Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE LA CULTURE
ET DE LA COMMUNICATION

—

CONSEIL SUPÉRIEUR DE LA PROPRIETE
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

Présidents de la mission : Jean-Pierre Dardayrol et Jean Martin
Rapporteurs : Charles-Pierre Astolfi et Cyrille Beaufils

Rapport présenté au CSPLA le 13 février 2018
Son contenu n'engage que ses auteurs

Janvier 2018

Avant-propos des présidents

Le dialogue avec les représentants des auteurs et des industries de la création, les échanges avec les entreprises et les startups de la *high tech*, les larges recherches et les analyses approfondies des rapporteurs leur ont permis d'établir ce rapport relatif à l'état des lieux actuel de la *blockchain* et de ses variantes.

Les lecteurs y trouveront chacun une information abondante, vérifiée ; au-delà, ils y trouveront aussi certainement, matière à réflexion et à projection(s), fonctions de leur situation personnelle, de leur histoire, de leur environnement et de leurs ambitions.

Afin de préparer ces démarches, importantes et exigeantes, les présidents de la mission souhaitent donner leur vision projective à l'issue de leur mission, de façon simple et brève, en quelques points.

Nous ne savons pas ce que la *blockchain* va devenir, mais la *blockchain* existera sous des formes multiples (ici, il serait plus pertinent de dire les *blockchains* pour prendre en compte la diversité des concepts et des réalisations qui rencontreront le succès parmi de nombreux échecs).

En l'état, la technique de la *blockchain* ne donne pas prise au droit de la propriété littéraire et artistique.

Les acteurs des industries culturelles et leurs publics constituent un système d'information, par leurs actes de création, de production, de diffusion et d'exploitation, lequel évolue constamment et vise à l'optimisation pour des motifs multiples d'efficacité économique et de développement de nouveaux produits et services ainsi que pour répondre à l'évolution des pratiques sociales et aux opportunités techniques.

La *blockchain* est un système multifonctionnel de gestion de l'information, qui vise, selon les configurations et les applications, à la sécurité, la transparence, l'instantanéité, à l'automaticité des opérations et vers un coût infinitésimal.

Il serait donc surprenant que ces deux mondes n'aient pas à coopérer fructueusement et tout comme il serait hasardeux de ne pas s'y préparer activement face au rythme accéléré des évolutions et de la déréglementation.

Il apparaît dès lors indispensable que les industries culturelles participent à ce mouvement, notamment avec des partenaires, au premier chef pour ne pas être parmi les perdants, les laissés pour compte.

Deux finalités de participation complémentaires mais différentes quant aux modalités, aux enjeux stratégiques et aux échéances de réalisations se dessinent : d'une part, l'optimisation de la gestion (en termes de coûts, ou de délais, ou de qualité…) et d'autre part, l'innovation de modèles (sociaux, économiques…).

Dès à présent, la recherche des opportunités concerne (de façon non limitative) d'une part, l'établissement de liens entre le monde physique et le monde numérique (cf. les « oracles ») et d'autre part, la traçabilité (des usages, des objets, etc.).

Les industries culturelles et créatrices ont, aujourd'hui dans ce domaine, mais pour un temps limité, une occasion de reprendre l'initiative dans un contexte marqué par la massification ubiquitaire des pratiques de « production » et de « consommation » ainsi que par la conjugaison de nouvelles vagues d'innovations dans les technologies de l'information (*big data* et intelligence artificielle notamment).

Rapport

Avant d'être une technologie transformatrice voire créatrice de nouveaux usages ou modèles d'affaires, la *blockchain* est un centre d'intérêt. De ses premiers pas dans une communauté d'initiés à sa légitimation en une de *The Economist*, ce concept a su susciter la curiosité ou l'adhésion de nombreux acteurs, certains commençant à proposer des services, des outils ou des usages innovants grâce à cette technologie et dépassant le cadre historique de sa première application, qui était la création d'une monnaie numérique.

Les fondements de la *blockchain* se concentrent dans deux promesses : pouvoir créer des « titres de propriété numérique » et donner la possibilité d'échanger ceux-ci sans requérir à une autorité centrale. Ce que recouvrent exactement ces titres de propriété est au choix des utilisateurs qui peuvent dès lors inventer leurs propres usages et leurs propres modèles d'affaires.

Les initiatives, les nombreuses *start-ups* et les industries qui gravitent autour de cette technologie construisent et enrichissent progressivement leurs concepts techniques, leurs modèles d'affaires, leurs filières et leurs centres de diffusion des compétences techniques, juridiques et managériales ; les industries culturelles ne faisant pas exception en la matière. Cependant, les potentiels de transformations commencent à être appréhendés par les acteurs les plus divers, à l'échelle mondiale, ceux-ci découvrant dans la *blockchain* des usages pertinents pour leur activité, voire trouvant dans celle-ci l'élan nécessaire pour construire des projets innovants.

Table des matières

Si Prométhée enchaîné constitue, depuis l'Antiquité, le symbole du progrès technique, ce sont aujourd'hui les chaînes mêmes, chaînes de blocs – ou *blockchains* – qui sont présentées comme une innovation, susceptible d'améliorer ou de remettre en question les modèles des acteurs historiques dans de nombreux secteurs économiques ou des administrations publiques.

« Machine à fabriquer de la confiance »[1], la *blockchain* est une mise en œuvre innovante de technologies connues que son fonctionnement complexe peut contribuer à mythifier. Une partie des promesses et mises en garde proférées quant à son développement reposent parfois sur une compréhension incomplète de ses capacités et de ses limites actuelles ainsi que de ses développements en cours ou à venir.

Bien comprise, la *blockchain* est cependant porteuse de véritables bénéfices en termes d'efficacité et de sécurité des transactions et des échanges d'informations, comme l'ont compris les nombreux acteurs qui se sont saisis de la technologie pour appréhender, via des réalisations pilotes parfois mises en commun, toutes ses potentialités.

Si certains acteurs des industries culturelles participent déjà à cette dynamique[2], le présent rapport a d'abord pour objet de susciter l'intérêt des membres du CSPLA pour cette technologie et de leur donner les premières clefs pour réfléchir à ses effets potentiels dans leur secteur et sur la propriété littéraire et artistique, et le cas échéant engager des opérations pilotes ou d'essais.

1 *The Economist*, 31 oct. 2015
2 « Les blockchains, une opportunité économique pour le droit d'auteur », SACEM, 21 nov. 2016,

1. Une technologie émergente aux potentialités en développement

La *blockchain* est née en 2008, comme le rappelle le rapide historique proposé en annexe à ce rapport, mais ses applications au-delà des monnaies virtuelles ont été envisagées un peu plus récemment. Fin 2015, l'hebdomadaire britannique *The Economist* était déjà en mesure de présenter certaines initiatives portées par des acteurs économiques, alors essentiellement privés, pour faire l'expérience des applications de la *blockchain* dans leur secteur. Le consortium de près de 70 banques, associées à la *start-up* R3 CEV, pour effectuer en commun des recherches sur ce thème dans le domaine des transactions interbancaires en était alors le meilleur exemple.

L'intérêt pour la technologie s'est ensuite renforcé pour inclure des États soucieux par exemple de fiabiliser leur cadastre ou les échanges de données médicales, ainsi que des groupes de luxe et des producteurs de diamants désireux de garantir la traçabilité de leurs produits. Plusieurs réalisations pilotes en ce sens ont été lancées et rendues publiques.

Plus récemment, en France, la Caisse des dépôts, dans le cadre du consortium *ad-hoc* LaBChain, et la Banque de France, pour l'émission d'identifiants de créanciers SEPA, ont réuni divers acteurs autour d'applications pilotes visant à appréhender le fonctionnement de la *blockchain* ainsi que les questions juridiques et managériales que sa mise en œuvre suscite.

Au-delà de ces initiatives concrètes, la *blockchain* suscite également la réflexion des pouvoirs publics et de premières tentatives d'inclusion dans les réglementations. Ainsi, par exemple, aux États-Unis, l'État du Vermont a reconnu, en juin 2016, une valeur juridique de preuve à la *blockchain*, à la suite d'un rapport conjoint de son secrétaire d'Etat, de son procureur général et de son commissaire à la réglementation financière.[3]

Dans le même temps, la *blockchain* a également fait son apparition en droit français. Le code monétaire et financier[4] prévoit, par exemple, depuis avril 2016, la possibilité d'enregistrer les transactions portant sur des minibons de caisse sous la forme d'un « *dispositif d'enregistrement électronique partagé* », faisant ainsi entrer, sous cette désignation, la *blockchain* dans le corpus juridique. De même, l'article 120 de la loi dite « Sapin II »[5] a autorisé le Gouvernement à prendre, par voie d'ordonnance[6], les mesures législatives nécessaires pour « *adapter le droit applicable aux titres financiers et aux valeurs mobilières afin de 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* », ce qui a conduit la direction générale du Trésor à

3 James Condos, William H. Sorrel, Susan L. Donegan, "Blockchain Technology: Opportunities and Risks", 15 janv. 2016

4Art. L. 223-12 CMF : « *Sans préjudice des dispositions de l'article L. 223-4, l'émission et la cession de minibons peuvent également 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'Etat.* »

5Loi 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

6 Ordonnace n°2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers

lancer une consultation publique pour recueillir les opinions des acteurs des marchés financiers sur ce sujet[7].

7 v. aussi la consultation lancée par l'autorité européenne des marchés financiers (ESMA) sur le même thème le 2 juin 2016

2. Les deux fonctions de la *blockchain* : enregistrer et transférer

Sans entrer trop avant dans les caractéristiques fonctionnelles et techniques, qui font l'objet d'une annexe au présent rapport, on peut résumer l'intérêt des *blockchains* en indiquant qu'elles permettent de stocker et de transférer de l'information de façon sécurisée, sans recours à un organisme centralisateur.

Les informations contenues dans la *blockchain* sont des résumés chiffrés, appelés *hash*, de transactions[8].

La *blockchain* tient donc le registre des transactions entre ses utilisateurs, ce qui leur permet d'échanger des « titres de propriété virtuels » (aussi appelés *tokens* ou jetons) et d'être les seuls à pouvoir revendiquer la ressource symbolisée par le titre qu'ils détiennent. C'est l'usage et le consensus entre les utilisateurs d'une même *blockchain* qui définissent ce que représentent ces titres ; un « titre » peut représenter une unité de monnaie mais aussi par exemple la propriété d'un actif financier.

Grâce à la tenue de ce registre de transactions, la *blockchain* donne à ses utilisateurs la possibilité de s'échanger des titres indépendamment de toute autorité centralisatrice en respectant plusieurs garanties :

- *transfert de propriété* : quand un utilisateur transfère un titre qu'il possède, celui-ci en perd le contrôle au profit du destinataire ;
- *authentification* : seul le propriétaire d'un titre peut transférer celui-ci ;
- *inaltérabilité* : un transfert ne doit pas pouvoir être annulé ou modifié *a posteriori* ; rendre un titre à son utilisateur originel supposera un second transfert, plutôt que l'annulation du premier ;
- *transparence :* tous les transferts doivent être publics et doivent pouvoir être inspectés par tous ou par un groupe privé.

Dans la mesure où elle enregistre des résumés chiffrés, la *blockchain* permet également de garder la trace d'un contenu numérique (texte, fichier musical, etc.) en enregistrant, à un instant donné, le résumé de ce contenu. Elle permet aussi d'automatiser les transactions entre ses utilisateurs.

De ces modalités de fonctionnement découlent donc les principaux usages et fonctionnalités de la *blockchain*.

8 Par exemple, le résumé chiffré de la présente phase par l'algorithme SHA-256 est cette suite de 64 caractères : 2e04f10f6569204b7de740cfdb797c4ea239c4c837c6d9692fe3b30dbb4def5a

3. Les fonctionnalités

La *blockchain* permet d'enregistrer, dans un temps court (de l'ordre de quelques minutes aujourd'hui sur les principales *blockchains*), des informations de façon décentralisée et sécurisée. Elle est donc porteuse de divers avantages dans des applications qui dépendent, aujourd'hui, de processus plus longs et coûteux pour un tel enregistrement.

Parmi ceux-ci, on peut citer, de façon générale :

- un gain de temps ;
- une automatisation des processus ;
- une réduction des coûts, grâce à l'accélération et à la réduction des moyens techniques et humains nécessaires ;
- une meilleure sécurité ;
- une plus grande transparence.

Au-delà de ces éléments, l'intérêt de la *blockchain* est sans doute mieux appréhendé en décrivant les trois grandes situations, ou cas d'usage, dans lesquels elle est amenée à se montrer particulièrement pertinente. Il s'agit de :

- l'enregistrement de transactions ;
- la preuve d'authenticité ;
- l'exécution automatique de contrats.

3.1. Les transactions sur la *blockchain*

La fonction première de la *blockchain* comme support de transactions est rappelée dans la partie précédente et détaillée dans l'annexe technique sur le modèle des échanges de monnaie virtuelle.

Cette utilisation est sans aucun doute la plus évidente pour la *blockchain*, car elle porte sur des actifs intrinsèquement numériques (monnaie virtuelle) ou dématérialisés, parfois de longue date (titres financiers), pour lesquels l'un des aspects les plus délicats des autres cas d'usage, qui concerne le lien avec le monde physique, est absent. Par le mécanisme de ces titres, la *blockchain* permet cependant aussi d'enregistrer des transactions numériques qui sont le reflet d'échanges dans le monde physique : de même qu'aujourd'hui la vente d'une automobile requiert le transfert de sa carte grise pour être valide, on peut imaginer que, demain, cette fonction soit remplie par le transfert du titre correspondant à cette voiture dans la *blockchain*.

3.2. Preuve d'origine et traçabilité

Le deuxième grand cas d'usage de la *blockchain* consiste à s'en servir non plus comme moyen d'enregistrer une transaction entre deux parties mais comme registre permettant à une personne d'établir l'antériorité de ses droits ou de son action sur un objet et de suivre ensuite l'évolution de celui-ci.

En effet, comme la partie 2 de ce rapport l'a expliqué, la *blockchain* permet d'enregistrer des *hash* de transactions de façon publique et irrévocable – sauf cas de corruption de la *blockchain*. Plutôt que le résumé d'une transaction, toutefois, le *hash* enregistré peut aussi correspondre à un document écrit. Un manuscrit de plusieurs centaines de pages, ou un contrat, peuvent ainsi être « *hashés* » puis insérés dans la *blockchain* à un moment précis. Muni d'un manuscrit ou d'un contrat, un autre utilisateur pourra alors vérifier qu'il correspond exactement à celui qui a été enregistré dans la *blockchain* à cette date. En effet, si le texte qu'il a entre les mains diffère ne serait-ce que d'une lettre de l'original, le *hash* correspondant sera entièrement différent de celui qui a été publié sur la *blockchain*.

Un peu comme une version modernisée du cachet de La Poste apposé sur une enveloppe fermée, la *blockchain* permet donc de garantir l'existence, à une date donnée, d'un document donné. Il faut en revanche bien mesurer que l'inscription dans la *blockchain* ne garantit nullement la véracité des informations contenues dans le document. Ce contenu n'a de force que la confiance mise dans celui qui l'a rédigé et enregistré. En outre, en raison du fonctionnement cryptographique de la *blockchain*, cette dernière ne garantit pas contre le vol d'identité : une personne réussissant à se procurer la clef privée d'une autre pourrait signer, en son nom, toute transaction sur le registre.

Une dernière limite à cet usage tient au fait que la *blockchain* ne permet pas l'enregistrement du document lui-même, mais seulement du *hash* de celui-ci. L'original informatique, à partir duquel la comparaison pourra être faite, doit donc être conservé ailleurs, ce qui suppose la maîtrise d'une capacité de stockage de données. Cela signifie, en revanche, que la simple lecture de la *blockchain* ne permet pas de connaître le contenu du document, préservant ainsi la confidentialité de ce qu'il contient.

3.3. L'exécution automatique de contrats sur la *blockchain*

Le dernier grand usage de la *blockchain* découle de sa capacité à servir de support à des *smart contracts* (« contrats intelligents ») qui automatisent l'exécution de contrats.

Les *smart contracts* sont des programmes informatiques qui réagissent à l'activation d'une condition (« si une catastrophe naturelle survient ») en provoquant un résultat (« alors, 10 000€ sont transférés du compte de l'assureur au compte de l'assuré »). L'inscription de tels « contrats » dans la *blockchain* permet, d'une part, de garantir leur exécution automatique dès que la condition est remplie – par exemple lorsque le résultat consiste en un échange de monnaie virtuelle – et, d'autre part, d'en assurer l'inaltérabilité *a posteriori*.

Ces *smart contracts* peuvent soit constituer une transcription, dans la *blockchain*, des conditions d'exécution d'un contrat existant par ailleurs, soit représenter eux-mêmes le contrat, s'ils sont la seule preuve de l'échange de volonté des parties.

Ils peuvent, en outre, être plus ou moins complexes, notamment s'ils font intervenir d'autres *smart contracts* dans une sorte de réaction en chaîne. Des organisations autonomes décentralisées (*decentralized autonomous organizations*, DAO) ont été conçues sur ce modèle. Elles figurent un fonds d'investissement dont les règles de fonctionnement (vote sur les projets d'investissement, reversement des dividendes, etc.)

ont été automatisées et inscrites dans la *blockchain*. La *start-up* Slock.it a, par exemple, lancé le programme « The DAO » et levé via la *blockchain* Ethereum près de 55 millions de dollars. Ambitieux, ce projet s'est aussi avéré fragile, puisque le code du *smart contract* contenait une faille exploitée par un acteur malintentionné pour dérober le tiers de ces fonds.

La réaction à ce vol a également illustré les difficultés de gouvernance de la *blockchain* : alors qu'une partie des utilisateurs considérait que le code du « contrat » avait force de loi, et que le vol ainsi opéré était donc légal, une autre a préféré revenir à un état de la *blockchain* antérieur au vol, en créant une bifurcation (*fork*) dans l'historique mais en remettant ainsi en cause le principe cardinal d'irrévocabilité de la *blockchain*.

Cet incident prouve que ce troisième usage de la *blockchain*, pour prometteur qu'il soit, doit être abordé avec la prudence habituelle à ce type de systèmes d'informations. D'une part, la qualité du code informatique nécessaire doit être assurée, comme dans toute application. Surtout, d'un point de vue juridique, cet usage ne laisse pas de susciter quelques interrogations, notamment en ce qui concerne son articulation avec le droit des contrats traditionnels. Si les conventions ont force de loi entre les parties, elles reposent néanmoins sur le bon vouloir de ces dernières pour en assurer l'exécution et requièrent, dans la plupart des cas, l'intervention d'un juge lorsqu'il s'agit de forcer l'une d'elles à remplir ses obligations. Le juge peut, à cette occasion, contrôler le contrat et s'assurer, par exemple, qu'il ne porte pas sur un objet illicite ou ne contient pas de clause léonine. À l'inverse, le *smart contract* rendant automatique l'exécution du contrat, le rôle du juge reviendra probablement, *a posteriori*, à « annuler » cette exécution à la demande d'une partie. Reste à savoir comment cette intervention s'articulera avec deux principes fondateurs de la *blockchain* : l'absence de tiers de confiance – comment reconnaître la « légitimité » de la décision juridictionnelle dans ce contexte et assurer sa force exécutoire ? – et l'irrévocabilité.

En outre, lorsque la condition qui déclenche l'exécution du *smart contract* est liée au monde physique, comme dans l'exemple de la catastrophe naturelle pour le versement d'une prime d'assurance, l'intervention d'un « oracle », chargé de renseigner la réalisation de cette condition, sera nécessaire pour faire le lien entre monde physique et *blockchain*.

C'est sans doute pour ces raisons que l'usage des *smart contracts* pourrait s'avérer peut-être plus approprié pour régler des rapports entre objets, notamment dans le cadre de l'internet des objets (*internet of things*). Une voiture sans conducteur pourrait ainsi se faire servir par une pompe à essence, avec un *smart contract* déclenchant le paiement lorsque le réservoir est rempli.

4. Des potentialités mobilisées, des exemples sectoriels

4.1. Une technologie applicable à de nombreux secteurs

L'usage le plus sommaire d'une *blockchain* consiste à créer une monnaie. Cette monnaie peut ensuite être échangée au sein de la *blockchain* ou contre d'autres monnaies (virtuelles ou non) via des plateformes de change.

D'autres usages sont envisagés ou proposés : par exemple, un titre pourrait représenter la possession d'une œuvre d'art dont les reventes successives seraient représentées par autant de transactions sur une *blockchain* ; ce qui permettrait à un acheteur potentiel de consulter l'historique de toutes les transactions de l'œuvre et, en remontant jusqu'à la première transaction impliquant cette œuvre, de s'assurer de son authenticité (par exemple, si la première transaction provient de l'artiste ou de son agent) ou du montant de chaque revente (si celui-ci est rendu public).

Le caractère abstrait des titres virtuels permet d'imaginer une infinité d'usages et de possibilités, en fonction de ce à quoi ces titres sont rattachés hors de leur *blockchain* d'appartenance. C'est donc le contexte dans lequel les utilisateurs utilisent une certaine *blockchain* qui fait son utilité pour une communauté donnée, la *blockchain* mettant à disposition un « livre de compte » numérique infalsifiable, complet et toujours à jour, mais ne faisant pas elle-même le lien avec son contexte d'utilisation.

4.2. La *blockchain*, support de transactions virtuelles : des applications dans le monde de la finance

Eu égard à ces applications initiales, c'est naturellement dans la sphère des transactions financières que la *blockchain* a suscité les premières expérimentations.

Les banques se sont ainsi intéressées parmi les premières à cette technologie, en particulier pour son utilisation en *back-office* pour régler les transactions entre banques. Si la *blockchain* paraît, à l'heure actuelle, peu susceptible de remplacer à court terme les moyens de paiement utilisés par les consommateurs, tels que la carte bancaire, eu égard au délai nécessaire à l'enregistrement d'une transaction (quelques minutes sur les *blockchains* Bitcoin et Ethereum) et à son coût (quelques centimes pour Bitcoin), ces mêmes caractéristiques représentent un véritable avantage lorsqu'il s'agit de l'utiliser pour la réconciliation de transactions interbancaires, telles que l'achat et la vente de titres financiers, en particulier non cotés, ou les virements internationaux, dont le délai (deux à trois jours) et le coût (plusieurs dizaines de milliards de dollars annuellement pour la gestion des échanges de titres) seraient ainsi nettement réduits. Le recours à un registre partagé permettrait également d'éviter la tenue de deux comptabilités séparées, une au sein de chaque banque partie à la transaction, et d'échapper aux incohérences qui surviennent inévitablement entre celles-ci. Les institutions financières espèrent ainsi gagner en efficacité en diminuant leurs coûts opérationnels, grâce à l'allègement des moyens humains nécessaires au fonctionnement du *back office*, mais aussi en réduisant les risques de contrepartie. La *blockchain* pourrait ainsi remplacer ou rendre beaucoup efficaces les chambres de compensation.[9]

9 Voir, pour une liste plus exhaustive des bénéfices potentiels pour l'industrie financière, v. la consultation de l'ESMA précitée

Si les applications dans la sphère financière en sont encore, pour l'essentiel, à la « preuve de concept », deux exemples permettent sans doute de concrétiser l'intérêt de ce secteur pour la *blockchain*. En août 2016, Bank of America Merrill Lynch, HSBC et l'autorité de développement de Singapour Infocomm ont développé une application permettant l'émission de lettres de crédit, destinées à financer le commerce à l'export, via la *blockchain*.[10] Cette dernière est utilisée pour permettre à chacune des quatre parties concernées – l'exportateur, l'importateur et leurs banques respectives – d'approuver à tour de rôle la transaction et d'en suivre le déroulement.

De même, en France, le consortium de banques et d'assureurs emmené par la Caisse des dépôts et consignations a expérimenté en novembre 2016 une utilisation de la *blockchain* à la frontière des transactions et des *smart contracts* pour la gestion des appels de marge pour les collatéraux lors du prêt de titres.[11] La *blockchain* a ici vocation à remplir une fonction de *middle-office* financier en effectuant un unique calcul de la valeur de l'appel de marge entre les deux institutions concernées.

4.3. La *blockchain*, preuve d'authenticité : l'exemple du suivi de biens et documents de valeur

Plusieurs applications ont été développées qui visent à prouver l'authenticité, dès l'origine, d'un bien puis éventuellement, en lien avec l'usage de transaction, à retracer l'histoire de ce bien en enregistrant ses étapes. La *blockchain* a donc ici valeur de preuve.

La *start-up* Everledger[12] a ainsi, depuis sa création, enregistré plus d'un million de diamants grâce à la *blockchain*. Dans un secteur où la garantie d'origine légale – contre les « diamants du sang », les diamants synthétiques et les fraudes à l'assurance – est clé, la *blockchain* permet d'enregistrer un diamant à partir d'une quarantaine de caractéristiques (couleur, poids, transparence, etc.). L'acheteur d'un diamant peut donc s'assurer qu'il possède bien celui qui, dès le départ, a été enregistré comme provenant d'une mine légale en Afrique du Sud, par exemple. Des *start-ups* se proposent d'étendre le même usage à d'autres secteurs dans lesquels la lutte contre la contrefaçon est importante, tels que les médicaments, les objets de luxe ou même le suivi de conteneurs dans le commerce international.

L'usage de la *blockchain* comme preuve d'authenticité peut également être mise à profit pour y adosser des documents de valeur significative. Les actes d'état civil, les diplômes ou les titres de propriété sont ainsi concernés. Plusieurs Etats, dont le Honduras – qui semble avoir par la suite renoncé au projet[13] – le Ghana[14] et la Géorgie[15] ont lancé des expérimentations sur leur cadastre en authentifiant les titres de propriété grâce à la *blockchain* pour garantir l'absence de modification ultérieure, par exemple de la part d'un fonctionnaire corrompu. De même l'Estonie a-t-elle adopté le système Keyless Signature

10« BofAML, HSBC, IDA Singapore Build Pioneering Blockchain Trade Finance App », 10 août 2016, communiqué de presse d'HSBC« BofAML, HSBC, IDA Singapore Build Pioneering Blockchain Trade Finance App », 10 août 2016, communiqué de presse d'HSBC
11 *Agefi*, 4 nov. 2016
12 https://www.everledger.io/https://www.everledger.io/
13 Blockchain Land Title Project 'Stalls' in Honduras", *CoinDesk*, 26 déc. 2015
14http://bitlandglobal.com/http://bitlandglobal.com/

Infrastructure développé par l'entreprise Guardtime[16] pour certifier divers documents administratifs, dont, à terme, les dossiers médicaux de près d'un million de patients.

4.4. La *blockchain,* sous-jacent de *smart contracts*

Outre l'exemple de l'assurance météorologique et celui, malheureux, de « *The DAO* » déjà cités[17] plusieurs applications de *smart contracts* sont envisageables. Elles restent cependant en France généralement pour l'heure à l'état de projet ou au stade de l'expérimentation.

Un exemple proche de celui d'assurance serait un *smart contract* de pari : la réalisation de la condition (victoire d'un cheval ou d'une équipe de football, par exemple) déclencherait une transaction financière entre les deux parieurs ou entre le parieur et le *bookmaker.*

Plus innovant serait l'exemple d'objets-entreprises. La chercheuse P. de Filippi a développé une « plantoïde »[18], intermédiaire entre un robot et une œuvre d'art qui sollicite la générosité de ceux qui l'admirent, collecte leurs paiements via la *blockchain* puis lance des appels d'offre pour la création de nouvelles plantoïdes. De même, une voiture ou un appartement pourraient se louer à des particuliers, recevoir des paiements, commander et recevoir des fournitures ou des réparations grâce à des *smart contracts*, etc.

16ksi-technology
17 À ce sujet, voir la partie 3.3
18*L'Echappée volée*, 28 mai 2016

5. Les opportunités pour le monde culturel

5.1. Des opportunités à construire pour les industries culturelles

La *blockchain* possède probablement de nombreux cas d'usages qui n'ont pas encore été explorés ou même imaginés. Les exemples cités dans la partie précédente participent tous d'un phénomène plus général que la *blockchain :* l'automatisation et la désintermédiation de processus et d'usages qui étaient jusque-là souvent centralisés (comme par exemple le transfert de monnaie, qui nécessite le passage par le système bancaire) ou qui n'étaient même pas envisageables sans une autorité centrale (comme la création monétaire, qui, historiquement, est toujours adossée à une banque centrale ou à une ressource disponible en quantité limitée, comme l'or).

Dans les industries culturelles, le nombre parfois important d'acteurs dans la chaîne de valeur d'un bien culturel et la complexité de traiter avec ceux-ci, par exemple dans le cas des relations avec les ayants-droits, pourraient constituer un terrain propice à de premières applications avec une *blockchain*. La dynamique ainsi engagée permettrait alors de concentrer les efforts sur les activités possédant une forte valeur ajoutée : conseil juridique, stratégie de diffusion, négociation de partenariats, tout en laissant à la *blockchain* une partie plus automatisable, avec, par exemple, l'identification, les paiements et le calcul du montant des redevances pour les ayants droit.

Au-delà de ces exemples et de ceux cités dans la partie précédente, le mouvement initié par la *blockchain* ne s'arrêtera pas aux portes des industries culturelles : elle créera de nouvelles pratiques et modifiera profondément des pratiques existantes dans ces industries, à tous les niveaux de la chaîne de valeur, du consommateur jusqu'au créateur. Dès lors, l'enjeu pour les acteurs du monde de la culture est d'identifier les services (existants ou non) dont une *blockchain* pourrait être le support, de tirer les leçons des retours d'expérience en Europe et partout dans le monde et sur ces bases d'entreprendre des réalisations pilotes, le cas échéant collectives voire transnationales.

5.2. Quelques exemples d'usages déjà existants

5.2.1. La blockchain comme support de transactions

Dans le secteur de la propriété littéraire et artistique, l'usage de *blockchains* comme support de transactions est également envisageable, que ce soit entre joueurs et éditeurs de jeux vidéos, ou entre les joueurs eux-mêmes. En effet, certains jeux vidéos en ligne nécessitent l'enregistrement des transactions entre joueurs, notamment pour résoudre les conflits en cas de fraude. Aujourd'hui effectué par des bases de données distribuées entre joueurs, cet enregistrement repose sur des algorithmes qui doivent concilier un équilibre entre sécurité, d'une part, et légèreté d'utilisation et coût réduit pour l'hébergeur d'autre part. Des solutions de la famille des *blockchains* pourraient permettre de renforcer le premier aspect tout en permettant de ne pas ralentir indûment le déroulement du jeu.

Dans une perspective peut-être plus éloignée, la *blockchain* pourrait servir à enregistrer les transactions entre consommateurs sur des produits culturels numérisables, permettant, par exemple, le développement d'un marché du livre numérique d'occasion en garantissant que le même livre n'est pas à la fois vendu et conservé par son premier propriétaire.

5.2.2. La blockchain pour la traçabilité

Le secteur de la propriété littéraire et artistique semble un lieu d'application naturel de l'usage de la *blockchain* pour assurer la traçabilité et l'authenticité de biens (numériques ou non). En effet, les problématiques de paternité d'une œuvre et d'authenticité, qui y sont centrales, pourraient bénéficier des nombreux avantages de cette technologie.

La description initiale[19] de cet usage a certainement fait songer le lecteur au dépôt d'un manuscrit. C'est donc très logiquement que la *start-up* Ascribe[20] propose à ses clients d'enregistrer la trace de leurs écrits sur la *blockchain,* pour être en mesure, par la suite, d'en revendiquer l'attribution, mais aussi pour les distribuer, par exemple sous la forme d'éditions limitées.

De même, en France, la *start-up* Seezart[21] souhaite proposer aux artistes d'enregistrer sur la *blockchain* les certificats d'authenticité de leurs œuvres lorsqu'elles quittent l'atelier, afin de fournir aux acheteurs ultérieurs une garantie supplémentaire de la provenance de l'œuvre. La *blockchain* permettrait également de suivre la vie de l'œuvre en enregistrant les changements de propriétaire ou, par exemple, les passages chez un restaurateur.

Cependant, lorsque plusieurs artistes ou acteurs (interprète, producteur, etc.) pourront prétendre à des droits sur une même œuvre, la question de la personne ayant qualité pour définir et publier dans la *blockchain* le partage de ces droits reste ouverte. Comme le souligne le rapport de l'université du Middlesex consacré à la musique sur la *blockchain*[22], les questions « qui entrera les données ? » relatives aux droits sur un morceau de musique et « comment ces données seront-elles vérifiées ? » seront essentielles à résoudre.

Le développement d'un tel usage risque également de se heurter aux difficultés de réunir dans un même registre l'ensemble des données relatives aux droits sur les œuvres musicales, comme l'échec de la Global Repertoire Database en 2014 l'a montré.

5.2.3. Des smart contracts *culturels*

Les *smart contracts* sont sans doute l'application de la *blockchain* dans le domaine de la propriété littéraire et artistique la plus souvent citée, notamment dans la perspective d'automatiser la collecte et le reversement des droits d'auteurs et des droits voisins.

Une *start-up* comme Ujo Music ambitionne ainsi de rendre obsolètes – ou de se substituer – aux organismes de gestion collective en permettant aux musiciens de percevoir directement et immédiatement les droits sur leurs œuvres lorsque celles-ci sont jouées. On pourrait ainsi concevoir que, dans une discothèque, un dispositif possédant un micro enregistre la musique diffusée, reconnaisse le morceau, identifie dans la *blockchain* les ayants droit et exécute le contrat en leur reversant le montant des droits correspondants. Si une telle application permettrait, dans des cas très simples (artiste unique, consommateur unique, tarif défini) l'absence d'intermédiaire, il est probable qu'elle requerra le plus souvent l'intervention de tierces parties, que ce soit aux stades de l'élaboration du morceau de musique (compositeur, interprètes, producteur, etc.), de la

19 Voir la partie 3.2 de ce rapport
20 https://ascribe.io https://www.ascribe.io/
21 http://www.seezart.com

définition de la répartition des droits ou encore de la négociation du tarif de diffusion (fixe ou en pourcentage du chiffre d'affaires, etc.). L'utilisation des *smart contracts* permettrait potentiellement de gagner en rapidité et en transparence, mais ne signerait certainement pas la disparition de ces intermédiaires, dont l'utilité se situe d'abord dans la mission de conseil et de représentation qu'ils peuvent fournir aux ayants-droits et aux artistes, ceux-ci conservant en outre un rôle non négligeable de prescripteurs aux yeux des consommateurs.

Une autre application des *smart contracts* dans les industries culturelles, peut-être à plus court terme, pourrait être la facilitation du financement collectif (*crowd funding*) sur le modèle d'une DAO. Un artiste pourrait ainsi solliciter des financements et proposer la réversion automatique de « dividendes » ou de copies de l'œuvre grâce à un *smart contract.*

5.3. Les potentialités actuelles et futures des différents types de *blockchain* doivent être mieux comprises

L'enthousiasme croissant pour la *blockchain* ne doit cependant pas occulter les interrogations sur les capacités et les conditions de mise en œuvre des différentes plateformes, immédiatement et à terme. Même si le stade de la maturité technique est atteint et que certains usages particulièrement pertinents ont réussi à trouver leur place, la pertinence de la *blockchain*, qui évoluera au cours du temps, reste à démontrer pour de nombreuses applications.

Chaque année, le cabinet de conseil américain Gartner, spécialisé dans les nouvelles technologies, publie une « courbe du hype » qui classe les nouvelles technologies par degré de maturité, notamment en ce qui concerne l'identification de leurs applications les plus adaptées. En 2017, la *blockchain* figurait au pic des « attentes exagérées », ce qui laisse présager certaines déceptions avant qu'elle ne soit mise en œuvre, à large échelle. Gartner retenait ainsi un horizon de 5 à 10 ans avant que la *blockchain* ne parvienne à un tel « plateau de productivité »[23], échéance classique pour ce type d'innovation.

Aux incertitudes sur le réel potentiel d'applications de la *blockchain* s'ajoutent en outre les tensions plus philosophiques qui demeurent entre le système de valeurs libertaire ayant présidé à sa naissance et son appropriation par des grands acteurs économiques ou institutionnels que cette technologie avait initialement pour ambition de supplanter dans l'esprit de ses premiers concepteurs.

Elles reflètent l'ambivalence de la *blockchain*, dont il est pour l'heure difficile de dire si elle viendra bouleverser les équilibres des secteurs économiques dans lesquelles elle trouvera à s'appliquer, favorisant l'émergence de *start-ups* proposant un modèle innovant fondé sur cette technologie, ou si elle viendra au contraire renforcer les acteurs existants en leur faisant gagner en efficacité et en sécurité. Il est imaginable qu'elle fasse parfois l'un, parfois l'autre.

Enfin, au-delà de ces questions théoriques, il convient de rappeler les problèmes pratiques susceptibles de surgir si le fonctionnement fiable de nombreuses applications venait à

23À titre d'exemple, Gartner classe au même niveau « d'attente exagérée » la maison connectée et les véhicules autonomes.

reposer sur quelques grandes *blockchains* (Bitcoin et Ethereum étant les plus souvent citées) dont la stabilité, la maîtrise et la gouvernance demeurent discutables, et qui ne manqueront sans doute pas d'évoluer. La volatilité récente de la monnaie *bitcoin*[24], la concentration des capacités de calcul permettant l'écriture de la *blockchain* dans un nombre très restreint d'Etats[25] et les difficultés d'émergence d'un consensus sur l'évolution technique de la *blockchain* Bitcoin en sont autant d'illustrations[26].

24*Quartz*, 31 déc. 2016
25 *The New York Times*, 29 juin 2016
26*Le Monde*, 22 mars 2016

6. Conclusion : la *blockchain*, quels enjeux pour la puissance publique ?

Au terme de cette exploration de la *blockchain* et de ses usages, les présidents de la mission voudraient souligner leur sentiment premier, qui est que cette technologie, porteuse de bénéfices substantiels pour les secteurs dans lesquels elle trouvera à s'appliquer, n'en est aujourd'hui qu'à un stade d'appropriation précoce mais qui évolue rapidement. La réaction des acteurs établis consiste pour l'essentiel en une posture proactive, qui s'exprime le plus souvent sous la forme d'applications pilotes destinées à mieux maîtriser le fonctionnement de la technologie, à prouver que certains concepts d'utilisations sont viables, à identifier des solutions aux problèmes contractuels et réglementaires posés, à construire de nouvelles relations d'affaires et à apprendre à accompagner ces changements. De même, les *start-ups* qui font de la *blockchain* le cœur de leur proposition de valeur sont, pour la plupart, dans les premières phases d'élaboration de leur offre et n'ont guère entamé sa mise en production à grande échelle.

Cependant, les changements majeurs que pourraient introduire les usages de cette technologie ne peuvent qu'inciter les acteurs du monde culturel à s'intéresser à celle-ci et à développer de premiers projets, l'innovation étant plus à même que l'attentisme de suivre (voire devancer) des pratiques culturelles en constante évolution.

Que ce soit sous la forme de rapports[27], d'expérimentations d'usages publics ou d'interventions législatives visant à faciliter les réalisations privées, les gouvernements ont, dans l'ensemble, saisi l'intérêt qu'il y a à accompagner positivement l'émergence de cette technologie et de ses utilisations sans l'entraver précocement par une réglementation dédiée.

Pour autant, la présente mission souhaite dessiner deux grandes pistes pour l'intervention de la puissance publique en matière d'appropriation de la *blockchain*.

La première concerne l'Etat comme régulateur des usages de la *blockchain*. Outre la reconnaissance de la valeur de preuve de la *blockchain*, potentiellement jurisprudentielle, l'utilisation croissante de cette dernière appellera une réflexion sur la définition des règles du jeu, qu'il s'agisse de protéger les consommateurs, par exemple en identifiant un responsable en cas de défaillance d'un *smart contract* ou en fixant les règles de qualité qu'une *blockchain* doit respecter pour être regardée comme fiable au regard d'un usage, de garantir l'exécution des décisions de justice dans la *blockchain* ou d'appliquer dans ce domaine les règles du droit au respect de la vie privée ou de la lutte contre la fraude (*know your customer*). Les questions de territorialité des opérations réalisées sur la *blockchain* se poseront aussi très probablement, comme aujourd'hui pour les transactions numériques.

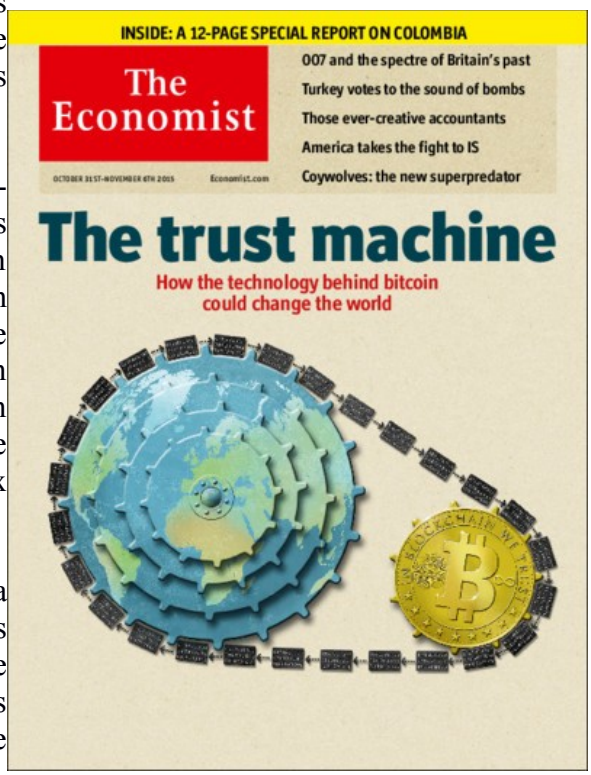
27Voir, outre le rapport précité de l'Etat du Vermont, celui du Government Office for Science du Royaume-Uni,

La seconde piste fait intervenir l'Etat comme acteur de la *blockchain*. Les premières applications gouvernementales de la *blockchain* décrites dans ce rapport sont autant d'exemples de l'État comme utilisateur de cette technologie. La puissance publique et ses représentants seront cependant sans doute aussi amenés à jouer le rôle de tiers de confiance, directement ou par délégation, qu'il s'agisse de garantir la validité des informations entrées dans une *blockchain* ou de certifier, au bénéfice de ceux qui n'ont pas les connaissances ou le temps nécessaires pour en décortiquer le code, la fiabilité de cette dernière. Ce renforcement de la sécurité pourrait aussi passer par une réflexion sur l'opportunité de développer des capacités de « minage » nationales ou européennes, afin éviter qu'un seul État ne concentre, sur son territoire, la puissance de calcul nécessaire à l'altération de *blockchains* d'importance stratégique. Enfin, et peut-être surtout, la puissance publique pourra accompagner des acteurs privés dans leurs réalisaations d'applications incluant la *blockchain*, par exemple en favorisant voire en suscitant le regroupement des parties prenantes et en soutenant les projets qu'elles portent.

Annexe 1 : histoire de la technologie *blockchain*

L'arrivée dans le paysage médiatique

La technologie *blockchain* a été conçue et décrite pour la première fois fin 2008, dans un article publié par Satoshi Nakamoto[28]. Le but de cette technologie était de permettre le déploiement d'une monnaie électronique, le *bitcoin*, tout en évitant le recours à une autorité centrale pour enregistrer et fiabiliser les transactions. Née au cœur de la crise financière, la *blockchain* était donc à l'origine conçue, dans une perspective libertaire, comme un moyen de permettre des transactions financières émancipées de l'intervention des banques et banques centrales.



Outre le développement du *bitcoin* lui-même, entre la première transaction dans cette monnaie en mai 2010 et l'atteinte, fin 2017, d'une valeur totale de *bitcoins* en circulation équivalente à 200 milliards de dollars, la *blockchain* a pris de l'ampleur en suscitant l'intérêt au-delà de son application première et en se détachant peu à peu de l'image parfois négative associée aux « crypto-monnaies ».

La une consacrée par *The Economist* à la *blockchain* le 31 octobre 2015 peut sans doute servir de jalon à la prise de conscience, par le grand public, des possibilités offertes par cette technologie dans de multiples secteurs.

L'hebdomadaire britannique mettait ainsi en avant la principale promesse de la *blockchain* : permettre à des personnes n'ayant pas confiance l'une en l'autre de collaborer sans avoir recours à une autorité centrale neutre.

La filiation scientifique et l'innovation capitale de Satoshi Nakamoto

Proto-monnaies virtuelles

Les premiers travaux qui donneront naissance aux monnaies virtuelles (ou crypto-monnaies) datent des années 1990, avec par exemple les recherches de Nick Szabo sur le « bit gold » ou celles de David Chaum sur « ecash ». Le point commun de ces monnaies est d'être créées et transférées grâce à des techniques cryptologiques plutôt que par une autorité centralisée.

Cependant, plusieurs verrous technologiques empêchent le développement de ces monnaies. En 2008, le dernier verrou technologique restant réside dans l'immatérialité des échanges : lorsqu'une donnée informatique est copiée, la copie et l'originale

deviennent indistinguables ; dès lors, l'idée même d'une monnaie virtuelle semble compromise : c'est le problème de la « double dépense » (*double spending)*.

Le whitepaper *de Satoshi Nakamoto et le* bitcoin

Le « *bitcoin whitepaper* » de Satoshi Nakamoto, publié en 2008, est la première proposition réaliste permettant de résoudre ce problème de la « double dépense », en introduisant le concept de *blockchain*, qui permet d'assurer l'unicité de l'utilisation d'un *bitcoin*.

L'histoire du « *bitcoin whitepaper* » est entourée d'une aura de mystère : l'auteur, Satoshi Nakamoto, est un pseudonyme ; celui-ci n'est revendiqué par aucune personne réelle. Sa première publication fut le « *bitcoin whitepaper* ». La qualité de cette première version, le faible nombre d'erreurs de programmation qui furent trouvés par la suite et la maturité de l'ingénierie derrière le *bitcoin* laissent même à penser qu'il pourrait s'agir d'un groupe de personnes derrière cet avatar plutôt qu'une seule personne physique.

Le premier programme informatique implémentant les fonctionnalités décrites dans le « *bitcoin whitepaper* » est publié en 2009, toujours par Satoshi Nakamoto. Après qu'une communauté s'est formée autour du bitcoin et que celle-ci est devenue suffisamment active pour se développer d'elle-même, Satoshi Nakamoto a transféré le code informatique du programme à la communauté bitcoin, laissant à celle-ci le soin de faire évoluer et de publier les mises à jour de la monnaie virtuelle. Il n'a plus fait d'apparition depuis lors.

Même si l'idée fondamentale développée par Satoshi Nakamoto est la création d'une monnaie, la solution technique qu'il propose a par la suite inspiré de nombreux chercheurs et développeurs informatiques qui ont vu dans cette technologie des usages qui dépassent la seule utilisation comme monnaie.

Annexe 2 : comment fonctionne une *blockchain* ?

Le premier service que rend une *blockchain*, qui est de permettre à un utilisateur de se prévaloir d'une ressource numérique, est rendu possible par une technique cryptographique, le chiffrement asymétrique, connue depuis déjà plusieurs décennies et utilisées dans des contextes dépassant les *blockchains*. L'idée est de chiffrer un titre virtuel (qui n'est autre qu'une suite de 0 et de 1) avec un code secret, de sorte que le titre ne puisse être déverrouillé et utilisé que par le détenteur de la clef. Un parallèle dans le monde physique pourrait être le dépôt d'un titre de propriété (papier) dans une boîte transparente fermée avec un cadenas : n'importe qui peut voir le titre de propriété mais seul celui-ci qui possède la clef du cadenas peut utiliser celui-ci.

La principale contribution scientifique et technique de Satoshi Nakamoto est d'avoir proposé un ensemble de techniques permettant d'assurer le second service, c'est-à-dire permettant aux utilisateurs de se transférer des titres virtuels sans aucun organe centralisé de décision.

Les transferts de titres sur une *blockchain* sont réparties dans des blocs ; chaque bloc est lié à celui qui le précède (d'où le terme de *blockchain* : chaîne de blocs). Une fois le bloc « courant » rempli d'ordre de transferts, les participants au réseau de la *blockchain* (les « mineurs ») sont invités à résoudre un puzzle cryptographique dépendant du bloc et de la solution au puzzle cryptographique du bloc précédent. La résolution de ce puzzle est entièrement aléatoire et s'apparente plutôt à une loterie : chaque participant a une chance proportionnelle à la puissance de son ordinateur de trouver la solution en premier. Le premier mineur à trouver la solution du puzzle l'annonce à tous les autres ; ceux-ci vérifient que la solution proposée est correcte, le bloc est accepté par tous, les transactions dans ce bloc sont réputées valides et un nouveau bloc est créé.

Si un mineur mal intentionné souhaitait modifier une transaction d'un ancien bloc, celui-ci devrait résoudre les puzzles cryptographiques de tous les blocs suivants car chaque puzzle cryptographique dépend et du bloc auquel il est associé et de la solution du puzzle cryptographique du bloc précédent, si bien que changer une ancienne transaction invalide tous les puzzles cryptographiques postérieurs au bloc contenant la transaction à modifier.

La résolution de ces puzzles par les mineurs correspond à la « *proof of work » (POW)* de la technologie *blockchain*. La puissance de calcul nécessaire à la résolution d'un de ces puzzles est substantielle sans être hors de portée pour un mineur, mais la puissance de calcul nécessaire à la résolution de *tous* les puzzles cryptographiques d'un coup étant gigantesque[29], la modification d'un bloc déjà accepté (déjà « miné ») est, à défaut d'impossible, tout à fait irréaliste.

Pour inciter les mineurs à participer à la résolution de ces puzzles cryptographiques et ainsi à valider les blocs et les transferts de titres circulant sur une *blockchain*, le premier mineur à trouver une solution a le droit de percevoir une récompense sous la forme d'un titre qui est créé pour lui.

29En réalité, la puissance de calcul nécessaire s'adapte automatiquement, de sorte que la difficulté des puzzles cryptographiques à résoudre augmente avec la puissance de calcul totale des mineurs sur la *blockchain*.

Grâce à ce système, l'ensemble des utilisateurs d'une *blockchain* peuvent se mettre d'accord sur l'acceptation d'un transfert de titres, sans pour autant avoir recours à une autorité centrale. Chaque utilisateur a une chance de miner le prochain bloc et tous les autres pourront vérifier facilement que ce minage est licite.

Enfin, notons qu'aucune restriction technique ne pèse sur les participants à une *blockchain*. Si n'importe qui peut « miner » sur la *blockchain* on dit que celle-ci est publique et on supposera que les nombreux participants, dotés chacun d'intérêts divergents n'ont pas la possibilité de se mettre d'accord pour subvertir la *blockchain*, le nombre garantissant alors l'intégrité de celle-ci. Si, au contraire, une *blockchain* n'est disponible qu'à un petit groupe de participants (et même si les transactions peuvent y être observées par n'importe qui), on dira que cette *blockchain* est privée (ou « de *consortium* »). Dans ce dernier cas, les participants se connaissant *a priori*, une structure de gouvernance peut être mise en place, permettant la résolution de conflit entre les participants ou le choix d'une autorité centrale sur la *blockchain* dont la liste des transactions et blocs qu'elle accepte fera foi, ce qui éloigne une telle utilisation du modèle initial de la *blockchain*.

Annexe 3 : copie de la lettre de mission

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère Culture Communication

Paris, le 08 JUIL. 2016

Monsieur Jean-Pierre Dardayrol
Maître Jean Martin

Conseil supérieur de la propriété littéraire et artistique

182, rue Saint-Honoré
75033 Paris Cedex 01
France

Téléphone : 01 40 15 82 16
Télécopie : 01 40 15 88 45

cspla@culture.gouv.fr

http://www.culturecommunication.gouv.fr/Politiques-ministerielles/Propriete-litteraire-et-artistique/Conseil-superieur-de-la-propriete-litteraire-et-artistique

Monsieur, Maître, cher Jean-Pierre, cher Jean

Le succès des technologies de l'Internet a renforcé, dès le début des années 1990, l'intérêt pour les systèmes et les protocoles décentralisés, de la part des chercheurs, des entreprises puis des pouvoirs publics. Parallèlement, le succès du commerce en ligne a accompagné les progrès de la cryptographie. Dans ce contexte général, une novation parait particulièrement prometteuse, bien que parvenue aujourd'hui à des degrés différents de maturité et de complexité d'usage : les chaînes de blocs.

Les chaînes de blocs permettent de construire des bases de données décentralisées, sécurisées et historicisées d'événements. Elles présentent plusieurs avantages, du fait de cette décentralisation, de leur résilience et du faible coût des transactions. Elles présentent aussi des inconvénients, par exemple en termes de latence, d'interopérabilité ou de consommation d'énergie.

Le monde de la finance s'étant engagé activement dans leur appropriation, les chaînes de blocs ont permis depuis la fin des années 2000 l'éclosion de plateformes industrielles et d'environnements de développement, permettant de créer des applications variées, dont la plus emblématique concerne une crypto-monnaie. Des applications sont désormais en train d'apparaître dans l'univers des biens culturels, tant en Europe qu'aux États-Unis. Elles apparaissent comme prometteuses en raison des simplifications, de la sécurité et des baisses de coûts de transactions, notamment contractuels, qu'elles pourraient apporter.

Compte tenu de cet état de l'art, je souhaite que vous exploriez d'une part, l'état des lieux de cette technologie, et d'autre part, ses impacts potentiels sur la propriété littéraire et artistique. Il s'agira notamment d'évaluer ses apports pour la gestion des droits, l'accès aux œuvres ou encore l'optimisation des divers modes d'exploitation. Vous analyserez également les évolutions possibles en matière de contrôle de l'utilisation des

œuvres, dans un environnement de services distants dématérialisés et un cadre européen et internationalisé.

Je vous remercie vivement d'avoir accepté de prendre en charge cette mission, que vous pourrez conduire en vous entourant d'un comité de pilotage dont vous déterminerez la composition et en veillant à recueillir la diversité des analyses et expertises. Vous serez assistés en qualité de rapporteur par Monsieur Cyrille Beaufils, auditeur au Conseil d'État. Le cas échéant, vous pourrez vous adjoindre un second rapporteur. Vous établirez un rapport de mission pour le printemps de 2017, qui fera l'objet d'un premier rapport d'étape pour la fin de l'année.

Je vous remercie d'avoir accepté cette mission et vous prie de croire, Monsieur, Maître, à l'expression de mes sentiments distingués.

Et bien plus amicaux.

Le Président

Pierre-François Racine

Ministère de la culture et de la communication
Conseil supérieur de la propriété littéraire et artistique
(CSPLA)
182 rue Saint-Honoré
75033 Paris Cedex 01

Annexe 4 : liste des personnes et institutions auditionnées (ordre alphabétique)

Association pour le commerce et les services en ligne (ACSEL)
- Eric Barbry, administrateur, représentant au CPSLA

Agence nationale de la sécurité des systèmes d'information (ANSSI)
- Côme Berbain, sous-directeur adjoint de la sous-direction expertise

Allmedia
- Pierre-Alexis Ciavaldini, fondateur associé

Assemblée nationale
- Lionel Tardy, député

Banque de France
- Thierry Bedoin, directeur de l'organisation du système d'information

Bensoussan avocats
- Eric Barbry

Blockchain France
- Alexandre Stachtchenko, co-fondateur
- Matthieu Riche, stagiaire

Caisse des dépôts et consignations
- Philippe Dewost, directeur adjoint, mission "Programme d'Investissements d'Avenir"
- Nadia Filali, responsable du programme "*blockchain*"

Crystalchain
- Sylvain Cariou, associé

Dailymotion
- Clément Reix, chargé d'affaires publiques

École 42
- Françoix-Xavier Petit, directeur de l'innovation et des partenariats

Editis
- Virgine Clayssen, responsable de la stratégie numérique

Fieldfisher
- Simon Polrot, avocat

Hachette Livre
- Arnaud Robert, directeur juridique

HADOPI
- Jean-Michel Linois-Linkovskis, secrétaire général
- Anna Butlen, directrice des affaires générales, chef du bureau des affaires juridiques
- Stephan Edelbroich, directeur des systèmes d'information
- Didier Wang, ingénieur à la direction des études et de l'offre légale
- Olivia Bacin, avocat

IDATE
- Yves Gassot, directeur général
- Bertrand Copigneaux, consultant senior en innovation

Institut des hautes études sur la justice
- Antoine Garapon, secrétaire général

Ledger
- Nicolas Bacca, directeur général et technique
- Vanessa Rabesandratana, directrice de communication

Ismay Marçais avocats
- Ismay Marçais, avocate

Ministère de la Culture
- Nicolas Orsini, adjoint au chef du département de l'innovation numérique
- Bertrand Sajus, chargé de mission au département de l'innovation numérique

Open law
- Benjamin Jean, président
- Camille Charles, chargée de mission

SACEM
- Jean-Noël Tronc, directeur général
- Christophe Waignier, directeur des ressources et de la stratégie
- Charlotte Aïdan, responsable juridique des affaires internationales

SGDL
- Marie Sellier, présidente
- et Maïa Bensimon, responsable juridique

Seezart
- Jurgen Dsainbayonne, directeur général
- Sandra Dsainbayonne, directrice des opérations
- Knuth Posern, directeur technologique

Stormancer
- Jean-Michel Deruty, président directeur général

Télécom Paristech
- Patrick Waelbrock, professeur d'économie industrielle et d'économétrie

Colloques

ADAGP
- « La Traçabilité de l'œuvre d'art ou la force de son histoire », 28 septembre 2017

AFNOR
- « Nouveaux mécanismes de notarisation des transactions Comment normaliser la "*Blockchain*" ? », 17 octobre 2016

Conventions – Institut des hautes études sur la justice
- « *Blockchain* : quels défis pour le monde du droit ? », 15 décembre 2016

Conseil d'Etat
- « L'a-territorialité du droit à l'ère numérique », 28 septembre 2016

Séminaire organisé par la mission pour les membres du CSPLA

- Intervenants :
  - Stéphane Bortzmeyer de l'AFNIC sur les aspects fonctionnels et techniques,
  - Patrick Waelbroeck, professeur à Telecom ParisTech sur les domaines d'usages et l'écosystème.
  - Christophe Waignier, SACEM, directeur des ressources et de la stratégie, sur l'usage de la *blockchain* pour la gestion des identifiants musicaux, dans le monde et par la SACEM

- Participants
  - Debora Abramowicz, Procirep
  - Maia Bensimon, SGDL
  - Laurent Bérard-Quélin, FNPS
  - Léa Bernard, SNE
  - Boris Bizic, SNPS
  - Danielle Bourlange, APIE
  - Jean-Frank Cavanagh, GFII
  - Jean-François Debarnot, INA
  - Flore Grainger, SNE
  - Marie-Christine Leclerc-Senova, SCAM
  - Tania Lesaché, SNEP
  - Antoine Marie, ADAMI
  - Thierry Maillard, ADAGP
  - Benjamin Montels, USNAT
  - Gwenaêlle Masseron, CFC
  - Idzard van der Puyl, Procirep
  - Hubert Tilliet, SACD