SMART CONTRACTS

ÉTUDES DE CAS ET RÉFLEXIONS JURIDIQUES

Aurélie Bayle, Anna van der Aa, Pierre Banzet, Alice Barbet-Massin, Hanna-Mae Bisserier, Claire Leveneur Leveneur, Thibaut Labbé, Frédéric Laffy, Xavier Lavayssière, John Le Guen, Laetitia Maffei

OPEN LAW*
* Le droit ouvert

coala

ECAN

Table des matières

Introduction

Cet ouvrage est né de la nécessité de se plonger sur des cas d'utilisation précis de la blockchain et des smart contracts et de prendre le recul d'une analyse technique, juridique et économique. En effet, l'activité médiatique, la spéculation économique et les annonces commerciales rendent difficiles aux professions juridiques en particulier, et d'expertise en général, l'abord d'un sujet qui exige déjà une approche pluridisciplinaire.

D'autant que derrière les mots se cachent des solutions techniques, mais aussi des nouvelles mécaniques économique et des changements culturels. Ainsi, dans ce domaine, la force de la complémentarité des regards techniques et juridiques est d'apporter des précisions d'ordre terminologiques sans lesquelles il n'est pas possible de penser les concepts. Le lexique à la fin de cet ouvrage a pour vocation de fournir des définitions précises en distinguant les acceptions techniques et usuelles.

La ligne directrice de notre étude est de partir de l'opération spécifique projetée par les parties, d'envisager ses modalités techniques et de mener une analyse juridique et économique de l'opération. Trois sujets concrets en particulier ont été retenus :

- La traçabilité des œuvres d'art qui pose la question de la valeur des inscriptions et de la connection entre inscription virtuelle et objet physique ;
- Le transfert de propriété, au travers l'exemple des minibons, ouverts à l'utilisation de la blockchain comme support de transactions par l'ordonnance n° 2016-520 du 28 avril 2016, et l'exemple des ventes immobilières ;
- Enfin le sujet des ventes publiques de jetons, les ICO, sous l'angle particulier des "utility token", jetons représentant un droit d'utilisation dans une application.

Blockchain et Smart Contract

Le concept de "blockchain"[1] est apparu en 2008 dans l'article publié sous le pseudonyme de Satoshi Nakamoto présentant le bitcoin, une "monnaie" décentralisée. Désignant initialement le stockage de l'ensemble des transactions sous la forme de blocs, le terme s'applique aujourd'hui par synecdoque[2] à l'ensemble du protocole (cf. lexique).

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).
[2] La synecdoque (du grec συνεκδοχή / sunekdokhê, « compréhension simultanée ») est une métonymie particulière pour laquelle la relation entre le terme donné et le terme évoqué constitue une inclusion ou une dépendance matérielle ou conceptuelle (https://fr.wikipedia.org/wiki/Synecdoque (consulté le 06/01/2018)).

Les “smart contracts” sont des programmes informatiques exécutés de façon autonome par un réseau utilisant un protocole blockchain. Le concept a été popularisé par le projet Ethereum, né en 2013, qui permet ainsi de programmer des fonctionnalités avancées. Des projets comme Hyperledger ou Cardano proposent des fonctionnalités similaires.

Dès son origine, le concept de smart contract entretient un rapport étroit avec le droit. Il a été pensé dans les années 1990 par Nick Szabo[3] comme un protocole informatique de contractualisation. Nick Szabo présente ainsi l’exemple des distributeurs automatiques qui par leur mécanismes garantissent, sous réserve de faille matérielle, le déroulement de la transaction, depuis l’insertion d’une pièce de monnaie jusqu'à la livraison du produit au vendeur comme à l’acheteur. Le smart contract se veut l’équivalent cryptographique de ce mecanisme physique

L’implémentation de ces dispositifs ouvre pour certains de leurs promoteurs la perspective d’une société où les rapports sociaux, ou au moins certains rapports commerciaux, seraient garantis par l'exécution autonome des programmes informatiques. Toutefois la pratique a montré la nécessité de penser en amont l’articulation de ces mécanismes et du droit.

Si les différentes implémentations diffèrent, on peut dégager les propriétés communes suivantes :

1. **Autonome** : Une fois déployé, il n'est pas possible de modifier ou d’empêcher l’exécution du smart contract sauf par des procédures prévues au préalable dans son code.

2. **Financier** : Il est possible via le smart-contract de gérer des fonds, recevoir des paiements et de générer un versement en cryptoactif.

3. **Traçable** : Chaque exécution est tracée par une transaction enregistrée dans la blockchain. De plus chaque interaction avec le smart contract est identifiée à une adresse individuelle, et donc un individu, ou un autre smart-contract.

4. **Déterministe** : Le programme s’exécute selon les procédures décrites par le code sans aléa, sous réserve d’erreur logicielle.

Ces technologies proposent un dialogue avec notre système juridique. Quels concepts juridiques peuvent s’adapter ? Quelles nouvelles pratiques sont susceptibles d’émerger? Une réglementation propre devrait-elle être envisagée ? Quels objectifs de la réglementation peuvent être assurés par des procédés techniques ? C’est pour explorer ces nouvelles questions que nous avons travaillé à démêler ce lien entre nouvelles technologies et droit.

Smart Contracts et institutions

La perte de confiance dans le système bancaire et financier résultant de la crise de 2008 n’est pas étrangère au succès, depuis 2009, du Bitcoin et autres cryptomonnaies. Ces réseaux ouverts, gouvernés en partie par des règles algorithmiques connues de tous, permettant de transmettre des unités de valeur sur l’ensemble de la planète offrent une

[3] Szabo, Nick. "Formalizing and securing relationships on public networks." First Monday 2.9 (1997).

alternative. Pour autant il est aussi envisagé d'utiliser le même ensemble de technologies au sein d'un réseau fermé pour optimiser des processus, faciliter les échanges et accroître la transparence.

Ces deux mouvements parallèles et en partie opposés donnent aux pouvoirs publics une attitude ambivalente. Ainsi, tandis que les ordonnances de 2016 et 2017 préparent la possibilité de l'utilisation de registres distribués pour la transmissions de certains titres en France (cf. infra. « Minibons et Titres Financiers »), la possibilité d'offrir et de vendre des unités de valeur au public est sujette au à des attitudes nuancées des différents régulateurs (cf. Infra « ICO »).

La Smart Contract Academy

La Smart Contract Academy est un programme collaboratif d'analyse juridique et économique relatif à l'impact des technologies blockchain sur une sélection de cas d'usages.

La Smart Contract Academy s'est réunie depuis son lancement le 20 mai 2017 au Square Innovation Lab. Sélectionnés sur candidature, la vingtaine de participants présente des profils complémentaires, à dominante juridique et avec en moyenne trois années d'expérience en programmation.

Les ateliers d'ingénierie participatifs se sont tenus de façon mensuelle, enrichis d'apports extérieurs et de la présence d'une équipe de mentors comprenant Primavera de Filippi, chercheuse au CNRS et fellow au Berkman Klein Center d'Harvard et Simon Polrot, confondateur de Variabl.io. Pionnier de la réflexion sur ces questions en France, ce groupe de travail à permis de nourrir la réflexion d'entreprises et institutions au cours de l'année.

Organisé dans la continuité du cycle Smart contracts mené en 2016, ce programme est issu d'un partenariat entre l'association Open Law* le Droit Ouvert, qui applique l'innovation ouverte à la transformation numérique du monde du droit, l'ECAN, entreprise de prototypage et de formation sur les technologies blockchain et Coala Lex, initiative internationale traitant des questions droit et blockchain.

Xavier Lavayssière

▸ Smart contract et droit français

Modalité d'exécution d'un contrat existant ou contrat à part entière ?
Dans la plupart des cas, un smart contract est une simple modalité d'exécution d'un contrat existant. La principale caractéristique qui le distingue d'un programme informatique classique est l'autonomie de son exécution. C'est le cas le plus courant que l'on voit dans les offres "smart contract" proposées par des entreprises existantes.

Dans le cas plus rare où les parties entendent utiliser uniquement le smart contract comme support contractuel, en l'absence de tout contrat préalable ce qui est parfois observé pour certaines Initial Coin Offerings (ICO), rien ne s'oppose en principe à la reconnaissance de sa valeur légale puisqu'en droit français, le contrat naît de l'accord de volonté des parties et son support peut être oral, écrit ou numérique. Il faudra toutefois vérifier que les conditions posées par l'article 1127-1 du code civil[4] sont remplies, en particulier celle relative à la communication des étapes à suivre pour conclure un contrat par voie électroniques.

Quelle sera la valeur juridique du code informatique traduisant cet accord de volontés ?

En matière civile, dans le cas d'une contestation entre un professionnel et un particulier dont la valeur n'excède pas 1500 euros, la preuve est libre : le contrat peut être prouvé par tout moyen. Il en va de même en matière commerciale, pour la preuve des actes de commerce quel que soit le montant de la transaction[5].

Lorsque la preuve n'est pas libre, le code informatique pourra être considéré comme un écrit en tant que « suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quel que soit leur support »[6], mais c'est seulement s'il remplit également les conditions relatives aux éléments d'identification et de conservation du programme (cf. fiche sur la preuve).

Le smart contract est un programme qui permet de garantir l'exécution d'engagements pris sans intervention humaine directe. Par principe le programme n'est pas modifiable une fois déployé sur la blockchain. Cette immutabilité est susceptible de créer des situations de fait difficiles à résoudre juridiquement. Les procédures de modification et les diverses situations susceptibles de survenir doivent donc être anticipées dans le code, entre les parties et dans le cadre juridique .

Par exemple, comment prendre en compte :

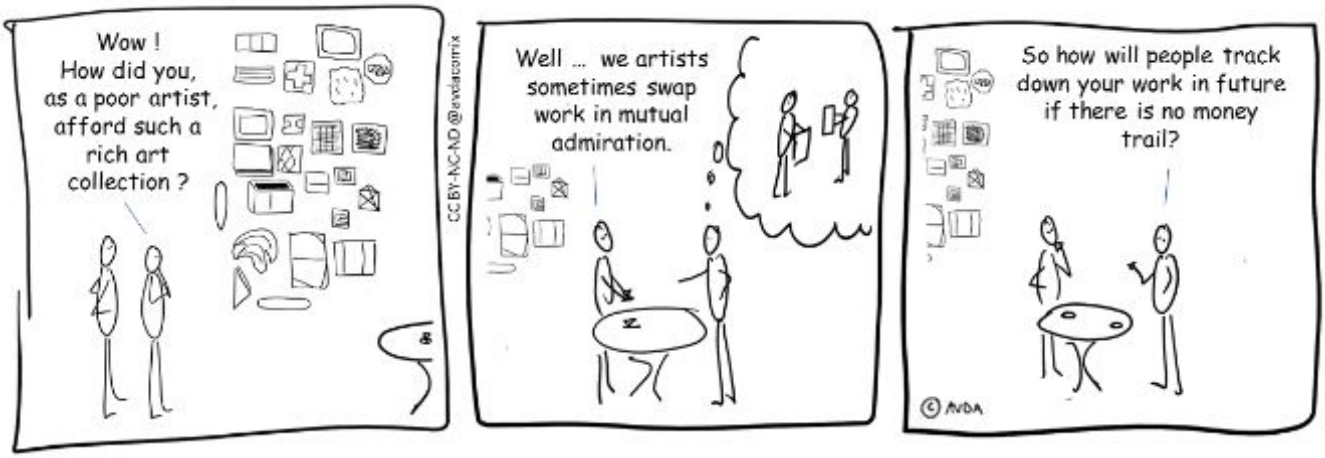
[4] Cet article s'applique à « *quiconque propose à titre professionnel, par voie électronique, la fourniture de biens ou la prestation de services, met à disposition les stipulations contractuelles applicables d'une manière qui permette leur conservation et leur reproduction* »
[5] Article L.110-3 du code de commerce.
[6] Article 1365 du code civil.

- La modification du contrat conformément à la volonté commune des deux parties ; la rétractation d'une des parties.
- La mauvaise exécution (ou inexécution) issue d'une erreur de manipulation ou tentative frauduleuse.
- Les bugs ou le mauvais fonctionnement du programme. Des questions de responsabilité civile peuvent se poser dans ce cas entre les parties et vis-à-vis des développeurs du programme informatique.
- Les effets de l'annulation du contrat original, de l'intervention du juge ou éventuellement d'arbitres, de l'ouverture d'une procédure collective…

Il faut aussi souligner que l'automaticité du processus empêche le jeu normal des dispositions sur l'inexécution du contrat des articles 1217 et suivants du code civil, dès lors qu'il n'y a en principe plus de place pour l'inexécution. Il faudra alors penser les remèdes aux difficultés d'exécution ou aux vices affectants le « smart contract », voire son contrat cadre, *a posteriori*, par des mesures correctrices : le contentieux risque se déplacer de l'inexécution ou de la mauvaise exécution vers le contentieux post exécution ;

I. La traçabilité des œuvres d'art

La question de l'échange d'œuvres d'art entre jeunes artistes est un sujet particulièrement riche et qui permet d'aborder la question de la traçabilité en général. Cette pratique consiste pour des artistes à échanger des œuvres par reconnaissance mutuelle. Il s'agit d'une pratique marginale qui pose des questions intéressantes en matière d'anonymat, de traçabilité et de valeur de la preuve.



Anna van der Aa

Enjeu de l'anonymat et traçabilité dans le marché de l'art

Le marché de l'art rassemble des acteurs aux profils très divers : artistes, galeries, maisons de vente, courtiers, institutions, collectionneurs, commissaires et critiques.

Les galeries représentent une partie des artistes, qu'elles se partagent traditionnellement selon des critères géographiques. Elles se scindent entre les galeries « locales » et celles qui ont réussi à suivre l'internationalisation du marché de l'art en ouvrant des antennes dans plusieurs villes. Les vendeurs comptent aussi les maisons de vente, au premier titre desquelles se trouvent Christie's et Sotheby's, ainsi que de nouvelles plateformes rassemblant un panel de galeries, comme Artsy, Artspace ou Artsper. Enfin, il y a les courtiers qui ont un rôle important dans un marché plus officieux.

Les institutions, avec les commissaires et les critiques, sont des canaux de légitimation de la cote de l'artiste. Depuis peu, les réseaux sociaux viennent alimenter l'aura de l'œuvre ou de l'artiste via des communautés plus ou moins spécialisées.

Les acheteurs couvrent un spectre large, allant du simple amateur au collectionneur averti, mêlant des préoccupations émotionnelles, d'investissement et de statut social. Les nouvelles institutions (musées, fondations) qui essaiment sur la planète (plus de 700 par an) et souhaitent apposer leur signature sur la carte, déroulent depuis une dizaine d'année une énergique politique d'acquisition. La financiarisation du marché a également pour conséquence l'arrivée des gestionnaires de fortune.

La cote d'un artiste repose sur un délicat équilibre entre ces divers acteurs. Cependant, le marché de l'art se caractérise par la position dominante d'un nombre réduit de collectionneurs, eux-mêmes souvent propriétaires de galeries, maisons de vente et institutions et qui ont un poids prépondérant dans la définition de la valeur de l'œuvre. Parallèlement à ces faiseurs de marché, on compte nombre de collectionneurs qui au contraire souhaiteraient conserver l'anonymat, tout en suivant ces tendances. Leur intérêt financier est de suivre le consensus. En agissant ainsi, ils le renforcent.

L'enjeu des galeries, courtiers et maisons de vente est de prôner leurs artistes auprès des faiseurs de marchés et d'assurer la discrétion de ceux qui souhaitent que leurs investissements restent confidentiels, tout en garantissant la traçabilité des œuvres et des transactions financières.

Fréderic Laffy et Lætitia Maffei

Les solutions techniques à l'anonymat & traçabilité?

L'une des caractéristiques souvent mise en avant pour les usages de la blockchain, comme un point positif ou négatif, est l'anonymat. En effet, cela peut être vu comme un avantage pour éviter d'exposer ses transactions à la vue des concurrents, pour ne pas dévoiler ses fournisseurs par exemple, mais aussi comme un inconvénient quand on parle

de transactions illégales. Quelles sont les techniques permettant de garantir une certaine forme d'anonymat à ces systèmes, tout en se prévalant de garantir la validité des transactions ?

Certains systèmes tels que le protocole Bitcoin ne sont que pseudo-anonymes. En effet, chaque utilisateur est identifié par une adresse bitcoin qui ne dit rien sur son identité réelle. Ce numéro circule cependant en clair dans la blockchain et il est possible de suivre toutes les transactions émises/reçues par ce dernier. On peut imaginer que par l'analyse de ces transactions, ou encore en rapprochant l'utilisation de cette adresse bitcoin à une localisation via la topologie du réseau, il serait possible de découvrir qui en est le propriétaire.

Pour garantir la validation, qui est un protocole défini publiquement, tout en assurant la confidentialité des données fournies (input) et des données renvoyées (output), certaines plateformes utilisent le chiffrement homomorphe (homomorphic encryption) sur ces données. La caractéristique de ce chiffrement est qu'une opération sur les données chiffrées donnera le même résultat que sur les données non chiffrées. Il est donc possible de travailler sur les données sans avoir besoin de savoir ce qu'elles contiennent. Il devient ainsi quasiment impossible de suivre les paiements d'un portefeuille (ou "wallet") donné : vu de l'extérieur, l'adresse de ce wallet ne sera jamais la même. Pour chiffrer et déchiffrer les données, des jeux de clés privée/publique sont utilisés. Cela garantit que seules les personnes détenant la clé privée seront en capacité de lire ces données en clair, préalablement cryptées grâce à la clé publique correspondante.

Pierre Banzet – TransChain

Exemple et présentation d'un smart contract

```solidity
pragma solidity 0.4.21;


contract ArtTradeBasic {

  event Transfer(address indexed _from, address indexed _to, uint256 _objectId);

  // Association des objets vers leurs propriétaires
  mapping (uint256 => address) internal objectOwner;

  // Renvoie le propriétaire d'un objet donné
  function ownerOf(uint256 _objectId) public view returns (address) {
    address owner = objectOwner[_objectId];
    return owner;
  }

  // Transfert la propriété d'un objet
  function transferObject( address _to, uint256 _objectId) public {

    // Vérifie que l'on est bien en présence du propriétaire
    require(ownerOf(_objectId) == msg.sender);

    // Changer la propriété de l'objet
    objectOwner[_objectId] = _to;

    emit Transfer(msg.sender, _to, _objectId);
  }

}

```

Le smart contrat ci-dessus utilise les mêmes principes qu'un jeton pour modéliser un titre de propriété sur une œuvre.

- Chaque objet est représenté par un identifiant unique
- Chaque identifiant est associé à une adresse sur Ethereum. L'association est enregistrée dans *objectOwner*
- La fonction *ownerOf* permet à une interface externe d'obtenir l'adresse du propriétaire d'un objet.
- La fonction *transferObject* permet de transférer la propriété. Elle vérifie dans un premier temps que l'adresse de l'émetteur de la transaction correspond bien au propriétaire actuel.

https://github.com/Xalava/ArtTrade

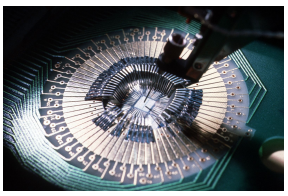
▸ Le lien entre un objet physique et une identité numérique

Le problème du lien entre une inscription numérique et un objet physique n'est pas nouveau. Mais l'immutabilité de l'inscription sur une blockchain, et la valeur probante que l'on souhaite lui donner, exige une précision accrue. Voici quelques-unes des solutions qui peuvent être retenues :

Identification par analyse
A partir d'une image ou d'une analyse d'une propriété précise d'un objet ou d'une œuvre, il est possible d'enregistrer certaines de ses caractéristiques et imperfections. Cette empreinte visuelle pourra alors être associée à l'empreinte numérique de l'objet dans le futur pour l'identifier, comme dans le cas de l'identification biométrique. La difficulté réside dans la sélection de points d'observation relativement uniques et stables dans le temps.

Tatouage
L'inscription d'un identifiant dans une œuvre ou un objet qui peut prendre plusieurs formes, comme un numéro de série inscrit au laser ou un simple QR code apposé. L'authenticité de l'objet n'est toutefois pas établie.

Défi cryptographique
Les solutions les plus rigoureuses sont à l'image de celles implémentées dans nos cartes à puce. Une puce contient une clé privée inaccessible et inconnue de tous qui permet de signer les messages qui lui sont présentés. Ainsi, même en connaissant l'identifiant public d'un objet, il n'est pas possible de le dupliquer.



Le droit de la preuve des œuvres d'art

L'auteur d'une œuvre de l'esprit est en théorie titulaire d'un droit d'auteur sur celle-ci dès qu'il met en forme sa création. Mais en pratique, il doit démontrer qu'il est effectivement à l'origine de cette œuvre. En effet, bien qu'une œuvre soit "du seul fait de sa création" protégée par le droit d'auteur[7] et ce, dès lors que le processus créatif a débuté[8], une preuve de cette création peut fréquemment se révéler essentielle. Aucune formalité, aucun

[7] C. propr. intell., art. L111-1.
[8] C. propr. intell., art. L111-2 : peu importe l'achèvement ou non de l'oeuvre.

dépôt ne concourt, en principe, à la naissance du droit d'auteur mais lors d'un litige en contrefaçon, l'auteur ayant initié l'action doit, prouver qu'il est réellement l'auteur de l'œuvre, que celle-ci est originale et que l'œuvre attaquée présente des ressemblances manifestes caractérisant la contrefaçon. Cette démarche répond aux exigences de droit commun de la preuve qui disposent que « celui qui réclame l'exécution d'une obligation doit la prouver » et « qu'il incombe à chaque partie de prouver, conformément à la loi, les faits nécessaires au succès de ses prétentions »[9]. Ainsi, la « plus personnelle de toutes les propriétés »[10] qui unit l'auteur et son œuvre doit être sécurisée par l'auteur avec la pré-constitution en amont de preuve. A défaut, ce "droit de propriété" pourrait se trouver gravement mis à mal[11]. Alors que le régime juridique de la preuve des œuvres d'art peut faire fi de certaines carences, les protocoles blockchain apparaissent être une solution probatoire prometteuse.

Problématiques juridiques et pratiques

Antériorité

Par principe, « la qualité d'auteur appartient, sauf preuve contraire, à celui ou à ceux sous le nom de qui l'œuvre est divulguée »[12]. Cette présomption de titularité des droits d'auteurs d'ordre publique relève exclusivement de la loi et non de règles posées par des sociétés d'auteur notamment[13]. L'auteur devra donc prouver qu'il a - antérieurement à un prétendu contrefacteur - divulgué son œuvre sous son nom pour bénéficier de cette présomption. Nombre de contentieux attestent que dater l'antériorité d'une œuvre par rapport à une autre est finalement devenu primordial pour démontrer sa qualité d'auteur lors d'un litige[14]. La preuve de l'antériorité d'une œuvre est un fait et peut donc juridiquement être rapportée par tous moyens[15]. Il est d'usage d'utiliser plusieurs méthodes pour apporter cette preuve, comme le dépôt administratif d'une enveloppe "soleau" auprès de l'Institut Nationale de la Propriété Intellectuelle (INPI), le dépôt d'une enveloppe numérique "MaPreuve", les constatations par des officiers ministériels (constat d'huissier et le dépôt chez le notaire), le dépôt auprès d'agents assermentés, des sociétés de gestion collective, ou des sociétés privées. Certaines de ces démarches, qui manquent de fluidité, peuvent se révéler lourdes administrativement avec un formalisme contraignant. Du reste, la preuve par faisceau d'indices peut toujours être - bien que difficilement - constituée (croquis, ébauches, esquisses, brouillons, notes, correspondances, photographies…).

Traçabilité

Les transactions d'œuvres d'art classiques se fondent, pour la plupart, sur des supports papier qui peuvent être facilement perdus, volés ou falsifiés (conventions diverses, certificats d'authenticité, catalogues raisonnés…). Parallèlement, les œuvres numériques - de plus en plus nombreuses - ne permettent pas nécessairement d'avoir une trace

[9]C. civ., art. 1353 et C. pr. civ., art. 9.
[10]Le Chapellier, lors de la présentation de la première loi sur le Droit d'Auteur à l'assemblée, 1791.
[11]Selon l'adage latin « Idem est non esse et non probari », soit « avoir un droit sans le prouver revient à ne pas avoir de droit ».
[12]C. propr. intell., art. L113-1.
[13]Cass. civ, 1ère ch., 29 mars 1989 n°87-14.895.
[14]Par exemple, dans l'affaire « Prada contre SARL Cupidon », les juges ont considéré que les auteurs « ne démontraient pas être titulaires [antérieurs] des droits qu'ils invoquaient ; d'où il suit que le moyen ne peut être accueillie » (Cass. civ., 1ère ch., 15 janvier 2015, n°13-22798).
[15]C. civ., art. 1358.

certaine des cessions ou de leurs différentes exploitations. Les mutations digitales du marché de l'art rendent donc incertaine la provenance des œuvres.

Authenticité

Le crédit important donné aux expertises judiciaires et aux catalogues raisonnés par les tribunaux pour établir l'authenticité d'une œuvre peut être très discutable[16]. Un risque artistique pèse ainsi sur l'acquéreur d'une œuvre d'art. En outre, dans le cadre d'expertises en maison de vente, les experts spécialistes consacrés à l'étude de certains artistes précis sont peu nombreux. Il n'est généralement plus possible de nommer les spécialistes d'un artiste car ces derniers se sont souvent déjà prononcés à l'occasion de la vente aux enchères. Dans ce cas, ce sont des experts généralistes d'une période ou d'un mouvement artistique qui interviennent, dont les avis sont, de ce fait, critiquables. Enfin, l'exactitude et la méthode du catalogue raisonné peuvent être contestées[17]. Il est, en effet, possible que deux catalogues existent[18] ou encore que l'auteur du catalogue décide lors d'une nouvelle édition de ne plus intégrer une œuvre[19].

Co-titularité et répartition

Avec le développement de nouvelles formes de créations à propriétés multiples, telles que les créations collaboratives ou créations assistées par ordinateur et/ou intelligence artificielle, il n'est pas aisé d'identifier les contributions de chacun et d'allouer des parts et valeurs précises y afférentes alors que les tribunaux deviennent très exigeants quant à la preuve à apporter pour la co-titularité d'une création.

Coût

Les méthodes pour prouver la titularité d'une œuvre sont l'enveloppe "Soleau" de l'INPI ou des alternatives plus onéreuses telles que le constat d'huissier, le dépôt auprès d'agents assermentés, des sociétés de gestion collective, ou des sociétés privées.

Solutions avec la blockchain

Les apports techniques des protocoles blockchain

Les fonctions mathématiques de hachage - fonction mathématique à sens unique - permettent d'obtenir à partir d'une valeur d'entrée, une valeur de sortie appelée "empreinte

[16]Erreur des experts sur l'époque d'une statuette : Affaire « Sesostris III », Cass. civ. 1ère, 27-02-2007, n° 02-13.420, FS-P+B, Cassation ; contradiction des experts spécialistes et généralistes : Affaire « Solario », TGI Paris, 1ère ch., 1ère sect., 18 mars 1998, JurisData n°041658 ; prise en compte pour l'authenticité de la présence d'une œuvre dans le catalogue raisonné : TGI Lyon, 1re ch., 3 juill. 1974 ; absence de prise en compte du catalogue raisonné : Paris, pôle 2, 1ère ch., 15 mai 2012, RG n°10/06202.

[17]Le catalogue raisonné est l'ouvrage par lequel sont répertoriées, décrites, situées, classées et reproduites, les œuvres d'un auteur.

[18]TGI Paris, 1ère ch., 2e sect., 29 mai 1996, RG n°554/1994, Galerie Tamenaga c./Sté Schmit, Maguy Roche, NP.

[19]Affaire de la « Martiniquaise accroupie dans l'herbe », TGI Paris, 1re ch., 2e sect., 3 déc. 1976 (infirmé par Paris, 1ère ch., sect. A, 15 juin 1981, Juris Data n°023245) ou affaire « Le petit laveur », Paris, 1ère ch., sect. A, 15 juin 1981, JurisData n°023245.

numérique" ou "hash", soit une suite de caractères alphanumériques. Par ce biais, il est possible d'ancrer une œuvre, et seule l'empreinte numérique, issue de son ancrage, sera conservée dans la blockchain. Le changement d'une seule lettre de la valeur d'entrée peut donner une valeur de sortie complètement différente. La vérification de l'empreinte et de l'œuvre permet donc de s'assurer que l'œuvre n'est pas modifiée, ce qui garantit son intégrité. Par ailleurs, il semblerait que l'empreinte numérique soit davantage adaptée aux œuvres numériques, car il est plus difficile techniquement de lier une empreinte numérique à une œuvre physique (cf encart)[20].

La blockchain est assimilée à un registre public traçant les transactions de manière transparente. Elle renseigne l'heure et la date d'une transaction par l'inscription de son empreinte numérique. En ce sens, la datation par la blockchain d'une œuvre est techniquement fiable sous certaines conditions[21], bien que cette datation ne puisse constituer une date certaine au sens du droit civil[22]. Un titulaire de droit pourrait ainsi se pré-constituer une preuve de l'antériorité de son œuvre. Cette preuve pré-constituée n'attestera pas, en revanche, de la date réelle de la création, mais de la date de l'ancrage de l'œuvre. L'antériorité de l'ancrage d'une œuvre ne garantira pas non plus la véracité de la paternité de l'auteur puisque la question de la vérification de la personne ayant qualité pour enregistrer une œuvre dans une blockchain reste ouverte[23].

Une inscription sur blockchain permettrait, par ailleurs, une traçabilité infalsifiable des actes juridiques portant sur des œuvres d'art : prêt, legs, cession de droits, mandats de représentation et droits d'exploitation des galeristes... Une convention pourrait, en effet, devenir opposable aux tiers au moment de l'ancrage. En outre, l'inscription d'une sûreté attachée à un droit de propriété intellectuelle pourrait s'effectuer sur blockchain et aurait pour effet de servir de publicité.

Cependant, la blockchain ne prouverait pas avec certitude l'authenticité mais définirait le moment précis de l'ancrage. La preuve par blockchain vérifierait uniquement, avec l'empreinte, l'existence d'une œuvre ancrée à un instant donné.

Pour la répartition des parts d'une œuvre, l'ancrage permettrait d'avoir une preuve à l'origine des contributions. La preuve de valeur ("Proof of Value") - consensus selon lequel la validation des contributions est collective à partir d'un modèle de notes attribuées par les membres de la communauté - serait une aide supplémentaire pour cette répartition. Les jetons (token) symboliseraient une part permettant de la louer, céder ou vendre la quote-part de son œuvre.

---

[20] Voir les cas d'usages de Monegraph et Ascribe. Cependant Everledger – registre mondial de diamant – a largement fait ses preuves avec des technologies puissantes permettant d'agréger des données sur les diamants enregistrés (plus d'un million de diamant sur la blockchain).

[21] La fiabilité technique dépend notamment de la technologie utilisée et de la répartition réseau.

[22] Selon l'article du 1377 code civil "L'acte sous signature privée n'acquiert date certaine à l'égard des tiers que du jour où il a été enregistré, du jour de la mort d'un signataire, ou du jour où sa substance est constatée dans un acte authentique.", conditions qui ne sont pas remplies par la datation par la blockchain.

[23] Voir les rapports : Conseil Supérieur 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, janvier 2018, p.16 et Marcus O'Dair et al., Music On The Blockchain, Blockchain For Creative Industries Research Cluster, Middlesex University, rapport n° 1, juillet 2016.

Le faible coût des transactions d'individu à individu opérées via la blockchain s'avère être aussi une solution moins onéreuse que l'intervention d'huissiers, d'agents assermentés, de sociétés de gestion collective, ou de sociétés privées[24].

La valeur probatoire de la blockchain en droit

La blockchain ne dispose ni de reconnaissance légale stricto sensu en tant que preuve, ni de reconnaissance par les tribunaux. Par assimilation à la preuve littérale, la blockchain pourrait avoir la valeur d'un écrit électronique. Pour cela, l'auteur doit être dûment identifié et l'écrit électronique doit être établi et conservé dans des conditions de nature à en garantir l'intégrité[25]. Avec la blockchain cette "intégrité" requise pourrait être garantie par l'empreinte numérique (voir développement sur la fonction de hachage). Lors de transaction sur des blockchains publiques, il semble toutefois difficile de s'assurer systématiquement de l'identité de l'auteur de la transaction qui est anonyme/pseudonyme. En effet, la clé privée (signature) permet d'authentifier l'auteur (création d'un lien entre signataire et transaction) mais pas de l'identifier.

En outre, la blockchain utilise des procédés de la signature électronique (le chiffrement asymétrique et la fonction de hachage) mais la question se pose de savoir si celle-ci pourrait être qualifiée de signature électronique au sens juridique[26]. Pour cela, la signature électronique sur blockchain doit consister « en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache »[27]. Il existe trois catégories de signature électronique en droit français : simple, avancée ou qualifiée. Leur valeur juridique dépend de la fiabilité du système d'information qui permet de les créer. Le droit positif prévoit sous certaines conditions une présomption simple de fiabilité de ce procédé lorsque la signature électronique est qualifiée[28]. Pour être qualifiée, la signature doit, tout d'abord, être considérée comme avancée[29] puis répondre à certaines exigences du règlement dit "eIDAS" concernant son dispositif[30].

Premièrement, il semblerait que la condition d'identification du signataire soit encore difficilement remplie avec une blockchain publique (voir développement sur l'écrit électronique). Deuxièmement, pour bénéficier d'une présomption de fiabilité, il conviendrait que la signature sur blockchain soit générée à l'aide d'un dispositif de création de signature qualifiée qui repose sur un certificat qualifié de signature. Concrètement, il devrait être fait appel aux services d'un prestataire de service de confiance agréés pour obtenir un certificat qualifié de signature. Or, ces impératifs

[24]Par exemple, avec blockchain bitcoin, pour que le mineur ajoute rapidement une transaction à un bloc, il convient de dépenser environ 400 Satoshi par bytes de frais de transaction pour une transaction. Etant précisé qu'une transaction classique représente 226 bytes, les frais de transaction moyens s'élèvent donc approximativement à 14 euros par transaction. Plus la transaction est élevée, plus les frais de transaction seront proportionnellement faibles.

[25]C. civ., art. 1366.

[26]Voir : C. civ., art. 1367 et le décret n°2017-1416 du 28 sept. 2017 relatif à la signature électronique.

[27]C. civ., art. 1367, al.2.

[28]Article 1 du décret n°2017-1416 du 28 septembre 2017 relatif à la signature électronique.

[29]La signature est avancée dès lors qu'elle satisfait à quatre conditions techniques : a) être liée au signature de manière univoque, b) permettre d'identifier le signataire, c) avoir été créée à l'aide de données de création de signature électronique que la signature peut, avec un niveau de confiance élevée, utiliser sous un contrôle exclusif et d) être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable (article 26 du règlement n°910/2014 du 23 juillet 2014).

[30]Article 28 et 29 du règlement n°910/2014 du 23 juillet 2014.

semblent aller à l'encontre de l'architecture même de la blockchain qui a pour objectif de ne pas faire intervenir de tiers certificateur agréé.

Ce faisant, même si la signature électronique sur blockchain ne satisferait pas aux exigences requises par la signature électronique qualifiée et avancée, elle pourrait constituer à tout le moins une signature électronique simple[31]. Dans l'hypothèse d'un litige mettant en cause cette signature, il s'agira de convaincre le juge, notamment à l'appui d'expertises.

Aussi, l'horodatage sur blockchain pourrait bénéficier de la qualification d'horodatage électronique à condition de remplir les obligations mentionnées par le règlement dit "eIDAS". L'horodatage électronique qualifié présume la date et l'heure exacte qu'il indique et l'intégrité des données auxquelles se rapportent cette date et cette heure[32]. L'horodatage électronique qualifié exige aussi toutefois l'intervention d'un prestataire de service de confiance qualifié[33]. De la même manière que pour la signature électronique non qualifiée, si l'horodatage électronique n'était pas qualifié, il ne pourrait pas non plus être refusé comme preuve en justice[34].

Dans ce contexte, il conviendrait que le règlement dit "eIDAS" puisse faire l'objet d'une application souple lorsque des éléments de preuve par blockchain sont en cause. Il serait opportun aussi que l'Agence nationale de la sécurité des systèmes d'information (ANSSI) prenne position sur des bonnes pratiques à adopter permettant d'offrir une certaine sécurité juridique aux opérateurs quant au cadre juridique applicable. De même, il pourrait être envisageable de mettre en place un système de labellisation au même titre que celui de la Commission Nationale de l'Informatique et des Libertés (CNIL) eu égard à la conformité des produits et procédures relatifs au traitement de données à caractère personnel.

L'affaire récemment portée par la société "BlockchainyourIp" devant les tribunaux français précisera, en matière d'administration de la preuve, dans ce cas précis, si ce protocole blockchain - qui ancre dans la blockchain Bitcoin l'empreinte numérique de documents - pourrait être accepté dans ce litige[35]. A minima, en matière de contrefaçon, les juges ont déjà retenu des faisceaux de présomptions graves, précises et concordantes[36]. Au demeurant, la liberté de la preuve inhérente aux actions en contrefaçon devrait permettre d'utiliser la blockchain comme mode de preuve à un procès. Il conviendra inévitablement que les juges soient suffisamment formés pour vérifier les empreintes avec leurs œuvres correspondantes sans la nécessaire immixtion d'un huissier de justice en amont pour dresser un procès-verbal et d'un sapiteur technique pour traduire cette preuve lors du procès. Une intervention du législateur consacrant un nouveau mode légal de preuve ou une nouvelle présomption légale en matière de blockchain permettrait de lever tout doute.

[31]L'article 25 du règlement n°910/2014 du 23 juillet 2014 précise que « l'effet juridique et la recevabilité d'une signature électronique comme preuve en justice ne peuvent être refusés au seul motif que cette signature se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée ».

[32]Article 41 al. 2 du règlement n°910/2014 du 23 juillet 2014.

[33]Article 42 al. 1, c, du règlement n°910/2014 du 23 juillet 2014.

[34]Article 41 al. 3 du règlement n°910/2014 du 23 juillet 2014.

[35]http://blockchainyourip.com/ (consulté le 06/02/2018).

[36]CA Paris 4e ch., 29 avril 182 PIBD III 158 ; CA Amiens 4 février 1913 Ann. 1974, 73.

Il s'agira aussi qu'il se positionne sur la force probante de la blockchain, entre un acte authentique ou un simple acte sous-seing privé[37].

En définitive, la blockchain dans le domaine de l'art s'avérerait appropriée pour attester de la "vie" d'une œuvre, soit dater, tracer le processus de création, ainsi que sa chaîne de droits. Toutefois, à ce stade, elle ne peut pas se substituer intégralement aux modes de preuve existants. Il semble qu'il serait encore nécessaire d'intégrer un tiers de confiance pour garantir, notamment, l'authenticité et la paternité dans certaines blockchains[38]. Sans l'intervention d'un tiers certificateur, de surcroît, la signature et l'horodatage sur blockchain ne pourront bénéficier d'une fiabilité présumée. Alors que le processus de dématérialisation de la preuve est amorcé depuis plusieurs années, les autorités publiques doivent donc s'emparer des opportunités offertes par la blockchain au sujet de la preuve pour permettre à la France de conserver son attractivité et son statut de précurseur face à cette technologie.

Alice Barbet-Massin
Doctorante
Univ. Lille, CNRS, UMR 8026-CERAPS
August Debouzy

[37]Voir les discussions au parlement d'un amendement qui proposait de reconnaître la blockchain comme un acte authentique dans les opérations de règlement-livraison : Amendement N°CF2 déposé le 13 mai 2016 par Laure de La Raudière députée d'Eure-Et-Loire.

[38] Voir l'entreprise Seezart qui délivre son propre certificat d'authenticité qui n'est pas une garantie suffisante comparé à celui d'un expert.

▸ Smart contracts : Et le droit de la consommation ?

Le Code de la consommation, dans son article préliminaire[39], définit le consommateur comme « toute personne physique qui agit à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale ou libérale ». Le consommateur peut interagir avec un professionnel par voie électronique, en achetant en ligne ou souscrivant à certaines prestations dématérialisées. Or des transactions entre un professionnel et un consommateur peuvent être réalisées par l'intermédiaire d'un réseau blockchain.

Dès lors, se pose un certain nombre de problèmes concernant l'applicabilité des règles consuméristes à l'écosystème blockchain. Plusieurs cas d'usage en témoignent.

Par exemple, la création d'une assurance utilisant la technologie blockchain comme socle (Axa - Fizzy) pour automatiser et sécuriser les remboursements en cas de retard d'avion. Cette assurance enregistre les transactions dans une blockchain publique (Ethereum), via des smart contracts qui eux-mêmes sont interconnectés et programmés en fonction des données du trafic aérien mondial. Dès lors qu'un retard de plus de deux heures est constaté, les conditions du smart contract sont réalisées, et le souscripteur reçoit son indemnisation. Dans ce mécanisme, aucune intervention n'est, en théorie, requise post-formation du contrat, et cela renforce indubitablement la confiance entre compagnie d'assurance-vol et passager.

Ainsi, la blockchain ajoute de la confiance et une assurance d'être automatiquement remboursé ou indemnisé, dans un secteur où auparavant les démarches administratives pouvaient être lourdes et de fait, peu utilisées voire délaissées de par leur complexité et la perte de temps qu'ils engendraient. La blockchain apporte de la confiance par son architecture même, dans des situations et cas d'usages où les acteurs n'en avaient jusqu'alors que peu ou pas.

De fait, la multiplication des services et entreprises utilisant la blockchain comme moyen de sécurisation et de traçabilité, ou encore de support de smart contracts, pose la question du droit de la consommation. Mais comment l'appliquer ? Comment vérifier par exemple qu'un consommateur a bien été informé du prix et des conditions générales d'utilisation d'un produit commandé automatiquement au moyen d'un smart contract ? Doit-on, dans cette hypothèse, admettre le jeu du droit de rétractation offert au consommateur qui conclut un contrat à distance ? Comment vérifier que les droits du consommateur sont respectés si la serrure d'une location de vacances est automatiquement bloquée faute d'avoir reçu à temps le prix de la location ?

En attendant le développement de règles de droit propres à la blockchain, on peut sans doute imaginer que les circonstances ne diffèrent pas de la situation actuelle avec le commerce électronique. Si certains contentieux peuvent être évités, il sera toujours possible de saisir le juge pour faire valoir ses droits.

[39] Créé par LOI n°2014-344 du 17 mars 2014 - art. 3

En revanche, cette interaction entre juges, blockchain et smart contracts nécessitera une certaine adaptation et formation des juges aux complexités de la technologie blockchain, et l'appel à des experts judiciaires en la matière pour retranscrire toutes ces complexités au tribunal.

Aurélie Bayle

II. Le transfert de propriété

Minibons et titres financiers

Le droit français est un des premiers à avoir donné une consécration légale aux protocoles blockchain en introduisant un nouvel article dans le code monétaire et financier à ce sujet, issu de l'ordonnance n° 2016-520 du 28 avril 2016 relative aux bons de caisse : cette ordonnance a été prise suivant une habilitation du législateur afin de moderniser le régime juridique applicable aux bons de caisse et de permettre notamment l'inscription de leur émission dans une blockchain[40].

Le législateur est allé plus loin en autorisant, par la loi du 9 décembre 2016 dite « Sapin II », le gouvernement à prendre par voie d'ordonnance les mesures 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 non cotés[41]. Une première consultation publique a été initiée par la Direction générale du Trésor le 24 mars 2017 afin de recueillir les observations de l'ensemble des acteurs intéressés dans ce domaine, quant aux principes et au degré de réglementation à retenir dans le cadre de cette réforme. Le public a également eu

[40]JO du 29 avril 2016, n° 101, Rapport au Président de la République relatif à l'ordonnance n°2016-520 du 28 avril 2016 relative aux bons de caisse.

[41]Loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, art. 120.

l'occasion de se prononcer sur un projet d'ordonnance publié le 19 septembre 2017. Une ordonnance n° 2017-1674 du 8 décembre 2017 a finalement été adoptée à l'issue de ce processus d'élaboration de la norme, processus de plus en plus prisé par les rédacteurs européens.

L'ordonnance relative aux minibons

L'ordonnance n°2016-520 du 28 avril 2016 relative aux bons de caisse a pour objet de « moderniser le régime juridique applicable aux bons de caisse et de procéder aux adaptations nécessaires pour permettre l'intermédiation de ces titres sur les plateformes de financement participatif des conseillers en investissements participatifs (CIP) et des prestataires de services d'investissement (PSI) »[42].

Ces titres, qui sont remis par des sociétés en contrepartie d'un prêt qui leur est accordé[43] sont inscrits au nom de leur titulaire dans un registre spécialement tenu par leur émetteur[44]. À côté des règles de droit commun, cette ordonnance est plus particulièrement venue consacrer une nouvelle catégorie de bons de caisse – les minibons – dont le régime est détaillé aux articles L.223-6 à L.223-13 du code monétaire et financier (ci-après «CMF»). Contrairement aux bons de caisse traditionnels, ces instruments ont la particularité de pouvoir être échangés sur des plateformes de crowdfunding disposant du statut de conseiller en investissements participatifs ou de prestataire de services d'investissement.

L'intérêt du dispositif repose avant tout sur l'introduction d'un nouvel article L.223-12 dans le CMF, qui prévoit que l'émission et la cession de minibons peuvent désormais être inscrites dans un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations, autrement dit une blockchain. Pour certains, cette possibilité est une véritable révolution pour le droit des titres, ouvrant des perspectives pour le moins stimulantes[45] : le but est de remplacer le registre classique de titres et les ordres de mouvements par un protocole blockchain et éventuellement de lui ajouter une fonction permettant d'effectuer le paiement des transactions.

Cependant, l'article L.223-12 tel qu'il est rédigé ne suffit pas à entrevoir la réalité de la révolution annoncée puisque les conditions d'émission et de cession de minibons sur un protocole blockchain dépendent d'un décret en Conseil d'Etat. L'article L.223-12 précise en effet que ce dispositif d'enregistrement électronique partagé doit permettre l'authentification des opérations « dans des conditions notamment de sécurité, définies par décret en Conseil d'Etat ». Le rapport au Président de la République énonce à cette fin qu'un « groupe de travail devra déterminer les conditions de réalisation d'un tel projet, afin notamment de garantir que la technologie est assez sûre et mature pour assurer la tenue d'un registre électronique distribué fiable, sécurisé et susceptible d'être audité ».

Depuis la parution de l'ordonnance, le décret n'est toujours pas publié : les instances gouvernementales doivent encore être éclairées sur le sujet - en particulier sur ses caractéristiques techniques - et s'interrogent sur la stratégie de réglementation de ce

[42] JO du 29 avril 2016, n° 101, op. cit.
[43] C. mon. fin., art. L.223-1.
[44] C. mon. fin.. art. L.223-4.
[45] R. Vabres, "Bons de caisse, minibons, blockchain... résurrection ou révolution ?" Droit des sociétés n° 7, Juillet 2016.

nouveau domaine. La consultation lancée le 24 mars 2017 permet de confirmer cette idée d'un besoin d'information et de réflexion à l'échelle réglementaire.

Par ailleurs, l'article L.223-13 du CMF précise que « le transfert de propriété des minibons résulte de l'inscription de la cession dans le dispositif électronique mentionné à l'article L.223-12, qui tient lieu de contrat écrit pour l'application des articles 1321 et 1322 du Code civil ». Cette présomption légale est importante puisqu'elle permet l'assimilation de l'inscription dans une blockchain à un contrat écrit. Il conviendra de voir si cette assimilation sera étendue à d'autres secteurs.

L'ordonnance prévoit donc la possibilité d'émettre les minibons par enregistrement dans le registre distribué : cela rétablit une relation directe et non-intermédiée entre l'émetteur et l'investisseur. Attention toutefois car les enregistrements dans une blockchain ne constituent pas le minibon lui-même. En effet, l'horodatage du bloc contenant la transaction permet seulement de constituer une preuve fiable à une date certaine de la transaction effectuée, autrement dit de la relation entre l'émetteur et l'actionnaire/obligataire.

L'ordonnance relative aux titres financiers non cotés

La loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite « loi Sapin 2 », a habilité le gouvernement, dans son article 120, à réformer par voie d'ordonnance « 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 » (autrement dit, les titres financiers non cotés).

Publiée au journal officiel du 9 décembre 2017, l'ordonnance n° 2017-1674 du 8 décembre 2017 vient modifier certaines dispositions du code de commerce et du CMF. Parmi les options proposées dans le cadre de la première consultation du 24 mars 2017, cette ordonnance a le mérite d'avoir suivi l'avis de la quasi-totalité des répondants en jetant les bases législatives qui permettront l'inscription d'une émission ou d'une cession de certains titres financiers dans un protocole blockchain[46].

Sont plus particulièrement visés les titres de créance négociables, les parts ou actions d'organismes de placement collectif, les titres de capital émis par les sociétés par actions et les titres de créance autres que les titres de créance négociables, à condition qu'ils ne soient pas négociés sur une plateforme de négociation[47]. Les titres financiers qui seraient inscrits en compte auprès d'un dépositaire central, que ce soit au chef (i) de l'article 3(2) du règlement n° 909/2014 du 23 juillet 2014[48] , (ii) du choix de leur porteur ou (iii) du choix de la société émettrice, ne sont donc pas compris dans le périmètre de la présente ordonnance.

[46]C. com., art. L.228-1 modifié ; JORF n° 0287 du 9 décembre 2017, texte n° 23, Rapport au Président de la République relatif à l'ordonnance n° 2017-1674 du 8 décembre 2017.

[47]JORF n° 0287 du 9 décembre 2017, op. cit.

[48]Autrement dit les titres qui sont négociés sur une plateforme de négociation et ceux qui sont transférés à la suite d'un contrat de garantie financière au sens de la directive 2002/47/CE du 6 juin 2002.

Le nouvel article L.211-3 du CMF prévoit ainsi que « l'inscription dans un dispositif d'enregistrement électronique partagé tient lieu d'inscription en compte ». Cette inscription dans une blockchain devient ainsi une alternative à la traditionnelle inscription des titres financiers en comptes-titres tout en conservant la même valeur. Pour certains, cette alternative constitue une véritable avancée[49]. Cette initiative succède d'ailleurs de très peu aux modifications législatives entreprises par l'État du Delaware en date du 21 juillet 2017 pour démocratiser l'utilisation de la technologie blockchain pour la tenue des registres actionnaires ou encore la gestion des opérations sur titres[50].

Cependant, comme pour le nouvel article L.223-12 du CMF, il est aussi fait renvoi à des conditions définies par décret en Conseil d'Etat pour permettre l'inscription effective des titres financiers dans une blockchain, notamment pour déterminer les solutions en matière de gouvernance, de responsabilités et d'exigences de sécurité. Le gouvernement devra donc étudier avec précision les aspects techniques et juridiques pour résoudre ces questions. Les contours des mesures essentielles de la réforme demeureront donc incertaines jusqu'à la publication d'un décret en Conseil d'Etat, au plus tard le 1er juillet 2018[51].

Cette ambition de réformer le droit français afin qu'il puisse intégrer les évolutions technologiques doit toutefois être saluée. Cette démarche s'inscrit dans une volonté de renforcer la compétitivité de la France sur la scène internationale et notamment de sa propension à attirer des acteurs innovants.

Claire Leveneur, doctorante à l'université Paris II Panthéon-Assas

[49]F. G'SELL et J. DEROULEZ, « Projet d'ordonnance relative à l'utilisation de la technologie blockchain pour la transmission de certains titres financiers. Une avancée réelle, des précisions attendues », JCP G n°41, 9 oct. 2017, 1046.

[50]Delaware State Senate, 149th General Assembly, Senate Bill no. 69.

[51] Ordonnance n° 2017-1674 du 8 décembre 2017, art. 8.

Vente immobilière, notariat et blockchain

Un acte authentique obligatoire ?

En droit français, une vente immobilière peut être valablement conclue tant par acte authentique que par acte sous seing privé, selon l'article 1582 du code civil.

Pour être opposable aux tiers, l'acte de vente doit cependant obligatoirement être publié au service de la publicité foncière. Seuls les actes authentiques peuvent ainsi être publiés au fichier immobilier[52]. L'acte authentique est celui reçu par un officier public ayant qualité et compétence pour instrumenter et avec les solennités requises[53]. Les décisions juridictionnelles, les actes dressés par les notaires, les huissiers ou encore les autorités administratives (maire, préfet) sont autant d'actes authentiques, reçus par des officiers publics.

Ainsi, l'acte authentique, établi par le notaire puis enregistré au service de la publicité foncière, emporte date certaine et opposabilité aux tiers, contrairement à l'acte sous seing privé qui n'est opposable qu'entre les parties. Il est donc toujours préférable et presque indispensable en réalité de recourir à un acte authentique établi par un notaire pour s'assurer de son efficacité.

Les protocoles blockchain permettraient-ils d'offrir les mêmes qualités que l'acte authentique délivré par le notaire ? Selon certains partisans, « la technologie Blockchain offrira demain la même certitude s'agissant de la qualité des parties qui souhaitent effectuer une transaction immobilière, de même que pour la certification du titre de propriété du vendeur, la disponibilité des fonds pour l'acheteur, la conclusion et l'horodatage de l'acte de vente, ou encore la conservation et l'inviolabilité de l'acte de vente »[54].

Les obstacles à l'utilisation des protocoles blockchain

Toutefois, cela ne peut être affirmé avec certitude, ne serait-ce que quant à la capacité et à la qualité des parties : comment contrôler ces données si les identités des parties sont cryptées à travers leurs clés publiques respectives et sans être en mesure de s'assurer que la personne à l'origine de la transaction est bien la personne physique à qui a été attribué le couple clé privée – clé publique ?

Dans le même sens, il faut rappeler qu'un amendement à la loi Sapin 2[55] avait été présenté afin d'assimiler les opérations effectuées dans le cadre d'une blockchain à l'acte authentique défini à l'article 1369 du code civil. Cet amendement a été rejeté en bloc : le législateur n'est pas prêt à une telle assimilation. Il ne faut donc pas déclarer avec précipitation que les protocoles blockchain permettront à coup sûr de remplacer les

[52]Article 710-1 du code civil.
[53]Article 1369 du code civil.
[54]S. DRILLON, « La révolution Blockchain », RTD com. 2016, p. 893, n°22
[55]Amendement n°227 présenté par Laure de La Raudière dans le cadre de l'examen du projet de loi Sapin 2 du 9 décembre 2016 : « Les opérations effectuées au sein d'un système organisé selon un registre décentralisé permanent et infalsifiable de chaîne de blocs de transactions constituent des actes authentiques au sens du deuxième alinéa de l'article 1317 du code civil »

notaires, en particulier dans les ventes immobilières, en décrétant une valeur équivalente à celle de l'acte authentique pour les actes passés via les protocoles.

Les protocoles : authentifier ou certifier ? De la différence avec le rôle du notaire

Une question intéressante se pose quant au rôle des protocoles de la Blockchain : doit-elle certifier ou authentifier ?
Selon la terminologie juridique[56], « authentifier » signifie soit « Rendre un acte authentique, lui conférer l'authenticité », soit « Vérifier et attester l'authenticité d'un document ou d'un écrit », étant entendu que l'authenticité est la « qualité dont est revêtu un acte du fait qu'il est reçu ou, au moins, dressé par un officier public compétent, suivant les solennités requises ».
D'une façon distincte, « certifier » signifie « pour une autorité, rendre certain un acte ou un fait en affirmant, après vérification, sa véracité, son authenticité, son origine, sa conformité ».

Or, en anglais, le verbe authenticate se traduit à la fois par authentifier et certifier : cette double traduction permet de comprendre pourquoi existe le débat qui anime les initiés quant au rôle authentificateur ou certificateur de la Blockchain. Dans le vocabulaire classique (non juridique), l'authenticité renvoie également au caractère d'un écrit, d'un discours, d'une œuvre authentique : c'est le caractère de ce qui émane réellement de l'auteur auquel on l'attribue[57] .
Dans le cadre de la Blockchain, les écrits utilisent souvent le verbe authentifier : en définitive, il faut l'entendre alors selon le sens commun, comme rattachement à l'auteur réel à qui l'écrit ou la signature est attribuée et non dans le sens juridique initial. Dans ce cas, authentifier se rapproche de certifier.

Toutefois, à l'heure actuelle, pour les notaires, les protocoles sont une technologie de certification et non d'authentification[58]: il est plus clair à leur sens d'utiliser le terme de certification pour éviter de laisser croire que l'inscription d'un acte sur un protocole blockchain pourrait lui conférer l'authenticité au sens juridique. C'est ainsi que le métier de notaire se distingue et se rehausse au-dessus de cette technologie, qui permet seulement de conserver des empreintes numériques de documents, et non de contrôler l'identité, la capacité, les pouvoirs des parties lors de l'horodatage des documents : ce contrôle est la condition nécessaire et indispensable pour conférer l'authenticité. En effet, le notaire est un officier public délégataire de la puissance publique : c'est pourquoi le contrôle qu'il exerce sur l'acte, tant instrumentum que negotium, permet de donner force exécutoire à l'acte, en plus de la force probante d'un acte authentique.

Vérification de la validité de l'acte (conformité de l'acte aux textes de loi et diverses normes applicables, capacité des parties à contracter, etc.), de son opportunité (devoir de conseil "impartial et désintéressé") et garantie de l'efficacité de l'acte : le rôle du notaire est bien plus poussé que le seul enregistrement de l'acte à une date certaine que proposent les protocoles grâce à l'horodatage.

[56]Gérard CORNU, Vocabulaire juridique, PUF, 11e éd.
[57]Le Robert, Dictionnaire de la langue française.
[58]Gaëlle MARRAUD DES GROTTES, « La blockchain : un secteur encore en phase d'exploration, mais très prometteur », RLDI n°138, juin 2017, p. 39.

Plus encore, « les attributs attachés à l'acte authentique trouvent leur origine dans une délégation de puissance publique, laquelle est compensée par la soumission du notaire à un contrôle des actes qu'il reçoit, pour s'étendre à l'ensemble de son activité, y compris celle relevant de faits extra professionnels »[59]. Ainsi, un consensus existe autour du notaire tiers de confiance du fait de son travail de contrôle (qui de ce fait engage sa responsabilité professionnelle et la solidarité de l'ensemble de la profession en raison de l'assurance de responsabilité professionnelle obligatoirement souscrite par tous…). Ces éléments sont inexistants dans le cas des protocoles blockchain : il n'y a aucun contrôle des actes enregistrés, si ce n'est d'en vérifier l'exactitude par rapport aux données figurant déjà sur un protocole blockchain donné ; par exemple, vérifier que le bien immobilier – bien identifié – à vendre n'a pas déjà été vendu.

Le titre de propriété ne prouve pas le droit de propriété

Comme le dit à juste titre William DROSS, « le titre n'établit en effet nullement le droit de propriété de l'acquéreur sur la chose mais simplement le fait que la chose lui a été transmise »[60]. En d'autres termes, il ne faut pas confondre la preuve de l'instrumentum, c'est-à-dire de l'acte de transfert de propriété – ce que la Blockchain serait capable d'apporter en toute fiabilité – et la preuve du droit de propriété que l'acte est censé relater[61].

En droit français, l'article 712 du code civil précise les modes d'acquisition de la propriété : « La propriété s'acquiert aussi par accession ou incorporation, et par prescription » : la propriété ne s'acquiert pas uniquement par un titre de propriété et en particulier par un contrat de vente immobilière. La preuve du droit de propriété étant libre, il ne peut être établi avec certitude l'acquisition du droit de propriété par la seule présence d'un contrat de vente immobilière sur un protocole blockchain. En effet, en cas de litige entre une personne faisant valoir un titre de propriété et un possesseur, le juge prendra en compte toutes les preuves apportées. Toutefois, l'apparence joue un grand rôle et la loi accorde une protection spécifique aux possesseurs de biens immobiliers lorsque leur possession est troublée, et les autorise à faire valoir leur droit de propriété sur le bien possédé au terme d'un délai de dix ou trente ans : c'est la prescription acquisitive.

Pourrait-on intégrer des blocs « possession » dans un protocole blockchain pour compiler des faits de possession ? Il pourrait alors y avoir contradiction entre le titulaire du droit de propriété désigné par le dernier bloc et le véritable propriétaire dont la possession trentenaire a emporté un effet acquisitif. Cela montre là encore que la preuve du transfert de propriété sur un protocole blockchain ne peut pas être incontestable face à un usucapion valable. Les faits de possession doivent être qualifiés souverainement par les juges du fond.

Ces éléments permettent d'asseoir d'autant plus l'utilité du notaire qui effectue ce travail d'appréciation in concreto, vérifiant l'origine de la propriété du bien immobilier dont l'acquisition est projetée. Les protocoles blockchain, technologie de validation in abstracto, ne peuvent pas s'insérer correctement dans ce schéma.

[59] V. STREIFF « Blockchain et propriété immobilière : une technologie qui prétend casser les codes », Droit & Patrimoine, n°262, oct. 2016

[60] W. DROSS, Droit des biens, LGDJ, 2e éd., 2014, p. 49 n°46

[61] V. STREIFF « Blockchain et propriété immobilière : une technologie qui prétend casser les codes », Droit & Patrimoine, n°262, oct. 2016.

De plus, la prescription acquisitive pose un problème en raison de son effet rétroactif. En effet, le possesseur dont le droit de propriété est reconnu à l'issue du délai de dix ou trente ans est réputé avoir toujours été propriétaire, à compter du premier jour de possession. Une telle donnée paraît difficile voire impossible à intégrer dans la blockchain, si l'on suggérait d'enregistrer le jugement de reconnaissance du droit de propriété du possesseur dans la blockchain. De plus, il existe en droit français une règle d'inopposabilité au nouveau propriétaire des droits constitués par l'ancien propriétaire sur l'immeuble : comment articuler ces éléments dans le monde horodaté et irréversible de la blockchain ?

En matière de propriété immobilière, les solutions à développer autour de la blockchain devront donc très certainement être accompagnées d'une évolution du droit en vigueur pour reconnaître des effets à l'inscription sur la Blockchain, à la manière de l'ordonnance du 28 avril 2016 s'agissant des minibons, mais de façon bien plus poussée eu égard aux spécificités de la propriété immobilière en droit français. Peut-être pourra-t-on, à terme, envisager la conclusion d'une vente immobilière entièrement dématérialisée sur la Blockchain, avec des smart contracts régissant les nombreuses conditions suspensives accompagnant une telle transaction, le transfert de propriété et l'inscription au service de la publicité foncière.

Claire Leveneur, doctorante à l'université Paris II Panthéon-Assas

▸ La traçabilité des biens de consommation

Un des premiers cas d'usage dans le cadre de la grande consommation concerne l'environnement de la supply chain, c'est-à-dire l'ensemble des maillons du réseau de livraison des produits et services depuis la production des matières premières jusqu'à

la prise en possession par le client final. On y inclut les étapes d'approvisionnement et achat, de gestion des stocks, de logistique, de manutention, de stockage, de distribution et livraison, etc. Les domaines peuvent être variés, agroalimentaire, automobile, pharmaceutique, œnologie, mais les principes sont similaires.

Pour ces chaînes de production, la blockchain permettrait la transmission d'informations sûre quant à la provenance et du parcours des denrées : on imagine à terme pouvoir scanner le code-barre ou QR-code d'un produit et découvrir via une interface en simultané toutes les étapes du cycle de productions et de vie du produit, un projet français s'y attelle d'ailleurs. Autrement dit, l'identifiant suit le produit à toutes les étapes de sa production jusqu'à ce qu'il parvienne entre les mains du consommateur final.

Ce cas d'usage de la blockchain s'inscrit parfaitement dans le mouvement de transparence imposé de plus en plus aux grandes firmes agroalimentaire, surtout après l'implosion de nombreux scandales (notamment, vache folle, lasagnes, grippe aviaire, contamination des canards, etc). Avec l'implémentation de la blockchain au sein du suivi logistique des produits, le temps de traçabilité des produits passe de plusieurs jours voire semaines, à simplement quelques minutes et rendrait les fraudes plus difficiles

Évidemment, la blockchain pourrait servir à l'ensemble des produits (non seulement alimentaires et/ou rares), mais il convient dans un premier temps que les acteurs, distributeurs et les producteurs, industriels, internationaux ou locaux quelque soit leur rôle et échelle, se fassent à cette nouvelle technologie, et s'équipent en conséquence si le besoin se fait sentir de coordonner blockchain et IoT.

Avec 26 000 projets blockchain en 2016, on peut d'ailleurs affirmer que les différents secteurs ont clairement entendu le potentiel de la technologie. Pour autant, reste à envisager, en cas d'expansion des blockchains as a service, le sort des utilisateurs finaux et leur rôle au sein de ce nouvel écosystème.

Aurélie Bayle - be-studys (be-ys Group)

III. Les offres de jetons ou Initial Coin Offerings

La valorisation des jetons d'utilité

En proposant une solution robuste et élégante au problème de la transmission numérique de valeur, le bitcoin a ouvert la voie à une multitude de protocoles et d'unités de valeur associées. La présentation initiale sous le titre "Bitcoin: A Peer-to-Peer Electronic Cash System", laisse entendre que l'objet principal de l'invention était de fournir un moyen de paiement. Pourtant, c'est aujourd'hui tout une nouvelle catégorie d'actifs qui semble se dessiner. Derrière des terminologies variées se cachent des usages et des réalités juridiques et techniques différentes.

Cryptomonnaies et jetons

Sur le plan technique se distinguent les unités de valeur natives d'un réseau et les unités secondaires échangées au moyen de ce réseau.

Les unités de valeur primaires d'un réseau sont généralement désignées sous le terme de cryptomonnaies, En premier lieu, elles permettent de rémunérer les "mineurs" ou validateurs pour contribuer par leur matériel et leur dépense en énergie au fonctionnement et à la sécurité du réseau. Cette rémunération à chaque bloc est d'ailleurs ce qui tient lieu de création monétaire. Ces unitées sont ensuite échangées au travers du réseau.

Les unités de valeurs secondaires sont plus souvent désignées sous le terme de jetons (tokens). Puisque par définition un protocole blockchain permet d'enregistrer des opérations, il est possible à partir d'un réseau existant de définir une nouvelle unité de valeur que l'on échangera par l'intermédiaire de transactions dont la valeur faciale dans la cryptomonnaie primaire serait pratiquement nulle. C'est ce que permettent les colored coin sur le réseau Bitcoin par exemple, ou les smart contracts sur le réseau Ethereum.

Débarrassé des contraintes logistiques de sécurisation du réseau, assurées par la cryptomonnaie primaire, ces jetons peuvent innover en matière de politique monétaire : Une émission unique d'une quantité limitée de jetons ? Une production continue régulière? Un montant fixe de nouveaux jetons pour chaque utilisateur unique? etc.

Ces deux types d'unités de valeur sont peu à peu désignés comme cryptoactifs pour deux raisons. D'une part le terme ne comporte pas de référence à la monnaie, ce qui ménage la susceptibilité des banques centrales. D'autre part le terme reflète la principale utilisation de ces instruments, la représentation d'une valeur.

Les propriétés communes aux cryptomonnaies et aux jetons

- Le transfert de propriété

Chaque transaction consiste à transférer le contrôle d'une unité ou fraction d'unité depuis une paire clé publique/clé privée à une nouvelle paire. La transaction est signée par la clé privée du propriétaire initial et contient l'adresse publique, déduite de la clé publique, du récepteur. L'atomicité des transactions garantit que la transaction échoue ou réussisse complètement. Les unités ne peuvent donc pas être en suspend entre deux comptes.

- Fongibilité

Les cryptomonnaies et tokens sont partiellement fongibles. En théorie, chaque unité ou fraction d'unité à la même valeur. Toutefois, il est possible de suivre le parcours d'une unité en particulier depuis sa création jusqu'au dernier échange. Dès lors, il est possible d'associer à cette information un droit particulier. C'est l'idée des colored coin sur le réseau bitcoin, préfigurant ainsi l'idée des jetons.

- Fractionnabilité partielle

Un bitcoin est divisible jusqu'au Satoshi, représentant 10^-8 bitcoins. L'éther est divisible jusqu'au wei, représentant 10^-18 ethers. Pour chaque jeton, la divisibilité maximale est définie au moment de sa conception.

Les jetons d'utilité

Plusieurs tentatives de classification des jetons selon leurs usages, leur support technique et les droits associés ont vu le jour. Une des catégories les plus souvent développées est le jeton d'utilité : il s'agit d'un jeton qui permet de faire fonctionner un service décentralisé.

Le jeton d'utilité est présenté comme un élément technique du service. Comme un jeton de caddie, ce ne serait qu'un moyen d'arbitrer les usages. Pourtant il revêt plusieurs rôles comme forger la communauté, rémunérer les acteurs du réseau qui font fonctionner le service … In fine, dans beaucoup de projets, ce jeton constitue surtout un moyen de paiement dont la valeur d'utilité dépend de son cours en euros ou dollars. Et la modalité technique, ou la simple contrepartie d'un financement participatif, laisse place à un véritable instrument financier.

Valorisation

Dès lors qu'il s'agit d'un instrument financier, se pose la question de sa valorisation. Il existe des méthodes classiques basées sur la recherche de la valeur fondamentale de l'actif en fonction des futurs revenus et des risques, ainsi que des méthodes relatives comparant un actif à d'autres actifs présentant des caractéristiques similaires sur les marchés. Dans le cas des jetons d'utilité, ces méthodes sont difficiles à appliquer. Le jeton ne représente pas directement un droit sur des revenus financiers et la catégorie étant nouvelle il y a peu de points de comparaison.

Un premier facteur d'évaluation pour un jeton est sa politique monétaire : rythme d'émission, quantité en circulation, répartition … Le modèle du bitcoin et de ses premières alternatives consiste en un démarrage en douceur qui fait des premiers possesseurs des ambassadeurs. Une fois adopté, le nombre maximum d'unités fixé contribue à donner un sentiment de rareté. A l'inverse, les jetons sont souvent vendus au démarrage du projet dans une quantité prévisible, calculée en fonction de la demande du marché.

Pour un jeton d'utilité, un deuxième facteur est l'utilisation du service et mécanismes communautaires. Si le service est utilisé, la demande en jeton devrait se prolonger. Prenons l'exemple d'un service de stockage de fichiers. Le jeton s'évalue en comparant la demande pour le service, l'espace de stockage mis à disposition et le nombre de jetons en circulation. Cette masse de jeton en circulation est elle-même évaluée en retirant du nombre total de jetons émis les jetons hors marché, soit parce qu'ils sont possédés par des investisseurs qui souhaitent les conserver sur le long terme, soit parce qu'ils sont mis en réserve (mécanisme de proof of stake, canaux de paiement …)

Enfin, un troisième facteur est la marque et réputation du projet. En effet, les différents jetons constituent des moyens de paiement et des réserves de valeur pratiquement équivalents. La réputation du projet, en dehors de toute valeur d'utilité peut contribuer à la popularité du jeton sur le long terme.

Xavier Lavayssière

ICO

L'ICO ou Initial Coin Offering est une expression de langage courant servant à désigner le fait pour des personnes d'émettre (d'envoyer, d'attribuer) des unités numériques (tokens) au moyen d'un registre décentralisé de type blockchain durant une période de temps déterminée en contrepartie d'une somme d'argent ou de monnaies virtuelles. Autrement dit, une ICO est une levée de fonds

Une ICO consiste à vendre ou troquer une unité numérique en échange d'une autre unité numérique ou d'une monnaie ayant cours légal. C'est une opération d'échange et en tant que telle, elle interroge le juriste sur sa qualification et le régime juridique qui lui est applicable.
La difficulté d'une qualification des offres d'ICO sont leur multiplicité. Chaque ICO propose un token dont l'usage est spécifique au projet envisagé par les émetteurs. Par ailleurs, un token peut avoir plusieurs fonctions au sein d'un projet.

L'offre de vente des tokens fait en général l'objet d'une large publicité via les réseaux sociaux, des sites internet spécialisés, sur papier, dans des colloques, conférences

portant sur les nouvelles technologies, ou par le bouche à oreille. Les recettes générées par ces opérations sont parfois spectaculaires. Parmi les dernières ICO réalisées, on peut relever celle de la fondation Tezos pour un montant équivalent à 232 millions de dollars ou celle de Brave pour un montant de 35 millions de dollars.

On observe l'existence d'un marché secondaire des tokens. Cette possibilité de revente peut être libre ou conditionnée par les créateurs des tokens. L'opération de revente est en général effectuée via des plateformes d'échanges exprimant un prix.

Comment qualifier juridiquement ces unités numériques ?

Qu'est-ce qu'un token ?

Le token est une unité numérique associée à une signature électronique. Cet ensemble de données sert à authentifier une demande de transaction (d'une requête) dans un protocole blockchain. L'unité numérique n'est pas dissociable d'une adresse sur la blockchain et ne peut être transférée que par celui qui possède la clé privée associée à cette adresse.

Quelle différence entre un token et une monnaie virtuelle ?

Les tokens et monnaies virtuelles sont des unités numériques supportées et gérées par un protocole blockchain. Cependant, le terme de monnaie virtuelle est déjà une piste de qualification. En effet, le terme de monnaie renvoie le juriste à la notion de paiement : une monnaie sert à faire des paiements, autrement dit à éteindre une obligation. Seulement, le code monétaire et financier prévoit que la monnaie de la France est l'euro. Autrement dit, n'est reconnu par la loi comme pouvant servir à effectuer des paiements que l'euro. Cependant, la règle n'est pas d'ordre public et les parties peuvent y déroger par contrat (CJUE 22 oct. 2015, C 264/14). Ainsi, le bitcoin et les autres unités numériques peuvent servir à faire des paiements si les parties se sont entendues sur le fait que le transfert d'unité numérique d'une personne avec une autre valait paiement et pourrait servir à éteindre l'obligation.

C'est donc l'acceptation sociale en tant qu'unité de compte et de valeur qui permettra d'établir une distinction entre une monnaie virtuelle et une autre unité numérique émise sur une blockchain. Cette convention devra néanmoins être prouvée par celui qui cherchera à s'en prévaloir. Il est donc conseillé de garder une preuve de la convention.
Il n'y a pas d'agrément ou de statut particulier à respecter pour les émetteurs de monnaies conventionnelles.

L'écosystème des ICO :

Plusieurs acteurs sont impliqués directement ou indirectement dans les ICO :
Le récepteur (appelé également, acheteur, investisseur, détenteur, porteur ou encore contributeur) est l'adresse qui reçoit le token en échange d'un travail, d'une somme d'argent de monnaie virtuelle ou à la suite d'un don.
Le porteur de projet (appelé aussi émetteur, créateur, vendeur, bénéficiaire ou développeur) est celui qui crée le token à l'aide d'un protocole blockchain et envoie (transfère) le token à une adresse.

Les fournisseurs de service de portefeuilles, de comptes ou de signatures électroniques.
Les éditeurs/développeurs de smart contracts développent ou proposent des programmes pré-rédigés.
Il existe aussi des auditeurs qui révisent le code et fournissent un avis sur la qualité de la programmation. Ces audits peuvent s'étendre à des conseils et avis sur la qualité du modèle d'affaire de l'opération. Parfois, ces informations sont disponibles sur des sites en ligne.

Les plateformes d'échanges servent à échanger des devises contre des monnaies virtuelles ou à échanger des monnaies virtuelles. Elles fixent les prix de revente des tokens.

Les banques sont parfois sollicitées pour recueillir les fonds envoyés par les contributeurs lorsque le versement se réalise en devises.

Conclusion

Les tokens sont des objets techniques dont la qualification sera propre à chaque opération. Pour l'heure, il n'y a pas un régime juridique unitaire, c'est-à-dire un régime qui pourrait s'appliquer à toutes les ICO. De plus, appréhender la législation applicable aux ICO implique de prendre en considération les législations du pays de chacune des parties au contrat (la partie créatrice du token et la partie qui reçoit le token).

Afin d'éviter de potentielles sanctions de l'exercice illégal de certaines activités bancaires et financières, il est prudent de se rapprocher de professionnels et de consulter l'AMF avant de réaliser des activités publicitaires ou marketing concernant un projet d'ICO.
Soulignons que ces protocoles ne sont pas matures et des erreurs de programmation ont été rapportées (ex : les attaques concernant les portefeuilles "multi-sig" proposés par l'entreprise Parity).
Enfin, les blockchains sont des protocoles complexes et mouvants, susceptibles de modifications. Ces changements peuvent par exemple entraîner des modifications des règles de validation des transactions, affecter le prix des transactions, et impacter la valeur des tokens.

Hanna-Mae Bisserier

▸ La profession de juriste face à la transformation des pratiques du droit

L'essor actuel des Legaltechs, ces entreprises utilisant la technologie pour fournir des services juridiques, poussées aussi bien par des profils techniques que juridiques, démontre la volonté des juristes de vouloir moderniser leurs pratiques ; au-delà de cette volonté, c'est une nécessité. L'apparition de nouvelles pratiques, de nouvelles technologies et, de surcroît, l'émergence de modèles économiques, sociaux et culturels nouveaux nécessitent une adaptation de la profession de juriste[62]. Une personne qui « dit le droit » ne peut efficacement le faire sans être en adéquation avec son interlocuteur, ou en méconnaissance de ses spécificités, et de sa réalité économique et sociale.

Les développements de cas d'usage pour la technologie blockchain en est un parfait exemple ; au-delà de l'engouement autour de cette technologie, juristes, informaticiens, institutions et Etats collaborent pour appréhender les changements que cette technologie va entraîner. Et en amont de ces changements, il est nécessaire de comprendre des paradigmes nouveaux et la philosophie inhérente à cette innovation.

Au surplus d'appréhender juridiquement les implications de cette technologie, les juristes se penchant sur le sujet travaillent différemment ; ils font évoluer leurs pratiques, que ce soit via des méthodes de travail collaboratives comme en témoigne cet ouvrage ou encore dans leur positionnement auprès de projets nouveaux, accompagnant dès l'origine voire participant à l'émergence de startups qui se proposent de bousculer le monde juridique.

Cette dynamique, portée par la connexité avec des nouvelles technologies ne doit pas être l'apanage de ce seul sujet. L'ensemble de la profession doit se faire porter de façon analogue. Favoriser une transformation numérique et organisationnelle des pratiques juridiques est un levier d'efficacité mais aussi d'accessibilité du droit, et en ce sens, elle est essentielle.

Thibaut Labbé

[62] http://www.justice.gouv.fr/publication/chantiers_justice/Chantiers_justice_Livret_01.pdf

Lexique

Adresse : une adresse correspond à un identifiant, généralement dérivé d'une clé publique, qui permet d'identifier un utilisateur ou un smart contract sur un réseau blockchain.

Ancrage : processus par lequel une empreinte cryptographique ou condensat est inscrite dans la blockchain par l'intermédiaire d'une transaction.

Bitcoin : le bitcoin désigne un protocole, une unité de valeur et un réseau. Le protocole, décrit initialement en 2008, repose sur un mécanisme de consensus au sein d'un réseau pair à pair. L'unité de valeur, le bitcoin est née avec le lancement du réseau en janvier 2009, elle sert à rémunérer les mineurs qui sécurisent les transactions en les validant au sein de blocs. Généralement, Bitcoin avec une majuscule désigne le protocole, le réseau et la communauté, tandis que l'unité est présentée comme bitcoin.

Blockchain : Une blockchain désigne un protocole informatique permettant d'établir un registre de transactions horodatées, organisé sous la forme d'une chaîne de blocs, par consensus au sein d'un réseau sans confiance préalable entre les acteurs.

Le terme blockchain est apparu pour la première fois dans la description du bitcoin sous la forme *block chain* ou chaîne de blocs. Il désigne alors l'ensemble des transactions passées stockées regroupées par blocs périodiques, contenant chacun une référence au précédent bloc ce qui permet notamment de les ordonner. C'est par synecdoque qu'il a acquis le sens actuel englobant l'ensemble des protocoles reposant sur des principes similaires au Bitcoin : un réseau pair à pair d'échange d'informations, un système d'adresses et signatures, un base de données répliquée et horodatée et un mécanisme de consensus.

Clé publique / Clé privée : Terminologies employées dans le cadre de la cryptographie asymétrique. Une paire composée d'une clé publique et d'une clé privée est produite par l'utilisateur. La clé publique est transmise sur les réseaux. Un correspondant peut l'utiliser pour alors chiffrer un message qui ne pourra être lu que par l'utilisateur. A l'inverse, le propriétaire de la clé privée peut aussi l'utiliser pour signer un message. La signature pourra être alors vérifiée au moyen de la clé publique. C'est le procédé de signature utilisé pour les transactions.

Applications décentralisée, ou DApp : Une Dapp est une application qui fonctionne sur un réseau pair-à-pair. Ces programmes existent depuis la création des premiers réseaux pair-à-pair et ne sont pas spécifiques à la blockchain.

Empreinte cryptographique / Hash : valeur de sortie d'une fonction à sens unique de hachage cryptographique, servant à déterminer, à partir d'un contenu indifférent, une donnée de taille arbitraire, ayant comme caractéristiques d'être rapide à calculer, résistant aux collisions (probabilité de retrouver le même hash pour deux contenus différents), et irréversible (impossibilité de retrouver le contenu d'origine grâce au seul hash).

Minage : le minage est une méthode qui consiste à valider un ensemble de transactions, regroupée sous forme de bloc. Le mineur vérifie les transactions, puis ajoute quelques informations comme le hash du bloc précédent et la date. Ensuite, dans un réseau utilisant le proof-of-work, le mineur doit ajouter un nombre tel que le hash du bloc complet ait certaines caractéristiques. Cette opération est rémunérée pour les mineurs, qui obtiennent, en échange de la validation d'un bloc, d'un solde de cryptomonnaie.

Mineurs : ils sont des utilisateurs de la blockchain qui valident les transactions par le processus de minage. Un mineur peut utiliser un poste individuel ou être de véritable entreprises regroupant des centaines d'unités de calcul pour miner dans des fermes de minage. Les mineurs sont souvent organisés au sein de "pools" de mineurs.

Nœud : un nœud d'un réseau blockchain est une instance logicielle connectée au réseau au travers d'autres nœuds. Un nœud peut envoyer au réseau de nouvelles transactions, relayer les transactions qui transitent et miner les blocs.

Oracles : ces entités ont la responsabilité de vérifier et certifier, avec un processus prédéterminé, les informations issues de l'extérieur de la blockchain que les utilisateurs souhaitent intégrer. Une fois vérifiées, ces informations certifiées par les oracles ont vocation à déclencher l'exécution de smart contracts. Pour prendre l'exemple des paris hippiques, l'oracle sera en charge de récupérer les données depuis les sites officiels de paris sportifs ou les fédérations hippiques, éventuellement en les recoupant, pour donner l'arrivée des chevaux avec une quasi-certitude.

Proof-of-work : la preuve de travail est un calcul cryptographique permettant la validation d'un bloc dans la blockchain. Au fil de l'historique de la blockchain, la difficulté de calcul s'adapte pour maintenir la validation. Cette méthode est souvent pointée du doigt pour sa consommation énergétique, notamment du fait des 'fermes de minage'.

Proof-of-stake : la preuve d'enjeu, contrairement au proof-of-work, est une méthode cryptographique ayant vocation à être moins énergivore. Elle se base sur la quantité de cryptomonnaie que possède chaque utilisateur : la probabilité de valider un bloc est proportionnelle au solde mis en enjeu par l'utilisateur en question.

Smart Contract : Dans le contexte blockchain, les smart contracts sont des programmes informatiques exécutés de façon autonome par le réseau. L'expression a été introduite par Nick Szabo en 1993 comme un procédé de contractualisation ayant recours à l'informatique et la cryptographie.

Auteurs

Aurélie Bayle
Anna van der Aa
Pierre Banzet
Alice Barbet-Massin
Hanna-Mae Bisserier
Claire Leveneur
Thibaut Labbé
Frédéric Laffy
Xavier Lavayssière
Laetitia Maffei

Contributeurs

Freitas Gibran
Doucoure Abdoulaye
Paillet Antonin
O'rorke William
Levavasseur Cyril
Baudouin Valentine
Buser David
Hirigoyen Maxime
Jacquier Laetitia
Cattalano-Cloarec Garance
Weidler-Bauchez François

Merci à Christine Hennebert, Marc Zeller, Primavera de Filippi et Simon Polrot pour leurs relectures et conseils.