des transactions, les protocoles *blockchains* pourraient répondre en partie (aux) spécifications » du règlement européen n° 910/2014 du 23 juillet 2014 (règlement eIDAS). Par ailleurs, le même règlement précise expressément qu'un horodatage qui n'est pas un horodatage qualifié ne doit jamais être rejeté pour ce seul motif, et que sa recevabilité et son effet juridique doivent donc tout de même être appréciés par le juge.

En septembre 2018, le député Jean-Michel Mis déposait un amendement à l'article 40 de la loi PACTE³ qui suggérait d'ajouter à l'article 1358 du Code civil un alinéa, dont la rédaction serait la

² Article 25 du Règlement 910/2014 du Parlement Européen et du Conseil du 23 juillet 2014 (eIDAS) : « L'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite. »

Article 41 du Règlement 910/2014 du Parlement Européen et du Conseil du 23 juillet 2014 (eIDAS) : « Un horodatage électronique qualifié bénéficie d'une présomption d'exactitude de la date et de l'heure qu'il indique et d'intégrité des données auxquelles se rapportent cette date et cette heure. L'effet juridique et la recevabilité d'un horodatage électronique comme preuve en justice ne peuvent être refusés au seul motif que cet horodatage se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences de l'horodatage électronique qualifié. » qu'il est bien délivré par les prestataires sus-mentionnés ».

³ TA AN n° 1088, 2017-2018 ; amendement n° 1317.

suivante : « À cet effet, tout fichier numérique enregistré dans un dispositif électronique d'enregistrement partagé (DEEP), de nature publique ou privée vaut preuve de son existence et de sa date, jusqu'à preuve contraire, dès lors que ledit DEEP répond à des conditions définies par décret ». Ce décret en Conseil d'État devait fixer les contours et les conditions de cette présomption de preuve, en assurant un contrôle par l'État des qualités essentielles que devront présenter les DEEP pour en bénéficier. Cette tentative a finalement avorté au moment de l'adoption définitive de la loi.

En France, aujourd'hui, la *Blockchain* n'est pas encore totalement reconnue comme ayant force de preuve car on estime qu'il y a encore un risque que la clef privée ou publique soit erronée ou hackée et qu'ainsi, cela soit compliqué de prouver que l'on est bien celui qui est à l'origine de la transaction. On peut effectivement prouver la certification mais pas parfaitement prouver la propriété de ce qui a été certifié. C'est justement le point essentiel sur lequel on débat encore aujourd'hui. En revanche, la reconnaissance de la preuve *blockchain* est beaucoup plus avancée dans d'autres endroits du monde, c'est que nous allons voir maintenant grâce à quelques exemples.

3.2. Etats des lieux dans le reste du monde

D'abord, l'Italie a reconnu juridiquement l'horodatage *blockchain* lors de l'entrée en vigueur de la loi (n° 12/19) relative au soutien et à la simplification des entreprises et de l'administration publique, le 13 février 2019. En effet, l'article 8 ter, 3^e de cette loi prévoit que : « le stockage d'un document informatique par l'utilisation de technologies basées sur des registres distribués produit les effets juridiques de l'horodatage électronique visé par l'article 41 du règlement (UE) n° 9010/2014 du Parlement européen et du Conseil du 23 juillet 2014 ». Le législateur italien accorde donc à l'*« horodatage électronique blockchain »* les effets de l'horodatage visés par le règlement eIDAS. De cette manière, c'est la recevabilité de cette preuve en justice qui est indirectement admise, même si un certain nombre de questions techniques et juridiques demeurent éludées. En l'absence d'intervention de prestataire de services de confiance qualifié dans les *blockchains* publiques, l'horodatage *blockchain* reconnu comme preuve en droit positif italien semble ne pouvoir revêtir que le caractère de l'horodatage électronique simple. Cette preuve produira des effets simples et devra être admise par le juge en vertu du principe de non-discrimination. Pour ce qui est des *blockchains* privées, le gérant pourra prévoir contractuellement l'obligation de faire intervenir un tiers de confiance pour bénéficier de la force probante supérieure de « l'horodatage électronique *blockchain* qualifié » en vertu de la présomption d'exactitude de date et heure, et d'intégrité des données.

Ensuite, à Monaco, on peut signaler une proposition de loi n° 237 relative à la *blockchain* adoptée le 21 décembre 2017, qui qualifie juridiquement les inscriptions d'actes juridiques dans la *blockchain* comme étant présumées constituer « une copie fidèle, opposable et durable de l'original, portant une date certaine ».

En outre, aux Etats-Unis, nous pouvons relever trois exemples frappants de cette évolution. Un premier exemple nous est fourni par le Tennessee, avec la loi n° 1662 du 22 mars 2018, qui modifie le « *Tennessee Uniform Electronic Transactions Act* », prévoit que les documents protégés par la *blockchain* sont considérés comme des documents électroniques et que la signature cryptographique produite et stockée par la *blockchain* sous forme électronique est une signature électronique. Un second exemple nous est offert par le Nevada, avec le « *Nevada Uniform Electronic Transactions Act* » modifié par les « *Nevada Blockchain Statues* » promulgués le 5 juin 2017 qui considèrent les enregistrements dans la *blockchain* comme des documents électroniques. Le dernier de ces exemples ici envisagés est celui du Vermont, qui avec la loi 12 V.S.A. §, promulguée le 2 juin 2016, prévoit à son article 1913 que les documents de la *blockchain* sont auto-authentifiables en vertu de la loi 902 du Vermont sur la preuve.

Enfin, par une décision du Tribunal de Hangzhou du 28 juin 2018 [HAN 18], a pour la première fois reconnu des éléments inscrits sur la *blockchain* (concernant le protocole bitcoin) comme étant des preuves authentifiantes valables lors d'un litige de contrefaçon. Un homme prétendait avoir des droits

sur une image qu'il avait fait certifiée sur une *blockchain*. Le juge a reconnu la valeur probatoire de cette certification faite sur la *blockchain* et lui a attribué les droits afférents à cette image. En gros, c'est comme si demain, en France, l'INPI était complètement remplacée par la *Blockchain*. Cette décision semble toutefois difficilement transposable au sein de nos juridictions car le Tribunal de Hangzhou nommé « tribunal de l'Internet » était une juridiction pilote spéciale.

Depuis quelques mois, la question de la preuve *blockchain* se retrouve à nouveau sous le feu d'actualité avec l'arrivée des NFT qui présentent de nouveaux défis et de beaux exemples d'applications dans le domaine de la propriété intellectuelle.

4. Conclusion

Les NFT (*Non Fungible Token*) ou jetons non fongibles fonctionnent grâce à la technologie *blockchain* mais ils revêtent une forme particulière : ce sont des jetons codés de manière à ce qu'ils soient impossibles à reproduire ou qu'ils puissent être reproduits et numérotés en petit nombre. Cette spécificité ouvre de nouvelles possibilités en matière de preuve d'authenticité ou de certification d'œuvres digitales (photo, vidéo, musique, etc.) et de nombreuses initiatives se développent sur le sujet.

Le caractère non reproductible des jetons NFT est codé dans des « smart contract ». Le « smart contracté » ne peut être modifié, y compris par son créateur, qu'à partir du moment où il est créé dans une *blockchain* et lui donne de ce fait une force obligatoire qui lui vaut l'appellation de « contrat intelligent ». Lors de la création d'un NFT par un artiste, celui-ci va associer une œuvre à un jeton numérique via un « smart contract ». Il va y apposer sa signature numérique et enregistrer le tout dans une *blockchain*. Dans le cas des NFT, l'artiste détermine les droits de propriété intellectuelle, c'est-à-dire d'exploitation, qu'il accorde via des jetons. Les NFT étant non fongibles par définition, il n'y a pas de transfert automatique des droits de propriété intellectuelle liés à l'œuvre à laquelle le jeton est attaché. L'acheteur n'achète donc pas l'œuvre mais un droit limité sur une œuvre.

Si le processus de création et d'enregistrement des NFT dans une *blockchain* est sécurisé par les caractéristiques technologiques de celle-ci, rien ne garantit pour autant l'authenticité de l'œuvre liée au NFT. Pour cela, il est nécessaire que soit certifié, en dehors de la *blockchain*, par un huissier par exemple. Dans ce cas, il peut intervenir pour certifier plusieurs éléments qui sont autant de faiblesses dans le processus de création d'un NFT : la création de l'œuvre par l'artiste, la création du jeton, la signature numérique de l'artiste ainsi que le certificat d'authentification de l'œuvre. Les certificats réalisés par l'huissier peuvent eux-mêmes être enregistrés dans une *blockchain*.

Logion travaille actuellement sur un projet de NFT (jeton non tangible). La première chose que Logion peut apporter en ce domaine, c'est la certification, la sécurisation des sources. Ensuite, la seconde chose qu'il pourrait apporter c'est un cadre légal au sein de ces NFT et là, c'est plutôt un rôle de curator qu'il jouerait. A l'issue de cela, on aurait donc un token pourvu d'une vraie force juridique : un propriétaire clairement défini dans un cadre légal clairement défini, relié un actif clairement déterminé et sécurisé. Et c'est de tout cela que va naître la force probante.

Comme toute technologie, la *blockchain* est amenée à évoluer en permanence. On peut donc s'interroger sur la possibilité d'une réelle pérennité de celle-ci. De plus, comme nous avons pu le voir, la *blockchain* repose sur le critère de la confiance que les opérateurs ont en celle-ci. Or, la confiance est fragile – surtout si des failles informatiques surviennent ... En revanche, comme nous avons pu le voir, la *blockchain* a de grandes potentialités s'agissant de la protection des droits de la propriété intellectuelle. Ce sont des droits qui s'inscrivent dans la durée (70 ans), ceci confère donc à la preuve offerte par cette technologie une certaine pérennité.

Bibliographie

- [BAR 18] BARRAUD B., « Les *blockchains* et le droit », *Revue Lamy Droit de l'immatériel*, Lamy (imprimé) / Wolters Kluwer édition électronique, p.48-62, 2018.
- [BAR 19] BARSAN I., « Public blockchains: the privacy-transparency conundrum », *RTDF*, n° 2, 2019.
- [BIN 20] BINCTIN N., « Coopétition et brevets : enjeux juridiques », available at <https://www.openscience.fr/Coopetition- et-brevets- enjeux-juridiques>, 2020.
- [GUR 18] GURKAYNAK G., YILMAZ I., YESILALTAY B., BENGI, BERK B., « Intellectual property law and practice in the blockchain realm », *Computer Law and Security Review*, vol. 34, p. 847-862.
- [HAN 18] HANGZHOU INTERNET COURT, PROVINCE OF ZHEJIANG PEOPLE'S REPUBLIC OF CHINA, Case n° 055078 (2018) Zhe 0192 No. 81 Huatai Yimei/Daotong, June 27, 2018 ; DEROULEZ J., « *Blockchain* et preuve : la Chine en pointe ? », *Actualités du Droit*, 7 sept. 2018.
- [JOL 18] JOLY L., « La *blockchain* est-elle une révolution pour la propriété intellectuelle ? », *Dalloz IP/IT*, p. 536 et s., 2018.
- [MAL 18] MALAURIE-VIGNAL M., « Enjeux et défis de la *blockchain* dans ses relations avec la propriété intellectuelle », *Dalloz IP/IT*, p.531, 2018.
- [MIN 18] MINISTÈRE DE LA CULTURE ET DE LA COMMUNICATION – CONSEIL SUPERIEUR DE LA PROPRIÉTÉ LITTÉRAIRE ET ARTISTIQUE, Rapport de la mission sur l'état des lieux de la *blockchain* et ses effets potentiels pour la propriété littéraire et artistique, janv. 2018.
- [SIX 21] SIX N., HERBAUT N., SALINESI C., « BLADE : Un outil d'aide à la décision automatique pour guider le choix de technologie *Blockchain* », available at <https://www.openscience.fr/BLADE-Un-outil-d-aide-a-la-decision-automatique-pour-guidier-le-choix-de>, 2021.
- [TOU 19] TOUNSI W., « Systèmes de gestion de la confiance : une étude rétrospective sur la confiance numérique », in *Cybergelligence et confiance numérique, la cybersécurité à l'ère du cloud et des objets connectés*, ISTE Éditions, 2019.