



SMART CONTRACTS : ETUDES DE CAS ET REFLEXIONS JURIDIQUES

Livre blanc et recommandations

RESUME

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

Ce programme est issu d'un partenariat entre l'association Open Law*, le Droit Ouvert, l'ECAN et Coala Lex. Les ateliers d'ingénierie participatifs ont été enrichis d'apports extérieurs et de la présence d'une équipe de mentors.

Enrichi du rapport à France Stratégie

Table des matières

Abstract	4
Introduction.....	10
Blockchain et Smart Contract	11
Smart Contracts et institutions.....	18
La Smart Contract Academy.....	19
I. La traçabilité des œuvres d'art.....	23
Enjeu de l'anonymat et traçabilité dans le marché de l'art	23
Exemple et présentation d'un smart contract.....	25
Le droit de la preuve des œuvres d'art	27
Problématiques juridiques et pratiques.....	28
Antériorité	28
Traçabilité	28
Authenticité.....	29
Co-titularité et répartition.....	29
Coût.....	29
Solutions avec la blockchain	30
II. Le transfert de propriété	37
Minibons et titres financiers	37
L'ordonnance relative aux minibons.....	38
L'ordonnance relative aux titres financiers non cotés	39
Vente immobilière, notariat et blockchain	41
Les protocoles : authentifier ou certifier ? De la différence avec le rôle du notaire	42
Le titre de propriété ne prouve pas le droit de propriété	44
► La traçabilité des biens de consommation	46
III. Les offres de jetons ou Initial Coin Offerings	47
La valorisation des jetons d'utilité	47
Cryptomonnaies et jetons	47
Les propriétés communes aux cryptomonnaies et aux jetons	48
Les jetons d'utilité	49
Valorisation.....	49
ICO	50
Conclusion.....	52
► La profession de juriste face à la transformation des pratiques du droit.....	54

Lexique	55
Auteurs.....	58
Contributeurs.....	58
Fiche 1 Analyse juridique des <i>tokens</i> (ou jetons)	61
1. Appréhender la nature juridique des tokens	62
1.1. Une nature juridique appréhendée au travers de leurs caractéristiques	62
1.2. Typologie des tokens	62
1.3. Possibles qualifications juridiques des tokens	65
2. Recommandations	67
Fiche 2 Smart-contract et Droit des contrats	68
1. Définition	68
2. Concept et implémentations	69
3. Propriétés.....	72
4. Smart-contract et droit français.....	73
5. Conséquences de l'exécution autonome	74
6. Recommandations	75
Fiche 3 Preuve et signature numérique.....	76
1. Enjeux	76
2. Etat des lieux concernant la preuve sur la blockchain	77
2.1. La preuve sur une blockchain privée	77
2.2. La preuve sur une blockchain publique	77
2.2.1. La preuve d'un acte sous seing privé sur une blockchain.....	78
2.2.2. Le cas particulier de l'acte authentique	82
2.2.3. La preuve d'un fait juridique sur une blockchain	83
3. Propositions	85
4. Conclusions : recommandations.....	86
Fiche 4 Fiscalité	87
1. Contexte : un secteur en croissance sans un cadre adapté.....	87
2. État des lieux : des règles incomplètes, sources d'incertitudes.....	88
3. Recommandations	91
Fiche 5 Enjeux de conformité et droit au compte	95
1. Contexte : une véritable problématique d'accès à un compte bancaire	95
2. Recommandations	96
Rédacteurs	97

Table des illustrations

Creative Commons by Abdoulaye Doucoure – Ethercourt

: la monnaie dans tous ses états.....	5
: des crypto monnaies aux crypto actifs	5
: des crypto monnaies aux crypto actifs	6
: complémentarité des juristes et des développeurs	7
: objectifs du travail de recherche	7
: livre blanc.....	8
: qualification des ICO's	8
: Initial Coin Offering	50
: contexte des ICO	50
: exemple de smart contract d'émission de tokens	53

Creative Commons by Xavier Lavayssi  re - ECAN

: ligne directrice du livre blanc.....	10
: chiffrement	11
: minage	12
: protocoles	13
: machine de Turing	14
: impacts juridiques des protocoles blockchain	15
: applications de smart contracts.....	16
: f��d��ration de citoyens, laboratoires, communaut��s, collectivit��s et entreprises	16
: festival p��dagogique des blockchains.....	17
: code is law	19
: objectifs de la #SCademy 1/2	20
: : objectifs de la #SCademy 2/2	20
: ArtTrade	25
: Applications d��centralis��es	56
: coûts de transactions	57
: SCAToken.....	61
: token ERC 20.....	64
: (smarts) contracts	68
: Ethereum	69
: programmation du smart contract	70
: Solidity	70
: browser-solidity	71
: transaction	71
: v��rification d'une transaction.....	72
: smart contract	80

Creative Commons Anna van der A

: tra��abilit�� des œuvres d'art.....	23
---------------------------------------	----

Abstract

The concept of "blockchain"¹ emerged in conversations in 2008 thanks to the article published under the pseudonym Satoshi Nakamoto presenting bitcoin, a decentralized "currency". Initially designating the storage of all transactions in the form of blocks, it gained popularity as a "store of value".

Inspired from that protocol, emerged more and more applications, mostly open source. As they need money to develop and grow, those projects innovated in their fundraising methods, bypassing traditional and regulated investment actors.

The loss of confidence in the banking and financial system resulting from the 2008 crisis is not foreign to the success, since 2009, of Bitcoin and other tokens.

Contrary to popular belief, the word "blockchain" doesn't designate a single technology, but potentially as many protocols as applications.

Most Crypto assets being marketable, they raise concerns of governments trying to protect citizens. Indeed, they are promised different counterparties, with few information about their rights in case of scams.

Because of the gap between those disruptive technologies and legal professionals doesn't help tackling that issue, this work tries to bridge that gap and approach those technologies through legal lenses and question our legal system:

- What legal concepts can be adapted?
- What new practices are likely to emerge?
- Should clean regulation be considered?
- What regulatory objectives can be achieved through technical processes?

It is to explore these new issues that we have worked to unravel this link between new technologies and law: from the specific operation envisaged by the Parties, we consider the technical modalities and conduct a legal and economic analysis.

The Smart Contract Academy is a collaborative program of legal and economic analysis related to the impact of blockchain technologies on a selection of use cases. The participants presented complementary profiles and, pioneering the reflection on these issues in France, allowed to nourish the reflection of companies and institutions during the year.

Together, we worked on defining the concepts because behind the words are hidden technical solutions, but also new economic mechanics and cultural changes. Thus, in this field, the strength of the complementarity of the technical and legal looks is to provide terminological clarifications without which it is not possible to think the concepts. The lexicon at the end of this book is intended to provide precise definitions by distinguishing between technical and usual acceptances.

Three specific topics were selected: traceability, transfer of ownership and public sales of tokens, known as ICO.

Through this study, we try to understand why tokens are technical objects whose qualification will be specific to each operation: Blockchains are complex and moving protocols that can be modified.

What's more, these changes can result in changes to transaction validation rules, affect transaction prices, and impact the value of tokens.

¹ Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

1 MONNAIE



- fiat = fiduciaire/scripturale
 - effet libératoire
 - créée par organe central identifié (Etat)
 - valeur accordée par l'Etat
- électronique = représentation d'une monnaie fiat
 - organe créateur identifié là encore (ex : Paypal)
 - suppose une REMISE DE FOND
- virtuelle = "non-fiat" ou "alternative"
 - organe créateur non forcément identifié
 - pas de remise de fonds
 - acceptation par le marché et pas l'Etat
 - acceptation volontaire - effet libératoire

La monnaie dans tous ses états

2 ACTIFS FINANCIERS

A partir du moment où une publicité est faite sur des investissements, il est compréhensible que l'Autorité des Marchés Financiers cherche à protéger les investisseurs, en régulant comme ça a été le cas en Chine en début septembre 2017.

En regardant le droit financier, on peut être tenté de qualifier certains tokens de "biens divers" mais cela exclue leur organisation de celle des "sociétés créées de fait"...

La législation sur le crowdfunding est une piste que nous creusons pour qualifier les crowdsales !



Des crypto monnaies aux crypto actifs

3 PROBLEMATIQUE



Possibles questions de KYC face à la pseudonymisation



Autant d'usages potentiels que d'utilisateurs



"Bac à sable" d'expérimentation en cours d'évolution



Vision statique inadaptée au potentiel évolutif du projet



Difficulté de la détermination du droit applicable.



L'écosystème évolue à une vitesse exponentielle

La France essaie de ne pas être à la traîne

Des crypto monnaies aux crypto actifs

4 METHODOLOGIE



Définir les classes d'actifs.
Définir les critères.
Définir les conséquences.
Mettre en perspective avec le droit français.
Transposer en droit français.

Répertorier les cas d'usage.
Analyser les caractéristiques.
Recouper les cas d'usage.
Construire une interface d'achat et d'identification.
Coder un Backend d'ICO publique.

Complémentarité des juristes et des développeurs

5 OBJECTIFS



Dans un premier temps nous proposons au régulateur à travers France Stratégie nos points de vue sur ces questions de qualifications juridiques.

Nous produisons un livre blanc qui va reprendre les résultats de nos travaux.

Nous essayons de publier du code open source dans un but pédagogique.

Objectifs du travail de recherche

SYNTHESE

Quelles sont les règles à suivre ?

Livre blanc en ligne

Contenu du livre blanc



ICO et Droit : conseils

Qu'est ce qu'une ICO ?

Qu'est ce qu'une blockchain ?

Qu'est-ce qu'un token ?

Quelles sont les questions juridiques à propos des ICO ?

Conseils

Qualification des ICO's

Abdoulaye DOUCOURÉ – Ethercourt M. L.

SMART CONTRACTS

ÉTUDES DE CAS ET RÉFLEXIONS JURIDIQUES

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

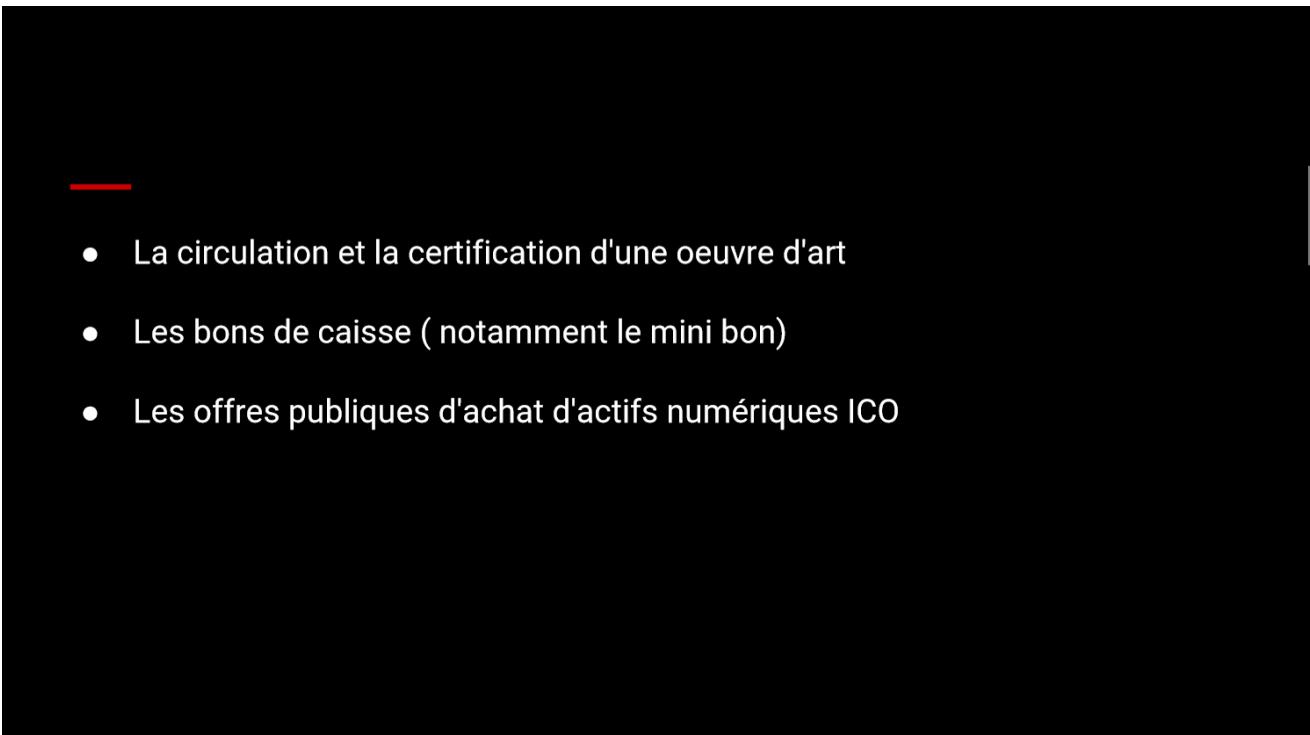


Introduction

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 économiques 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 acceptations 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 circulation et la certification d'une oeuvre d'art
 - Les bons de caisse (notamment le mini bon)
 - Les offres publiques d'achat d'actifs numériques ICO

Ligne directrice du livre blanc

- La traçabilité des œuvres d'art 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.

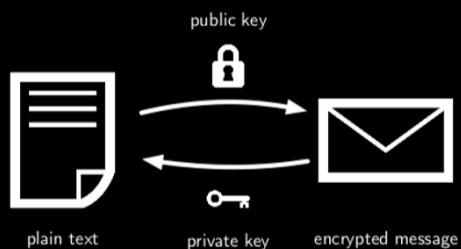
Blockchain et Smart Contract

Blockchain technologies

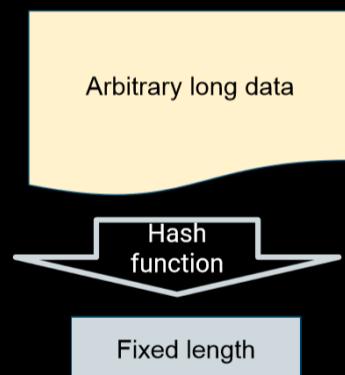


Basic cryptography

Public private key



Hash functions



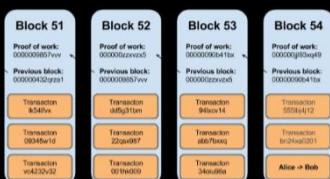
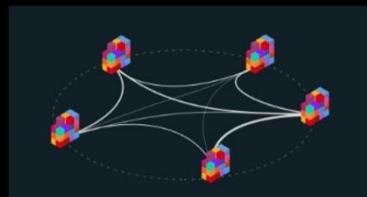
Chiffrement

Blockchain

Transaction

Network

Mining



Minage

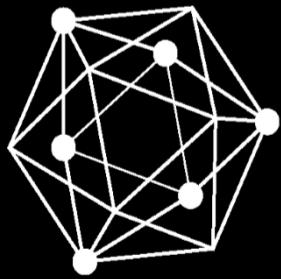
Technologies



2009



2013



2015

Diversité des Protocoles

Le concept de "blockchain"² 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 synecdoque³ à l'ensemble du protocole (cf. lexique).

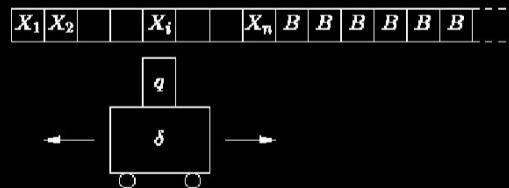
Les "smart contracts" sont des programmes informatiques exécutés de façon autonome par un réseau utilisant un protocole blockchain. Le concept a été popularisé par le projet

Ethereum, né en 2013, qui permet ainsi de programmer des fonctionnalités avancées. Des projets comme Hyperledger ou Cardano proposent des fonctionnalités similaires.

² Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

³ La synecdoque (du grec συνεκδοχή / sunekdokhē, « 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)).

Turing machine



Machine de Turing

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 Szabo⁴ comme un protocole informatique de contractualisation. Nick Szabo présente ainsi l'exemple des distributeurs automatiques qui par leurs 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 mécanisme physique.

⁴ Szabo, Nick. "Formalizing and securing relationships on public networks." First Monday 2.9 (1997).

Impact on Law



Current use cases

- Proof
- Identity
- Registers
- Deeds

Impacts juridiques des protocoles blockchain

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.

Use cases



Applications de smart contracts

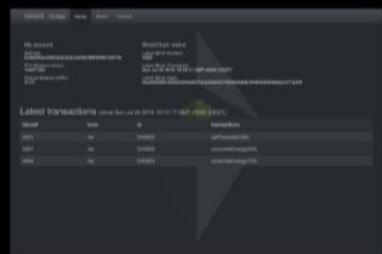
Daisee



CitizenWatt



Ethereum



DApp (web)

MONITORING

AUTOMATION

INTERFACE

Fédération de citoyens, laboratoires, communautés, collectivités et entreprises



Festival pédagogique des blockchains

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 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.

Conflicts



Code is law

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 à des attitudes nuancées de la part 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, fondateur de Variabl.io. Pionnier de la réflexion sur ces questions en France, ce groupe de travail a 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 Lavayssi  re

Les objectifs



Les objectifs de la #SCademy 1/2

-
- Former des juristes sur le sujet blockchain et des Smart Contracts et les non-juristes aux enjeux juridiques qu'ils peuvent présenter
 - Analyser en profondeur des cas d'usage d'actualité, leur modèle économique et le cadre juridique
 - Cr  er une premi  re collection en libre acc  s de Smart Contracts accompagn  s de leur analyse juridique, afin d'inspirer et faciliter le d  ploiement de nouveaux produits et services

Les objectifs de la #SCademy 2/2

► 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 que l'on observe le plus souvent dans les solutions reposant sur les smart contracts.

Dans le cas plus rare où les parties entendent utiliser uniquement le smart contract comme support contractuel, en l'absence de tout contrat préalable comme 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 civil⁵ 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 transaction⁶.

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 »⁷, mais c'est seulement s'il remplit également les conditions relatives aux éléments d'identification et de conservation du programme (cf. infra “Le droit de la preuve des œuvres d'art”).

Le smart contract est un programme qui permet de garantir l'exécution d'engagements pris sans intervention humaine directe. En principe le programme n'est donc 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 par les parties dans le programme et dans le cadre juridique.

⁵ 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* »

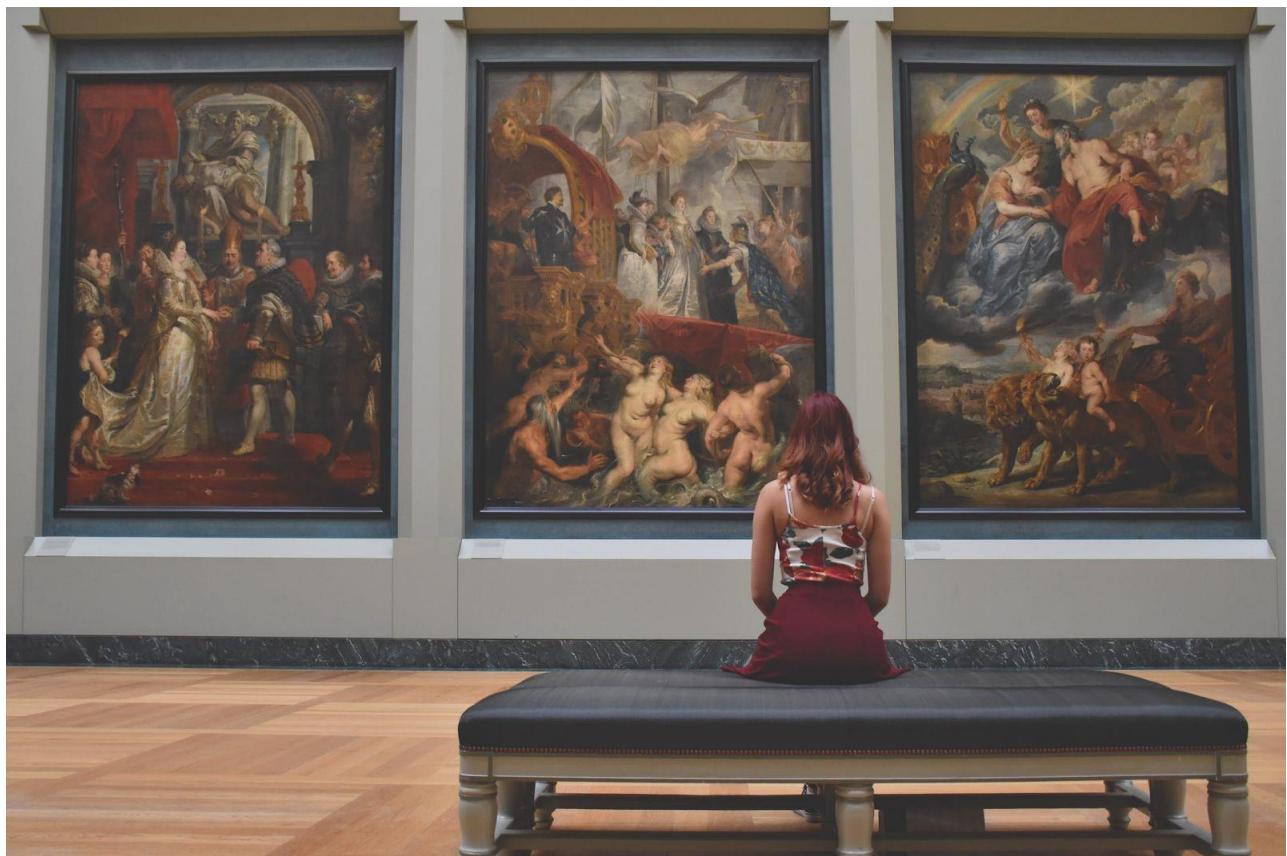
⁶ Article L.110-3 du code de commerce.

⁷ Article 1365 du code civil.

Par exemple, comment prendre en compte :

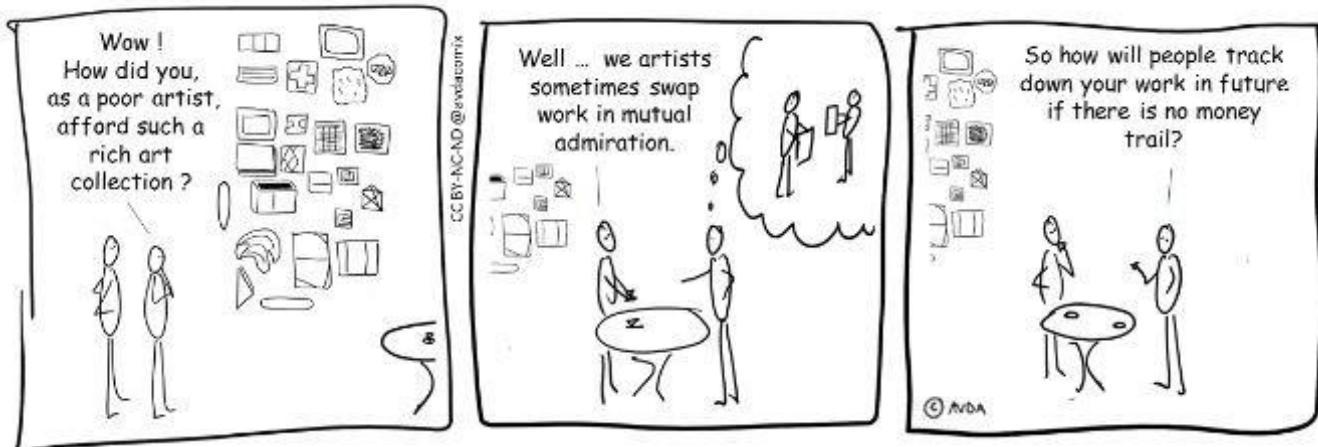
- La modification du contrat conformément à la volonté commune des deux parties ; la rétractation d'une des parties.
- La mauvaise exécution (ou inexécution) issue d'une erreur de manipulation ou tentative frauduleuse.
- Les bugs ou le mauvais fonctionnement du programme. Des questions de responsabilité civile peuvent se poser dans ce cas entre les parties et vis-à-vis des développeurs du programme informatique et des acteurs du réseau.
- 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.



Traçabilité des œuvres d'art

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 essaient 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 discréetion 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

```

1  pragma solidity 0.4.21;
2
3
4  contract ArtTradeBasic {
5
6      event Transfer(address indexed _from, address indexed _to, uint256 _objectId);
7
8      // Association des objets vers leurs propriétaires
9      mapping (uint256 => address) internal objectOwner;
10
11     // Renvoie le propriétaire d'un objet donné
12     function ownerOf(uint256 _objectId) public view returns (address) {
13         address owner = objectOwner[_objectId];
14         return owner;
15     }
16
17     // Transfert la propriété d'un objet
18     function transferObject( address _to, uint256 _objectId) public {
19
20         // Vérifie que l'on est bien en présence du propriétaire
21         require(ownerOf(_objectId) == msg.sender);
22
23         // Changer la propriété de l'objet
24         objectOwner[_objectId] = _to;
25
26         emit Transfer(msg.sender, _to, _objectId);
27     }
28
29 }
30

```

ArtTrade contract

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"⁸ protégée par le droit d'auteur⁹ et ce, dès lors que le processus créatif a débuté⁹, une preuve de cette création peut fréquemment se révéler essentielle. Aucune formalité, aucun 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 »¹⁰. Ainsi, la « plus personnelle de toutes les propriétés »¹¹ 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 mal¹². 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.

⁸ C. propr. intell., art. L111-1.

⁹ C. propr. intell., art. L111-2 : peu importe l'achèvement ou non de l'oeuvre.

¹⁰ C. civ., art. 1353 et C. pr. civ., art. 9.

¹¹ Le Chapellier, lors de la présentation de la première loi sur le Droit d'Auteur à l'assemblée, 1791.

¹² 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 ».

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 »¹³. Cette présomption de titularité des droits d'auteurs d'ordre public relève exclusivement de la loi et non de règles posées par des sociétés d'auteur notamment¹⁴. L'auteur devra donc prouver qu'il a - antérieurement à un préteud 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 litige¹⁵. La preuve de l'antériorité d'une œuvre est un fait et peut donc juridiquement être rapportée par tous moyens¹⁶. 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 certaine des cessions ou de leurs différentes exploitations. Les mutations digitales du marché de l'art rendent donc incertaine la provenance des œuvres.

¹³ C. propr. intell., art. L113-1.

¹⁴ Cass. civ, 1ère ch., 29 mars 1989 n°87-14.895.

¹⁵ Par exemple, dans l'affaire « Prada contre SARL Cupidon », les juges ont considéré que les auteurs « ne démontrent pas être titulaires [antérieurs] des droits qu'ils invoquaient ; d'où il suit que le moyen ne peut être accueilli » (Cass. civ., 1ère ch., 15 janvier 2015, n°13-22798).

¹⁶ C. civ., art. 1358.

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 discutable¹⁷. 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 contestées¹⁸. Il est, en effet, possible que deux catalogues existent¹⁹ ou encore que l'auteur du catalogue décide lors d'une nouvelle édition de ne plus intégrer une œuvre²⁰.

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.

¹⁷ 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.

¹⁸ Le catalogue raisonné est l'ouvrage par lequel sont répertoriées, décrites, situées, classées et reproduites, les œuvres d'un auteur.

¹⁹ TGI Paris, 1ère ch., 2e sect., 29 mai 1996, RG n°554/1994, Galerie Tamenaga c./Sté Schmit, Maguy Roche, NP.

²⁰ 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.

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 numérique" ou "hash", soit une suite de caractères alphanumériques. Par ce biais, il est possible d'ancre 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)²¹.

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 conditions²², bien que cette datation ne puisse constituer une date certaine au sens du droit civil²³. Un titulaire de droit pourrait ainsi se pré-constituer une preuve de l'antériorité de son œuvre. Cette preuve pré-constituée n'attesterait 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 ouverte²⁴.

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.

²¹ 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'agrérer des données sur les diamants enregistrés (plus d'un million de diamant sur la blockchain).

²² La fiabilité technique dépend notamment de la technologie utilisée et de la répartition réseau.

²³ 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.

²⁴ 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.

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.

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 privées²⁵.

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'intégrité²⁶. 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.

²⁵ 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.

²⁶ C. civ., art. 1366.

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 juridique²⁷. 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 »²⁸. 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 qualifiée²⁹. Pour être qualifiée, la signature doit, tout d'abord, être considérée comme avancée³⁰ puis répondre à certaines exigences du règlement dit “eIDAS” concernant son dispositif³¹.

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 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 simple³². 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 heure³³.

²⁷ Voir : C. civ., art. 1367 et le décret n°2017-1416 du 28 sept. 2017 relatif à la signature électronique.

²⁸ C. civ., art. 1367, al.2.

²⁹ Article 1 du décret n°2017-1416 du 28 septembre 2017 relatif à la signature électronique.

³⁰ 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).

³¹ Article 28 et 29 du règlement n°910/2014 du 23 juillet 2014.

³² 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 ».

³³ Article 41 al. 2 du règlement n°910/2014 du 23 juillet 2014.

L'horodatage électronique qualifié exige aussi toutefois l'intervention d'un prestataire de service de confiance qualifié³⁴. 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 justice³⁵.

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 "Blockchainyourlp" 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 litige³⁶. A minima, en matière de contrefaçon, les juges ont déjà retenu des faisceaux de présomptions graves, précises et concordantes³⁷. 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. 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 privé³⁸.

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 blockchains³⁹. Sans l'intervention d'un tiers certificateur, de surcroît, la signature et l'horodatage sur blockchain

³⁴ Article 42 al. 1, c, du règlement n°910/2014 du 23 juillet 2014.

³⁵ Article 41 al. 3 du règlement n°910/2014 du 23 juillet 2014.

³⁶ <http://blockchainyourip.com/> (consulté le 06/02/2018).

³⁷ CA Paris 4e ch., 29 avril 182 PIBD III 158 ; CA Amiens 4 février 1913 Ann. 1974, 73.

³⁸ 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.

³⁹ Voir l'entreprise Seezart qui délivre son propre certificat d'authenticité qui n'est pas une garantie suffisante comparé à celui d'un expert.

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

► Smart contracts : Et le droit de la consommation ?

Le Code de la consommation, dans son article préliminaire⁴⁰, 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.

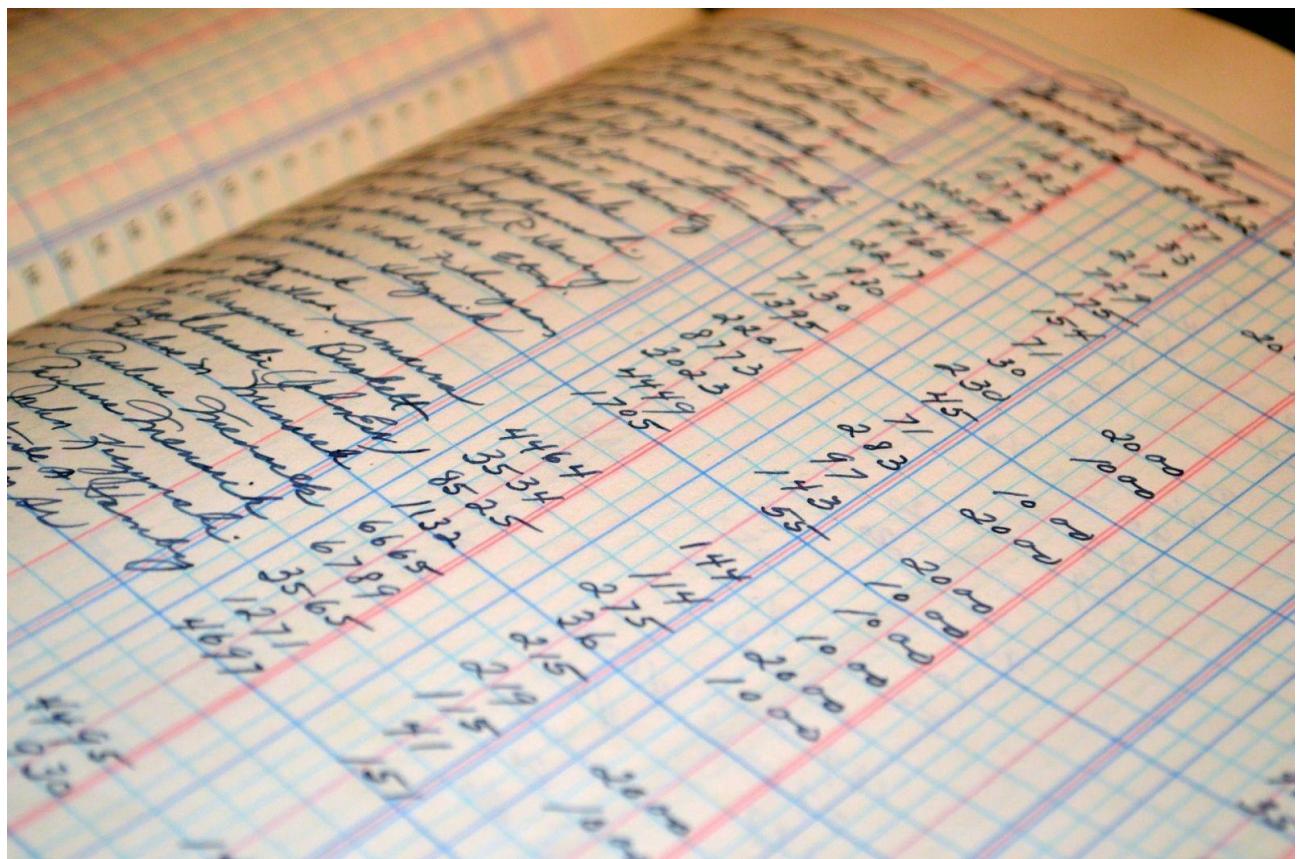
De fait, la multiplication des services et entreprises utilisant la blockchain comme moyen de sécurisation et de traçabilité, ou encore de support de smart contracts, pose la question du droit de la consommation. Mais comment l'appliquer ? Comment vérifier par exemple qu'un consommateur a bien été informé 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.

⁴⁰ Crée 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 blockchain⁴¹.

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 cotés⁴¹. 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 l'occasion⁴² 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.

⁴¹ 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.

⁴² 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'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)⁴³ ».

Ces titres, qui sont remis par des sociétés en contrepartie d'un prêt qui leur est accordé⁴⁴ sont inscrits au nom de leur titulaire dans un registre spécialement tenu par leur émetteur⁴⁵. 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 stimulantes⁴⁶ : 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 ».

⁴³ 42JO du 29 avril 2016, n° 101, op. cit.

⁴⁴ C. mon. fin., art. L.223-1.

⁴⁵ C. mon. fin.. art. L.223-4.

⁴⁶ R. Vabres, "Bons de caisse, minibons, blockchain... résurrection ou révolution ?" Droit des sociétés n° 7, Juillet 2016.

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 nouveau⁴⁷ 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-intermédiaire 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 blockchain⁴⁸.

⁴⁸ 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.

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 négociation⁴⁹. 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 2014⁵⁰, (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.

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 avancée⁵¹. 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 titres⁵².

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 2018⁵³.

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

⁵⁰ 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.

⁵¹ 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.

⁵² Delaware State Senate, 149th General Assembly, Senate Bill no. 69.

⁵³ 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 immobilier⁵⁴. L'acte authentique est celui reçu par un officier public ayant qualité et compétence pour instrumenter et avec les solennités requises⁵⁵. 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 vente⁵⁶ » .

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 ?

⁵⁴ Article 710-1 du code civil.

⁵⁵ Article 1369 du code civil.

⁵⁶ S. DRILLON, « La révolution Blockchain », RTD com. 2016, p. 893, n°22

Dans le même sens, il faut rappeler qu'un amendement à la loi Sapin 2⁵⁷ 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 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 juridique⁵⁸, « 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'attribue⁵⁹.

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.

⁵⁷ 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 »

⁵⁸ Gérard CORNU, Vocabulaire juridique, PUF, 11e éd.

⁵⁹ Le Robert, Dictionnaire de la langue française.

Toutefois, à l'heure actuelle, pour les notaires, les protocoles sont une technologie de certification et non d'authentification⁶⁰ : 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 déléguétaire 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.

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 »⁶¹. 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 inexistant 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.

⁶⁰ Gaëlle MARRAUD DES GROTTES, « La blockchain : un secteur encore en phase d'exploration, mais très prometteur », RLDI n°138, juin 2017, p. 39.

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

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 »⁶². 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 relater⁶³.

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 usucaption 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.

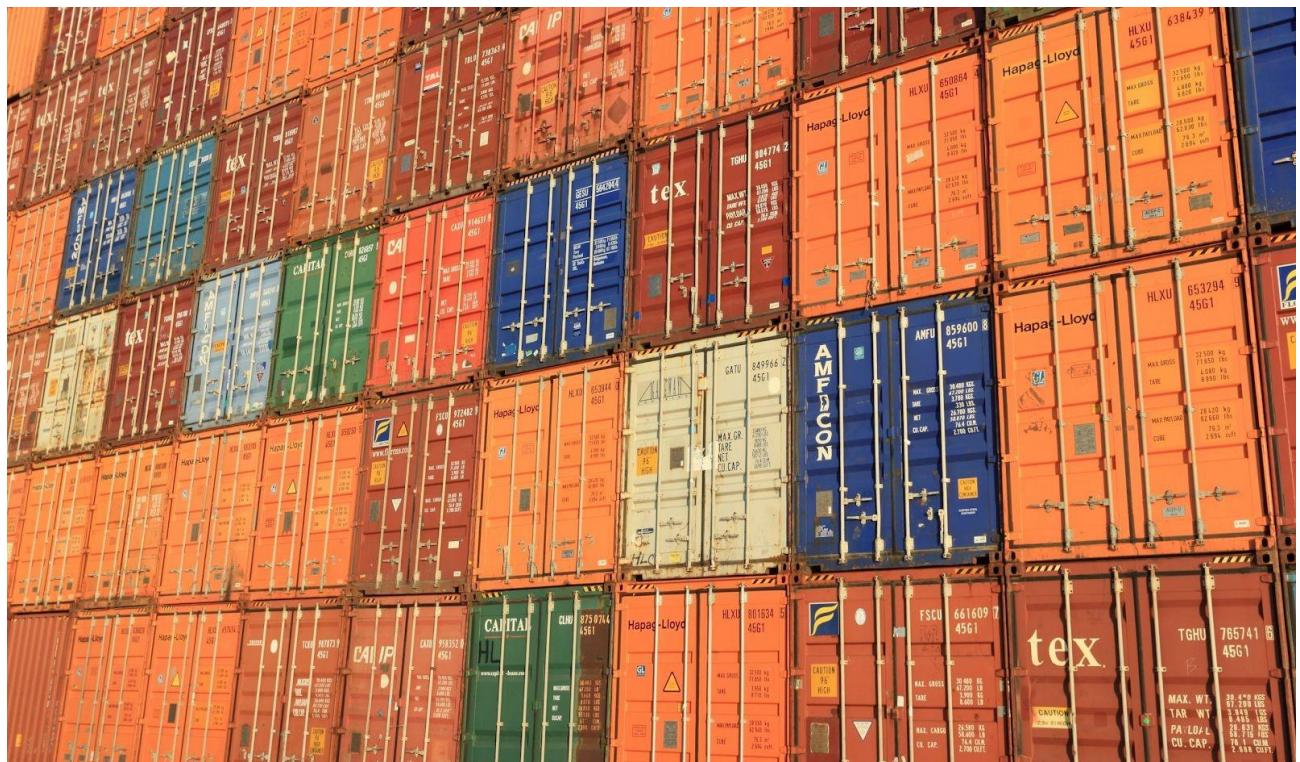
De plus, la prescription acquisitive pose un problème en raison de son effet rétroactif. En effet, le possesseur dont le droit de propriété est reconnu à l'issue du délai de dix ou trente ans est réputé avoir toujours été propriétaire, à compter du premier jour de possession. Une telle donnée paraît 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 ?

⁶² W. DROSS, Droit des biens, LGDJ, 2e éd., 2014, p. 49 n°46

⁶³ V. STREIFF « Blockchain et propriété immobilière : une technologie qui prétend casser les codes », Droit & Patrimoine, n°262, oct. 2016.

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 production 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 receveur. 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 Lavayssi  re

Initial Coin Offering

Etablir des qualifications juridiques des ICO

Initial Coin Offering

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.

Contexte

Proposer à l'échange des jetons (stockant des informations chiffrées) octroyant des droits dans un programme informatique : levée des fonds pour un projet en "cryptomonnaies"

Contexte des ICO

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

```

1  pragma solidity ^0.4.22;
2
3  contract AttendanceToken {
4      string public name="Ethercourt Training Attendance";
5      string public symbol="ETA";
6      uint8 public decimals=18;
7      uint _totalSupply;
8
9      address public owner;
10
11     mapping(address => uint) balances;
12
13     uint public deploy_date;
14     mapping(address => bool) public hasRequested;
15
16    constructor() public {
17        deploy_date = now;
18        owner = msg.sender;
19    }
20
21    function getName() public view returns (string) {
22        return name;
23    }
24
25    function setName(string _name) public {
26        require(owner == msg.sender);
27
28        name = _name;
29    }
30
31    function claimToken() public {
32        require(now < deploy_date + 24 hours, "You claimed too late");
33        require( ! hasRequested[msg.sender], "You are not allowed to claim!");
34
35        hasRequested[msg.sender] = true;
36
37        _totalSupply += 100;
38        balances[msg.sender] += 100;
39    }
40
41    function totalSupply() public view returns (uint) {
42        return _totalSupply;
43    }
44
45    function balanceOf(address _who) public view returns (uint) {
46        return balances[_who];
47    }
48
49    function transfer(address _to, uint256 _value) public returns (bool) {
50        require(balances[msg.sender] >= _value, "Insert coin...");
51
52        balances[_to] += _value;
53        balances[msg.sender] -= _value;
54
55        emit Transfer(msg.sender, _to, _value);
56
57        return true;
58    }
59
60    event Transfer(address indexed from, address indexed to, uint value);
61 }
```

exemple de smart contract d'émission de tokens

► 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 juriste⁶⁴. 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

⁶⁴ http://www.justice.gouv.fr/publication/chantiers_justice/Chantiers_justice_Livret_01.pdf

Lexique

Adresse : une adresse est une chaîne de caractères, 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. L'information est inscrite comme un message accompagnant un virement et permet par la suite de prouver l'antériorité de l'existence d'un document numérique.

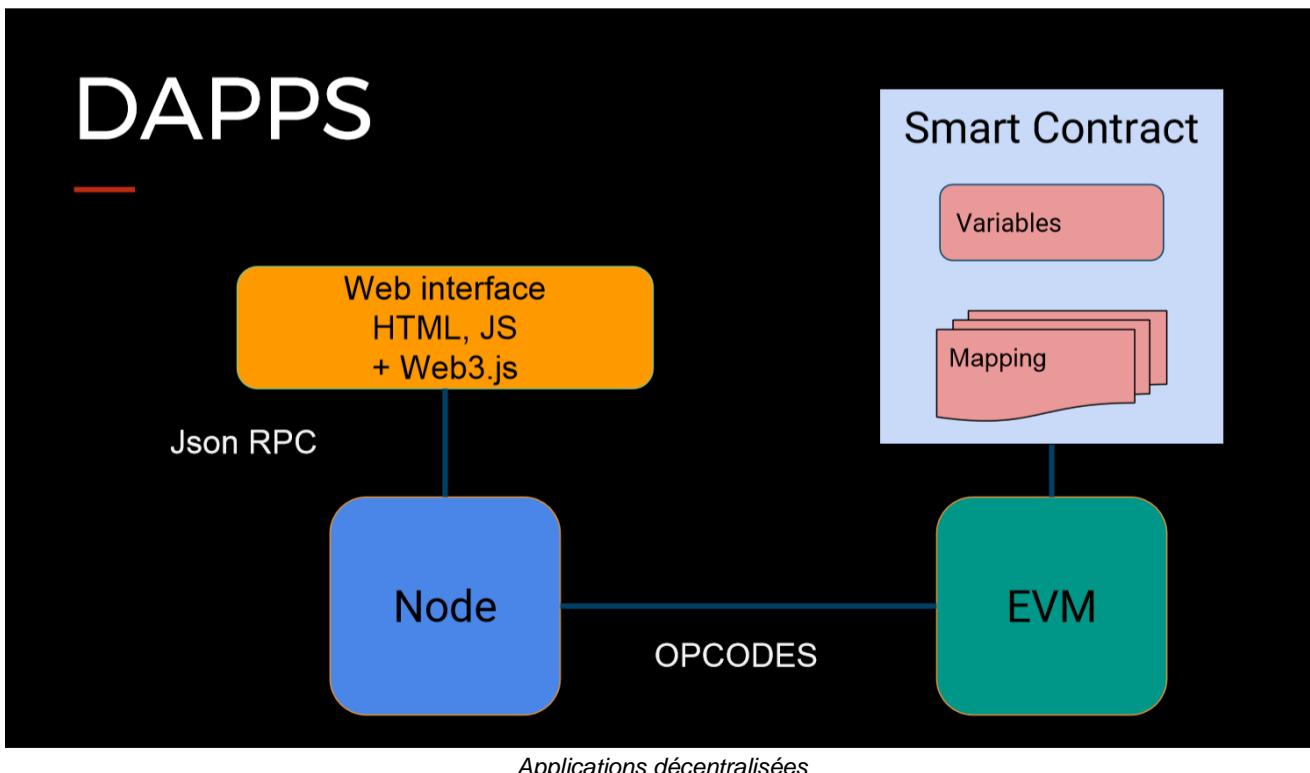
Bitcoin : le bitcoin désigne un protocole, une unité de valeur et un réseau. Le protocole, décrit initialement en 2008, repose sur un mécanisme de consensus au sein d'un réseau pair à pair. L'unité de valeur, le bitcoin est née avec le lancement du réseau en janvier 2009, elle sert à rémunérer les mineurs 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 décentralisées, 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 ou hash : valeur de sortie d'une fonction à sens unique de hachage cryptographique. Ces fonctions produisent des condensats (hash) de longueur fixe à partir d'un contenu quelconque. Ils ont pour 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, ni de produire un contenu cohérent à partir d'un hash donné).

Minage : le minage est une méthode qui consiste à valider un ensemble de transactions regroupées 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, une somme 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 véritables entreprises regroupant des centaines d'unités de calcul dans des "fermes de minage". Les mineurs sont souvent organisés au sein de "pools" de mineurs qui mutualisent les efforts et les gains.

Price and gas

0.00000002 Ether

10^18wei: ether

0.02e12 wei

200000000000 wei

20 gigawei

0.02 szabo

Coûts de transactions

Nœud : un nœud d'un réseau blockchain est une instance logicielle connectée au réseau composé des 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 pré-déterminé, 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 période de validation (10 minutes pour bitcoin). 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 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 à la somme mis en jeu 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 Labb  
Fr  d  ric Laffy
Xavier Lavayssi  re
Laetitia Maffei

Contributeurs

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

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

France Stratégie

Rapport du sous-groupe juridique

Le groupe de travail de France Stratégie sur les blockchains a constitué un sous-groupe juridique pour examiner le cadre légal et règlementaire dans lequel les cas d'usages de la blockchain s'inscrivaient et proposer des axes d'amélioration.

Les membres du groupe de travail juridique ont invité des acteurs spécialisés du secteur à participer aux travaux de ce groupe.

Ce document constitue le rapport établi par ce sous-groupe.

La technologie dite « blockchain » et ses mécanismes de consensus permettant de garantir l'unicité d'inscriptions et la transférabilité d'unités de comptes numériques font naître de nouvelles problématiques juridiques que le droit français n'appréhende pas encore parfaitement. Il n'est pas isolé ; en dehors d'initiatives sporadiques, l'état du droit « de la blockchain » est encore balbutiant. C'est une opportunité pour la France de se positionner à l'avant-garde dans un domaine à l'importance stratégique.

Sans revenir en détail sur les caractéristiques techniques de la technologie, ce rapport s'attachera à analyser ses différents cas d'usage au regard des enjeux juridiques qu'ils posent. Il porte un double objectif de diagnostic et de proposition.

Dans un premier temps, il établit un état des lieux des problématiques juridiques posées par la blockchain aux acteurs qui souhaitent s'en saisir et développer des activités autour de cette technologie, qu'elles soient commerciales, industrielles, sans but lucratif ou d'intérêt général. Dans ce contexte, les participants au rapport ont identifié les points de tension, les problématiques qui seraient de nature à freiner ou bloquer les expérimentations ou projets en cours.

Dans un second temps, des propositions concrètes permettant d'amoindrir ou de supprimer les points de tension identifiés ont été formulées pour les principaux cas d'usage, en miroir de ces problématiques. Elles l'ont été en gardant à l'esprit la nature expérimentale de ces technologies et le besoin de définir des cadres appropriés qui pourront s'adapter aux futures évolutions de la technologie.

Parmi celle-ci, trois propositions nous semblent devoir être mises particulièrement en avant car elles répondent à des impératifs immédiats vécus par les acteurs du secteur :

- **Question de la preuve** : le groupe de travail pointe l'insécurité naissant de l'absence de régime de preuve spécial relatif à l'inscription sur blockchain et recommande une adaptation du droit existant pour permettre la prise en compte, sous certaines conditions détaillées dans la fiche correspondante, d'une inscription sur blockchain comme preuve. À court terme, il est possible d'adopter une réforme visant à renforcer, dans le code civil, la force probante des informations figurant sur une blockchain selon des modalités techniques à préciser. Dans une perspective de plus long terme, il faudra d'engager une réflexion devant aboutir à la révision du règlement eIDAS afin de reconnaître pleinement la fiabilité de la signature électronique et de l'horodatage sur la blockchain sans intervention d'un tiers certificateur.
- **Fiscalité**. Le groupe de travail a également identifié la question fiscale, et plus particulièrement l'imprécision qui pèse aujourd'hui sur le traitement fiscal des opérations, comme étant un frein important au développement des activités relatives à la blockchain sur le territoire français. *A contrario*, une politique fiscale claire et adaptée à cette nouvelle classe d'actif serait de nature à attirer des acteurs sérieux sur le territoire. La recommandation du groupe de travail est de clarifier, par la loi, le régime fiscal des cybermonnaies.

En pratique, ceci suppose de clarifier fiscalement le régime des opérations d'achat, de vente mais aussi les échanges et autres utilisations de cybermonnaies et *tokens*. Il est également recommandé de clarifier l'exonération des échanges d'actifs numériques de la taxe sur la valeur ajoutée.

- **Ouverture de compte bancaire.** Le groupe de travail a enfin constaté que de nombreux acteurs étaient confrontés à une problématique liée à l'ouverture et au fonctionnement de leurs comptes bancaires. Les contraintes imposées aux établissements de crédit en matière de lutte contre le blanchiment et le financement du terrorisme ne tient pas compte des particularités des cybermonnaies. Ceci est de nature à poser un obstacle à l'ouverture et au fonctionnement de tels comptes voire à provoquer leur fermeture, quand bien même les transactions réalisées avec ces actifs ne seraient pas suspicieuses. Le groupe de travail recommande d'imposer aux entreprises gérant des plateformes d'échange des obligations de vérification d'identité et d'origine des fonds (KYC et AML) ainsi que la communication aux titulaires de comptes de toutes les informations leur permettant de satisfaire les exigences réglementaires applicables aux établissements de crédit. Ceci permettra aux établissements bancaires de satisfaire leurs propres obligations en la matière afin de ne pas bloquer le fonctionnement de ces comptes.

Le corps de ce rapport est structuré en fiches de synthèse correspondant aux cas d'usage identifiés de la technologie d'une part, et aux branches du droit concernées d'autre part. Chaque fiche est appréhendable séparément mais certaines problématiques spécifiques se répondent naturellement.

Bonne lecture.

Au nom du sous-groupe juridique,

Simon Polrot

Fiche 1

Analyse juridique des *tokens* (ou jetons)

Responsable de rédaction : Hélène Lefebvre, Avocate associée, Fieldfisher LLP

Le jeton ou "token" est un objet numérique sur une blockchain, et peut résulter de deux processus de création distincts :

1. soit, il est créé directement par le code-source du protocole de la blockchain et généré par une activité de minage, on parle alors aussi de cybermonnaies pour les principaux réseaux (bitcoin, ether ...);
2. soit il est créé par un « smart-contract », sur une chaîne préexistante, qui détermine notamment leur nombre initial et leurs modalités d'émission.

Les tokens sont initialement proposés dans le cadre des Initial Coin Offering (« ICO ») ou distribués directement, avec ou sans contrepartie⁶⁵. Ils sont ensuite le plus souvent échangés entre pairs ou sur des places de marché ou plateformes leur permettant ainsi d'acquérir une valeur de marché, bien que celle-ci soit généralement volatile.

Minimal token

```
contract SCAToken {
    mapping (address => uint256) public balanceOf;

    function SCAToken( uint256 initialSupply ) {
        balanceOf[msg.sender] = initialSupply;           // Give the creator all initial tokens
    }

    function transfer(address _to, uint256 _value) {
        if (balanceOf[msg.sender] < _value) throw;          // Check if the sender has enough
        if (balanceOf[_to] + _value < balanceOf[_to]) throw; // Check for overflows
        balanceOf[msg.sender] -= _value;                    // Subtract from the sender
        balanceOf[_to] += _value;                          // Add the same to the recipient
    }
}
```

SCAToken

⁶⁵ La question du traitement juridique des ICO fait l'objet d'une consultation publique de l'Autorité des Marchés Financiers concomitante à la réalisation de ce rapport et ne sera par conséquent pas examinée en détail.

1. Appréhender la nature juridique des tokens

1.1. Une nature juridique appréhendée au travers de leurs caractéristiques

1.1.1. Caractéristiques multiples

Les tokens sont librement programmés lors de leur création. Chaque token étant programmé pour une utilisation déterminée, leurs caractéristiques peuvent être multiples (voir leur typologie en section 1.2 ci-dessous). Ainsi, qualifier juridiquement le token ne peut reposer sur le simple fait qu'un instrument est qualifié génériquement de "token" ; il convient de prendre en compte leurs caractéristiques précises.

1.1.2. Utilisation double

En outre, ces instruments pourront être programmés pour une utilisation donnée (ses caractéristiques de départ) et être, en cours de cycle, utilisés d'une manière différente par les détenteurs du token. En tout état de cause, la plupart des tokens peuvent être utilisés comme "cybermonnaie", c'est-à-dire une unité de compte numérique à valeur d'échange. Un même instrument pourra donc, par exemple, avoir été créé pour représenter un droit de vote dans un projet et être également utilisé comme instrument d'échange.

1.2. Typologie des tokens

S'il est impossible de dresser une liste exhaustive des cas d'usages, les principaux tokens que l'on peut voir sur le marché à la date de ce rapport correspondent aux caractéristiques suivantes :

- a. tokens applicatifs : ces tokens sont utilisés dans une application décentralisée déterminée et permettent d'accéder à un service donné, comme les "RLC", émis par IEx.ec et permettant d'accéder à de la puissance de calcul ;
- b. tokens de réputation : ces tokens sont utilisés aux fins d'apprecier la fiabilité d'un utilisateur de la technologie blockchain. Dans ce contexte, le nombre de tokens attribués à l'utilisateur peut refléter son niveau de fiabilité, l'on pourra citer les tokens "REP" émis par Augur.
- c. tokens donnant droit à un revenu ou un dividende : le token est créé en lien avec un projet particulier et donne le droit de recueillir des revenus liés au projet à des intervalles prédéfinis. Les tokens "The DAO" offraient un droit à percevoir des revenus issus des projets financés.
- d. tokens de vote : ces tokens représentent un nombre de voix prédéterminé et pourront être utilisés dans un *smart-contract* de vote. Les tokens "MKR" de "maker DAO" donnent ainsi un droit de vote à leurs détenteurs.
- e. tokens représentant des points de fidélité : le token est attribué à un client à chaque utilisation d'un service déterminé, ce token, à l'image du token émis par "Plutus", pourra ensuite être utilisé en paiement ou selon d'autres modalités.
- f. tokens représentant une valeur spécifique : ces tokens peuvent correspondre à une valeur déterminée exprimée par exemple en devise. A titre d'illustration, un token ETH-EURO, par exemple, pourrait être programmé de manière à ce que sa valeur soit toujours égale à un euro.
- g. tokens de preuve : ces tokens peuvent apporter la preuve de la propriété, de la possession ou du transfert d'un actif non virtuel. Le token est alors lié audit actif et le transfert du token matérialise le transfert de propriété de l'actif non virtuel.

En synthèse, il est cependant possible d'établir plusieurs catégories de tokens en lien avec leur utilisation :

1. **Tokens d'investissement.** Cette catégorie comprend les cas où des instruments financiers traditionnels, tels que des actions ou des parts d'une société voire des parts ou actions d'un fonds d'investissement, sont représentés par un token. Ces tokens peuvent donc donner des droits similaires à ceux existants pour des instruments financiers classiques, mais avec la particularité d'exister en tant que token sur une blockchain. Ces tokens d'investissement devraient logiquement tomber dans le champ d'application des réglementations existantes en matière d'instruments financiers ; toutefois il pourrait être pertinent d'examiner une possible adaptation de ces réglementations pour prendre en compte les améliorations technologiques des tokens concernées, notamment l'influence en termes de transparence.
2. **Tokens « biens de consommation ».** Cette catégorie est composée des tokens représentant l'accès à des biens ou services sous forme d'un actif digital consommable, tels qu'une licence d'utilisation ou des droits d'accès à une plateforme digitale. L'objectif de ces tokens est d'être utilisé, "consommé". Ces Tokens de consommation ne sont pas *a priori* des instruments financiers.
3. **Tokens “monétaires”.** Il s'agit de jetons qui sont utilisés comme valeur d'échange (“monnaie”) au sein d'une communauté définie pour accéder à des biens ou des services au sein de cette communauté.
4. **Autres tokens.** Cette catégorie recouvre les tokens qui ne sont ni des tokens d'investissement, ni des tokens « biens de consommation ». Etant donné le caractère récent des utilisations des tokens, nous ne pouvons présager des nombreuses variations et de la manière dont elles seront effectivement utilisées dans le cadre du fonctionnement d'un réseau basé sur des tokens. Ainsi, il est d'autant plus difficile de concevoir les limites précises entre les différentes catégories de tokens, et d'anticiper quelles prescriptions légales seraient ou ne seraient pas nécessaires pour encadrer ces tokens.

ERC 20 Token

```
contract ERC20 {  
    function totalSupply() constant returns (uint totalSupply);  
    function balanceOf(address _owner) constant returns (uint balance);  
    function transfer(address _to, uint _value) returns (bool success);  
    function transferFrom(address _from, address _to, uint _value) returns (bool success);  
    function approve(address _spender, uint _value) returns (bool success);  
    function allowance(address _owner, address _spender) constant returns (uint remaining);  
    event Transfer(address indexed _from, address indexed _to, uint _value);  
    event Approval(address indexed _owner, address indexed _spender, uint _value);  
}
```

Geth

```
geth --networkid "4768" --datadir  
"/home/jordan/Desktop/data4" --ipcpath  
"/home/jordan/.ethereum/geth.ipc" --rpc --nodiscover  
--rpccorsdomain "http://localhost:8545" --rpcapi  
"eth,personal"
```

```
geth attach ipc:/tmp/ethereum_dev_mode/geth.ipc
```

Token ERC 20

1.3. Possibles qualifications juridiques des tokens

1.3.1. Qualification générale

D'une manière générale, il est possible de voir dans un token un droit ou bien incorporel. Parfois, le token peut aussi se rattacher à un régime juridique déjà existant.

1.3.2. Monnaie électronique

La monnaie électronique est une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique⁶⁶. Certains tokens peuvent être qualifiés comme de la monnaie électronique même si tous les tokens monétaires ne répondent pas à la qualification de monnaie électronique.

1.3.3. Services de paiement

Les *tokens* (en ce compris les cybermonnaies) ne rentrent pas *a priori* dans la catégorie des services de paiement (au sens des directives européennes DSP I et DSP II).

⁶⁶ Article L. 315-1 du Code monétaire et financier

1.3.4. Titres financiers

Certains tokens, notamment les tokens donnant droit à des revenus et/ou des droits de gouvernance dans une structure (une société ou toute autre forme d'organisation) pourraient s'apparenter à des instruments financiers.

Les instruments financiers, qui comprennent les valeurs mobilières, ont pour caractéristiques d'être (i) émis, notamment, par une personne morale, (ii) inscrits en compte ou susceptible de l'être, (iii) cette dernière inscription s'effectuant au profit du propriétaire des titres, (iv) négociables et (v) dématérialisés. Pour autant, la définition de valeur mobilière au sens de la directive MIF2 est plus large que la seule définition française et pourrait conduire certains tokens à être caractérisés comme tel. En effet, la définition de valeur mobilière dans la directive MIF2 peut être interprétée très largement.

A cet égard, il convient de noter que la SEC aux Etats Unis d'Amérique s'appuie sur la jurisprudence Howey de la Cour Suprême pour caractériser un instrument ou un droit de « *Security* ». Or l'un des critères clé pour distinguer un « *Security* » (lequel est en droit américain défini très largement), d'un autre bien ou droit réside notamment dans la contrepartie financière accordée aux porteurs de tokens, sous forme de dividendes ou de revenus ou promesse de revenus, autrement dit l'existence d'un rendement financier (critère d'ailleurs retenu pour caractériser en France un « bien atypique »).

Le même besoin de clarification existe pour certains tokens et leur qualification en créance ou titre de créance obligataire, notamment suite à l'arrêt de la cour de Cassation du 23 novembre 2017.

Les titres financiers, qui comprennent les valeurs mobilières⁶⁷, sont, en droit français, une catégorie d'instruments financiers, et ont pour caractéristiques d'être (i) émis, notamment, par une personne morale, (ii) inscrits en compte ou susceptible de l'être⁶⁸, (iii) cette dernière inscription s'effectuant au profit du propriétaire des titres, (iv) négociables et (v) dématérialisés⁶⁹.

⁶⁷ Au sens de l'article L. 228-1 du Code de commerce

⁶⁸ Articles L.211-3 à L. 211-13 du Code monétaire et financier

⁶⁹ Ils se transmettent par virement de compte à compte, article L. 211-16 du Code monétaire et financier

1.3.5. Conclusion

Une analyse au cas par cas des caractéristiques du token est nécessaire afin de qualifier juridiquement un token et d'analyser si ce dernier peut ou non être assimilé à une catégorie juridique déjà existante. Nous pensons que les tokens ne doivent pas déroger à l'application du droit commun et/ou aux droits spéciaux, le cas échéant applicable. Ce qu'il convient d'éviter, c'est d'imposer un cadre juridique entièrement nouveau à des tokens qui sont appréhendables par le droit existant. Nous pensons au contraire que la plupart des catégories juridiques existantes permettent de caractériser juridiquement de très nombreux tokens. Cette analyse préalable est d'autant plus nécessaire que, selon la qualification juridique du token, la vente de celui-ci répondra à tel ou tel régime juridique. Ainsi, un token qualifié de valeur mobilière devra répondre à la réglementation sur l'offre au public de titres, alors qu'un token qualifié de vente d'un service répondra plutôt au droit de la vente à distance.

Si la question de la vente de tokens n'est pas couverte spécifiquement par ce rapport car elle fait l'objet concomitamment d'une initiative de place de la part de l'autorité des marchés financiers, il convient de noter que les conclusions de cette consultation seront déterminantes pour la détermination du statut des *tokens*.

2. Recommandations

1. *Clarification du cadre juridique des tokens.* Compte tenu du fort développement de l'industrie, il semble nécessaire de préciser le cadre juridique des *tokens*. Cette clarification devra cependant prendre en compte les qualités intrinsèques du token et son utilisation effective. Une tentative de réglementation par une approche globale, qui aurait pour objectif de faire entrer tous les tokens dans un champ restreint sans prendre en compte les caractéristiques de chacun d'entre eux serait inadaptée.

De façon pragmatique, le groupe de travail conseille le lancement d'une consultation avec les acteurs de la place afin d'identifier les catégories juridiques dans lesquelles les tokens pourraient entrer en fonction de leurs caractéristiques spécifiques. Compte tenu des modalités de création d'un token, certains d'entre eux devraient appartenir à plusieurs catégories.

Une fois ces catégories définies et expliquées, les émetteurs de tokens seraient responsables de la catégorisation de ceux-ci et de l'application de la réglementation y afférente. Dans un souci de prévisibilité juridique, il serait également souhaitable de mettre en place une procédure d'examen préalable par un certain nombre d'institutions publiques des caractéristiques d'un token afin de faire valider *a priori* la catégorisation juridique de ceux-ci.

- 1) *Cadre réglementaire existant et extension possible.* Les plateformes effectuant pour le compte de leurs clients des opérations d'achat ou de vente de cybermonnaies contre une monnaie ayant cours légal sont soumises à agrément car elles effectuent une prestation de service de paiement (ex. encaissement de fonds pour le compte de tiers). Eu égard au développement rapide des tokens et au fait que ceux-ci peuvent faire l'objet d'échanges sans qu'une devise ayant cours légal ne soit impliquée, ce cadre réglementaire pourrait être étendu aux plateformes d'échange ne proposant que des échanges de cybermonnaies.

Quelle que soit l'approche de réglementation choisie, il conviendra d'analyser les textes déjà applicables, afin d'éviter de soumettre un token particulier à plusieurs réglementations et de prévoir, en cas de conflit entre textes applicables, quelle réglementation devra primer.

Fiche 2

Smart-contract et Droit des contrats

Responsables de rédaction : Anne-Hélène Le Trocquer, Avocat Associé, De Gaulle Fleurance et Associés et Xavier Lavayssière, Fondateur, ECAN



(Smarts) Contracts

1. Définition

Un smart-contract, ou contrat intelligent, est un **programme informatique exécuté de façon autonome** par un réseau reposant sur les technologies blockchain. L'expression est une référence au concept plus large de protocole informatique de contractualisation formalisé par Nick Szabo dans les années 90⁷⁰.

⁷⁰ Szabo, N. (1996). Smart contracts: building blocks for digital markets

2. Concept et implémentations

Ethereum project

2013



2016



Ethereum

Un smart-contract est habituellement rédigé dans un langage informatique de haut niveau⁷¹, lisible par tout développeur.

⁷¹ Un langage de programmation de haut niveau est un langage proche des langages naturels, par opposition aux langages de bas niveau plus proches du fonctionnement des machines. Les langages de Smart Contracts sont inspirés de langages de programmation usuels: Solidity et Viper sur Ethereum, Go sur Hyperledger sous l'appellation Chaincode...



Programmation du smart contract

Solidity language

Javascript flavoured

Types
uint, int, bytes32, [...] ...

Special Key Words
throw

Specific Variables

- this *address of current contract*
- this.balance *remaining balance*
- msg.sender *sender of the call*
- msg.value *amount in wei*
- msg.data *bytes version*
- msg.gas *remaining gas*
- now *block timestamp*

Solidity

The screenshot shows the Ethereum Browser-Solidity interface. On the left, the Solidity source code for `ballot.sol` is displayed, containing functions for managing a campaign, getting雕塑名字 (sculpture name), and choosing a successor. On the right, the interface shows the Solidity version (0.4.4+commit), the target blockchain (Ropsten Test Net), and the compiled bytecode. A sidebar titled "TwinFlowers" shows the address of the deployed contract and its interface details.

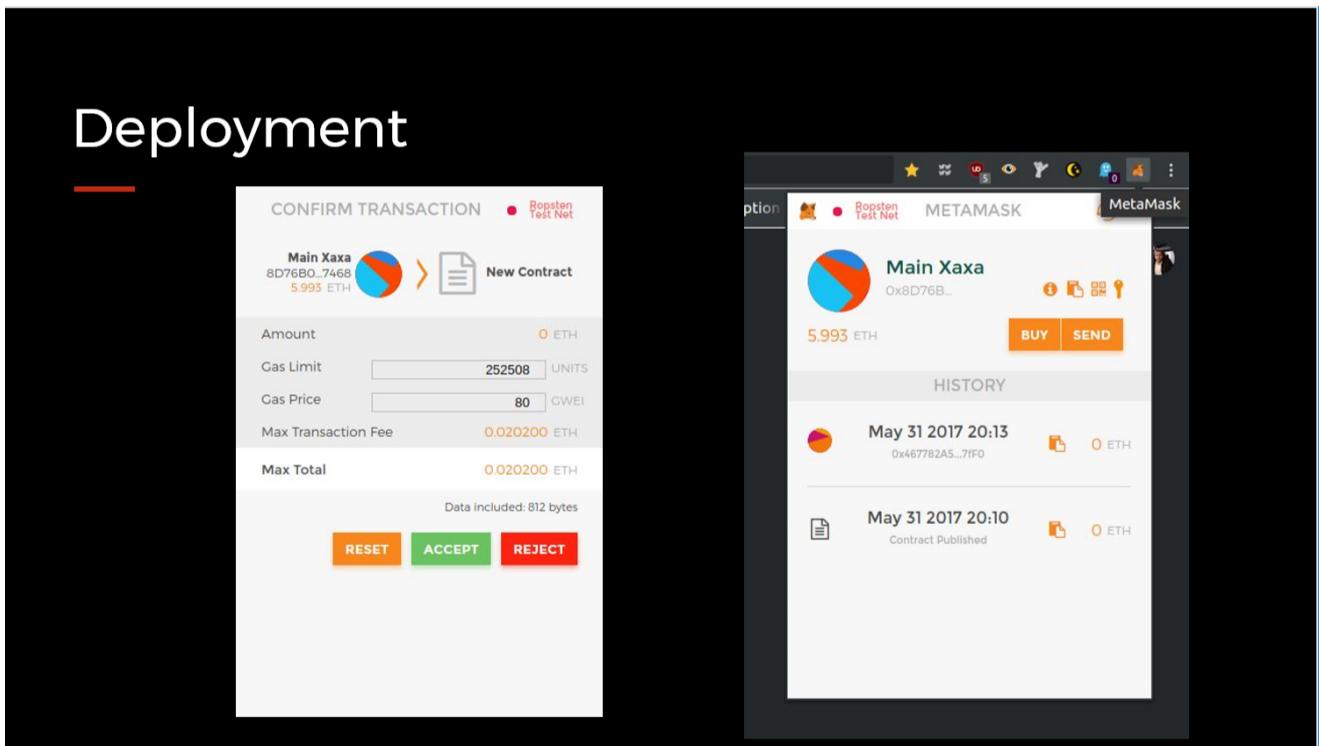
```

ballot.sol
52     // If len(campaign) < now:
53     uint amount = msg.value;
54     contributors[contributors.length-1] = Contributor({addr: msg.sender, amount: amount, name: d
55     amountRaised += amount;
56     DonationComplete(msg.sender, amount, donatorName);
57   }
58
59   function askScultureName() returns (string) {
60     return scultureName;
61   }
62
63   // Seems best way to have
64   function getContributor(uint index) public returns(string, uint, address) {
65     return (contributors[index].name, contributors[index].amount, contributors[index].addr);
66   }
67
68   // TODO at each donation you receive info, a picture of you with the sculpture
69
70   // checks if the goal or time limit has been reached and choose successor
71   // TODO ask for proposal, vote par les contributeurs, vote pondéré par le montant des donations
72   function chooseSuccessor(address successor) {
73     uint support = amountRaised * 1/10;
74     uint payForward = amountRaised * 8 /10 ;
75
76     if (msg.sender == artist){
77
78       if (amountRaised >= fundingGoal){
79         if (artist.send(support))
80           throw;
81         if (parent.send(support))
82           throw;
83         if (successor.send(support))
84           throw;
85         // TODO lancer le nouveau contrat
86         if (artist.send(this.balance))
87           throw;
88       }
89     }
90
91   }
92
93   // endCampaign = true;

```

Solidity Browser

Le code est ensuite compilé (transformé) dans un langage machine puis déployé sur un réseau blockchain.



Transaction

Le smart-contract est alors accessible au travers d'un identifiant et il est possible d'interagir avec lui par l'intermédiaire de transactions blockchain avec un client logiciel.

The screenshot shows the Etherscan Verify interface. At the top, it displays the address 0x8D76B07BeD241350CEAb2e3Aa568100AFc727468. Below this, there's an overview section with ETH Balance (5.99395702 Ether) and No Of Transactions (8 txns). The 'Transactions' tab is selected, showing two recent transactions:

TxHash	Block	Age	From	To	Value	[TxFee]
0xeb3a9a65a05ca58...	1032236	2 hrs 19 mins ago	0x8d76b07bed24135...	OUT → 0x467782a5ab90af6...	0 Ether	0.00099284
0x06f3a79d1c38422...	1032223	2 hrs 22 mins ago	0x8d76b07bed24135..	OUT → Contract Creation	0 Ether	0.00505014

Vérification d'une transaction

L'éditeur du smart-contract ne maîtrise alors ni l'exécution ni l'interface finale avec laquelle l'utilisateur interagit avec le smart-contract. Déployé sur un réseau blockchain public, ces programmes peuvent gérer de façon native des fonds au travers d'une cryptomonnaie ou d'un jeton.

3. Propriétés

- 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 tokens.
- 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.

4. Smart-contract et droit français

Le smart-contract est en pratique :

- soit une modalité d'exécution d'une relation contractuelle ;
- soit lui-même le support du contrat.

Dans le premier cas, la principale caractéristique qui le distingue d'un logiciel classique est l'autonomie de son exécution (voir infra).

Dans le deuxième cas, que l'on voit notamment dans le cas de certaines *Initial Coin Offerings* (ICO)⁷², 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 parties⁷³ et son support peut être oral, écrit ou numérique voir infra).

4.1. Smart-contract en tant que modalité d'exécution d'une relation contractuelle préexistante

Lorsqu'il s'agit d'un acte d'exécution automatique d'un contrat préexistant, deux approches peuvent être proposées pour en préciser la nature juridique.

Dans une première hypothèse, quand aucun accord de volonté supplémentaire n'est nécessaire pour déclencher la prestation (ex. remboursement dans le cadre d'une assurance retard) c'est un acte d'exécution d'une obligation d'un contrat préexistant et à ce titre aucun régime spécifique n'est à créer.

Dans une seconde hypothèse, si une volonté est nécessaire pour mettre en œuvre le *smart-contract*, il peut alors être considéré comme un contrat à part entière. Le contrat initial peut alors s'envisager comme un contrat cadre et le smart-contract comme un contrat d'application en précisant les modalités d'exécution⁷⁴.

⁷² Dans le cas où l'ICO consiste en la vente automatique d'un token au travers d'un Smart Contract. C'est ainsi le cas de The DAO, en mai 2016, et des projets français iExec et Beyond the Void. Les projets plus récents tendent toutefois à faire signer un contrat au préalable, l'échange sur la blockchain n'étant alors qu'une modalité d'exécution.

⁷³ Article 1101 du code civil

⁷⁴ « Le contrat cadre est un accord par lequel les parties conviennent des caractéristiques générales de leurs relations contractuelles futures. Des contrats d'application en précisent les modalités d'exécution » Article 1111 du code civil.

4.2. Smart-contract en tant que support unique du contrat

Dans les cas où le smart-contract est le seul support d'un contrat, il semble nécessaire que le consentement de l'ensemble des parties soit clairement recueilli et qu'il soit exempt de vice pour que ce contrat numérique soit valable (1127 et s. du Code civil).

Il conviendra notamment ici de vérifier que les conditions posées par l'article 1127-1 du Code civil (applicable à « [q]uiiconque 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* ») soient appliquées, en particulier celle relative à la communication des étapes à suivre pour conclure ledit contrat par voie électronique, ainsi que des conditions générales et/ou particulières d'utilisation qui, avec le contrat principal, forment l'ensemble contractuel applicable entre les parties.

Quant à la valeur de l'écrit sous forme de programme, il convient de distinguer les situations. En matière civile, dans le cas d'une contestation entre un professionnel et un particulier dont la valeur n'excède pas 1 500 euros, le contrat peut être prouvé par tout moyen, de même en matière commerciale pour les actes de commerce quel que soit le montant de la transaction (L. 110-3 du Code de commerce). Dans les autres cas, si le programme 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* » (Article 1365 du Code civil), il faudra considérer les éléments d'identification et de conservation du programme (cf. fiche preuve).

5. Conséquences de l'exécution autonome

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 donc susceptible de créer des situations de fait difficiles à résoudre juridiquement. Les procédures de modification et situations doivent donc être anticipées dans le code, entre les parties et dans le cadre juridique :

- La modification avec l'accord des deux parties et la rétractation d'une des parties.
- La mauvaise exécution issue d'une erreur de manipulation ou tentative frauduleuse.
- Les bugs ou mauvais fonctionnement du programme. Des questions de responsabilité extra contractuelle peuvent se poser dans ce cas entre les parties et vis-à-vis des prestataires et éditeurs de solutions majoritairement « open source »⁷⁵.
- Les effets de l'annulation du contrat original, de l'intervention du juge ou éventuellement d'arbitres, de l'ouverture d'une procédure collective...

Juridiquement il faut constater que l'automaticité du processus empêche le jeu normal des dispositions sur l'inexécution du contrat des articles 1217 et suivants du Code civil. C'est donc en effet par des mesures correctrices que les remèdes aux difficultés d'exécution ou aux vices affectants le « smart-contract », voire son contrat cadre, doivent être pensés.

⁷⁵ Les programmes open sources sont des programmes dont le code source est publié de façon publique et comportant généralement une clause limitative de responsabilité des auteurs. Les plus connues ont la GNU Public Licence, MIT License et BSD License.

6. Recommandations

- 1) Préciser explicitement, potentiellement par la loi, les conditions dans lesquelles un smart-contract pourrait avoir une valeur de contrat formel, de façon similaire au travail accompli en matière de contrats sous forme électronique. Ce travail s'effectuera en lien avec les recommandations proposées en matière de preuve.
- 2) Développer un référentiel de bonnes pratiques pour le développement de smart-contract sécurisés, notamment quand ils sont amenés à manipuler des fonds.

Fiche 3

Preuve et signature numérique

Responsable de rédaction : Florence G'sell, Professeur agrégé de droit privé

Les algorithmes utilisés par les chaînes de blocs participent à l'état de l'art des meilleures solutions cryptographiques connues. Les caractéristiques techniques de ces chaînes de bloc permettent de faire en sorte que les informations inscrites sur les blockchains soient accessibles sans risque d'interruption et ne soient ni effaçables, ni modifiables ni répudiables. Elles sont publiquement visibles et auditables par tout participant au réseau. Tel est l'apport de la technologie blockchain dont le droit de la preuve doit tenir compte.

1. Enjeux

Les questions de la preuve électronique et de la signature numérique constituent des enjeux majeurs pour le déploiement de la technologie blockchain. De nombreux développements en cours portent, en effet, sur des applications permettant d'effectuer diverses transactions ou de certifier la réalisation de certains événements (livraison de marchandises, création d'une œuvre originale etc...). Il convient donc de faire en sorte que ce qui se trouve sur la blockchain puisse disposer d'une portée probatoire avérée, faute de quoi l'investissement dans cette technologie se révèlera dépourvu d'intérêt dans la mesure où il faudra recourir aux tiers de confiance traditionnels.

Le droit français étant fondé sur un système de preuve légale, ce sont les textes législatifs et réglementaires qui prévoient la portée juridique des différents éléments de preuve soumis au juge. Dès lors que la blockchain ne peut être assimilée à l'un des moyens de preuve actuellement reconnus juridiquement et qu'aucun texte n'en prévoit la portée juridique, alors l'incertitude prédomine. Il est, en effet, impossible d'anticiper ce que le juge français pourrait décider face à un élément de preuve émanant d'une blockchain. Cette situation est génératrice d'une insécurité juridique de nature à freiner l'attrait de cette technologie pour les opérateurs.

Il convient donc de s'assurer que la preuve de type « blockchain » se voit conférer une portée juridique reflétant la fiabilité revendiquée par la technologie.

2. Etat des lieux concernant la preuve sur la blockchain

Les questions probatoires ne se posent pas dans les mêmes termes selon que la blockchain est privée ou publique.

2.1. La preuve sur une blockchain privée

Sur une blockchain privée et permissionnée, il suffit que le(s) gestionnaire(s) du réseau propose(nt) aux utilisateurs autorisés à y accéder une convention de preuve prévoyant que lesdits utilisateurs acceptent de considérer comme recevables en cas de litige des éléments techniques issus de la blockchain.

En cas de litige, le juge statuera sur la validité de la convention de preuve judiciaire et sur sa portée. Cela signifie qu'il suivra en principe les stipulations de la convention de preuve mais pourra, le cas échéant, être amené à apprécier lui-même la portée des éléments de preuve soumis par les parties. La Cour de cassation n'a pas accepté, conformément à l'article 1356 du Code civil, qu'une convention de preuve prévoie des présomptions irréfragables, qui ne peuvent être renversées, au bénéfice de l'une des parties (Cass. com. 6 décembre 2017, n°1517, 16-19615).

Bien que les difficultés probatoires puissent être réglées, sur des blockchains privées, par des conventions de preuve suffisamment précises et licites (pas de clause abusive, par exemple), cette situation n'est pas entièrement satisfaisante. Il se peut fort bien, par exemple, que l'on soit confronté en pratique à des conventions de preuve insuffisamment rédigées et que cela génère du contentieux. Il serait certainement préférable que le droit commun règle une fois pour toute la question de la preuve sur la blockchain.

2.2. La preuve sur une blockchain publique

Sur une blockchain publique et entièrement décentralisée, la conclusion de conventions de preuve n'est pas envisageable. La preuve sur la blockchain pose alors de réelles difficultés. Il convient d'aborder d'abord la preuve des actes juridiques, qui sont en général des actes sous seing privé librement conclus entre deux personnes privées (2.2.1), avant de dire quelques mots du cas particulier des actes authentiques (2.2.2.), puis d'évoquer le cas des simples faits juridiques (2.2.3.).

2.2.1. La preuve d'un acte sous seing privé sur une blockchain

La preuve des actes sous seing privés conclus sur une blockchain obéit à des règles générales figurant dans le Code civil (a) et pose la question plus spécifique de la signature électronique (b) ainsi que celle de l'horodatage (c).

a- Règles de preuve des actes sous seing privés

Les actes sous seing privés sont ceux qui ont été simplement conclus entre deux personnes privées, le cas échéant avec l'assistance d'un professionnel qui peut être le rédacteur de l'acte. La grande majorité des contrats les plus usuels font l'objet d'un acte sous seing privé.

♦ Cas où un écrit papier ou son équivalent numérique est exigé

En droit français, les contrats civils portant sur une somme supérieure à 1500 euros doivent être prouvés par écrit (art. 1359 C. civ.). L'article 1365 du code civil prévoit que « *L'écrit consiste en une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quel que soit leur support* », ce qui englobe les écrits numérisés et le code informatique. L'article 1366 du code civil ajoute que « *l'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité* ». Pour qu'un écrit électronique soit assimilé à un écrit papier et que les exigences légales soient respectées, deux conditions sont posées: l'identification de l'auteur et la garantie du maintien de l'intégrité de l'acte. Sur une blockchain, le second point peut être considéré comme acquis. En revanche, la première condition renvoie à la problématique de la signature électronique évoquée plus bas (v. *infra* B) : si les exigences légales relatives à la signature électronique ne sont pas respectées, alors l'élément de preuve émanant d'une blockchain n'est pas assimilable à un écrit papier et la preuve du contrat conclu sur la blockchain n'est pas rapportée. En revanche si les modalités de signature électronique respectent les exigences légales, alors l'écrit électronique est réputé assimilé à un écrit papier.

L'écrit papier est parfois requis par des textes spéciaux relatifs à des contrats spécifiques (contrat d'édition, vente de fonds de commerce, cession de créance etc...) non pas à titre probatoire mais en tant que condition de fond. Il faut en ce cas également respecter les conditions précitées si l'on souhaite recourir à un support électronique, de manière à ce que l'écrit électronique se voit reconnaître la même portée que l'écrit papier.

Il faut signaler, à ce sujet, que l'ordonnance n° 2016-520 du 28 avril 2016 relative aux bons de caisse a introduit, dans le Code monétaire et financier, un article L. 223-13 qui prévoit que : « *Le transfert de propriété de minibons résulte de l'inscription de la cession dans le dispositif d'enregistrement 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.* ». L'inscription de la cession dans un registre distribué (aux caractéristiques sont à préciser) est donc réputée tenir lieu de contrat écrit, ce qui constitue un changement notable d'avec le droit positif actuel. Les textes d'application de cette ordonnance ne sont toutefois pas encore parus et devraient (logiquement) imposer le respect des conditions posées par l'article 1365 C. civ. (garantie du maintien de l'intégrité de l'acte et identification de l'auteur) ce qui renvoie, là encore, aux exigences relatives à la signature électronique qualifiée. Il est donc vraisemblable que les textes d'application n'admettent l'assimilation de l'inscription dans un DLT à un écrit que pour les plateformes faisant intervenir des tiers de confiance et permettant des signatures électroniques qualifiées. Il est donc, à cet égard, fort probable que ces plateformes soient relativement permissionnées et centralisées.

◆ Cas où tout moyen de preuve est admis

L'exigence d'écrit ne concerne pas les contrats commerciaux (art. L110-3 C. com.) ou les contrats civils portant sur moins de 1500 euros. Sauf règles particulière, ces contrats bénéficient d'un principe de liberté de la preuve, ce qui signifie que tout moyen de preuve peut être employé pour les établir : présomptions, témoignages etc...

Il est donc possible de produire tous documents et éléments électroniques, même si ceux-ci ne remplissent pas les conditions requises par la loi pour être assimilés à de l'écrit papier. Ils seront librement appréciés par le juge, ce qui implique une certaine incertitude. Le plus vraisemblable est que le juge, en présence d'éléments de preuve provenant d'une blockchain, nommera un expert chargé d'apprecier la portée probatoire des différents éléments produits.

b- La signature électronique

La signature électronique sur la blockchain comporte des spécificités liées aux techniques cryptographiques particulières utilisées et notamment à l'articulation clé privée/clé publique (v. sur ce point, Paris Europlace, *Les impacts des réseaux distribués et de la technologie blockchain dans les activités de marché*, Rapport du groupe Fintech, 26 octobre 2017, pp. 84-90).

L'article 1367 du code civil prévoit que « *Lorsque [la signature] est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État* ». Il y a donc, ici, deux situations : soit l'on se trouve dans un cas de figure dans lequel la présomption de fiabilité de l'identification joue car les exigences réglementaires sont remplies, soit les conditions fixées par le décret ne sont pas remplies et la fiabilité est à l'appréciation du juge.

C'est désormais le décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique, pris en application du Règlement 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit Règlement eIDAS, qui fixe les conditions requises pour la fiabilité d'un procédé. Ce décret dispose que « *la fiabilité d'un procédé de signature électronique est présumée, jusqu'à preuve du contraire, lorsque ce procédé met en œuvre une signature électronique qualifiée* ».

Est une signature électronique qualifiée :

- *une signature électronique avancée,*
- *conforme à l'article 26 du règlement susvisé*
- *et créée à l'aide d'un dispositif de création de signature électronique qualifié répondant aux exigences de l'article 29 dudit règlement, qui repose sur un certificat qualifié de signature électronique répondant aux exigences de l'article 28 de ce règlement.* »

Pour que la fiabilité d'une signature électronique sur la blockchain soit présumée, il faudrait donc non seulement que cette signature puisse être considérée comme une signature électronique avancée mais aussi qu'elle constitue une signature qualifiée ce qui suppose l'intervention d'un prestataire de service de confiance agréé, telle que le règlement eIDAS le prévoit.

Basic contract

```
contract BasicContract {
    mapping (address => bool) public parties;
    string contractText;

    function BasicContract( string text ) {
        parties[msg.sender] = true;
        contractText= text;
    }

    function sign() {
        parties[msg.sender] = true;
    }

    function getText() constant returns (string) {
        return contractText;
    }

    function hasSigned() constant returns (bool) {
        return parties[msg.sender];
    }
}
```

Smart contract

Le règlement eIDAS distingue entre trois types de signatures électroniques, qui apparaissaient déjà dans la Directive 1999/93/CE de 1999 : la signature simple, la signature avancée et la signature qualifiée. La signature électronique simple ne correspond à aucune spécificité technique et ne jouit pas d'une portée particulière en matière probatoire.

La signature *avancée* doit, en revanche, correspondre à quatre particularités techniques précisées par l'article 26 du règlement eIDAS :

- a) être liée au signataire de manière univoque ;
- b) permettre d'identifier le signataire ;
- c) avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif et
- d) être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable.

Ces conditions paraissent remplies en présence d'une chaîne de blocs dès lors que des modalités sont mises en place afin que la condition c) soit respectée, ce qui implique que l'utilisateur ait, par exemple, le contrôle de sa clé privée grâce à un code personnel ou un mot de passe personnalisé lui conférant un contrôle exclusif. Il reste que la signature avancée ne bénéficie pas d'une présomption de fiabilité, même si le juge devrait lui conférer une portée probatoire plus importante que la signature simple.

Pour pouvoir bénéficier de la présomption de fiabilité, la signature sur la blockchain doit constituer une signature *qualifiée*, ce qui signifie qu'elle doit remplir les conditions précitées pour constituer une signature avancée mais également être « *créée à l'aide d'un dispositif de création de signature électronique qualifié répondant aux exigences de l'article 29 dudit règlement, qui repose sur un certificat qualifié de signature électronique répondant aux exigences de l'article 28 de ce règlement* ». Cela signifie concrètement qu'il convient de recourir aux services de prestataires de service de confiance agréés afin d'obtenir des certificats qualifiés de signature électronique (v. annexes I et II du règlement).

En l'état actuel des choses, donc, les signatures sur la blockchain qui ne font pas intervenir de tiers certificateurs dans les conditions prévues par le règlement eIDAS ne bénéficient pas de la présomption de fiabilité. Dans le même temps, la signature blockchain constitue vraisemblablement une signature avancée au sens du règlement, ce qui est toutefois insuffisant pour faire de la signature blockchain l'équivalent d'une signature manuscrite. Par ailleurs, le recours à un tiers certificateur agréé, renchérit le coût de l'investissement dans la technologie blockchain et constitue précisément ce que les architectures distribuées doivent permettre d'éviter. Une telle situation n'est pas satisfaisante : il conviendrait ici que la blockchain permette, précisément, de s'affranchir du recours aux services d'un tiers certificateur tout en offrant une réelle sécurité juridique.

c- L'horodatage électronique

L'horodatage sur la blockchain est sûr une fois qu'il est intervenu, mais comporte une particularité propre à cette technologie, à savoir le fait qu'il n'est pas instantané (au moins 10 minutes sur la blockchain Bitcoin, voire plusieurs heures si le réseau est encombré). Il s'agit là d'une limite qu'il faut garder à l'esprit.

Le règlement eIDAS prévoit, dans son article 42, les exigences applicables aux horodatages électroniques qualifiés, qui bénéficient « d'une présomption d'exactitude de la date et de l'heure qu'il indique et de l'intégrité des données auxquelles se rapportent cette date et cette heure » (art. 41 Règlement préc.). Or l'horodatage électronique qualifié fait, lui aussi, intervenir un prestataire de service de confiance qualifié.

Les dispositions de droit interne vont dans le même sens. Le décret n° 2011-434 du 20 avril 2011 relatif à l'horodatage des courriers expédiés ou reçus par voie électronique prévoit que l'horodatage électronique est présumé fiable si le prestataire de service d'horodatage et le module d'horodatage utilisés satisfont à certaines exigences qu'il précise. Il n'est donc pas possible à celui qui n'est pas un prestataire de service d'horodatage électronique qualifié au sens du décret de proposer un service d'horodatage électronique sur la blockchain qui bénéficie d'une présomption de fiabilité.

A défaut de respecter les spécificités requises par ces textes et de faire intervenir un prestataire qualifié, l'horodatage blockchain ne bénéficie pas d'une présomption d'exactitude ou de fiabilité et est librement apprécié par le juge. L'intervention d'un tiers certificateur constitue, là encore, une contrainte de nature à compliquer et surenchérir le coût de l'investissement dans la technologie blockchain. Il convient donc certainement d'adapter les règles relatives à l'horodatage sur la blockchain pour tenir compte de sa fiabilité.

2.2.2. Le cas particulier de l'acte authentique

L'acte authentique est, au contraire de l'acte sous signature privée, reçu par un officier public, en général un notaire. La force probatoire de l'acte authentique tient au fait qu'il « *fait foi jusqu'à inscription de faux* » (art. 1371 C. civ.). Cela signifie que le juge doit tenir pour vrai ce qui figure dans l'acte authentique : le contenu de celui-ci s'impose à lui car l'officier public l'a personnellement constaté.

Il est tentant de vouloir conférer l'authenticité aux transactions réalisées sur la blockchain, ce qui aboutirait à leur conférer une portée probatoire qui s'imposerait au juge jusqu'à « inscription de faux ». L'idée a déjà été envisagée. Un amendement déposé à l'Assemblée Nationale en 2016 prévoyait ainsi d'insérer, après le deuxième alinéa de l'article L. 330-1 du code monétaire et financier, un alinéa ainsi rédigé :« *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. L'Autorité des marchés financiers habilite le système répondant aux conditions de sécurité et de transparence définies dans un décret pris en conseil d'État.* » (amendement n°CF2 déposé le 13 mai 2016 par Mme de la Raudière au projet de loi dit « Sapin 2 » relatif à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique).

En principe, l'authenticité concerne les actes personnellement constatés par des personnes spécialement habilitées pour ce faire. Assimiler une transaction réalisée sur une blockchain à un acte authentique va sans doute au delà des besoins actuels, compte-tenu des cas d'usage pour l'heure envisagés. Si l'on souhaitait un jour réaliser sur la blockchain des transactions pour lesquelles la loi exige actuellement qu'un acte authentique soit dressé, il suffirait de renoncer simplement à l'exigence d'acte authentique. Par exemple, pour que les transactions immobilières soient, dans le futur, réalisées sur la blockchain, il suffirait simplement de renoncer à exiger l'établissement d'un acte notarié pour pouvoir procéder à la publicité foncière.

Conférer l'authenticité à l'acte intervenu sur une blockchain n'apparaît donc pas, pour l'heure, indispensable. Relevons ici en passant que la question de la « force exécutoire », souvent soulevée à propos de l'exécution automatique des actes conclus sur une blockchain (en cas de *smart contract*), relève d'une autre problématique que celle de l'authenticité et du droit de la preuve (v. la fiche relative aux *smart contracts*).

2.2.3. La preuve d'un fait juridique sur une blockchain

En dehors des transactions réalisées sur la blockchain – qui constituent des actes juridiques – de simples faits juridiques extérieurs à la blockchain peuvent y être enregistrés

♦ Le cas des oracles

Lorsque le fait considéré s'est déroulé à l'extérieur du réseau, par exemple dans le monde physique (livraison d'une marchandise), l'information est entrée dans la blockchain manuellement, le plus souvent à l'aide d'oracles. Ce système d'oracles permet ainsi d'enregistrer dans la blockchain que telle marchandise a été livrée tel jour à telle heure (ce qui repose la question de la portée de l'horodatage évoquée plus haut).

Une fois que l'information est entrée dans la blockchain, il n'est plus possible de la modifier ou la falsifier. Il reste que sa fiabilité est entièrement dépendante de la confiance que l'on peut avoir dans l'oracle. Il existe actuellement plusieurs systèmes d'oracles en cours de perfectionnement. Il apparaît délicat de conférer, pour l'heure, une portée probatoire renforcée aux informations transmises par les oracles dès lors que la technologie employée n'apparaît pas encore mature ni totalement dépourvue de failles de sécurité.

Le juge appréciera donc souverainement la portée probatoire des éléments issus d'une blockchain et versés afin d'établir de tels faits juridiques. En cas de contestation, il désignera probablement un expert et se penchera sur les autres indices dont il dispose.

♦ La blockchain comme registre

L'élément extérieur que l'on cherche à enregistrer dans la blockchain peut ne pas être un événement du monde physique mais un fait d'un autre ordre : création d'une œuvre originale ou obtention d'un diplôme, par exemple. En ce cas la fonction de hashage permet de s'assurer que l'œuvre ou le diplôme considéré n'est pas altéré ou modifié. Ici, la technologie blockchain présente l'avantage considérable de faire en sorte que l'intégrité de ces éléments enregistrés et horodatés est garantie.

Couplée à des outils de stockage, la blockchain peut ainsi servir de registre numérique infalsifiable pour un très grand nombre de documents. L'expérimentation de la blockchain dans le cadre de la dématérialisation des registres d'état civil a ainsi été envisagée par deux amendements déposés dans le cadre des discussions relatives au projet de loi sur l'Etat au service d'une société de confiance (amendements n°385 et n°755 du 19 janvier 2018) actuellement discuté au Parlement. Il est certainement regrettable que ces amendements aient été, pour l'heure, rejetés, même si l'hypothèse d'un recours à la blockchain pour les registres d'état civil n'est pas écartée pour autant.

Il serait, en tout état de cause, souhaitable que le droit français reconnaissse pleinement la fiabilité de la conservation de documents originaux au moyen de la technologie blockchain. Or les documents électroniques correspondant à l'empreinte numérique enregistrée sur la blockchain remplissent, sans aucun doute, les conditions prévues par l'article 1379 du Code civil concernant les copies. L'article 1379 alinéa 2 du Code civil prévoit en effet qu'est « *présumée fiable jusqu'à preuve du contraire toute copie résultant d'une reproduction à l'identique de la forme et du contenu de l'acte, et dont l'intégrité est garantie dans le temps par un procédé conforme à des conditions fixées par décret en Conseil d'État* ». Et la technologie blockchain correspond aux exigences posées par le décret d'application n°2016-1673 du 5 décembre 2016, qui prévoit notamment, dans son article 3, que « *l'intégrité de la copie résultant d'un procédé de reproduction par voie électronique est attestée par une empreinte électronique qui garantit que toute modification ultérieure de la copie à laquelle elle est attachée est détectable* ». Il n'apparaît donc pas que le droit positif doive substantiellement être modifié ici, si ce n'est, peut-être, pour intégrer dans le texte du décret une disposition propre à la blockchain prévoyant expressément que le recours à cette technologie permet, si certaines conditions techniques sont respectées, d'obtenir des copies fiables.

Il reste toutefois, là encore, et malgré la confiance que l'on peut accorder aux techniques cryptographiques mises en œuvre sur la blockchain, à s'assurer que le document numérique dont l'empreinte est enregistrée sur la plateforme correspond bien au document original. Il paraît difficile, à ce stade, d'envisager une autre solution que celle de l'intervention d'un tiers de confiance, sauf dans le cas où c'est l'émetteur du document (l'Etat pour les actes d'état civil, l'école pour les diplômes etc...) qui procède lui-même à son inscription sur une blockchain. Certaines start up proposant l'enregistrement d'œuvres originales sur la blockchain prévoient ainsi l'intervention, en cas de contestation, d'un huissier chargé d'attester que le document écrit ou électronique initial et son empreinte numérique enregistrée sur la blockchain sont identiques.

En tout état de cause, il n'apparaît pas que ce cas d'usage appelle une évolution du droit de la preuve en tant que tel si ce n'est pour rendre opposable l'horodatage réalisée sur la blockchain lors de l'enregistrement de l'empreinte numérique du document.

3. Propositions

Les exigences actuelles en matière probatoire (signature et horodatage *qualifiés*) sont extrêmement contraignantes en ce qu'elles imposent le recours à un tiers certificateur, sans lequel on ne peut présumer la fiabilité de l'identification du signataire ou de l'exactitude de l'horodatage. Une incertitude en résulte, car le juge sera libre d'apprécier ces éléments de preuve comme il le souhaite. Il est vraisemblable qu'il désignera un expert à cette fin, ce qui aura pour effet d'allonger et renchérir le coût des procédures.

Il conviendrait donc certainement de modifier les textes existants à ce sujet afin de faire en sorte que la signature et l'horodatage intervenus sur une blockchain répondant à des spécifications techniques satisfaisantes bénéficient de la présomption de fiabilité.

Sur le fond et dans la longue durée, il apparaît donc souhaitable que les règles eIDAS évoluent afin de tenir compte des spécificités techniques de la technologie blockchain auxquelles les textes existants ne sont actuellement pas adaptés. Il conviendra de déterminer les conditions permettant de reconnaître une plus grande portée probatoire à la signature électronique et à l'horodatage intervenus sur la blockchain. La réflexion devrait être entamée à ce sujet au niveau européen. Et il faudra, à cet égard, déterminer les caractéristiques techniques justifiant d'accorder la présomption de fiabilité, étant précisé qu'il n'apparaît pas souhaitable d'aller au-delà d'une simple présomption réfragable, compte-tenu des difficultés pouvant toujours survenir (vol de clé privée etc...).

Dans cette attente, le droit interne pourrait lui-même évoluer de manière à donner un portée renforcée à la preuve émanant d'un registre distribué présentant des caractéristiques techniques satisfaisantes, sans pour autant imposer un recours redondant et onéreux à un tiers certificateur.

S'agissant de la signature électronique sur la blockchain, qui constitue une signature avancée au sens du Règlement eIDAS, il paraît difficile de présumer sa fiabilité en droit interne sans contredire le Règlement. Il serait néanmoins possible de travailler de concert avec l'ANSSI pour déterminer des modalités techniques d'identification particulièrement fiables et dont le juge pourrait tenir compte. Cette démarche devrait également être menée à propos de l'horodatage.

Par ailleurs, s'agissant des prestataires de confiance agréés actuellement habilités à délivrer certificats et cachets, il serait souhaitable d'entamer une réflexion en collaboration avec l'ANSSI afin d'obtenir des retours d'expérience et d'élaborer des bonnes pratiques.

Enfin, les transactions conclues au moyen de signatures avancées sur la blockchain pourraient se voir conférer une portée probante renforcée en étant, par exemple, qualifiées de commencements de preuve par écrit au sens de l'article 1362 du Code civil.

4. Conclusions : recommandations

Nous recommandons :

- d'engager dès maintenant une réflexion devant aboutir à la révision du règlement eIDAS afin de reconnaître pleinement la fiabilité de la signature électronique et de l'horodatage sur la blockchain sans intervention d'un tiers certificateur ainsi que la fiabilité des algorithmes de signature issus des blockchains, même dans une utilisation isolée ;
- de réfléchir, dans cette perspective, aux modalités techniques devant être retenues afin de pouvoir reconnaître une pleine force juridique à la signature juridique et à l'horodatage réalisés sur une blockchain ou sur une chaîne ou structure de données satellite (dite "sidechain", ou "arbre de Merkle"), dont la force probante découle de la blockchain principale ;
- d'impliquer l'ANSSI de manière à faire apparaître de bonnes pratiques concernant « l'offre blockchain » actuellement développée par les tiers certificateurs agréés ;
- d'adopter dès à présent une réforme visant à renforcer la force probante des informations figurant sur une blockchain selon des modalités techniques à préciser. L'article 1362 du Code civil pourrait, par exemple, se voir ajouter un quatrième alinéa prévoyant que « l'écrit électronique enregistré dans un dispositif d'enregistrement électronique partagé répondant à des caractéristiques prévues par décret en Conseil d'état tient lieu de commencement de preuve par écrit ».

Fiche 4

Fiscalité

Responsable de rédaction : Antoine Gabizon, Avocat Associé, Fieldfisher LLP

1. Contexte : un secteur en croissance sans un cadre adapté

À ce jour, les règles énoncées ciblant spécifiquement la technologie blockchain visent uniquement le bitcoin et portent sur le traitement fiscal des gains et de la TVA.

Il eut été étonnant que le développement exponentiel des activités sur la blockchain, la capacité accrue de procéder à des opérations libellées en monnaie virtuelle, l'attrait des opérations d'ICO, l'émission de ces objets non identifiés juridiquement que sont les "*tokens*" (ou jetons émis sur la blockchain par les opérateurs sur le système) n'apporte pas son lot d'interrogations d'un point de vue fiscal.

C'est d'autant plus crucial pour les Etats que le volume financier des opérations concernées ne cessent lui-même de croître et que s'agissant d'activités qui sont à la fois décentralisées territorialement, digitalisées et qui s'exécutent de manière automatique au travers de "*smart contract*", la déperdition de profits taxables pourrait prendre une ampleur encore plus importante que ce que l'on connaît actuellement avec l'usage d'internet.

Pour les entreprises qui développent cette nouvelle activité, l'incertitude fiscale qui règne sur leurs activités dans la majorité des pays développés est une source d'inquiétude. Cette inquiétude est d'autant plus grande qu'elle se double de la forte volatilité des cryptomonnaies, parfois d'un manque de liquidité, de leur volatilité ainsi que de l'insécurité qui pèse sur les clés informatiques supposées garantir la détention de ces actifs. Cette situation pousse les opérateurs soit à adopter des positions qui pourraient s'avérer excessivement prudentes et de nature à ralentir leur développement, ou, à l'inverse à chercher à délocaliser leurs activités vers des pays dont la réglementation apparaît de nature à sécuriser le traitement fiscal.

Prenant conscience du succès grandissant du bitcoin, l'administration fiscale a donc édicté en juillet 2014 un certain nombre de principes destinés à en définir le régime fiscal.

Cependant, les nouvelles activités qui se sont développées autour de la blockchain ont considérablement évoluées depuis la parution de ces commentaires en 2014.

En effet, ces commentaires ne nous éclairent pas sur les échanges de cybermonnaies ou encore sur l'émission de *tokens* dans le cadre d'une ICO, qui permet de financer des sociétés en utilisant des smart-contracts sur la blockchain.

La sécurisation du traitement fiscal des activités se développant autour de la blockchain est un enjeu considérable pour l'attraction de projets innovants en France s'appuyant sur cette nouvelle technologie.

2. État des lieux : des règles incomplètes, sources d'incertitudes

2.1. Personnes physiques réalisant des gains à titre occasionnel

Les gains provenant de la revente de bitcoins sont, d'après l'administration, taxables dans la catégorie des bénéfices non commerciaux (BNC)⁷⁶.

Ces commentaires excluent l'application de l'article 150 UA du Code général des impôts (CGI) relative au traitement des plus-values sur biens meubles réalisées par un particulier non professionnel. Pourtant, en matière professionnelle, l'administration reconnaît que l'achat revente de bitcoins est assimilable à une activité d'achat-revente de biens meubles incorporels. Son analyse n'est donc pas cohérente avec la qualification qu'elle retient en matière de BIC.

De plus, il n'est pas certain que ces commentaires trouvent à s'appliquer en présence d'autres cybermonnaies que le bitcoin, dès lors que la doctrine administrative est d'interprétation stricte.

Par ailleurs, les commentaires posent également difficulté dans le cas d'échanges entre cybermonnaies (par exemple des échanges de bitcoins contre des ethers). Dans cette situation, une interprétation prudente des commentaires administratifs conduit à la constatation d'un produit taxable, bien que la situation ne soit pas expressément visée.

Cette position nous paraît également critiquable au regard de la notion de revenu disponible. Les risques liés à la sécurité, à la liquidité et à la volatilité des cybermonnaies fragilisent la constatation d'un revenu disponible entre les mains du particulier, au sens de l'article 156 du CGI.

Enfin, la constatation d'un profit taxable évaluée à la date de l'échange peut amener le contribuable à supporter une charge d'impôt sans qu'il ait les fonds pour y faire face et alors même qu'il n'a aucune garantie sur la pérennité de ce gain virtuel.

Cela étant, l'administration fiscale pourrait naturellement objecter que ce constat est propre en réalité à toute opération d'échange de biens qui ne comporte pas, par définition, de flux financiers.

2.2. Personnes, physiques ou morales, exerçant une activité à titre professionnel

Pour les personnes, morales ou physiques, exerçant une activité d'achat-revente de bitcoin à titre professionnel, les commentaires ne fournissent qu'un éclairage partiel sur le traitement de ces opérations et de nombreuses interrogations subsistent⁷⁷.

L'achat-revente de bitcoins à titre habituel est considéré comme une activité commerciale relevant de la catégorie des bénéfices industriels et commerciaux.

Ces précisions ne fournissent que très peu de réponses aux problématiques rencontrées par les entreprises utilisant les cybermonnaies.

En particulier, les commentaires n'envisagent pas clairement les opérations réalisées en cybermonnaie. Il s'agit notamment des acquisitions de biens ou services par un paiement en cybermonnaie mais également des opérations d'échanges (échange de bitcoins contre des ethers par exemple) y compris dans le cadre de ventes de tokens, l'échange (de bitcoins, ethers ou autres) contre des tokens dont on sait qu'ils peuvent avoir des caractéristiques très diverses décidées par son émetteur.

⁷⁶ Doctrine administrative BOI-BNC-CHAMP-10-10-20-40, n° 1080.

⁷⁷ Doctrine administrative BOI-BIC-CHAMP-60-50, n° 730.

En l'absence de précisions, l'application des principes énoncés à l'article 38 du CGI sur le bénéfice imposable conduit en principe à traiter ces opérations comme des échanges de biens.

Cette situation peut se révéler très délicate pour les entreprises qui peuvent alors faire apparaître un bénéfice imposable significatif sans être en mesure de faire face à l'impôt correspondant dès lors que l'impôt s'y rapportant ne peut, par hypothèse, pas être acquitté en cybermonnaie et que la capacité de conversion des actifs concernés en monnaie légale peut ne pas être suffisante à date de paiement du solde de l'impôt et du versement des acomptes d'impôts sur les sociétés.

Une telle solution pose également des problèmes sur le plan comptable, au regard des principes généraux édictés par le Plan Comptable Général (PCG) et notamment le principe comptable de continuité d'exploitation et le principe de bonne information. En effet, les commissaires aux comptes rencontrent des difficultés pour la certification des comptes de sociétés ayant un volume important de cybermonnaies, en raison de leur très forte volatilité et du manque de liquidité de ces biens. Il a pu notamment être considéré que certains tokens en fonction de leurs caractéristiques ne répondent pas à la définition d'un actif dont la valeur est déterminable de façon suffisamment fiable ou d'une créance certaine à faire figurer à l'actif. Dans ces situations, les professionnels comptables (expert-comptable et commissaire aux comptes) envisagent l'enregistrement d'un engagement hors bilan.

Sans même en arriver à de telles extrémités, dans la lignée de la jurisprudence de la Cour de justice de l'Union Européenne et à défaut de règle comptable spécifique, les cybermonnaies pourraient être comptabilisées comme un moyen de paiement et voir alors s'appliquer les règles propres aux avoirs ou créances en monnaie étrangère.

Or, l'article 38, 4 du CGI impose leur évaluation à la clôture de chaque exercice et la constatation des écarts de change pour la détermination du résultat fiscal.

Certes, une éventuelle parade consiste à considérer que ces règles ne peuvent être appliquées dans le cas des cybermonnaies dans la mesure où il ne s'agit pas de monnaie ayant cours légal. Mais cette analyse reste incertaine en l'état de la réglementation.

Une comptabilisation en tant qu' "autres immobilisations financières" (qui suppose un investissement dans la durée) ou en tant que stocks (dans le cas des sociétés qui poursuivent un but spéculatif) est alternative envisageable, mais dans l'attente des recommandations des autorités comptables, elle reste également aléatoire.

Enfin, la très forte volatilité du cours peut conduire l'entreprise à voir disparaître la presque totalité de son patrimoine instantanément et ne plus être en mesure de faire face aux impositions dues, ce qui de facto entraîne des conséquences pour les commissaires aux comptes et notamment une procédure d'alerte du Président du Tribunal de commerce conformément aux dispositions du Code de commerce.

2.3. L'activité de minage

Le minage est défini par l'administration comme l'activité qui consiste à contribuer de la puissance de calcul au réseau afin qu'il fonctionne et soit sécurisé en contrepartie de l'attribution de bitcoins.

L'administration considère que l'attribution de ces bitcoins est faite à titre gratuit et exclut une imposition au moment de l'attribution. Une telle règle n'allait pas de soi. Non seulement car le minage est une activité qui a un coût (matériel informatique et électricité dépendante) mais également parce qu'elle conduit à reporter la taxation au moment de l'utilisation du bitcoin soit par une conversion contre une monnaie ayant cours légal, soit par un échange contre des biens et des services.

Cette solution est salutaire en ce qu'elle ne pénalise pas le mineur en le forçant à vendre une partie de ses gains pour pouvoir payer l'impôt.

On peut souhaiter qu'une telle solution soit étendue aux autres cybermonnaies et, plus généralement aux échanges entre cybermonnaies, en reportant la taxation du profit au moment de l'utilisation des cybermonnaies contre des biens (à l'exclusion d'autres cybermonnaies) ou services ou lors de leur conversion en monnaie *fiat*.

2.4. En matière de droits de mutation à titre gratuit et d'impôt sur la fortune (ISF)

Nous précisons en premier lieu que l'ISF a été supprimé à compter du 1^{er} janvier 2018 par le projet de loi de finances pour 2018 et est remplacé par un impôt qui n'inclut pas dans sa base les bitcoins et autres cybermonnaies.

Cependant, les difficultés soulevées en matière de valorisation appellent à une réponse en matière de mutations à titre gratuit.

L'administration précise que les "*unités de compte virtuelles stockées sur un support électronique*", font partie du patrimoine taxable du contribuable ou du défunt⁷⁸.

Nous noterons que cette fois-ci, la définition est plus large et ne se limite pas au cas spécifique du bitcoin.

La valorisation est un sujet délicat pour les raisons déjà précédemment évoquées : les problèmes de liquidités pour cybermonnaies, leur forte volatilité ou encore les risques en matière de sécurité et de pérennité du patrimoine qu'elles représentent.

Des commentaires de l'administration sur les méthodes de valorisation prenant en compte ces facteurs seraient appréciables.

2.5. En matière de TVA

L'administration n'a, à ce jour, apporté aucune précision sur le traitement des opérations réalisées en cybermonnaies. Sans entrer dans les détails, c'est la Cour de justice de l'Union européenne (CJUE, 22 octobre 2015, aff. C-294/14, Hedqvist) qui a été amené à préciser implicitement que sont exonérés de TVA les opérations d'échange de bitcoins contre des devises ayant cours légal dès lors que les bitcoins sont assimilables à des devises (moyen de paiement) au sens de la directive TVA.

Les opérations d'échange de bitcoins contre des monnaies ayant cours légal sont donc exonérées de TVA en application de l'article 261 C, 1-d du CGI en France.

Les opérations concernant les cybermonnaies présentant les mêmes caractéristiques (ethers notamment) devraient donc suivre le même raisonnement et relever de l'exonération prévue en France à l'article 261 C, 1-d du CGI. La poursuite du raisonnement nous amène donc à exonérer de TVA les opérations d'échanges réalisées entre certaines cybermonnaies ayant ces caractéristiques (par exemple, vente de bitcoins contre des ethers).

Pour autant, l'incertitude demeure pour les autres tokens dont on sait qu'ils peuvent recouvrir des réalités très différentes.

⁷⁸ Doctrine administrative BOI-ENR-DMTG-10-10-20-10, n°10 et BOI-PAT-ISF-30-20-10, n°80

3. Recommandations

Pour clarifier le régime fiscal des gains en cybermonnaies et autres tokens, le groupe de travail formule les propositions suivantes.

3.1. Pour les particuliers réalisant des gains à titre occasionnel

S'agissant de la taxation des revenus, plusieurs solutions peuvent être envisagées :

- Une première solution, qui a le mérite de ne pas nécessiter l'intervention du législateur, serait de reconnaître que les gains en cybermonnaie correspondent à des plus-values sur biens meubles soumises au régime de l'article 150 UA du CGI.

L'application de ce régime permettrait notamment aux particuliers d'être exonérés lorsque leur prix de cession ne dépasse pas 5 000 € et d'être imposé sur une base forfaitaire dans les autres cas (au taux de 19 % auquel il convient d'ajouter les contributions sociales).⁷⁹

Nous devons constater qu'un tel régime semble plus adapté aux gains de cybermonnaies réalisés à titre occasionnel que le régime de déclaration d'un revenu d'activité en BNC préconisé par l'administration pour les gains tirés de la vente de bitcoins.

En effet, on comprend mal ce qui permet automatiquement d'exclure ces gains du régime des gains en capital. L'application du régime des bénéfices non commerciaux conduit à une taxation lourde des contribuables ayant réalisé des plus-values en revendant leurs cybermonnaies, comme s'il s'agissait de revenus d'activité et non d'un gain en capital. Alors que le gouvernement allège considérablement la fiscalité du capital, un tel régime pour les plus-values sur la cybermonnaie apparaît excessivement sévère.

Il faudrait alors selon nous rapporter la doctrine administrative relative au traitement des bitcoins dans la catégorie des bénéfices non commerciaux. Cela conduirait à l'application d'un taux forfaitaire de 19 %, auxquels s'ajouteraient les prélèvements sociaux au taux de 17,2 % (à compter du 1er janvier 2018).⁸⁰

- Une autre solution serait d'inclure ces gains dans le champ du prélèvement forfaitaire unique de 30% prévue par la loi de finances pour 2018.

Cette solution nous semble particulièrement justifiée dans la mesure où, dans la plupart des cas, les tokens sont émis par l'intermédiaire d'une ICO en vue de financer l'activité de jeunes sociétés et peuvent donc s'apparenter à un investissement contribuant au développement d'un secteur économique porteur, bien qu'ils n'aient pas les mêmes contreparties ni ne confèrent les mêmes droits qu'une part dans une société. L'un des objectifs affichés du gouvernement étant de favoriser l'investissement par des mesures incitatives et par la simplification des régimes fiscaux, l'extension du champ du prélèvement forfaitaire unique aux gains de cybermonnaies pourrait tout à fait s'inscrire dans ce cadre.

Ceci nécessitera d'assimiler les gains sur actifs numériques à des plus-values sur cession de biens meubles incorporels tels que définis à l'article 150-0-A du CGI.

⁷⁹ Cette proposition a été initialement rédigée à l'attention de France Stratégie en fin d'année 2017

⁸⁰ C'est cette solution qui a été retenue par le conseil d'Etat en date du 26 avril 2018 : <http://www.conseil-etat.fr/Actualites/Communiques/Modalites-d-imposition-des-bitcoins>

A l'appui de ces propositions, il n'est pas inutile de souligner qu'elles sont globalement cohérentes avec les niveaux d'imposition constatés dans d'autres pays. Ainsi, sous réserve des incertitudes qui peuvent apparaître à raison de cadres législatifs relativement imprécis, on constate les pratiques suivantes (dans le cas des revenus considérés comme non spéculatifs uniquement) :

Etats	Taux d'imposition
Allemagne	Imposition au titre des plus-values privées au taux de 25%
Etats-Unis	Régime des plus-values à long terme : application d'un taux marginal de 20 %
Israël	Imposition au titre des plus-values privées au taux forfaitaire de 25%
Italie	Pas d'imposition en l'état de la réglementation
Royaume-Uni	Imposition pour un investisseur au taux forfaitaire de 28%

S'agissant des échanges entre cybermonnaies (par exemple bitcoins contre des ethers ou d'autres tokens), des précisions de l'administration seraient les bienvenues afin de confirmer l'analyse selon laquelle les gains latents de cybermonnaie ne constituent pas un revenu disponible du contribuable, au sens de l'article 156 du CGI. L'imposition serait alors reportée et n'interviendrait qu'au fur et à mesure de l'utilisation des cybermonnaies pour l'acquisition de biens (autres que des cybermonnaies) ou de services.

3.2. Pour les opérations commerciales en cybermonnaies

En ce domaine, une première solution serait de savoir si, dans l'attente de pouvoir disposer de principes précis en ce domaine, il serait fiscalement acceptable de considérer que les opérations d'échanges entre cybermonnaies puissent être comptabilisées en engagement hors bilan. Les actifs numériques ne seraient donc imposables qu'au fur et à mesure de leur utilisation contre des achats de biens ou de services de toute nature, ou bien encore de leur conversion en monnaie légale, à l'exception toutefois des conversions vers d'autres cybermonnaies. Cette solution de court terme n'est cependant pas adaptée à une appréhension complète et cohérente des actifs numériques par la fiscalité. Ceci d'autant plus que les arguments qui militent pour cette solution d'un point de vue comptable ne sont pas à l'abri de toute critique.

Une autre solution serait de préciser le champ d'application des commentaires de la doctrine administrative applicable en matière de bénéfices industriels et commerciaux et de bénéfices non commerciaux qui devrait conduire à reporter la taxation du produit des opérations réalisées en bitcoin (ou tout autre unité de valeur comparable) au moment de leur utilisation pour l'achat de biens ou de services ou encore leur conversion en monnaie légale. Dans ce cas la valeur inscrite en comptabilité serait neutralisée extra-comptablement. Cette solution trouverait notamment à s'appliquer aux opérations d'échanges de cybermonnaies en matière d'ICO (échange de tokens émis par la société contre des bitcoins et autres cybermonnaies) en reportant la taxation des cybermonnaies reçus en échange des tokens au moment de leur conversion en monnaie légale ou de leur utilisation pour l'achat de biens ou de services.

Alternativement, une solution plus sécurisante que la précédente car inscrite dans la loi mais aboutissant in fine à un résultat comparable, serait d'étendre le mécanisme de report

d'imposition prévu à l'article 38-6 du CGI relatif à certains dérivés de crédit, qui permet de reporter l'imposition du profit constaté sur une position au dénouement de l'opération, le cas échéant en prévoyant une période maximale dans le temps. Le débouclage interviendrait à nouveau au moment de l'achat de biens ou de services ou encore de la conversion de la cybermonnaie en monnaie légale.

Il n'est toutefois pas certain que l'administration fiscale accepte d'adhérer à ces solutions dans la mesure où elles pourraient être perçues comme emportant un traitement fiscal plus favorable que celui tenant d'une simple clarification. Elles ne pourraient s'envisager qu'à la condition que le pouvoir législatif et l'administration fiscale acceptent de considérer que le développement de ces nouvelles activités mérite d'être soutenu sur le plan fiscal.

Une autre solution, peut-être plus réaliste et compatible avec les objectifs et les contraintes budgétaires de l'administration, serait de considérer que les opérations réalisées en cybermonnaies sont imposables sur la base de leur contre-valeur au jour de réalisation des opérations ou de leur inscription au bilan mais de confirmer que les avoirs détenus ensuite en cybermonnaies échappent à la règle de taxation des écarts d'évaluation prévue à l'article 38,4 du CGI, s'agissant de moyens de paiement qui n'ont pas de cours légal au sens de ces dispositions.

3.3. En matière de TVA

En matière de TVA, deux options semblent pouvoir être envisagées.

- Une première solution consisterait à confirmer et étendre le principe d'exonération des échanges de cybermonnaies contre des euros à toutes les opérations d'achat, vente ou échange d'actifs numériques. L'administration confirmerait alors l'application de la solution retenue par la CJUE assimilant les bitcoins à un moyen de paiement à tous les échanges entre cybermonnaies et l'appliquerai aux émissions et aux échanges de tokens en cybermonnaies, ainsi qu'aux échanges de tokens entre eux. Cette solution trouverait notamment à s'appliquer en matière d'ICO.

Mais comme on l'a indiqué, cette solution présente une incertitude en tant que les tokens présentent recourent des qualifications et des situations juridiques multiples, de sorte que leur assimilation à des moyens de paiement purs et simples n'est pas systématique.

- Une seconde approche, plus complexe, serait de transposer aux émissions de tokens les principes énoncés par l'administration fiscale pour les émetteurs de bons cadeaux ou la commercialisation de monnaie numérique.

Dans ces deux hypothèses, l'administration fiscale indique que la simple émission de ces bons ou des supports de paiement (cartes, tickets, bons prépayés, etc.) permettant l'achat de produits ou de services n'est pas soumise à la TVA. C'est l'utilisation des bons qui déclenche la taxation dans la mesure où au moment de l'émission, la nature exacte des prestations ou des biens que le bénéficiaire choisira ultérieurement d'obtenir contre la remise de ceux-ci n'est pas connue, tout comme ne sont pas déterminés la date de réalisation de ces prestations ou livraisons de biens et les fournisseurs chargés d'en assurer l'exécution (cf. rescrit du 18 septembre 2007, n° 2007/31 TCA ; BOI-TVA-CHAMP-10-10-10, n° 80 et suivants, et lettre DLF du 20 mai 2009).

Dans la perspective de la directive européenne visant à harmoniser les règles concernant le régime de TVA applicable aux bons afin de garantir un régime fiscal uniforme dans l'ensemble des États membres qui doit entrer en vigueur à compter du

1er janvier 2019 (directive 2016/1065/UE), cette solution conduirait à placer par anticipation les tokens dans le régime de taxation des bons à usages multiples qui se définissent comme des bons dont on ne connaît pas l'usage précis au moment de leur émission. Selon la directive, l'imposition de ces bons à la TVA n'est prévue qu'au moment de la remise matérielle au fournisseur ou au prestataire du bien ou des services qu'ils servent à acquérir.

Ce raisonnement devrait s'appliquer à certains tokens qui permettent l'achat de biens ou de services, sans que l'on connaisse précisément leur sort définitif au moment de l'émission.

En tout état de cause, les opérations au cours desquelles ces actifs numériques (cybermonnaies ou tokens) seraient utilisés en paiement de prestations ou d'achats de biens seraient naturellement soumises à TVA dans les conditions de droit commun.

Fiche 5

Enjeux de conformité et droit au compte

Responsable de rédaction : Arnaud Grünthaler, Avocat Associé, Fieldfisher LLP

1. Contexte : une véritable problématique d'accès à un compte bancaire

Les établissements de crédit en France sont soumis à une obligation de lutte contre le blanchiment et le financement du terrorisme ("KYC-AML"), qui se traduit, notamment par l'obligation d'identification de leur client ainsi que de l'origine des fonds d'un client, en particulier lors de la réalisation d'une transaction sur un compte bancaire.

Aux termes de l'article L.561-2 du Code monétaire et financier (issu de l'article 2 de l'Ordonnance n°2016-1635 du 1^{er} décembre 2016), "*toute personne qui, à titre de profession habituelle, soit se porte elle-même contrepartie, soit agit en tant qu'intermédiaire, en vue de l'acquisition ou de la vente de tout instrument contenant sous forme numérique des unités de valeur non-monétaire pouvant être conservées ou être transférées dans le but d'acquérir un bien ou un service, mais ne représentant pas de créance sur l'émetteur*".

Il est donc considéré que les émetteurs de *tokens* et les professionnels achetant et revendant des cybermonnaies sont soumis à une obligation de lutte contre le blanchiment et le financement du terrorisme et doivent, de ce fait, identifier les acheteurs des tokens ou cybermonnaies ainsi que l'origine des fonds utilisés.

Cependant, en pratique, nous constatons que les émetteurs de tokens ou les vendeurs professionnels de cybermonnaies ont la plus grande difficulté à ouvrir et maintenir ouvert un compte bancaire classique auprès d'un établissement de crédit en France dans le cadre de leur activité. Ces difficultés apparaissent dès la constitution des sociétés émettrices lorsque les projets de statuts adressés à la banque mentionnent un objet lié à une activité faisant référence à la cybermonnaie. Cette problématique s'entend également à l'ensemble des entreprises gérant des cybermonnaies ou tokens dans le cadre de leur activité générale, soit parce qu'elles l'acceptent comme moyen de paiement, soit parce que ces actifs numériques sont intégrés à leur offre de produit.

Pour bon nombre d'entre-elles, les établissements bancaires auxquels elles s'adressent refusent les ouvertures de compte, arguant que ces activités sont dangereuses. Dans certains cas, les établissements acceptent des fonds mais les bloquent instantanément au motif que ces sociétés ne sont pas en mesure de respecter leurs obligations en matière de KYC-AML en l'absence d'identification précise de leur origine.

Cette problématique naît principalement du fait que les matrices de risques et autres procédures internes appliquées par les établissements bancaires dans le cadre de leurs propres obligations de lutte contre le blanchiment et le financement du terrorisme n'intègrent pas les cybermonnaies à leur cadre d'analyse. En pratique, la méconnaissance des cybermonnaies et autres actifs numériques par les certains de ces départements conduit les établissements bancaires à refuser automatiquement de gérer les comptes des entreprises ayant des cybermonnaies à leur patrimoine, ayant organisé une opération de vente de token (ICO) ou plus simplement les utilisant dans le cadre de leur activité.

Or, l'une des raisons pour laquelle les banques sont parfois conduites à clôturer des comptes bancaires tient au caractère largement insuffisant des données que les plateformes d'échange fournissent aujourd'hui à leurs clients. Il est en pratique très difficile d'obtenir de ces plateformes des documents unifiés permettant de justifier d'opérations d'achat ou de vente précises. En l'absence de ces documents, les banques sont conduites à considérer que l'origine des fonds n'a pas pu être démontrée.

Les émetteurs de *tokens* ainsi que les acheteurs-revendeurs de cybermonnaies doivent alors trouver des alternatives en tentant d'ouvrir des comptes bancaires auprès de prestataires étrangers (banques ou prestataire de services de paiement) ou en immatriculant les sociétés faisant référence à un objet social générique sans préciser l'utilisation de cybermonnaies. Ces solutions temporaires ne règlent pas d'avantage le problème de fond, et dans le second cas un blocage ultérieur des fonds est commun lors du fonctionnement effectif du compte.

Un tel blocage est préjudiciable au développement du marché français et à l'attractivité de la place de Paris pour toute activité liée au commerce ou à l'utilisation de cybermonnaies ou de *tokens* dans la mesure où les alternatives envisagées sont systématiquement recherchées en dehors de France.

2. Recommandations

- Une obligation d'information devrait être imposée aux entreprises gérant des plateformes d'échange, qui auraient à fournir un état des achats/vente permettant aux particuliers de justifier de l'origine des fonds utilisés dans le cadre de transactions sur cybermonnaies. Dans le cas de vente de tokens, ce reporting permettrait également aux émetteurs de satisfaire leur propre obligation de KYC-AML et de satisfaire le KYC des banques en fournissant cette information communiquée par les exchanges aux souscripteurs de tokens.

Dès lors, une information des banques pourrait lever des ambiguïtés et la prise en compte effective des mesures développées par les émetteurs de tokens et vendeurs de cybermonnaies.

Les émetteurs de tokens pourraient également avoir recours à l'utilisation des services de prestataires spécialisés qui permettent une identification des souscripteurs dans le cadre d'une vente de ces tokens et qui réalisent les diligences techniques d'un KYC-AML. L'utilisation de tels prestataires de services pourrait conforter les banques dans la réalisation par les émetteurs d'un KYC-AML et de fait permettre aux banques de satisfaire leurs propres obligations en la matière lors du transfert de fonds des exchanges vers les comptes bancaires classiques des émetteurs.

Rédacteurs

Rédacteurs principaux			
Nom	Fonction	Société	Site internet
Simon Polrot	Directeur exécutif	VariabL	www.variabl.io
Helène Lefebvre	Avocat associé	Fieldfisher LLP	http://www.fieldfisher.com/
Anne-Hélène Le Trocquer	Avocat associé	De Gaulle Fleurance & Associés	http://www.degaullefleurance.com/
Xavier Lavayssière	Directeur	ECAN, Smart Contract Academy	https://ecan.fr
Florence G'sell	Professeur de droit	Université de Lorraine	
Antoine Gabizon	Avocat associé	Fieldfisher LLP	http://www.fieldfisher.com/
Arnaud Grunthalter	Avocat associé	Fieldfisher LLP	http://www.fieldfisher.com/
Contributeurs signataires			
Nom	Fonction	Société	Site internet
Alain Roset	R&D	La Poste	https://legroupe.laposte.fr/
Alexandre Stachtchenko	Cofondateur	Blockchain Partner	www.blockchainpartner.fr
Claire Leveneur	Doctorante - "Blockchain et droit privé"	Université Paris 2 Panthéon-Assas	
Clément Lesaege	Directeur de la technologie	Kleros	https://kleros.io
Fabrice Heuvrard	Commissaire aux comptes et expert-comptable	Cabinet Fabrice Heuvrard	
Georgie Courtois	Avocat associé	De Gaulle Fleurance & Associés	http://www.degaullefleurance.com/
Hubert de Vauplane	Avocat associé	Kramer Levin LLP	https://www.kramerlevin.com/en/
Jean-Michel PAILHON	Vice-Président	Ledger	https://www.ledger.fr/
Laurent Henocque	Président	KeeeX	https://keex.me
Luc Grynbaum	Avocat - Professeur	De Gaulle Fleurance & Associés	http://www.degaullefleurance.com/
Michelle Abraham	Avocat associé - Chargée de cours	Cabinet Michelle Abraham	www.cabinetmichelleabraham.fr
Primavera De Filippi	Chercheuse	CERSA/CNRS	
William O'Rorke	Juriste	Blockchain Partner	www.blockchainpartner.fr
Abdoulaye Doucoure	Data analyst	Ethercourt M. L.	www.ethercourt.ml