Bureau de dépôt : Louvain 1
Hebdomadaire, sauf juillet et août
ISSN 0021-812X
P301031

larcier

Journal des tribunaux

http://jt.larcier.be
10 novembre 2018 - 137e année
36 - No **6748**
Georges-Albert Dal, rédacteur en chef

Doctrine

Blockchain : une révolution pour le droit[1] ?

La blockchain tient la une de nos journaux. Cette technologie récente hait la centralisation des flux et des données et repose sur une décentralisation complète entre pairs tout en assurant la sécurité et la traçabilité des opérations. Elle déborde désormais largement ses applications en matière monétaire : le bitcoin et autres « crypto-monnaies ». Les administrations, les auteurs, les notaires peuvent l'utiliser ; elle peut servir aux transactions portant sur les œuvres d'art, les certificats immobiliers, les assurances, ... Constitue-t-elle une révolution pour le droit ? En tout cas, elle l'interroge ou plutôt en interroge diverses branches : le droit de la propriété intellectuelle, le droit financier, le droit de la protection des données ou encore le droit des contrats qu'entend remettre en cause le « smart contract », souvent associé au fonctionnement des blockchains. Au terme de l'analyse, la réponse est nuancée : si questionnement réel il y a, la révolution du droit par la blockchain n'est pas pour demain !

1. La blockchain : une histoire courte mais un phénomène en pleine expansion. — Né en 2009, sous la plume d'un pseudonyme, S. Nakamoto[2], le système bitcoin a depuis fait florès à la une des journaux et, aujourd'hui, s'est vu rejoindre par bien d'autres « crypto-monnaies ».

Ce phénomène s'appuie sur une technologie dite de la « blockchain », qui connaît bien d'autres applications que celles qui affectent le monde financier, mais qui sont tout aussi révolutionnaires. Il s'agit, dans le secteur de la distribution, de la création, de l'énergie, des sociétés, des professions réglementées (avocats, notaires, etc.), de nos administrations publiques, de l'assurance, de développer grâce aux seules vertus du réseau de l'internet, un système auto-suffisant de certification et d'authentification sans recourir à la force de l'État et des intermédiaires que ce dernier a institués — ou qui se sont développés sous son contrôle — et de créer ainsi la confiance.

2. Une révolution pour nos acteurs socio-économiques... et pour le Droit ? — Joël de Rosnay[3] écrit : « pour la première fois dans l'histoire des révolutions technologiques, l'une d'entre elles, au-delà de la révolution internet, a la capacité d'agir sur le pouvoir vertical et centralisé exercé par les États sur la monnaie, sur celui des banques, des transactions financières, des notaires et les cessions immobilières, des monopoles énergétiques, sur la distribution d'électricité ou de carburants. Il semblait impossible d'imaginer de tels bouleversements avant le développement de la Blockchain »[4].

Bouleversements donc mais, au-delà de ceux-ci, faut-il y voir la consécration de la fameuse maxime de Lawrence Lessig[5] — *Code is Law* — ou comme le proclame l'auteur français, S. de

(1) Les auteurs tiennent à remercier le professeur J.N. Colin (Faculté d'informatique de l'UNamur) et M. M.A. Lemaire (consultant auprès de la Commission européenne), pour leurs explications techniques et l'intérêt de leurs réflexions. La présente contribution est arrêtée au 1er août 2018.

(2) « Satoshi Nakamoto est le pseudonyme du fondateur inconnu du bitcoin et de la première blockchain », nous dit Wikipedia, https://fr.wikipedia.org/wiki/Satoshi_Nakamoto. Nakamoto partagea ses idées sur la *Cryptography Mailing List* en 2008 : « Bitcoin P2P e-cash paper », disponible à l'adresse : http://satoshi.nakamotoinstitute.org/emails/cryptography/1/. Il semble que les premiers principes à la base de la technologie de la blockchain aient été avancés par l'équipe du professeur belge, J.-J. Quisquater (U.C.L.ouvain).

(3) J. De Rosnay, « Préface », *in La blockchain décryptée*, Paris, éd. Blockchain France, 2016, publiée sur le site : https://blockchainfrance.net/decouvrir-la-blockchain/la-blockchain-decryptee-les-clefs-dune-revolution/.

(4) Même reflexion *in The Economist* qui, le 31 octobre 2016, titrait en une : « The trust machine : How the technology behind bitcoin could change the world ? », avec l'article de J. Berkeley, « The trust machine : The technology behind bitcoin could transform how the economy works ? », disponible sur : https://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economyworks-trust-machine.

(5) L. Lessig, « Code is Law - On Liberty in Cyberspace », *Harvard Magazine*, 2000, disponible sur https://har-

Charentenay, d'un nouveau droit, débarrassé de son auteur classique, l'État[6] ? Nous ne le pensons pas.

3. Plan de l'exposé. — Notre propos est donc, dans un premier temps, de décrire cette technologie de la blockchain et son fonctionnement, d'en dresser les éléments caractéristiques et de présenter certaines de ses applications (I).

Ensuite, nous envisagerons plusieurs questions juridiques soulevées par cette technologie (II). Elles sont nombreuses et touchent au droit des obligations, à la protection des données, à la propriété intellectuelle, au droit financier, au droit pénal et de la procédure pénale, au droit administratif, au droit des sociétés, au droit de la concurrence, etc. Dans la présente contribution, on peut difficilement les aborder de manière exhaustive. Aussi nous limitons-nous à certaines d'entre elles, d'une part, celles que la blockchain soulève de manière transversale, quelles que soient les mises en œuvre concrètes (II.A) et, d'autre part, celles qui sont spécifiques aux applications les plus répandues, à savoir les crypto-monnaies et les *smart contracts* (II.B).

C'est à partir de telles considérations que nous pourrons en conclusion juger de l'ampleur du tsunami que constitue — ou pas — la « Blockchain Law », au regard de ce que nous pensons être le Droit, et d'étudier quelques pistes de régulation de ce phénomène, ou plutôt de ces phénomènes, issus d'une technologie au principe unique mais aux applications diversifiées.

1 La blockchain : définition, fonctionnement et applications

A. Éléments caractéristiques et mode de fonctionnement

4. Définition et fonctions principales de la blockchain. — Suivant la définition donnée par Wikipedia, la blockchain constitue « une base de données distribuée qui gère une liste d'enregistrements protégés contre la falsification ou la modification par les nœuds de stockage. À proprement parler, une blockchain est un historique décentralisé des transactions effectuées depuis le démarrage du système réparti »[7]. On peut également mentionner la définition proposée par Blockchain France, qui vise « une technologie de stockage et de transmission d'informations, transparente, sécurisée et fonctionnant sans organe central de contrôle »[8][9].

Les utilisateurs ne recourront à la blockchain que s'ils ont suffisamment confiance en la technologie, dans sa fonction de registre infalsifiable, pour y constater des transferts de crypto-monnaies ou y inscrire les instructions auto-exécutables d'un *smart contract* (sur cette question de confiance, *infra*, n° 5). Cette confiance ne résulte pas de l'intervention d'un organe de contrôle, d'un intermédiaire ou d'un tiers de confiance. Dans le cas de la blockchain, elle s'appuiera uniquement sur la technologie, qui préserve l'intégrité des données[10] inscrites chronologiquement dans le registre décentralisé, tout en assurant la transparence des opérations.

Plusieurs éléments caractéristiques de la blockchain lui permettent d'atteindre ces fonctions et objectifs.

On en dénombre trois principaux : (i) un registre distribué *peer-to-peer* (*infra*, n° 6), qui s'appuie (ii) sur la cryptographie asymétrique et (iii) sur un processus de validation (*infra*, n° 7)[11].

5. Les blockchains : de l'absence d'autorité centrale à la question de la confiance. — Qu'il s'agisse de réseaux distribués au sens large ou de blockchains au sens strict, le point important est l'absence d'autorité centrale.

Sans doute est-ce l'élément le plus caractéristique.

Dans un réseau commun à divers utilisateurs, la confiance est créée de manière traditionnelle par une autorité centrale. Celle-ci a normalement vérifié l'identité des utilisateurs du réseau et c'est elle qui enregistre leurs échanges ; en cas de contestation entre les participants du réseau, il lui incombera de contribuer, le cas échéant, à résoudre le litige[12]. Cette fonction est normalement exercée par des professionnels spécialisés, qui interviennent comme intermédiaires (on songe aux institutions bancaires[13] ou aux plateformes de l'économie collaborative, par exemple) ou en tant que tiers (dits) de confiance, à l'instar des notaires ou, dans le monde électronique, des prestataires de services de confiance[14]. Ce besoin de confiance explique que, même dans des réseaux dits *peer-to-peer*, des registres centraux ont été créés et confiés à un prestataire du service unique et clairement identifié[15].

Comment dès lors créer la confiance lorsqu'aucune autorité centrale n'existe ? Comment s'assurer que toute évolution du registre distribué soit fiable et sécurisée tout en restant transparente pour tous les membres du réseau[16] ?

vardmagazine.com/2000/01/code-is-law-html.
(6) S. DE CHARENTENAY, « Blockchain et Droit : Code is deeply Law », 2017, disponible sur https://blockchainfrance.net/2017/09/19/blockchain-et-droit/ : « mais au-delà des questions techniques et juridiques, si l'on prend le temps d'observer la blockchain dans sa génétique, elle se révèle être un système d'échange de valeurs objectivables, sans l'État. Sous cet angle, la blockchain offre une perspective politique prometteuse selon laquelle elle peut devenir une matrice juridique autonome et alternative aux États ». De manière prudente, lire aussi K. KÜNNAPAS, « From Bitcoin to Smart contracts : Legal Revolution or Evolution from the Perspective of *de lege ferenda* ? », *in* T. KERIKMÄE et A. RULL (dir.), *The future law and e-Technologies*, Berlin, Springer, 2016, pp. 111-132.
(7) https://fr.wikipedia.org/wiki/Blockchain.
(8) https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/.
(9) Il est intéressant de noter que le législateur français a indirectement caractérisé la notion, pour autoriser son utilisation dans le domaine des « minibons » : aux termes de l'article L. 223-12 du Code monétaire et financier, « l'émission et la cession de minibons peuvent également être inscrites dans un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations, dans des conditions, notamment de sécurité, définies par décret en Conseil d'État » (voy. aussi l'article L. 211-3 du CMF pour les titres non cotés).
(10) M. MEKKI, « Le contrat, objet des *smart contracts* (partie 1) », *Dalloz IP/IT*, 2018, pp. 409 et s. (les données sont d'après lui « immuables, inaltérables et infalsifiables »).
(11) Sur les éléments caractéristiques de la blockchain, voy. J. GOSSA, « Les blockchains et *smart contracts* pour les juristes », *Dalloz IT/IT*, 2018, pp. 393 et s. ; M. MEKKI, « Le contrat, objet des *smart contracts* (partie 1) », *Dalloz IP/IT*, 2018, pp. 409 et s. ; M. RASKIN, « The Law and Legality of Smart Contracts », *Geo. L. Tech. Rev.*, 2017, pp. 318 et s. ; M. CANOVA, « Blockchain et Propriété intellectuelle - Une alliance révolutionnaire », février 2018, disponible sur https://lex4.com/blockchain-et-propriete-intellectuelle-une-alliance-revolutionnaire ; A. TORDEURS, « Une approche pédagogique de la blockchain », *Revue internationale des services financiers*, 2017/4, pp. 6 et s. ; T.E. TJONG TJIN TAI, « Juridische aspekten van blockchain en smart contracts », *T.P.R.*, 2017, pp. 566 et s. ; D. DE JONGHE et V.I. LAAN, « Blockchain in de realiteit », *Computerrecht*, 2017/251, pp. 347 et s. ; J. LINNEMANN, « Juridische aspecten van (toepassing van) blockchain », *Computerrecht*, 2016/218, pp. 319 et s. ; Blockchain France, *La Blockchain décryptée*, *op. cit.*, pp. 1 et s. ; A. WRIGHT et P. DE FILIPPI, « Decentralized Blockchain Technology and the rise of Lex Cryptographia », Working paper, 2015, pp. 4 et s., disponible sur http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664.
(12) Sur la question de la confiance dans un réseau sans autorité centrale, point fondamental pour comprendre la technologie « blockchain », lire l'excellent article de A. WRIGHT et P. DE FILIPPI, « Decentralized Blockchain Technology and the rise of Lex Cryptographia », Working paper, 2015, pp. 11-12, disponible sur http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664.
(13) Ainsi, la banque reçoit les demandes de paiement ou de virement, vérifie l'état des comptes, opère les transactions, dénonce les insuffisances d'avoir et contrôle l'ensemble des transactions opérées par son truchement (sur ce point, lire la comparaison entre le système bitcoin et le système bancaire traditionnel, par T.E. TJONG TJIN TAI, « Juridische aspekten van blockchain en smart contracts », *T.P.R.*, 2017, pp. 566 et s.).
(14) Pour les services de signatures, de cachets, d'horodatage ou de recommandés électroniques visés par le règlement européen sur l'identification électronique et les services de confiance (règlement eIDAS — voy. les références reprises *infra*, n° 37).
(15) Ainsi pour ne reprendre qu'un exemple historiquement célèbre, le réseau NAPSTER où NAPSTER jouait le rôle de gardien du registre des transactions opérées par les membres du réseau de partage de musiques ou d'images électroniques.
(16) Sur cette question de la confiance, lire le rapport du STOA (Science and Technology Option Assessment - Scientific Foresight Unit - European Parliament), « How Blockchain technology can change our lives », Rapport de février 2017, PE 581.948 ; Rapport du Groupe FinTech, Paris EUROPLACE, *Les impacts des réseaux distribués et de la technologie blockchain dans les activités de marché*, Paris, 23 octobre 2017, p. 12, disponible sur le site : www.paris-europlace.com/fr/file/2867/download?token=h3_Q1t6V. Comme le note Michèle Fink (*Blockchain Regulation*, Max Planck Institute for Innovation and Competition Research Paper, n° 17-13, p. 4) : « Trustless trust makes it possible to trust the outputs of a system without trusting any actor within it. The set-up of the blockchain allows actors to

Les principales composantes de la blockchain, que nous examinons dans les numéros qui suivent, permettent de comprendre que ses utilisateurs acceptent de placer leur confiance dans la technologie, plutôt que dans un intermédiaire.

Le principe posé, encore faut-il le nuancer directement : si la désintermédiation est effectivement à l'œuvre dans les blockchains publiques, elle est moins flagrante dans les blockchains privées ou de consortium, où les règles sont fixées par un prestataire déterminé (ou un groupe de prestataires). On constate également que les *smart contracts* peuvent requérir l'intervention d'un tiers (appelé « Oracle »), pour constater électroniquement certains événements susceptibles de déclencher l'exécution du contrat. Nous y reviendrons (*infra*, n° 43).

6. La blockchain repose sur un registre distribué. — La blockchain doit permettre à tous les utilisateurs d'un réseau électronique dédicacé, qu'il soit public ou privé, de pouvoir enregistrer et gérer des données, souvent de nature transactionnelles, dans un vaste registre qui opère comme un « grand livre comptable ». Ce registre (ou cette base de données) est qualifié de « distribué » (*distributed ledger*, en abrégé *DL*), « en cela que tout participant actif (ou nœud) du réseau dispose de sa propre copie et peut le consulter et éventuellement le modifier en résolvant un problème cryptographique. Aucun organe central de contrôle n'est ainsi requis »[17].

Ainsi, le registre repose sur un réseau de type *peer-to-peer* (pair à pair), organisé autour d'une base de données distribuée, c'est-à-dire reproduite ou reproductible en temps réel (ou presque) en chaque point du réseau. Le caractère « distribué » des données constitue un élément important de la sécurité de la blockchain (par rapport à une base de données centralisée) : pour falsifier les informations, il faudra en effet modifier celles-ci sur tous les nœuds du réseau où la base de données est répliquée, ce qui exige de mobiliser des efforts considérables, voire inimaginables.

Les réseaux utilisant la *Distributed Ledger Technology* (en abrégé, la *DLT*) peuvent recourir à la technologie blockchain, ou pas. S'ils le font, le registre ne se structure pas document par document, mais comme une suite chronologique de « blocs » où figurent les données constatant les opérations (par exemple, « Alice verse 1 BTC (Bitcoin) à Bob »). Ces blocs sont liés entre eux et ils s'ajoutent les uns aux autres de façon chronologique (moyennant un horodatage des opérations), pour former une « chaîne de blocs » (la blockchain), dont la sécurité et l'intégrité sont également assurées grâce à la cryptographie asymétrique et au processus de validation (*infra*, n° 7).

7. Créer la confiance dans une blockchain : l'apport essentiel de la cryptographie, associée à des règles de consensus et à des processus de validation. — La confiance en la blockchain vient également de la robustesse de deux procédures conjointes utilisant des algorithmes de cryptage.

La première émane de l'émetteur du message. Elle repose sur l'utilisation par ce dernier d'un système de cryptographie asymétrique (ou à double clé : une clé publique, connue de tous, et une clé privée, connue uniquement de son titulaire). Le message — ou, plus précisément, un condensé (*hash*) de celui-ci — est crypté avec la clé publique du destinataire et la clé privée de l'émetteur dont ce dernier doit assurer la confidentialité. Cette utilisation de la cryptographie asymétrique garantit l'origine et l'intégrité du message (le fait que c'est bien tel émetteur qui en est l'auteur et que ce message n'a pas pu être modifié). La transaction pourra être ainsi décodée par le récepteur du message[18].

La seconde procédure est plus originale. Les diverses transactions sont en effet validées par des acteurs du réseau : les « mineurs »[19]. Ceux-ci vérifient l'identité des émetteurs et la capacité de ces derniers à émettre la transaction. En matière financière, par exemple, il s'agira de vérifier que l'émetteur dispose du nombre de bitcoins suffisant pour honorer la transaction ; en matière de certificats de qualité, le contrôle doit permettre de vérifier que l'émetteur est la personne ayant été reconnue par le réseau comme étant capable de certifier cette qualité.

Les transactions sont alors regroupées par blocs, selon leur ordre d'arrivée (chaque bloc peut contenir jusqu'à mille messages). Les vérifications de chaque transaction étant opérées, c'est le bloc en tant que tel qui est ensuite validé, avant d'être attaché aux autres blocs.

Cette validation est opérée selon les règles de fonctionnement de la blockchain adoptées par consensus.

Il existe plusieurs mécanismes de validation, selon les technologies utilisées par les différentes blockchains.

Sur la blockchain bitcoin, c'est la *Proof of Work* (la « preuve de travail ») qui est mobilisée. Le mineur doit résoudre un problème mathématique complexe. Il doit donc mettre en œuvre sa force de travail pour y parvenir et valider le bloc. S'il y parvient en premier et que le bloc est ensuite validé par au moins 51 % des mineurs, il recevra une récompense, consistant en l'octroi de bitcoins (c'est d'ailleurs à cette seule occasion que de nouveaux bitcoins sont mis en circulation). La complexité du problème est telle que seuls des serveurs isolés d'une taille colossale ou des serveurs mutualisant leurs puissances de calcul[20] peuvent les résoudre[21]. Parallèlement, ces opérations ont ainsi un coût économique et écologique non négligeable, qui devrait être pris en compte au moment de promouvoir la technologie blockchain fondée sur ce type de mécanisme de validation.

Parmi les autres mécanismes, on retient par exemple la *Proof of Stake* (en fonction de la quantité de crypto-monnaie que le mineur possède) ou la *Proof of Capacity* (en fonction de sa capacité de stockage).

À l'issue du processus de validation, le bloc est daté et inscrit dans la chaîne des blocs sur le registre. Ledit registre est ensuite reproduit chez chacun des participants du réseau (chaque nœud). Tous les utilisateurs du réseau ont par ailleurs accès à ce registre, et donc à chaque transaction présente dans les blocs, ce qui garantit la « transparence ». Le récepteur reçoit alors la transaction (dans l'exemple précité, le BTC appartient désormais à Bob, et plus à Alice). Une fois entrée dans le réseau, la transaction enchaînée à l'intérieur de blocs, eux-mêmes enchaînés par la vertu de la technologie, devient immuable. On ajoute que l'ensemble des opérations prend une dizaine de minutes chez bitcoin (qui utilise le processus de validation de la *Proof of Work*), nettement moins (une quinzaine de secondes) dans les autres systèmes (p. ex. : Ethereum).

8. DAO. — Un dernier concept doit être introduit : celui de *Distributed Automated Organizations* (DAO). Le rapport STOA le définit comme suit : *a bundle of smart contracts, cumulating in a set of governance rules that are automatically enforced and executed through blockchains*[22]. En d'autres termes, les applications décentralisées utilisant la technologie de la blockchain (aussi appelées les DApps) se dotent de règles inscrites dans des lignes de code des programmes informatiques : la DAO traduit donc en programme auto-exécutant les règles de fonctionnement et de gouvernance de l'application utilisant la blockchain. Ces règles, précise le co-fondateur de la start-up Slock-it[23] (qui offre, via la technologie blockchain, des services de location de biens immeubles), constituent le ferment d'une « organisation incorruptible qui appartient aux personnes qui ont aidé à la créer, à la

trust the technology, which dispenses from the need to trust the technology itself ».

(17) Rapport du Groupe FinTech, *op. cit.*, p. 12.

(18) Sur ces fonctions de la cryptographie, lire J.-N. Colin, « Du secret à la confiance... Quelques éléments de cryptographie », *in* H. Jacquemin (dir.), *L'identification électronique et les services de confiance depuis le règlement eIDAS*, Bruxelles, Larcier, 2016, pp. 12-14.

(19) L'indépendance, les uns par rapport aux autres, des vérificateurs présents et membres du réseau est fondamentale pour assurer la confiance dans la validité des échanges. Sur cette indépendance des « mineurs », c'est-à-dire ces vérificateurs et la délicate question des « pools de mineurs », lire les réflexions et les informations données sur la *Hashing Distribution* entre les sociétés qui se sont spécialisées en la matière (G.Hash.IO, BTC Guild, BitMinter *et al.*), : J.-L. Verhelst, *Bitcoin, Blockchain and beyond*, Self published book, 2017, pp. 60 et s. L'auteur note que le 13 juin 2014, la part de marché de GHash IO en ce qui concerne les activités de minage sur le réseau Bitcoin grimpa à 51 % de la puissance de calcul disponible sur le réseau, ce qui provoqua une chute quasi instantanée de la valeur du Bitcoin, faute de maintien de la confiance : « There are currently no regulations for mining activities, but common sense mandates that there should be a healthy distribution of the mining share » (*ibidem*, p. 61).

(20) Il semble que de telles opérations soient menées principalement par des sociétés ou consortia chinoises.

(21) Les chiffres sont impressionnants : « Début 2015, l'ensemble de la puissance de calcul de Google représentait 1 % de celle de bitcoin. Depuis, la puissance de Bitcoin a été multipliée par 4 » (Blockchain France, *La Blockchain décryptée*, *op. cit.*, p. 5).

(22) STOA, *op. cit.*, p. 20.

(23) Propos tenus par Stéphane Tual, cofondateur de Slock-it. Ces propos sont repris *in* Blockchain France, *op. cit.*, p. 12.

financer et dont les règles sont publiques ». Elles sont « "auditables" — tout étant dans le code » et donc transparentes aux utilisateurs du réseau et immuables, sauf à modifier l'organisation du réseau.

Avec la DAO, l'organisation devient totalement autonome et la technologie remplace le management humain. Le UK Chief Scientific Advisor, dans un rapport récent[24], analyse les perspectives de multiplication de ces DAO dans nos sociétés et prédit une nouvelle ère de nos démocraties[25] où notre gouvernance publique et privée pourrait être remplacée par ces DAO à la gouvernance totalement décentralisée et purement technique.

On relèvera que de telles DAO ne sont pas nécessairement sans risques. « The DAO », lancée en 2016 sur Ethereum, l'illustre. Elle a permis de réunir plus de 150 millions de dollars, dont près de 40 millions ont été détournés par des hackers. Plus précisément, ceux-ci ont utilisé le code d'une manière qui n'avait pas été anticipée, en exploitant une faille du système mis en place : ils n'ont donc pas *hacké* le code même si leur comportement n'était certainement pas en ligne avec l'esprit de la DAO[26].

9. Blockchains publiques et/ou privées. — On distingue les blockchains publiques et privées.

Blockchain France explique les différences entre les deux modèles comme suit : « Bitcoin et Ethereum constituent les deux principales blockchains publiques. D'autres existent également, de moindre ampleur : Litecoin, Dogecoin, etc.

» Dans le cas des blockchains privées (parfois appelées "de consortium"), le processus d'approbation est contrôlé par un nombre restreint et choisi de nœuds. Par exemple, une quinzaine d'institutions financières pourraient se mettre d'accord et organiser une blockchain dans laquelle un bloc devrait être approuvé par au moins 10 d'entre elles pour être valide. Il existe donc une double modification au système originel, puisque non seulement les participants au processus d'approbation sont limités et sélectionnés, mais en outre ce n'est plus la règle de la majorité qui s'impose. Le droit de lire la blockchain, c'est-à-dire l'accès au registre, peut être, lui, soit public, soit réservé aux participants du réseau.

» Il existe également des cas de blockchains privées où le processus d'approbation est limité à un unique acteur, bien que les autorisations de lecture par exemple puissent être publiques. Ce peut être le cas par exemple lorsque plusieurs départements d'une même entreprise dialoguent autour d'une blockchain en interne »[27] ou lorsqu'une société (par exemple d'assurances) offre ce service à ses clients dans le cadre de la création ou de l'exécution de transactions.

Il est évident que les blockchains publiques où chacun peut disposer d'une copie du registre sont plus résistantes aux attaques dans la mesure où on n'imagine pas que ladite attaque puisse atteindre tous les nœuds du réseau, alors que dans le cadre de blockchains privées appartenant à des consortiums restreints, l'intégrité du registre est testée via un nombre limité d'acteurs et donc se présente comme plus vulnérable à des cyber-attaques.

Les initiatives dans le domaine des blockchains privées se multiplient, à travers les applications lancées, soit en consortium par des entreprises ou groupes d'entreprises[28], soit par des entreprises isolées[29]. Cet engouement s'explique par les vertus de la technologie : rapidité et sécurité des transactions, y compris leur confidentialité. Le fait que, dans un réseau privé, la rémunération des mineurs n'est pas nécessaire séduit également les acteurs, dans la mesure où cela contribue à réduire les coûts de transaction. Par ailleurs, on peut imaginer que ces blockchains privées s'arriment à une blockchain publique. Ainsi, Microsoft annonce un partenariat avec Ethereum, une blockchain publique bien connue. Il s'agit de permettre à ceux qui le souhaitent de développer un certain nombre d'applications basées sur des blockchains privées, logées sur Azure, le cloud généraliste de Microsoft[30].

10. Blockchain avec ou sans crypto-monnaie ; avec ou sans *smart contract*. — Comme on le verra dans les applications, la blockchain peut d'abord être utilisée dans sa fonction de registre immuable et infalsifiable. Ses éléments caractéristiques permettent toutefois de remplir d'autres fonctionnalités. La plus connue est le transfert de bitcoins d'une personne à une autre (plus précisément, le registre mentionne qu'« Alice a transmis 2 BTC à Bob »). D'autres crypto-actifs ou crypto-monnaies ont depuis lors été créés. Par ailleurs, on peut inscrire dans le code des instructions (transférer une somme d'argent, verser une indemnisation par application d'un contrat d'assurance, débloquer une porte, etc.) qui s'auto-exécutent à un moment donné ou suite à la survenance d'un événement déterminé. Il s'agit des *smart contracts*, sur lesquels nous reviendrons plus longuement par la suite (*infra*, n^os^ 43 et s.).

B. Quelques cas d'application — La blockchain dans tous ses états

11. Des applications dans tous les secteurs de la vie sociale. — Le bitcoin est la première application[31] (*the vanguard*) de la blockchain et, depuis 2009, elle continue à défrayer régulièrement la chronique. La technologie est toutefois très prometteuse, en ce que ses applications dépassent cette hypothèse spécifique et pourraient toucher tous les secteurs de la vie sociale.

Sans prétendre à l'exhaustivité[32], nous présentons un bref tour d'horizon de ces applications, qui permettent d'entrevoir les nombreuses questions juridiques soulevées par cette technologie (*infra*, point II).

12. Le secteur bancaire et financier à l'heure de la blockchain. — La blockchain trouve dans les secteurs bancaires et financiers de nombreuses applications. Certains s'aventurent d'ailleurs à prédire la mort des banques dans leur rôle d'intermédiaires financiers[33]. La raison de ce succès se comprend par la réduction des coûts permise par le recours à la blockchain, tout en garantissant par ailleurs la sécurité et la rapidité des transactions.

Au-delà des premières utilisations de la blockchain dès 2009 (avec le bitcoin), d'autres applications se sont développées : elles utilisent la crypto-monnaie pour lever des fonds, sans passer par les bourses traditionnelles et le marché du capital d'investissement. Tel est le cas des ICO (*Initial Coins Offering*), sur lesquelles nous reviendrons (*infra*, n^o^ 42). D'autres applications se profilent[34] : dans le cadre des transac-

(24) M. Walport, Chief Scientific Adviser to HM Government, *Distributed Ledger Technology. Beyond Block Chain*, p. 14, rapport disponible à l'adresse suivante : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.
(25) Dans le même sens, A. Wright et P. de Filippi, « Decentralized Blockchain Technology and the rise of Lex Cryptographia », Working paper, 2015, p. 19, disponible sur http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664.
(26) Voy. M. Raskin, « The Law and Legality of Smart Contracts », *Geo. L. Tech. Rev.*, 2017, p. 337 : « strictly speaking, however, the hacker did not « hack » the code in a malicious way, but rather used the terms of the existing smart contracts to accomplish something others later found objectionable, i.e. the diversion of their money. Consider this using a legal loophole to effect a result that was clearly within the letter of the law, but not within it spirit ».
(27) Blockchain France, *La blockchain décryptée*, *op. cit.*, pp. 7 et s. Sur ce point, voy. aussi Rapport STOA, *op. cit.*, p. 5.
(28) On parle alors de consortium blockchain mis sur place par un nombre limité de participants pour accroître son avantage concurrentiel vis-à-vis des autres membres du secteur en offrant des services blockchain (l'exemple souvent cité est celui de R3 Corda dans le secteur bancaire qui réunit une quarantaine de banques de grande envergure. L'ambition est de définir des standards de transferts interbancaires utilisant la technologie des blockchains et de remplacer ainsi SWIFT (http://www.r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed.ledger-designed-for-financial-services) ou pour répondre aux besoins d'un secteur particulier.
(29) Ainsi, la blockchain Quorum, lancée par la banque J.P. Morgan, « Distributed Ledger Technology », disponible sur le site : https://www.jpmorgan.com/global/distributed-ledger-technology.
(30) Blockchain France, *op. cit.*, p. 26.
(31) D. De Jonghe et V.I. Laan, « Blockchain in de realiteit », *Computerrecht*, 2017/251, p. 347.
(32) Sur les applications, voy. notamment *ibidem*, pp. 350 et s. ; STOA, *op. cit.*, pp. 6 et s. ; Rapport Groupe FinTech, *op. cit.*, pp. 23 et s. ; Blockchain France, *La Blockchain décryptée*, *op. cit.*, pp. 15 et s. Les professionnels du droit pourraient également être impactés. On songe aux notaires (B. Verheye, « Blockchaintechnologie en het notariaat bij vastgoedtransacties : Damocles' zwaard of opportuniteit ? », *T. not.*, 2018, pp. 212 et s.) ou aux métiers de la justice (P. Henry et P. Hofströssler, « De toekomst van de advocatenberoep - L'avenir de la profession d'avocat », 25 février 2018, pp. 103 et s., disponible sur https://justice.belgium.be/sites/default/files/rapporttoekomstadvocatuurrapportavenirprofessiond_avocatfinal.pd.
(33) À cet égard, voy. les propos du Chief Technical Officer de la plateforme Bitcoin, David François, repris et discuté par le rapport de Blockchain France, *op. cit.*, Partie 2 : les Banques.
(34) Le rapport FinTech (*op. cit.*,

tions en bourse, des applications blockchain pourraient permettre aux réseaux, sans intermédiaires traditionnels, de jouer à la fois le rôle d'une bourse, d'une chambre de compensation, d'un dépositaire central voire d'un système de règlement-livraison, toutes les transactions étant enregistrées dans un registre décentralisé accessible à tous les utilisateurs du réseau. On imagine la profonde mutation que le développement de la blockchain pourrait entraîner dans le secteur bancaire et financier, en particulier en ce qui concerne certains intermédiaires comme les courtiers, les bourses, les chambres de compensation, etc.

13. Blockchain et assurances. — Avec la blockchain, des assurances *peer-to-peer* (dite « entre amis » — et donc, sans intermédiaire)[35] pourraient voir le jour, où chaque ami serait prêt à mettre une certaine somme en jeu, et accepter de mutualiser le risque encouru en cas de sinistre subi par l'un des pairs (par exemples d'une mise au chômage, d'un problème de santé, etc.).

Ce n'est toutefois pas là que se situe le potentiel de développement des blockchains dans le secteur des assurances (potentiel bien compris par certains acteurs, vu les investissements que des sociétés comme Axa ou Loyds consentent en la matière). L'idée est d'automatiser l'exécution des contrats d'assurance par l'insertion de *smart contracts* liant le paiement de l'indemnité à la vérification d'événements par le biais d'« oracles ». L'exemple de l'assurance indemnisant les retards de vol des avions est souvent présenté. Le paiement du montant assuré est garanti par l'émission automatique d'un message à la blockchain, message provenant de la compagnie aérienne et attestant l'annulation ou le retard du vol. Parmi les autres illustrations, on cite aussi les assurances des agriculteurs contre la grêle ou tout autre événement naturel abîmant les récoltes : un *smart contract* prévoirait le versement automatique d'indemnités sur la base de l'oracle du service météorologique de l'État confirmant les intempéries. Au-delà, comme le note un auteur, la technologie « va permettre l'automatisation de la souscription des polices, de la gestion des sinistres et de l'indemnisation, l'assurance retard d'avion, l'assurance anti-pollution, l'assurance décès, l'assurance automobile seront en premier lieu concernées. Le consommateur pourra être remboursé sans même remplir de déclaration de sinistre, le tout grâce aux *smart contracts*, dont la mise en place s'opère sans tiers de confiance »[36].

14. Blockchain et œuvres ou inventions[37]. — La technologie de la blockchain semble être en mesure d'apporter nombre d'avantages à la gestion et à la protection tant de la création que de l'exploitation des œuvres et inventions[38]. La Commission européenne et l'Office de l'Union européenne pour la propriété intellectuelle (EUIPO) semblent convaincus de l'intérêt de la technologie et ont entamé des études à ce sujet[39].

Le premier apport réside dans la plus grande facilité de démonstration des droits de propriété intellectuelle par leur prétendu titulaire, démonstration préalable à la concession de droits sur cette œuvre. En droits d'auteur, celui qui invoque l'existence ou l'absence de droits sur une création doit le prouver. Cette démonstration peut porter tant sur le contenu que la date de la création. La blockchain, par la création d'un registre immuable ouvert à tous et la sécurité qu'elle apporte, est une solution de loin préférable à celles qui reposent sur le dépôt notarial ou auprès d'huissiers.

Un autre avantage de la technologie en discussion est d'apporter une protection à l'ensemble du processus créatif ou innovant, qui peut être long et délicat et impliquer différents auteurs dans le cadre d'une œuvre collaborative. Le créateur ou l'entreprise innovante peuvent en effet craindre le détournement par un concurrent ou un salarié de l'œuvre en gestation, et non encore protégée. Le participant à une œuvre collective peut craindre son apport non reconnu. L'inscription des différentes phases dans les blocs enregistrés permettra la démonstration de l'origine et de l'avancement progressif de la création. Cet avantage trouve un écho particulier à l'article 2 de la récente directive européenne sur le secret d'affaires[40]. Cette disposition protège le secret si celui-ci présente une valeur commerciale et si l'entreprise rapporte la preuve de la mise en œuvre de « dispositions raisonnables destinées à garder leurs informations secrètes ». L'utilisation de la technologie blockchain offre aux entreprises le moyen de fournir la preuve tangible des diligences accomplies pour protéger le secret d'affaires.

Le troisième avantage concerne l'exploitation des œuvres[41], l'œuvre protégée étant numérisée dans la blockchain et dûment enregistrée. Ainsi, la startup Médiachain, aujourd'hui rachetée par Spotify, recourt à la blockchain pour l'accès aux œuvres, le paiement des redevances et la répartition des droits musicaux entre auteurs. D'autres sociétés vont plus loin et proposent aux auteurs d'introduire eux-mêmes leurs œuvres dans la blockchain. L'œuvre est alors accessible à tous, moyennant le paiement d'une redevance dont un *smart contract* lié à l'œuvre vérifiera l'exécution. Ce mécanisme permet dès lors à l'auteur de toucher directement la redevance sans devoir passer par une société de gestion des droits[42].

15. Blockchain : authenticité et traçabilité de produits, en particulier les produits de luxe. — L'exemple de l'application proposée par la société Everledger suffira à illustrer notre propos et permet au lecteur d'imaginer bien d'autres applications, en matière d'œuvres d'art, de montres ou de voitures de luxe. En l'occurrence, il s'agit, grâce à la technologie blockchain, d'offrir aux clients un service de provenance, de certification et de traçabilité des diamants. Les qualités de chaque diamant, une sorte de « passeport digital », sont enregistrées après un *hashing* qui permet de sécuriser cette empreinte numérique de la pierre. Les transactions[43] opérées à propos de ce diamant sont consignées systématiquement dans les chaînes suivantes, de manière à ce que chaque maillon de la transaction puisse retracer l'origine et le circuit suivi par le bien répertorié dans les différents blocs. On conçoit l'intérêt du système qui permet un contrôle complet de la *supply chain* des biens et ainsi d'éviter les trafics illicites et les fraudes fréquents dans les secteurs des produits de luxe[44].

pp. 23 et s.) étudie ainsi les applications sur le marché secondaire et dans le domaine des produits dits dérivés.

(35) À cet égard, l'expérience de *Friendsurance*. En l'occurrence, dans le cadre d'une DAO, les assurés eux-mêmes fixent les règles traduites en code informatique. Le système enregistre de manière totalement transparente et sécurisée, les primes versées par chaque membre et en fonction des risques couverts les indemnisations attribuées aux membres. Les surplus sont automatiquement calculés et redistribués aux membres.

(36) G. Marraud des Grottes, « La blockchain : un secteur encore en phase d'exploration, mais très prometteur », *R.L.D.I.*, 2017, p. 33.

(37) Sur ce point de manière beaucoup plus complète, lire l'article de M. Lognoul, *Blockchain et propriété intellectuelle : quelles perspectives ? - Quelles opportunités*, à paraître.

(38) Sur ce point, entre autres, l'article de M. Canova, « Blockchain et propriété intellectuelle : une alliance révolutionnaire », disponible sur le site : https://lex4.com/blockchain-et-propriete-intellectuelle-une-alliance-revolutionnaire/, ou V. Fauchoux et A. Gouaze, « Pourquoi la blockchain va révolutionner la propriété intellectuelle ? Application pratique au secteur de la mode », *Propriétés intellectuelles*, octobre 2017, pp. 63 et s.

(39) Communication de la Commission au Parlement européen, au Conseil et au Comité économique et social européen, « Un système équilibré de contrôle du respect de la propriété intellectuelle pour relever les défis sociétaux d'aujourd'hui », COM(2017) 707 final, 29 novembre 2017, p. 9 et EUBlockathon2018, Office de l'Union européenne pour la propriété intellectuelle, 22 au 25 juin 2018.

(40) Article 2 de la directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites, *J.O.U.E.* L 157/1 à L 157/18 du 15 juin 2016. Sur cette directive, lire notamment, V. Cassiers, « La directive 2016/943/UE du 8 juin 2016 sur les secrets d'affaires », *J.T.*, 2017, p. 385.

(41) W. Blocher, A. Hoppen et P. Hoppen, « Software lizenzen auf der Blockchain », *Computerrecht*, 2017, p. 337.

(42) *Cfr* les développements de Ascribe (http://www.ascribe.io) et de Mycelia (http://myceliaformusic.org/) : « Grâce à une telle blockchain, dès qu'un artiste serait écouté, il pourrait être directement rémunéré. C'est d'ailleurs une technologie sur laquelle la start-up Mycelia travaille pour court-circuiter les labels et plates-formes, qui se font rémunérer par les artistes tout au long de la chaîne de production. Avec ce système, inspiré des *smart contracts*, Mycelia veut permettre, à terme, à des artistes d'être directement rémunérés par leur public. Les artistes pourraient bénéficier d'une répartition dynamique et en temps réel de leurs droits, sans aucune intervention tierce. Une garantie pour les artistes d'être payés en fonction de leurs productions. Mais les géants du Net sont-ils prêts pour cette révolution ? » (R. Bloch, « La blockchain peut-elle révolutionner le droit d'auteur ? », *Les Échos*, 16 mars 2018, disponible sur le site : https://www.lesechos.fr/idees-debats/sciences-prospective/0301447937425-la-blockchain-peut-elle-revolutionner-le-droit-dauteur-2162314.php). D'autres applications de la blockchain aux *peer-to-peer streaming services* existent, ainsi Resonate (https//resonate.is) ou Opus (https//opus-foundation.org).

(43) Dont le paiement peut être assuré par un *smart contract*, ce qui est le cas dans l'application développée par Everledger.

(44) À cet égard et d'autres avantages encore, lire le rapport STOA, *op. cit.*, pp. 16 et s.

16. Blockchain et secteur de l'énergie. — C'est surtout à propos des énergies alternatives et du phénomène de l'autoproduction de l'énergie qu'est évoqué l'intérêt de la technologie blockchain, en particulier dans le cadre de communautés de producteurs développant des réseaux locaux de production et de distribution d'énergie, aussi appelés *smart grids*. Ainsi, Solar Coin[45] utilise la technologie blockchain pour (i) garantir l'origine de l'énergie produite, en l'occurrence par des panneaux solaires, (ii) offrir une prime en Solar Coin, une crypto-monnaie, émise en fonction des mwh produits et (iii) permettre la rencontre de l'offre et de la demande, en d'autres termes, l'achat d'énergie propre.

17. Blockchain et e-voting[46]. — Que les votes interviennent dans le cadre d'une consultation publique ou du fonctionnement des organes d'organisations privées (comme le vote d'actionnaires), ils sont généralement enregistrés et comptés de manière centrale. La blockchain permet aux votants d'exercer un contrôle complet sur leur vote, sans qu'une autorité centrale ne soit nécessaire. Le caractère immuable des registres permet en outre de déceler toute modification des votes, chacun pouvant constater une fraude éventuelle (un double vote, par exemple). On précise que seule l'existence du vote est visible, son contenu restant secret et crypté. Dans la mesure où le vote est fait à distance, la technologie ne prévient pas la possibilité d'influence, voire de coercition des votants mais ces inconvénients pèsent peu aux yeux des observateurs, eu égard aux avantages de ce système sûr, peu coûteux[47] et qui permet de concevoir le recours au vote électronique à distance de manière plus systématique. Si le mécanisme devait être mis en œuvre dans les matières publiques, il faudrait veiller au respect des principes constitutionnels d'universalité, d'égalité d'accès, de liberté de choix et de secret du vote.

18. Blockchain et e-gouvernement. — Le rapport sur la blockchain du conseiller scientifique en chef du gouvernement britannique, déjà cité[48], affirme que : « le premier rôle du gouvernement dans le support apporté au développement de cette technologie est de développer une vision claire de la façon dont la blockchain peut améliorer la gestion par le gouvernement et sa capacité de rendre des services aux citoyens. [...] Une chance s'offre pour le gouvernement de rendre possible un futur où la délivrance de services aux citoyens sera plus personnalisée, immédiate et efficiente. Chaque fois où c'est adéquat, les citoyens doivent avoir la possibilité de signaler leurs préférences et besoins en participant à des *smart contracts*. La mise en œuvre de registres distribués avec l'apport des *smart contracts* devrait conduire à des améliorations substantielles dans la conformité, la réduction des coûts et la responsabilité des opérations avec l'administration : le *UK Government Digital service*, en développant une plateforme électronique afin de délivrer ses services et des registres distribués, pourrait être au cœur de cette vision ».

La suite du rapport, comme d'autres[49], foisonne d'exemples, souvent repris du modèle estonien[50], qui illustrent les applications de la blockchain en matière d'e-gouvernement, tant en interne pour faciliter et sécuriser les flux entre administrations, que vis-à-vis des citoyens, en matière de certification de l'identité ou de la résidence, de cadastre, de justice, de paiements des pensions ou d'interventions dans le domaine de la santé[51].

19. Blockchain et économie collaborative. — Certains prédisent la mort des plateformes collaboratives (Airbnb, Uber, Booking, ...) avec le déploiement des blockchains, des DAO et des *smart contracts* y associés. Ici également, prévaut le principe selon lequel les tiers de confiance et les registres centraux des plateformes de l'économie collaborative ne sont plus nécessaires à l'heure où la technologie permet une décentralisation totale et, donc, la possibilité pour chaque citoyen de devenir un acteur à part entière des opérations. Il en résulterait — par un retour cynique du destin — une « ubérisation » des acteurs de la *sharing economy* par la blockchain[52].

Ainsi, Arcade City créé en 2016, en Australie et aux États-Unis, ou ZOOZ en Israël, développent un système de co-voiturage permettant aux chauffeurs de nouer directement des transactions avec leurs clients. On note que les services d'Arcade seraient intégrés à la blockchain Ethereum afin de bénéficier des services de vérification d'identité, de réputation et des services de paiement proposés par cette dernière. La société Slock-it est considérée comme un « Airbnb killer »[53], quand Open Bazaar entend mettre en connexion directe les acheteurs et les vendeurs, et ainsi rendre inutiles les services d'eBay.

20. Quelques tendances. — À travers la multiplication des applications de la technologie de la blockchain, se laisse entrevoir l'importance croissante de cette technologie dans tous les domaines de la vie économique, sociale et publique. Si la blockchain est née d'applications monétaires, ou plutôt de crypto-monnaies, cette question de l'utilisation de crypto-monnaies devient un accessoire au développement d'opérations économiques.

À cette remarque, s'en ajoutent deux autres.

La première est l'importance prise par les blockchains privées au détriment des blockchains publiques. C'est bien souvent dans le contexte d'un réseau de personnes ayant un lien social ou économique dans un secteur donné (par ex. le marché des œuvres d'art, de l'assurance, etc.) que la technologie se développe et offre un service plus efficace — parce que moins lourd en termes de procédures de sécurité. Il s'agit également de mettre en avant l'aspect « communautaire » de nombre d'applications. La technologie blockchain permet à des groupes de se fixer des règles entre elles ; ainsi, ces « amis » qui décident de créer leurs propres systèmes d'assurance.

La seconde réflexion a trait aux substituts offerts par la technologie blockchain aux systèmes centralisés de l'économie collaborative ou aux sociétés de gestion collective de droits d'auteur : on constate en effet que la technologie permet au simple citoyen, propriétaire de biens, prestataire de services ou auteur, de valoriser directement son offre auprès de la clientèle sans passer par un intermédiaire régulateur. On revient au rêve des créateurs de l'internet, de permettre à chacun d'être pleinement acteur dans la production et la distribution des produits, sans intermédiaire et en négociant directement en *peer-to-peer*. Il est vrai cependant que l'état expérimental des premières applications ne permet pas (encore) de conclure à leur succès et, au-delà, au triomphe de cette vision citoyenne du développement de la technologie.

2 De quelques questions juridiques soulevées par la blockchain

21. Plan de la présente section. — On distingue généralement trois fonctions principales à la blockchain. La première consiste à servir de registre de données. Les autres fonctions, complémentaires à la première (et qui s'appuient en tout cas sur cette fonction de registre), portent sur le transfert de crypto-monnaies (ou de crypto-actifs, de manière plus générale) et/ou l'exécution automatique de certaines opérations, par le recours à des *smart contracts*.

(45) Sur les activités de la Solar Coin Foundation, lire : https//solarcoin.org/nl/wallet-nederlands. Voy. aussi D. De Jongh et V. Laan qui donnent d'autres exemples : Share & Charge, Suncontract, Tennet,... (*op. cit.*, p. 251).
(46) Sur le e-voting, lire en particulier les réflexions du STOA, *op. cit.*, pp. 12 et s.
(47) Certains parlent de *liquid democracy* ou de *techno-democratic system*.
(48) Traduction libre de M. Walport, Chief Scientific Adviser to HM Government, *Distributed Ledger Technology. Beyond Block Chain*, p. 14, rapport disponible à l'adresse suivante : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.
(49) En particulier, lire le rapport Blockchain France qui, à côté d'exemples européens et américains, donne les exemples ghanéens ou géorgiens où se développent des projets en ce qui concerne les cadastres fonciers de ces États.
(50) Dès 2015, l'Estonie avait développé sa première application blockchain en matière d'e-residency, C. Sullivan et E. Burger, « E-residency and blockchain », *CL&SR*, 2017, pp. 407 et s. Depuis, le rapport anglais cité (pp. 80 et s.) fait référence à bien d'autres développements.
(51) Le rapport du STOA (*op. cit.*, p. 17) européen rejoint les conclusions du conseiller anglais.
(52) Voy. C. Zolynski, « La blockchain : la fin de l'ubérisation », *Dalloz IP/IT*, 2017, p. 385.
(53) La plateforme se présente comme suit sur son site internet : *the sharing economy's story doesn't end with taxis and vacation rentals. It's expanding to touch consumers and companies, employees and employers. We believe that Airbnb's will soon become fully automated, and small business owners will prefer to rent work spaces on demand rather than commit to complex leases* (https://slock.it/usn.html).

Nous examinons dans une première partie les questions juridiques communes à tout type de blockchain et résultant de sa fonction de registre (A). Ensuite, nous analysons plus spécifiquement les enjeux juridiques posés par les crypto-monnaies et les *smart contracts* (B).

Les branches du droit affectées par le phénomène et les utilisations de la blockchain sont nombreuses. Nous n'évoquerons ici que certaines d'entre elles, laissant de côté d'autres domaines comme les droits pénal, administratif ou de la concurrence pour n'aborder que les questions de droit financier, de droit civil, de droit de la propriété intellectuelle et de droit de la protection des données

A. Focus sur certaines questions transversales posées par la blockchain

1. Blockchain et propriété intellectuelle

22. Blockchain et propriété intellectuelle. — Blockchains privées ou publiques, avec ou sans *smart contracts*, toutes utilisent des programmes informatiques, des codes source, des codes objet et souvent des interfaces graphiques[54]. Il est donc légitime de s'interroger, en premier lieu, sur la propriété intellectuelle qui est liée à ces programmes[55] mais, peut-être au-delà, sur les règles écrites ou non et les programmes qui régissent les DAO et les *smart contracts*.

23. Droit d'auteur et programmes d'ordinateur. — Les concepteurs peuvent facilement être identifiés, qu'il s'agisse de graphistes, de codeurs ou de développeurs web travaillant ou non en entreprises ou à leur demande[56][57] ou qu'il s'agisse d'œuvres collectives ou de collaboration, notamment (mais non uniquement), lorsqu'il est question d'une DAO rédigée au sein d'une communauté d'utilisateurs.

De tels éléments peuvent-ils être protégés par le droit de la propriété intellectuelle, en particulier par le droit d'auteur ? En l'occurrence, on considérera, selon la jurisprudence et la doctrine constantes que tel sera le cas lorsque l'« œuvre » « relève de l'effort créateur et reflète la personnalité de l'auteur (ou des auteurs) », pour reprendre l'expression de la Cour de cassation française[58]. Cette protection par le droit d'auteur permettrait au(x) titulaire(s) du droit de se prévaloir des dispositions prévues par la directive 2009/24/CE du 23 avril 2009 concernant la protection juridique des programmes d'ordinateur, quant au droit d'adaptation, de traduction, de modification ou de reproduction permanente ou provisoire[59]. Ces prérogatives ouvrent le droit à exiger une rémunération de la part des utilisateurs de la blockchain. Si la création est une œuvre de collaboration, les co-auteurs exercent leurs droits de commun accord, ce qui leur permettra de confier la gestion de leurs droits à un des co-auteurs ou de s'interdire des blocages dans la commercialisation de l'œuvre. Si l'auteur ou les auteurs peuvent se targuer de leurs droits patrimoniaux, ils peuvent également renoncer à les exercer dans le cadre d'un choix délibéré d'*Open Source* et permettre ainsi la réutilisation par des tiers dans le cadre d'un développement ouvert et coopératif. On sait qu'Ethereum a opéré un tel choix, en distribuant ses codes source sous licence GNU. La fourniture par Ethereum de ses codes source présente un avantage, celui de bénéficier à son tour de manière gratuite des développements apportés par les utilisateurs[60].

24. Brevet. — Parmi les droits de propriété intellectuelle figure également le droit aux brevets. On sait que le programme d'ordinateur n'est pas en tant que tel brevetable mais que, si son fonctionnement a un effet technique supplémentaire, allant au-delà des effets techniques normaux, il peut ne pas être exclu de la brevetabilité. Ainsi, dans le cas d'une blockchain munie d'un *smart contract* dont l'effet serait d'éteindre le chauffage lorsque la chaleur atteint un certain degré ou de distribuer automatiquement les sources d'énergie entre producteurs excédentaires d'énergie et utilisateurs en besoin, la brevetabilité pourrait être imaginée. On note, à la suite du rapport FinTech, qu'aux États-Unis, fin 2016, 71 demandes de brevets concernant des blockchains avaient fait l'objet d'un dépôt.

25. Secrets d'affaires. — Reste à s'interroger sur l'applicabilité, aux blockchains, des protections nouvelles accordées au secret des affaires. Le « secret d'affaires », conformément à la directive 2016/943/UE[61], couvre les informations secrètes, c'est-à-dire non connues globalement par les tiers, ayant une valeur commerciale[62] et ayant fait l'objet, de la part de la personne qui en a le contrôle de façon licite, de dispositions raisonnables, compte tenu des circonstances, destinées à les garder secrètes[63]. Sans nul doute, les développements technologiques innovants d'une blockchain répondent à la condition de la valeur commerciale. Encore faut-il que la seconde condition de la protection ait été observée et qu'ils aient fait l'objet de mesures de maintien de la confidentialité à la hauteur de leur valeur et des risques d'atteinte à cette confidentialité.

---

(54) Ainsi, celles proposées par le site bitcoin.org qui permet de suivre de manière très conviviale l'évolution de cette crypto-monnaie.

(55) Il ne s'agit donc plus de s'interroger sur la façon dont les blockchains peuvent aider à la protection de la propriété intellectuelle, question étudiée *supra*, n° 14, mais en quoi les spécificités d'une blockchain ou de certains éléments de celle-ci peuvent bénéficier d'une protection par la propriété intellectuelle.

(56) Le rapport du Groupe FinTech (*op. cit.*, p. 73) évoque, à la suite de Me Bensoussan (« Le robot créateur peut-il être protégé par le droit d'auteur ? », *Planète Robot*, n° 4, article disponible sur le site https://www.alain-bensoussan.com/wp-content/uploads/2016/12/34125221.pdf), la possibilité de voir le programme réalisé par un robot ou un système d'intelligence artificielle. L'auteur cité affirme qu'« en l'état actuel du droit positif, seule une personne physique peut être auteur », ce qui exclut « les œuvres réalisées par un robot seul ». Si on peut suivre le raisonnement de l'auteur, on le nuance cependant : la directive 2009/24/CE du 23 avril 2009 concernant la protection juridique des programmes d'ordinateur n'exclut pas, en son article 2, § 1er, que le droit national accorde la titularité du droit à une personne morale, ce qui pourrait permettre au législateur de confier aux entreprises ayant développé elles-mêmes ou via leurs employés les systèmes d'intelligence artificielle de réclamer les droits d'auteur sur les productions dérivées du programme d'intelligence artificielle. À noter en ce sens que récemment, le Parlement européen le 27 janvier 2017, dans son *Rapport concernant des recommandations à la Commission concernant des règles de droit civil sur la robotique* (2015/212103, p. 32), a invité la Commission à adapter les critères d'éligibilité à la titularité de la propriété intellectuelle en cas d'œuvres générées par machine (sur ce point, de manière très critique et à raison, B. MICHAUX, « Singularité technologique, singularité humaine et droit d'auteur », *in Law, Norms and Freedoms in Cyberspace, Liber amicorum Yves Poullet*, coll. du CRIDS, n° 43, Bruxelles, Larcier, 2018, pp. 402 et s.).

(57) Par contre, il est clair que les mineurs dont le rôle est de trouver la solution d'une question mathématique complexe dans le cadre d'un problème qui leur est posé ne peuvent bénéficier d'aucun droit de propriété intellectuelle.

(58) Cass. com., 25 mars 1991, n° 89-11204. Voy. aussi Cass. civ., 22 septembre 2011, n° 09-71337, qui parle d'« apport intellectuel propre et effort personnalisé ». Sur ce point, lire les commentaires de P. DE FILIPPI et B. LAW, « Les *smart contracts* : les nouveaux contrats augmentés ? », *Revue de l'ACE*, septembre 2016, n° 137i : « les *smart contracts* peuvent être qualifiés d'œuvres soumises au droit d'auteur dès lors que la contribution de leur concepteur est suffisamment importante pour révéler son apport personnel ».

(59) Voy. les articles XI.294 et s. du C.D.E.

(60) En faveur de la promotion de l'utilisation de licences d'Open Source, lire outre P. DE FILIPPI et B. LAW, *op. cit.*, les réflexions de Calimaq (alias L. MAUREL), « Vers une convergence entre Blockchain et les licences Creative Commons ? », 16 mars 2016, disponible à l'adresse : https://scinfolex.com/2016/03/16/vers-une-convergence-entre-blockchain-et-les-licences-creative-commons/.

(61) Article 2 de la directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites, *J.O.U.E.* L 157/1 à L 157/18 du 15 juin 2016.

(62) Sur ce point, H. DE VAUPLANE, « La finance décryptée par le droit : la blockchain et la loi », *Alternatives économiques*, 14 février 2016, disponible sur le site : https://blogs.alternatives-economiques.fr/vauplane2016/02/14/la-blockchain-et-la-loi : « Cette question de la propriété ou du contrôle des codes source résonne de manière particulière dans l'industrie financière : il s'agit de la question de la protection des algorithmes utilisés dans certaines transactions financières et développés par des experts (les "quants") dans la mesure où la plupart de ces algorithmes ne peuvent être protégés par des brevets ou droits d'auteur ; dès lors, ces algorithmes sont gardés secrets. Ce qui n'est possible que dans une blockchain privée où les développements spécifiques apportés par l'éditeur ne sont pas toujours juridiquement protégés mais dans ce cas, ils ne sont pas ouverts, pas même aux participants de la chaine privée ».

(63) Art. 2(1) de la directive : « Aux fins de la directive, on entend par « secret d'affaires », « des informations qui répondent à toutes les conditions suivantes : a) elles sont secrètes en ce sens que, dans leur globalité ou dans la configuration et l'assemblage exacts de leurs éléments, elles ne sont pas généralement connues des personnes appartenant aux milieux qui s'occupent normalement du genre d'informations en question, ou ne leur sont pas aisément accessibles ; b) elles ont une valeur commerciale parce qu'elles sont secrètes ; c) elles ont fait l'objet, de la part de la personne qui en a le contrôle de façon licite, de dispositions raisonnables, compte tenu des circonstances, destinées à les garder secrètes » (V. CASSIERS, « La directive 2016/943/UE du 8 juin 2016 sur les secrets d'affaires », *J.T.*, 2017, p. 385).

26. Droit des bases de données. — Comme on l'a vu, l'ensemble des données des transactions se trouvent répertoriées au fur et à mesure de la constitution des blocs et de leur validation et est accessible suivant des interrogations multicritères. Ne s'agit-il pas là de bases de données dont le droit européen prévoit la protection ?

Les données inscrites dans les registres distribués de la blockchain représentent l'historique de tous les mouvements, toutes les transactions intervenues sur ce réseau global. L'ensemble de ces données est automatiquement et définitivement conservé dans la chaine de blocs sous forme de lignes de codes. Nous remarquerons que la législation actuelle relative à la propriété des bases de données devrait être appliquée à ces datas, composant essentiel de la blockchain. Ces registres de données pourraient constituer au sens de la directive européenne 96/9/CE du 11 mars 1996 concernant la protection juridique des bases de données, une banque de données, c'est-à-dire « un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodiques et individuellement accessibles par des moyens électroniques ou d'une autre manière ». La directive interdit l'extraction ou la réutilisation des bases de données ainsi définies. On s'interroge toutefois sur l'intérêt d'une telle protection. Certes, les interfaces d'interrogation ou de présentation peuvent être dignes de protection par le droit de la propriété intellectuelle, comme il a été évoqué au numéro précédent. Cependant, protéger les registres contre l'extraction et la duplication peut aller à l'encontre de l'essence même des blockchains dont le fonctionnement repose sur la multiplication de la reproduction au sein d'un réseau décentralisé et la possibilité pour chacun de les interroger et d'en extraire le contenu, sous réserve des limites du droit à la protection des données.

2. Blockchain et protection des données à caractère personnel

27. Blockchain et vie privée. — L'intérêt de la blockchain est, nous l'avons montré (*supra*, n^os^ 5 et s.), fondé sur le fait que le système de registre distribué permet à chaque utilisateur d'avoir la preuve des transactions, de préserver leur intégrité et de conserver un historique des diverses transactions. On conçoit dès lors la crainte exprimée par certains vis-à-vis d'une technologie qui permet non seulement le traçage des transactions opérées par les utilisateurs du réseau, soit directement, soit à travers un objet dont il a la maîtrise mais également, vu les caractéristiques du fonctionnement des blockchains, l'impossibilité de modifier les registres des transactions et donc les données à caractère personnel y contenues, sans respect des droits à la correction et à l'effacement conférés à la personne concernée par le RGPD.

Nombre d'auteurs s'interrogent dès lors sur la conformité des applications de la blockchain au règlement européen général de protection des données (en abrégé, le RGPD), récemment entré en application[64]. Nous aurons l'occasion de souligner les difficultés soulevées par la mise en œuvre des principes issus du règlement dans le cadre de la technologie de la blockchain ; encore faut-il préalablement se poser une question préjudicielle : le règlement s'applique-t-il ? Les transactions concernées par la blockchain concernent indiscutablement des personnes, et bien souvent des individus, qu'il s'agisse de transactions d'assurance, de locations d'immeubles, de certificats de qualité ; pour autant, y a-t-il traitement de données à caractère personnel ?

28. Le RGPD est-il applicable à la blockchain ? — Le RGPD s'applique aux traitements de données à caractère personnel. Celles-ci sont définies largement comme toute information se rapportant à une personne physique identifiée ou identifiable, y compris par référence à un identifiant, ou à un ou plusieurs éléments spécifiques propres à son identité[65]. Dans la plupart des applications blockchain, les transactions reprises dans le registre mentionnent l'émetteur et le destinataire, mais sous la forme d'une signature électronique[66]. Cette signature permet-elle d'identifier l'individu qui se cache derrière le procédé[67] ? Sans doute la réponse dépendra-t-elle de la qualité de la clé utilisée et de la fréquence de sa mise à jour. Certains systèmes de signature permettent d'ailleurs de générer, à chaque opération, une signature nouvelle, ce qui rend le décryptage de la signature privée tant de l'émetteur que du destinataire difficile. On parlera, à propos de telles signatures, de pseudonymes, catégorie intermédiaire entre la donnée anonyme et celle nominative, dont le contenu renvoie directement à un individu identifié ou identifiable. Le RGPD la définit[68] à travers l'opération qui la produit : « le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable ».

Faut-il pour autant considérer que toute donnée relative à une personne (au départ) mais « pseudonymisée » (par la suite) doit se voir appliquer le règlement ? Le considérant n^o^ 26 du règlement invite à plus de nuances : « Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable. Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles[69] au moment du traitement et de l'évolution de celles-ci ». Il s'agit donc de constater si, oui ou non, par des moyens raisonnables, l'identification des personnes concernées est possible[70]. À cet égard, deux théories s'affrontent : l'une, dite « objective », renvoie à la question de l'identifiabilité en soi ; l'autre, dite « subjective », prend en compte les moyens que la personne qui reçoit les données peut raisonnablement mettre en œuvre. Cette seconde conception a l'appui de la Cour de justice qui, dans l'affaire *Breyer*[71], a considéré que la donnée IP dynamique n'était pas nécessairement une donnée à caractère personnel dans la mesure où celui qui détient cette donnée peut démontrer qu'il n'a pas raisonnablement les moyens de relier l'adresse IP à une personne identifiable. Si l'on suit cette lecture « subjective », il faudra bien souvent conclure, du moins si on s'en tient aux seules données présentes dans la chaîne et accessibles à tous les utilisateurs de la chaîne, que les données des registres distribués sont « anonymes »[72] (on imagine mal le commerçant lever les secrets de la cryptographie mise en œuvre, suite au paiement en bitcoin qui lui est adressé). Notre réflexion n'exclut pas que la levée de l'anonymat ait lieu du fait de données circulant hors chaîne (ainsi, le commerçant peut avoir reçu un courriel précédant la commande et le paie-

(64) Règlement (UE) n^o^ 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.U.E.* L 119 du 4 mai 2016, pp. 1-88. Il est entré en application le 25 mai 2018.
(65) *Cfr* article 4, 1^o^), du RGPD.
(66) *Supra*, n^o^ 7.
(67) Comme le notent à propos du blockchain bitcoin P. DE FILIPPI et M. REYMOND (« La Blockchain : comment réguler sans autorité », *in* T. NITOT et N. CERCY (dir.), *Numérique : reprendre le contrôle*, Framabook, 2016, p. 81) : « les individus qui font des échanges en Bitcoin ne sont désignés dans la blockchain qu'à travers leur adresse Bitcoin, un identifiant global sous forme d'une chaîne de caractères de ce type : 37WctrDb1G1orXhJ8vgx7zS2WCuSuBk6EQ. Aucune autre information n'est disponible, ni sur leur identité hors ligne, ni sur la nature de leur transaction ».
(68) Article 4, 5^o^, du règlement.
(69) À cet égard, le rapport ODI (Open Data Institute) (*Applying blockchain Technology in Open Data Infrastructure*, ODI-TR-2016-001, disponible sur le site de l'ODI : https://theodi.org/topic/data-infrastructure/) attire l'attention sur deux risques : le premier réclame de se méfier des métadonnées qui peuvent créer de forts risques de réidentification ; un historique de géolocalisation inscrit dans une blockchain pourrait ainsi permettre rapidement de réidentifier un individu, même pseudonymisé. Le second est le fait que les technologies de décryptage progressent vite et que dès lors, ce qui est indéchiffrable au regard d'un état de la technologie risque de ne plus l'être quelques années ensuite.
(70) Sur cette question, lire V.L. SLAAN, « Privacy issues by blockchain : hoe voorkom of minimaliseerje die ? », *Computerrecht*, 2017, p. 255.
(71) C.J.U.E., 19 octobre 2016, *Breyer*, C-582/14.
(72) En ce sens, le rapport de décembre 2015 du Conseiller scientifique du gouvernement anglais, M. WALPORT, Chief Scientific Advisor to HM Government, *Distributed Ledger Technology. Beyond Block Chain*, p. 50, rapport disponible à l'adresse suivante : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

ment en bitcoin lui permet de lever le secret). En cas de contestation sur le caractère anonymisé des données grâce aux techniques de signature utilisées, il appartiendra aux responsables du traitement, c'est-à-dire ceux qui sont participants de la blockchain, de démontrer ce caractère anonyme.

29. Respect des principes établis par le RGPD en matière de blockchain. — Si le RGPD doit être observé, que peut-on dire de son application ?

La première question est celle de l'identification du responsable du traitement, c'est-à-dire celui qui définit les finalités et les moyens du traitement. À cet égard, il nous paraît que dans nombre de blockchains privées mises en place par une ou des entreprises pour servir ses ou leurs clients, un ou des fournisseurs d'énergie, une ou des compagnies d'assurances ou, bien sûr, l'État, c'est cet acteur qui est responsable seul ou conjointement, selon la définition de l'article 26 du RGPD : « lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, par voie d'accord entre eux ». Dans le cas de blockchains privées créées par des communautés d'utilisateurs[73] ou de blockchains publiques mises à la disposition de tous, dans ces réseaux où se multiplient les nœuds et où chacun peut accéder au registre et l'abriter, il est difficile d'identifier qui définit la finalité et les moyens comme c'était le cas lorsqu'un tiers de confiance coordonnait l'ensemble du réseau. Chaque utilisateur susceptible de décharger le registre distribué devrait alors être considéré comme responsable ou plutôt comme responsable conjoint[74].

Une autre possibilité, en particulier dans les blockchains publiques, où le nombre de personnes ayant accès aux registres distribués rend illusoire de conférer à chacun la qualité de responsable, serait de considérer que personne n'est responsable, et que dès lors le règlement reste privé d'une partie de son effectivité, faute de personnes pouvant être tenues du non-respect des principes et dispositions de ce règlement[75].

La dimension transfrontière des réseaux utilisant la blockchain obligera à appliquer la réglementation des flux transfrontières. Vu l'impossibilité de déterminer *a priori* les destinataires et leur localisation, c'est à l'intérieur du DAO que devra se trouver le consensus pour respecter les principes et règles du RGDP. On soulignera également l'obligation de *Privacy Impact Assessment*, et les conséquences en cas de brèches de sécurité, imposées par le RGPD[76].

D'autres questions restent en suspens. Comment gérer le droit à la portabilité exigée par le règlement en son article 20, droit qui devrait permettre à chaque utilisateur de reprendre ses données et de passer d'une blockchain à une autre ? La question n'est pas prête d'être résolue, alors même que l'interopérabilité des blockchains reste à construire. Le droit à l'oubli qui permet d'exiger l'effacement des données pose également question alors même que l'économie de la technologie de la blockchain repose sur l'immutabilité des écritures conservées dans le registre : « comme a pu l'indiquer l'Open Data Institute (ODI) britannique, pour supprimer une donnée, il faudrait que plus de la moitié des nœuds du réseau travaillent ensemble pour reconstruire la chaîne de blocs depuis le moment où la donnée a été ajoutée. Et pendant ce temps de résilience, qui peut être relativement long selon la taille de la blockchain, la donnée n'est pas actualisée. Surtout, cela signifie que toutes les données postérieurement enregistrées sur la blockchain seraient supprimées. Le risque, pour l'ODI, est alors que les données fausses ou incomplètes restent simplement sur la blockchain afin d'éviter que les données postérieures soient endommagées et perturbent le fonctionnement des programmes »[77].

30. Blockchain : droits à la rectification et à l'effacement. — Un dernier point est souvent soulevé lorsqu'est admise l'applicabilité du RGPD : celui du droit à la rectification, droit traditionnel reconnu par l'article 16 du RGPD et celui plus nouveau, du droit à l'effacement[78], consacré par l'arrêt *Google Spain*[79] dans un premier temps et repris ensuite par l'article 17 du RGPD[80].

Le fonctionnement même de la blockchain, qui nécessite de garder trace dans les registres distribués de l'historique de toutes les transactions validées dans les blocs est incompatible avec la possibilité d'une rectification et d'un effacement. Toute rectification ou tout blocage d'accès rendraient totalement impossible la preuve de l'ensemble des transactions et nuirait ainsi à l'ensemble des utilisateurs de la blockchain[81]. Il semble donc que le fonctionnement de la blockchain exige une exception à ces droits à la rectification et à l'effacement. Cette exception ne paraît pas pouvoir être trouvée dans la liste des exceptions prévues à l'article 17, § 3[82], qui visent des hypothèses différentes, ni dans la renonciation des personnes, même informées, à l'exercice de leur droit à la rétractation et à l'effacement[83]. On doit la trouver, comme l'article 23 le prescrit, dans les mesures législatives consacrant le droit de l'autorité publique à limiter les droits de la personne concernée lorsque l'intérêt supérieur de tiers (y compris de l'initiateur de la blockchain) est en jeu[84]. Si tel était le fondement retenu par les autorités européennes, l'article 23, § 2, du RGPD exige que le texte législatif prévoie des garanties. À tout le moins, devrait y figurer l'obligation d'information de toutes les personnes intéressées par l'utilisation de la blockchain, de cette limitation de ses droits à la rétractation et à l'effacement et sans doute, la condition de ne point faire figurer dans le registre décentralisé certaines données sensibles[85] ou le

(73) Voy. l'exemple de la communauté de personnes privées mutualisant leurs risques.
(74) À cet égard et dans le même sens, V.L. Sloan, « Privacy en blockchain : wanneer is er voor wie privacy werk aan de winkel ? », *Tijdschrift voor Internetrecht*, 2017, pp. 7 et s. L'auteur y discute longuement l'avis 1/2010 sur les concepts « responsables du traitement » et « sous-traitant », Working Paper 160, émis par le Groupe de l'article 29 le 16 février 2010.
(75) L'hypothèse est envisagée par V.L. Sloan (*ibidem*), même si ce dernier conclut peut-être trop vite que le règlement n'est pas applicable. À notre avis, il le reste dans la mesure où les autorités de contrôle peuvent veiller au respect des principes et dispositions et intervenir au cas où une blockchain sans responsable violerait le règlement.
(76) Respectivement, les articles 35 et 33 du RGPD.
(77) *Cfr* http://www.droit-blockchain.fr/blockchain-vie-privee/.
(78) Sur cette question, en particulier, P. de Filippi et M. Reymond, *op. cit.*, pp. 81-96.
(79) C.J.U.E., 13 mai 2014, *Google Spain et Google Inc. c. AEPD et Mario Costeja Gonzàlez*, C-131/12.
(80) Selon le RGPD, « la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique :
» a) les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;
» b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, § 1, point a), ou à l'article 9, § 2, point a), et il n'existe pas d'autre fondement juridique au traitement ;
» c) la personne concernée s'oppose au traitement en vertu de l'article 21, § 1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 2 ; ... ».
(81) « Dans la mesure où la blockchain est inaltérable et résistante à la censure et à la modification par conception, elle entre en conflit direct avec le droit à l'oubli » (P. de Filippi et M. Reymond, *op. cit.*, pp. 81-96).
(82) Ces exceptions, si elles existent en matière d'effacement, n'existe pas en matière de rectification.
(83) Il nous paraît en effet impensable que le droit puisse accepter la renonciation par soi-même à l'exercice d'un droit subjectif qu'il a lui-même créé. À cet égard, *contra*, l'article « Blockchain et vie privée » paru sur le site Blockchain et Droit (http://www.droit-blockchain.fr/blockchain-vie-privee/) qui affirme : « Si la définition de la blockchain semble incompatible avec le droit à l'effacement, existe-t-il des solutions permettant de remédier à cette situation ? À défaut de modification du GDPR, il nous semble qu'à partir du moment où une personne concernée serait clairement et préalablement informée qu'en cas de participation à une blockchain les conditions d'exercice de son droit à l'effacement sont rendues inapplicables, et que si cette renonciation est acceptée, ce droit à l'effacement pourrait devenir indisponible de manière légitime ».
(84) « Le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent, par la voie de mesures législatives, limiter la portée des obligations et des droits prévus aux articles 12 à 22 et à l'article 34, ainsi qu'à l'article 5 dans la mesure où les dispositions du droit en question correspondent aux droits et obligations prévus aux articles 12 à 22, lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir... les droits et libertés d'autrui » (article 23, § 2, du RGPD).
(85) Ainsi, le rapport de la STOA suggère que les données sensibles et en tout cas de santé ne puissent apparaître (*op. cit.*, p. 4).

contenu de transactions permettant une identifiabilité facile[86]. D'autres réflexions existent encore à ce sujet mais elles apparaissent peu réalistes au regard du fonctionnement des blockchains[87].

A contrario, nonobstant la définition précitée, une blockchain peut être modifiée par le consensus de sa communauté, notamment pour la corriger ou la faire évoluer, comme le démontre la récente décision de scission du bitcoin en 2017 ou la révision du *The DAO* d'Ethereum en 2016. Les communautés pourraient donc décider d'organiser pour des opérations délicates ce droit à l'effacement ou en tout cas en réglementer l'accès.

En conclusion, on reprendra cette réflexion tirée d'un article récent de spécialistes de la vie privée[88] « So, as with many issues that arise in data protection law, the appropriate answer to the question of whether a blockchain may be used to process personal data is not binary but rather "it depends" ».

3. Blockchain et responsabilité

31. Une activité génératrice de risques et, potentiellement, de responsabilités. — Dans le meilleur des mondes, et partant du principe qu'elle fonctionne de manière optimale au bénéfice de tous les acteurs concernés, la blockchain présente de nombreux atouts. Cette vision est évidemment théorique et, en pratique, il faut naturellement constater que, comme toute technologie, elle peut présenter des défauts (en termes de programmation ou de conception, notamment[89]), faire l'objet d'attaques informatiques[90] (avec une possible altération ou perte de données), voire être utilisée par certaines personnes pour commettre des actes illicites (des arnaques en matière d'ICO[91], par exemple).

Il s'agit donc d'une technologie génératrice de risques, pour des individus (ou des groupes d'individus) particuliers, et/ou pour la société en général. Des utilisateurs de la blockchain peuvent en effet subir un dommage lié à l'utilisation de celle-ci (perte financière, violation de données à caractère personnel, exécution automatique, mais erronée, de certaines opérations via des *smart contracts*, etc.).

En droit de la responsabilité civile[92], qu'elle soit de nature contractuelle ou extracontractuelle, on considère généralement que, pour obtenir la réparation du dommage subi, il incombe à la victime d'apporter la triple preuve de l'existence d'une faute, d'un dommage et d'un lien de causalité entre les deux. Ce schéma général doit être complété par des régimes spécifiques de responsabilités (associés à des mécanismes d'assurance), établis par la loi ou consacrés par la jurisprudence à la faveur d'une interprétation de certaines dispositions particulières, en vue de protéger les victimes des préjudices et de garantir la réparation de ceux-ci[93]. On observe d'ailleurs que, dans certains cas, le législateur a eu le souci de faciliter la tâche de la victime établissant des régimes de responsabilité objective ou en canalisant la responsabilité sur un débiteur facilement identifiable et normalement solvable (et/ou assuré).

Encore faut-il vérifier si ces régimes sont adaptés à la réparation des préjudices potentiellement causés par la *blockchain* ou son utilisation.

32. Écueils à surmonter pour obtenir l'indemnisation d'un dommage. — En première analyse, on peut d'après nous identifier quatre principaux écueils à surmonter par la victime souhaitant obtenir l'indemnisation de son dommage.

Le *premier* tient à la complexité des opérations réalisées au moyen de la *blockchain*, qui peut impliquer de nombreux acteurs, dont le rôle respectif n'est guère facile à caractériser. Dans l'exemple du bitcoin, il faut ainsi avoir égard aux parties à la transaction (Alice et Bob), aux mineurs ayant réalisé le *Proof of Work*, à toutes les personnes intervenant comme « nœuds » et, de manière générale, à la communauté bitcoin dans son ensemble — potentiellement, tous les membres qui en font partie — s'agissant d'un système totalement décentralisé. L'analyse est un peu différente pour Ethereum, qui se présente davantage comme une plateforme, mettant divers outils à la disposition de ses utilisateurs en vue de concevoir des *smart contracts*. Ethereum veille d'ailleurs à s'identifier — Ethereum Fondation, relevant du droit suisse[94]. Pour le reste, on peut distinguer différents acteurs : le concepteur du *smart contract*, le prestataire qui propose d'y recourir, les parties à la transaction initiale (et donc, au *smart contract*), l'oracle, voire la communauté Ethereum dans son ensemble (avec tous les membres — les nœuds — qui la constituent). Sans doute l'exercice est-il moins ardu lorsqu'il ne s'agit pas d'une blockchain publique, mais d'une blockchain privée ou de consortium, dans laquelle un prestataire (ou un groupe de prestataires, issus du monde bancaire, par exemple) se détache plus précisément, et fixe des règles claires.

À ce premier écueil lié à la diversité des acteurs, s'ajoute celui né de la mise en œuvre de différents régimes de responsabilité civile applicables, à commencer par la distinction entre un régime de responsabilité contractuelle ou extracontractuelle, voire des règles *ad hoc* (comme la responsabilité du fait des produits défectueux ou le système de responsabilité prévu par le RGPD, par exemple). Il faudra par ailleurs se demander si les dispositions légales ou réglementaires applicables ont été respectées (ce qui pourra donner lieu à discussions, vu la structuration complexe de certains montages, spécialement en droit financier — pour les ICOs, par exemple) ou si le manque d'information au stade précontractuel, voire l'erreur de programmation du *smart contract* constitue une faute susceptible d'engager la responsabilité de son auteur. On peut ainsi craindre que certains cas de figure suscitent moult discussions : *quid* si, par exemple, un nombre suffisant de nœuds — 51 % dans la blockchain bitcoin, par exemple — parviennent à s'entendre pour valider un bloc manifestement entaché d'irrégularité ? Qu'en est-il également de l'erreur de programmation tellement subtile qu'elle aurait pu être commise par un développeur normalement prudent et diligent ? Il appartiendra à la jurisprudence de se prononcer au cas par cas, le cas échéant, avec l'éclairage bienvenu d'un expert[95]. On ajoute que dans ce contexte, les parties identifiées (un programmeur ou le responsable d'une blockchain privée) chercheront généralement à se prévaloir de clauses limitatives ou exonératoires de responsabilité, figurant dans leurs Conditions générales[96].

On peut également se demander si certains intervenants pourraient invoquer le bénéfice du régime d'exonération de responsabilité, établi aux articles XII.15 et suivants du Code de droit économique[97]. On pourrait par exemple y songer pour Ethereum, dans son activité de plateforme fournissant aux utilisateurs des outils à l'aide desquels ils peuvent ensuite concevoir des *smart contracts*. Encore faudrait-il dé-

(86) « Imaginons une plateforme fictive basée sur la blockchain qui fonctionnerait comme un LinkedIn décentralisé, nourri par les contributions de ses utilisateurs. Cette blockchain serait un registre dans lequel n'importe qui pourrait ajouter des informations au sujet d'une personne en particulier — par exemple, en fournissant des liens vers un contenu déjà disponible sur internet. Toute personne qui souhaiterait en savoir plus sur un individu pourrait parcourir le contenu accumulé par l'entièreté des utilisateurs. Dans un tel scénario, il va sans dire que le droit à l'oubli pourrait légitimement être invoqué, car ce service permettrait à n'importe qui d'accéder à une sorte de profil public de la personne » (P. DE FILIPPI et M. REYMOND, *op. cit.*, pp. 81-96).
(87) Voy. par exemple l'article « Blockchain et vie privée », sur le site http ://www.droit-blockchain.fr/blockchain-vie-privee/.
(88) C. KUNER, F. CATE e.a., « Blockchain versus data protection », *Int. Data Privacy Law*, 2018, vol. 8, n° 2, p. 104.
(89) Voy. à cet égard la mise en garde affichée sur la page web présentant « Solidity », le langage de programmation à utiliser sur Ethereum pour concevoir les *smart contracts* : *since software is written by humans, it can have bugs. Thus, also smart contracts should be created following well-known bepractices in software development. This includes code review, testing, audits and correctness proofs. Also note that users are sometimes more confident in code than its authors. Finally, blockchains have their own things to watch out for, so please take a look at the section Security Considerations* (https://solidity.readthedocs.io/en/v0.4.24/).
(90) Ou d'une exploitation opportune de certaines failles du code informatique, comme avec The DAO d'Ethereum en 2016.
(91) *Infra*, nos 43 et s.
(92) À ce sujet, voy. les réflexions de T.F.E. TJONG TJIN TAI, « Juridische aspekten van blockchain en smart contracts », *T.P.R.*, 2017, pp. 595 et s. ; H. SCHURINGA, « Enkele civielrechterlijke aspecten van blockchain », *Computerrecht*, 2017, p. 375.
(93) Voy. par exemple la présomption de responsabilité du fait des choses (article 1384, alinéa 1er, C. civ.) ou la loi du 25 février 1991 relative à la responsabilité du fait des produits défectueux. À noter également, le régime particulier de responsabilité mis en œuvre par le principe d'*accountability* consacré par le RGPD (article 24) et entraînant un renversement de la charge de la preuve.
(94) https://www.ethereum.org/foundation.
(95) On pourra ainsi avoir égard à la jurisprudence rendue dans le domaine des contrats de l'informatique.
(96) Voy. a cet égard les clauses limitatives de responsabilité qui figurent dans les *Terms and Conditions* de la plateforme Ethereum : https://www.ethereum.org/terms-of-use.
(97) Ces dispositions permettent aux prestataires de services de la société de l'information de bénéficier d'une exonération de responsabilité civile et pénale pour certaines activités d'intermédiation (simple transport, stockage sous forme de copie temporaire des données et hébergement).

montrer qu'il s'est comporté comme un prestataire intermédiaire et, suivant la jurisprudence de la Cour de justice, que son activité revêt un caractère « purement technique, automatique et passif », impliquant que ledit prestataire « n'a pas la connaissance ni le contrôle des informations transmises ou stockées »[98]. Ce n'est en effet que lorsque « le prestataire n'a pas joué un rôle actif de nature à lui confier une connaissance ou un contrôle des données stockées » qu'il peut être qualifié de la sorte et, moyennant le respect des autres conditions établies par la loi, bénéficier du régime d'exonération de responsabilité civile et pénale.

Le troisième écueil consiste à connaître l'identité des personnes susceptibles de voir leur responsabilité engagée, eu égard au régime de responsabilité civile à mettre en œuvre. L'exercice se révélera très difficile, pour ne pas dire impossible dans les blockchains publiques, comme le bitcoin, où les parties s'identifient au moyen de leur clé publique (et d'un pseudonyme). On rappellera que, de manière générale, des obligations d'identification s'imposent à toute entreprise[99], ainsi qu'aux prestataires d'un service de la société de l'information[100]. Des obligations de collaboration reposent d'ailleurs sur ceux-ci, notamment pour identifier les auteurs d'infractions[101]. Quant à la communauté des utilisateurs dans son ensemble, elle constitue tout au plus une association de fait qui ne dispose pas de la personnalité juridique et ne peut donc pas faire l'objet de poursuites devant les cours et tribunaux. Ici aussi, l'écueil sera sans doute plus facile à dépasser dans les blockchains privées ou de consortium, puisque le prestataire pourra normalement être identifié.

Enfin, le quatrième écueil, et non des moindres, tient au fait que, comme toute application qui utilise l'internet, la blockchain ne s'arrête normalement pas aux frontières des États. Aussi faut-il identifier la loi potentiellement applicable au rapport juridique considéré, ainsi que la juridiction compétente pour connaître d'un litige éventuel. Le cas échéant, le DAO renverra à des clauses de médiation ou à l'intervention d'*Alternative Dispute Resolution Mechanisms*(ADR)[102].

33. Quelle répartition des risques ? — S'il est difficile d'identifier un débiteur potentiellement responsable en cas de dommage subi, suffisamment solvable et établi dans un for autorisant les recours de manière raisonnable, cela signifie que l'utilisateur de la technologie blockchain devra assumer seul le risque d'un mauvais fonctionnement ou d'une fraude au sein de celle-ci[103].

À l'analyse, c'est principalement dans les blockchains publiques que le problème pourrait se poser : si l'utilisateur est suffisamment conscient du risque pris, sans doute peut-on accepter qu'il lui incombe de le supporter, dès lors qu'il est généralement un participant — et un bénéficiaire — du système, autorisé à peser, avec d'autres, pour imposer un nouveau consensus (même si son poids reste probablement très faible). Encore faut-il s'assurer qu'il est effectivement conscient des risques pris. C'est sans doute à ce niveau que le travail doit être accompli, comme l'ont bien compris les autorités publiques (*cfr* les nombreuses mises en garde, du SPF Économie ou de la FSMA, à propos des ICO - *infra*, n^os^ 42 et s.).

S'il s'agit par contre de blockchains de consortium ou de blockchains privées, dans lesquelles il sera possible d'identifier un ou plusieurs acteurs clés, publics ou privés, les règles de responsabilité civile seront sans doute plus facile à mobiliser (quoiqu'on peut s'attendre à ce que les acteurs limitent — autant que la loi l'autorise — leur responsabilité éventuelle par l'adoption de clauses contractuelles *ad hoc*, tout en invoquant le bénéfice des exonérations de responsabilité applicables aux prestataires intermédiaires). En outre, il est probable que ce prestataire tire un avantage économique du recours à la blockchain (davantage que les utilisateurs, d'ailleurs), ce qui pourrait justifier qu'il assume — au moins partiellement — la responsabilité du préjudice susceptible d'en résulter, le cas échéant en faisant appel à une compagnie d'assurance pour mutualiser le risque.

4. Blockchain et services de confiance ?

34. Du tiers de confiance à la « trust machine ». — Dans un système ouvert comme l'internet, où les parties ne se connaissent pas nécessairement, l'intervention d'un tiers, dit « de confiance », a paru requise pour lever certains obstacles formels. Plus précisément, l'intervention de ce tiers aux parties permettait de dématérialiser les procédures, en encadrant l'accomplissement de formalités, principales ou accessoires, avec un niveau élevé de sécurité juridique. C'est le cas pour la signature électronique, le cachet, le recommandé et l'horodatage électroniques, ainsi que pour l'archivage électronique (mais dans une moindre mesure)[104].

Le législateur (européen et belge) est intervenu à plusieurs reprises. Actuellement, il faut principalement avoir égard au règlement (UE) n^o^ 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 et abrogeant la directive 1999/93/CE[105] (ci-après, « règlement eIDAS »)[106]. En droit belge, il est complété par une loi du 21 juillet 2016[107] — généralement qualifiée de « Digital Act »[108].

Pour assurer la confiance, le moyen mobilisé par le législateur consiste à faire intervenir un tiers, dont les activités sont précisément réglementées. Le règlement eIDAS fait une distinction fondamentale entre les prestataires et les services de confiance qualifiés, d'une part, les prestataires et les services de confiance non qualifiés, d'autre part. Les premiers sont soumis à des exigences plus lourdes, sur le plan technique et réglementaire, avant de lancer leur activité et en cours d'exercice de celle-ci. Parallèlement, leurs utilisateurs bénéficient d'un niveau de sé-

(98) C.J.U.E., 23 mars 2010, *Google France et Google*, aff. jointes C-236/08 à C-238/08, § 113 ; C.J.U.E., 12 juillet 2011, *L'Oréal* e.a. *c. eBay*, aff. C-324/09, § 110 ; C.J.U.E., 11 septembre 2014, *Papasavvas*, aff. C-291/13, § 41.
(99) Articles III.74 et s. du C.D.E.
(100) Article XII.6 du C.D.E.
(101) Article XII.20, § 2, du C.D.E. Voy. également l'article 46*bis* du Code d'instruction criminelle, qui permet au procureur du Roi de requérir « de l'opérateur d'un réseau de communications électroniques, et de toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques », qu'il lui communique les données d'identification des utilisateurs de leurs services.
(102) Il s'agit de mécanismes privés de règlement des conflits. Dans tous les cas, il s'agit d'assurer un accès à des moyens simples, efficaces, rapides et peu onéreux de résoudre les litiges nationaux et transfrontaliers résultant de la vente de marchandises ou de la prestation de services. Ces mécanismes ont fait l'objet d'une directive européenne (directive 2013/11/UE du Parlement européen et du Conseil du 21 mai 2013 relative au règlement extrajudiciaire des litiges de consommation et modifiant le règlement (CE) n^o^ 2006/2004 et la directive 2009/22/CE, *J.O.U.E.* L 165/63 du 21 mai 2013), transposée dans le livre XVI du Code de droit économique.
(103) À terme, on peut d'ailleurs craindre que le modèle n'y survive pas, sauf à considérer que le risque ne se réalise pas (ou tellement rarement qu'il reste sans incidence sur la confiance des utilisateurs).
(104) Pour les autres formalités (document électronique, écrit ou mentions manuscrites), la sécurité juridique peut être garantie sans l'intervention d'un tiers de confiance, mais moyennant la consécration de principes directeurs, applicables par ailleurs aux autres services de confiance.
(105) *J.O.U.E.* L 257 du 28 août 2014.
(106) Pour une analyse du règlement, voy. D. Gobert, « Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : évolution ou révolution ? », *R.D.T.I.*, 2014/56, pp. 27 et s. ; H. Jacquemin, « Preuve et services de confiance dans l'environnement numérique », *in Pas de droit sans technologie*, Bruxelles, Larcier, 2015, pp. 41 et s. ; H. Jacquemin (dir.), *L'identification électronique et les services de confiance depuis le règlement eIDAS*, Bruxelles, Larcier, 2016, 425 p.
(107) Loi du 21 juillet 2016 mettant en œuvre et complétant le règlement (UE) n^o^ 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 et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII « Droit de l'économie électronique » du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique, *M.B.*, 28 septembre 2016. Pour un commentaire, voy. D. Gobert, « La loi belge du 21 juillet 2016 mettant en œuvre le règlement européen eIDAS et le complétant avec des règles sur l'archivage électronique : analyse approfondie », octobre 2016, publié sur www.droit-technologie.org ; H. Jacquemin, « Les services de confiance depuis le règlement eIDAS et la loi du 21 juillet 2016 », *J.T.*, 2017, pp. 197-209.
(108) Cette loi introduit, dans le livre XII du Code de droit économique (sur le droit de l'économie électronique), un titre 2, intitulé « certaines règles relatives au cadre juridique pour les services de confiance ». Il complète, à divers égards, le régime établi par le règlement eIDAS, en introduisant un régime spécifique pour l'archivage électronique, tout en précisant, de manière ponctuelle, divers éléments du cadre normatif applicable à la signature, au cachet, au recommandé et à l'horodatage électroniques.

curité juridique élevé, eu égard, notamment, aux présomptions que la loi institue en leur faveur.

Avec la blockchain, un tout autre modèle est promu : c'est en effet la technologie — et l'ensemble des éléments constitutifs, de nature technique et organisationnelle, qui la caractérisent (*supra*, n^os^ 4 et s.) — qui garantit un niveau de confiance suffisamment élevé. L'objectif est d'ailleurs de se passer de ce tiers de confiance, voire de tout intermédiaire de manière générale, spécialement pour se dispenser des coûts — généralement sous la forme de commissions — afférents à la fourniture de leurs services.

35. Certaines composantes de la blockchain constituent-elles des services de confiance soumis au règlement eIDAS ? — La blockchain s'appuie sur plusieurs modules technologiques également utilisés pour la fourniture de services de confiance. On pense à la technique du *hash* et à la cryptographie asymétrique (combinaison d'une clé privée et d'une clé publique). C'est le cas pour le bitcoin, où les parties ne sont pas identifiées dans la chaîne des blocs par leur nom mais par une clé publique, qui peut être vue comme un pseudonyme.

On sait par ailleurs que certains procédés de signature électronique reposent précisément sur la cryptographie asymétrique.

Il ne semble pas requis que, pour accéder aux blockchains publiques les plus connues, l'utilisateur fasse appel à un prestataire de service de confiance — qualifié ou non qualifié — soumis au règlement eIDAS. Cet utilisateur peut d'ailleurs être établi aux États-Unis ou ailleurs, où le cadre normatif est nettement moins développé.

Dans certaines blockchains privées ou de consortium, une telle exigence pourrait néanmoins être imposée, de manière à garantir l'identité des utilisateurs. On verra d'ailleurs qu'en matière financière, c'est désormais une obligation dans la 4^e^ directive AML, telle que modifiée par la directive 2018/843/UE (*infra*, n^o^ 39). Pour le prestataire de services d'authentification, l'application du règlement eIDAS constitue également une source d'obligations, plus ou moins lourdes suivant qu'il opte pour la qualification ou pas. S'il n'est pas qualifié et n'offre pas de tels services, les obligations restent relativement limitées. L'article 19, § 1^er^, du règlement impose aux prestataires qualifiés et aux prestataires non qualifiés de prendre « les mesures techniques et organisationnelles adéquates pour gérer les risques liés à la sécurité des services de confiance qu'ils fournissent. Compte tenu des évolutions technologiques les plus récentes, ces mesures garantissent que le niveau de sécurité est proportionné au degré de risque. Des mesures sont notamment prises en vue de prévenir et de limiter les conséquences d'incidents liés à la sécurité et d'informer les parties concernées des effets préjudiciables de tels incidents »[109]. De même, en cas d'atteinte à la sécurité ou de perte d'intégrité ayant une incidence importante sur le service fourni ou sur les données à caractère personnel qui y sont conservées, une obligation de notification pèse sur les prestataires, vis-à-vis de l'organe de contrôle[110] et, le cas échéant, des bénéficiaires des services de confiance concernés[111], conformément à l'article 19, § 2, du règlement. S'il est qualifié, les obligations sont nettement plus lourdes, avec une obligation d'audit de conformité et d'autorisation préalable, ainsi que des obligations spécifiques auxquelles il faut répondre (et notamment des obligations d'identification, pour la fourniture d'un service qualifié[112]).

On relève que l'utilisation d'un pseudonyme par les participants n'est pas forcément un obstacle : l'article 5, § 2, du règlement eIDAS confirme que, « sans préjudice de l'effet juridique donné aux pseudonymes au titre du droit national, l'utilisation de pseudonymes dans les transactions électroniques n'est pas interdite ». Le certificat de signature électronique vise d'ailleurs l'« attestation électronique qui associe les données de validation d'une signature électronique à une personne physique et confirme au moins le nom ou le pseudonyme de cette personne »[113] et diverses obligations doivent être respectées dans ce cadre[114]. Le Digital Act a complété celles-ci, en établissant, à l'article XII.26, alinéa 1^er^, du C.D.E., que « sans préjudice d'autres dispositions légales ou réglementaires, lorsque le titulaire d'un certificat de signature électronique utilise un pseudonyme, le prestataire de services de confiance ayant délivré le certificat est tenu de communiquer aux autorités administratives ou judiciaires compétentes, à leur demande, les informations relatives à l'identité du titulaire dont il dispose et nécessaires à la recherche et à la constatation d'infractions ».

36. La blockchain dans son ensemble constitue-t-elle un service de confiance ? — Au sens du règlement eIDAS, le prestataire de confiance est « une personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de confiance qualifié ou non qualifié »[115]. Le prestataire de service de confiance qualifié est également défini[116]. Le service de confiance est quant à lui « un service électronique normalement fourni contre rémunération qui consiste :

» a) en la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, de services d'envoi recommandé électronique et de certificats relatifs à ces services ; ou

» b) en la création, en la vérification et en la validation de certificats pour l'authentification de site internet ; ou

» c) en la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services »[117].

En droit belge, il faut ajouter le service d'archivage électronique, visé au livre XII du Code de droit économique.

Compte tenu de leurs fonctionnalités, certains services offerts à travers la blockchain sont comparables à des services de confiance : des informations sont en effet stockées dans la chaîne de blocs (s'agit-il dès lors d'un service d'archivage électronique[118] ?) ; l'enregistrement chronologique des opérations permet d'établir la date de celles-ci avec un niveau élevé de sécurité juridique (s'agit-il dès lors d'un service d'horodatage électronique[119] ?).

En les qualifiant de services de confiance, on leur impose de respecter les obligations prescrites par le règlement eIDAS et le livre XII du C.D.E. Pour les services de confiance non qualifiés, on relève le respect des exigences en matière de traitements de données à caractère personnel[120], l'accessibilité aux personnes handicapées[121] et les exigences de sécurité[122]. Pour ces dernières, il incombe notamment au prestataire de service de confiance de prendre des « mesures techniques et organisationnelles adéquates pour gérer les risques liés à la sécurité ». On comprend immédiatement que, dans l'environnement blockchain, l'exigence sera délicate à mettre en œuvre. Pour les blockchains publiques, qui reposent sur un réseau *peer-to-peer*, dans le cadre duquel les informations ne sont pas stockées dans une unité centrale (ou chez un prestataire de service de confiance identifié) mais distribuées à l'identique chez tous les participants (les nœuds), on ne peut pas identifier un (et un seul) prestataire de service, auquel il incomberait de respecter les règles. Sauf à considérer que tous les membres de la communauté, en ce qu'ils forment une association de fait sans personnalité juridique, doivent être qualifiés de prestataires de service de confiance, auxquels il incombe de respecter la législation applicable.

(109) Dans le même sens, renforçant cette obligation de prendre des mesures de sécurité, les articles 24 et s. du RGPD.
(110) Il peut aussi s'agir d'autres organes compétents (le règlement cite l'organisme national compétent en matière de sécurité de l'information ou l'autorité chargée de la protection des données, autrement dit la Commission de protection de la vie privée, pour la Belgique).
(111) Cette exigence ne s'impose que « lorsque l'atteinte à la sécurité ou la perte d'intégrité est susceptible de porter préjudice à une personne physique ou morale à laquelle le service de confiance a été fourni ».
(112) Article 24, § 1^er^, du règlement eIDAS.
(113) Article 3, 14^o^, du règlement eIDAS.
(114) Voy. l'article 32, § 1^er^, e), et le point c) de l'annexe 1, du règlement eIDAS.
(115) Article 3, 19^o^, du règlement eIDAS.
(116) Article 3, 20^o^, du règlement eIDAS. Le règlement désigne ainsi « un prestataire de service de confiance qui fournit un ou plusieurs services de confiance qualifiés et a obtenu de l'organe de contrôle le statut de qualifié ». Deux conditions, tenant à la nature du service fourni et à l'autorisation administrative dont le prestataire a fait l'objet, se dégagent ainsi de cette définition.
(117) Article 3, 16^o^, du règlement eIDAS.
(118) Le service d'archivage électronique est le « service de confiance supplémentaire à ceux visés par l'article 3, paragraphe 16, du règlement n^o^ 910/2014, qui consiste en la conservation de données électroniques ou la numérisation de documents papier, et qui est fourni par un prestataire de services de confiance au sens de l'article 3, § 19, du règlement n^o^ 910/2014 ou qui est exploité pour son propre compte par un organisme du secteur public ou une personne physique ou morale (article I.8, 17^o^, du C.D.E.).
(119) Le service d'horodatage électronique désigne « des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant » (article 3, 33^o^, du règlement eIDAS).
(120) Article 5 du règlement eIDAS.
(121) Article 15 du règlement eIDAS.
(122) Article 19 du règlement eIDAS.

En pratique, et spécialement pour la mise en œuvre des règles de responsabilité, on conçoit sans peine qu'une telle solution se heurtera à des obstacles importants (comment identifier les membres de la communauté ? quelle est la loi applicable ? ont-ils commis une faute ? etc.). Les difficultés sont sans doute plus surmontables dans l'hypothèse des blockchains privées où le réseau est normalement « fermé » et géré par une personne identifiée, qui établit les règles du jeu.

Pour refuser l'application des règles en matière de services de confiance, on pourrait plaider que le règlement ne « s'applique pas à la fourniture de services de confiance utilisés exclusivement dans des systèmes fermés résultant du droit national ou d'accords au sein d'un ensemble défini de participants »[123]. Pour une blockchain privée, où les règles sont établies à l'avance entre les participants, on pourrait en effet considérer qu'il s'agit d'un système fermé, ce qui exclut l'application du règlement eIDAS. Il en irait de même si le prestataire de service de confiance n'est pas établi sur le territoire de l'Union[124].

Même si les dispositions du règlement eIDAS ne sont pas d'application, on pourrait souhaiter, *de lege ferenda*, qu'un régime comparable — en termes de sécurité juridique — soit également offert aux parties qui conservent leurs données dans une blockchain plutôt qu'en recourant à un prestataire de service de confiance. Ladite blockchain devrait sans doute respecter certaines obligations, mais rien n'empêche que, sur le plan technique, les fonctionnalités attendues soient préservées avec un niveau de sécurité supérieur à celui d'un prestataire de services de confiance, même qualifié. Une autorité de certification pourrait ainsi garantir que certaines exigences sont préservées par la blockchain, lui attribuer un label, et offrir aux parties qui y recourent pour archiver leurs données ou horodater certaines opérations une sécurité juridique comparable à celles qui résulte du règlement eIDAS et du Digital Act.

Dans l'intervalle, on pourrait également imaginer qu'un prestataire de service de confiance décide d'utiliser la blockchain comme un moyen technique, parmi d'autres (la cryptographie asymétrique, par exemple), pour fournir son service. La fonction d'intégrité doit être préservée pour l'archivage électronique (spécialement s'il est qualifié[125]), l'horodatage électronique[126] et le recommandé électronique[127]. La fonction d'intégrité assurée par la blockchain — avec la conservation du *hash* des données archivées — pourrait ainsi être utilement utilisée par un prestataire de service de confiance pour fournir son service.

B. Questions spécifiques posées par la blockchain comme technologie sous-jacente dans le secteur financier ou les *smart contracts*

1. La blockchain comme technologie sous-jacente dans le domaine financier

37. Recours à la blockchain dans le secteur financier ?— C'est dans le domaine financier — avec le bitcoin — que la blockchain a connu ses premières applications majeures à partir de 2009. Depuis lors, d'autres crypto-monnaies ont été créées — Litecoin, Ether, Ripple, etc. — la pratique développant par ailleurs la création de jetons (appelés *tokens*), émis à l'occasion d'une ICO (*Initial Coins Offerings*).

Au-delà des risques posés par ces nouveaux services (et leur utilisation à des fins criminelles), ils posent des questions juridiques complexes, principalement en termes de qualification et de détermination des règles applicables (en droit bancaire et financier, en droit fiscal, etc.). Sans prétendre à l'exhaustivité, nous en abordons l'une ou l'autre succinctement, en analysant les crypto-monnaies (*infra*, n° 39), puis les ICO (*infra*, n° 42).

Parallèlement, il est important de souligner que les caractéristiques de la blockchain — en termes de sécurité — offrent des perspectives intéressantes au monde bancaire, spécialement pour prévenir les fraudes ou accomplir les obligations KYC qui leur incombent. Aussi ne s'étonne-t-on guère que plusieurs institutions bancaires de premier plan aient décidé de s'associer — *cfr* par exemple le consortium R3 — de manière à tirer parti des avantages de la blockchain.

38. Bitcoin et autres crypto-monnaies. — Le bitcoin est la crypto-monnaie la plus connue. On peut difficilement entrer dans les détails du fonctionnement du mécanisme. Rappelons tout au plus qu'elle a été créée en 2009, en pleine crise financière mondiale, laquelle était également une crise de confiance généralisée vis-à-vis du monde bancaire traditionnel. Elle s'appuie sur la technologie blockchain (qu'elle a contribué à faire connaître et qui s'est, par la suite, déclinée en de très nombreuses applications). Les composantes de la blockchain (décentralisation, pair à pair, cryptographie asymétrique, etc.) garantissent en effet un niveau élevé de sécurité et suscite suffisamment de confiance auprès des utilisateurs. Par ailleurs, elle est totalement affranchie des institutions financières classiques, ce qui certes correspond aux objectifs initiaux, mais aussi, et surtout, séduit les milieux criminogènes. Le bitcoin peut faire l'objet de transactions entre les utilisateurs, identifiés par leur clé publique — Alice transmet 1 bitcoin à Bob — la blockchain servant dans cette hypothèse de registre des transactions, pour vérifier qu'Alice possédait effectivement ledit bitcoin et acter que, désormais, il appartient à Bob. Des bitcoins sont également créés à chaque validation d'un bloc par un mineur, en rémunération du travail fourni (ce qu'on appelle le *Proof of Work*).

Les qualificatifs foisonnent : monnaie virtuelle, crypto-monnaie, crypto-actif, monnaie numérique, etc. Ils traduisent la difficulté à laquelle le monde du droit est confronté au moment de qualifier juridiquement le bitcoin et les autres crypto-monnaies.

L'exercice est pourtant indispensable, puisqu'il conditionne l'application de certains régimes, ressortissant au droit financier (en ce compris le volet relatif à la lutte contre le blanchiment d'argent) ou au droit fiscal. D'emblée, notons que le bitcoin — à l'instar des autres monnaies virtuelles — n'est pas une monnaie ayant cours légal en Belgique[128]. Seul l'euro possède cette qualité.

D'un point de vue monétaire et économique, la BCE confirme cette exclusion pour divers motifs : l'absence de garanties qui l'accompagne (puisqu'il n'est pas émis par une autorité publique centrale), l'impossibilité de pouvoir payer en bitcoin auprès de la plupart des commerçants, l'absence de protection des consommateurs en cas de fraude et le caractère volatile de sa valeur. Elle conclut qu'il s'agit davantage d'un « actif spéculatif. C'est un instrument sur lequel vous pouvez parier et réaliser un gain, en courant le risque de perdre votre placement »[129].

Il est néanmoins intéressant de noter qu'une définition juridique des « monnaies virtuelles » a récemment été introduite dans la directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins de

(123) Article 2, § 2, du règlement eIDAS. Le considérant n° 21 du règlement donne l'exemple des « systèmes institués par des entreprises ou des administrations publiques pour gérer les procédures internes et utilisant des services de confiance [qui] ne devraient pas être soumis aux exigences du présent règlement », tout en précisant que « seuls les services de confiance fournis au public ayant des effets sur les tiers devraient remplir les exigences du présent règlement ». Conformément au principe de la liberté contractuelle, les parties pourraient donc décider, conventionnellement, de reconnaître des effets juridiques à un procédé de signature électronique ou d'horodatage électronique qui ne satisfait pas aux conditions du règlement.

(124) Sauf application du principe de reconnaissance mutuelle prévu à l'article 14 du règlement eIDAS.

(125) Le service d'archivage électronique est défini comme le « service de confiance supplémentaire à ceux visés par l'article 3, § 16, du règlement n° 910/2014, qui consiste en la conservation de données électroniques ou la numérisation de documents papier, et qui est fourni par un prestataire de services de confiance au sens de l'article 3, § 19, du règlement n° 910/2014 ou qui est exploité pour son propre compte par un organisme du secteur public ou une personne physique ou morale ». S'agissant du service d'archivage électronique qualifié, la loi présume que les données ont été conservées de « manière à les préserver de toute modification, sous réserve des modifications relatives à leur support ou leur format électronique » (article XII.25, § 5, alinéa 2, du C.D.E.).

(126) Article 41, § 2, du règlement eIDAS.

(127) Article 43, § 2, du règlement eIDAS.

(128) *Cfr* l'article 128 du TFUE.

(129) BCE, « Qu'est-ce que le bitcoin », https://www.ecb.europa.eu/explainers/tell-me/html/what-is-bitcoin.fr.html. Voy. aussi J.-L. Verhelst, *Bitcoin, Blockchain and beyond*, *op. cit.*, pp. 132 à 152. L'auteur conclut : *Bitcoin is not (yet) money and not (yet) a currency. It seems that Bitcoin behaves as a safe haven in short periods of heightened econmic uncertainty. Cryptocurrencies, in general, have the potential to become currencies if widely accepted*. Une décision récente d'un tribunal hollandais qualifie une crypto-monnaie de *vermogensrecht* (sur cette décision et son commentaire, lire W. Weij et M.C. Landerhartshold, « Ruis in de ether en de juridische kwalificatie(s) van cryptovaluta », *Tijdschrift voor Internetsrecht*, 2018, p. 66).

blanchiment de capitaux ou du financement du terrorisme[130] (ci-après, 4e directive AML — *Anti-Money Laundering*), telle que modifiée par la directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018[131]. Sont ainsi visées les « représentations numériques d'une valeur qui ne sont émises ou garanties ni par une banque centrale ni par une autorité publique, qui ne sont pas nécessairement liées non plus à une monnaie établie légalement et qui ne possèdent pas le statut juridique de monnaie ou d'argent, mais qui sont acceptées comme moyen d'échange par des personnes physiques ou morales et qui peuvent être transférées, stockées et échangées par voie électronique »[132]. Le législateur européen crée ainsi une définition de la notion pour la distinguer d'autres termes (« monnaie », « monnaie électronique », etc.)[133].

39. Enjeux juridiques et qualification. — Lorsqu'il est question du bitcoin, deux éléments caractéristiques sont généralement cités : la volatilité de son cours (par rapport à sa contre-valeur en devise traditionnelle), susceptible d'engendrer de généreuses plus-values ou des pertes retentissantes, d'une part ; les arnaques dont il fait l'objet et son utilisation, comme outil de transaction, dans un environnement criminel, d'autre part. Dans le premier cas, c'est principalement sous l'angle du droit fiscal que l'analyse — et la qualification — devra se faire ; dans l'autre, il conviendra de mobiliser les dispositions de droit (pénal) financier visant notamment à lutter contre le blanchiment ou le financement du terrorisme. Nous les examinons successivement.

40. Qualification en droit fiscal. — Les hauts et les bas du cours du bitcoin sont régulièrement rapportés par la presse spécialisée : évalué à 2.500 EUR en juillet 2017, il a dépassé les 15.000 EUR en décembre de la même année, avant de chuter à moins de 5.500 EUR, en février 2018. Aussi la question s'est-elle posée de la qualification, en droit fiscal, des opérations réalisées sur le bitcoin et des gains éventuellement obtenus suite à sa conversion en devise traditionnelle.

La Cour de justice de l'Union européenne a ainsi été saisie sur question préjudicielle, dans un litige opposant les autorités fiscales suédoises à M. Hedqvist, qui souhaite fournir des services d'échanges de devises traditionnelles contre du bitcoin (et inversement). La Cour rappelle d'abord que « la devise virtuelle "bitcoin" fait partie des devises virtuelles dites "à flux bi-directionnel", que les utilisateurs peuvent acheter et vendre sur la base de taux de change. De telles devises virtuelles sont analogues aux autres devises échangeables s'agissant de leur usage dans le monde réel »[134]. Elle décide que le bitcoin n'est pas un bien corporel et, dès lors, que les opérations d'échanges des bitcoins contre des devises traditionnelles (et inversement) ne constituent pas des livraisons de biens mais des prestations de services qui, en l'occurrence, sont effectuées à titre onéreux[135]. Elle ajoute que la différence entre « d'une part, le prix auquel l'opérateur concerné achète les devises et, d'autre part, le prix auquel il les vend à ses clients » est exonérée de T.V.A.[136].

Quant à l'imposition éventuelle des plus-values réalisées suite aux opérations d'achat-vente ou de conversion de bitcoins, elle varierait, en Belgique, entre 0 et 33 %, suivant qu'il s'agit d'une gestion normale de son patrimoine privé, en bon père de famille ou, au contraire, d'un acte de spéculation imposable au titre des revenus divers[137] (tenant compte notamment du montant investi, de la durée et de la fréquence des opérations)[138]. Quant aux bitcoins alloués aux mineurs, ils sont considérés comme des revenus professionnels et incorporés dans le revenu imposable globalement. On peut toutefois craindre que les contribuables ne déclarent pas spontanément les revenus issus de leurs spéculations en bitcoins et, eu égard à l'anonymat actuel des opérations et des acteurs, que l'administration fiscale éprouve de réelles difficultés pour les identifier et évaluer les gains obtenus.

L'espoir de gains — importants et rapides — a été instrumentalisé par certains escrocs, pour développer des arnaques au détriment des consommateurs, à travers des pseudo-plateformes d'investissement en crypto-monnaies, ou via de faux sites de *wallet* proposés aux consommateurs. Face à l'ampleur du phénomène, le SPF Économie a ainsi lancé une campagne d'information pour mettre en garde les consommateurs, à travers le site internet au nom évocateur « trop beau pour être vrai »[139].

41. Identification suivant la législation AML. — Eu égard à l'anonymat qui entoure les transactions en bitcoin, on ne s'étonne guère que les monnaies virtuelles soient fréquemment associées au blanchiment d'argent, au financement du terrorisme ou, plus globalement, à la criminalité organisée. La loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces, qui transpose en droit belge la 4e directive AML, impose toutefois aux entités assujetties, telles que listées à l'article 5 de la loi, diverses obligations de vigilance à l'égard des opérations et de la clientèle, parmi lesquelles figurent des exigences en termes d'identification et de vérification de l'identité (article 19 et s.).

Le dispositif normatif a été renforcé au niveau européen, suite aux modifications apportées à la 4e directive AML, par la directive 2018/843 du 30 mai 2018, de manière à viser expressément les monnaies virtuelles et les acteurs qui participent à leur émission et leur circulation. Le législateur européen définit non seulement les « monnaies virtuelles », mais également le « prestataire de services de portefeuille de conservation »[140], tout en imposant diverses obligations à celui-ci ainsi qu'aux prestataires de services d'échange de monnaies virtuelles. Comme le souligne le considérant no 7 de la directive 2018/843/UE, « les prestataires de services d'échange entre monnaies virtuelles et monnaies légales (c'est-à-dire les pièces de monnaie et les billets de banque désignés comme ayant cours légal et la monnaie électronique d'un pays, acceptés comme moyen d'échange dans le pays d'émission) ainsi que les prestataires de services de portefeuilles de conservation ne sont soumis à aucune obligation de la part de l'Union consistant à identifier les activités suspectes. Les groupes terroristes peuvent ainsi avoir la possibilité de transférer de l'argent dans le système financier de l'Union ou à l'intérieur des réseaux de monnaies virtuelles en dis-

(130) L'intitulé complet de la directive est : directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) no 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission.
(131) Directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les directives 2009/138/CE et 2013/36/UE. Les modifications introduites par cette directive devront être transposées par les États membres au plus tard le 10 janvier 2020.
(132) Nouvel article 3, 18o, de la 4e directive AML.
(133) Au considérant no 10 de la directive 2018/843/UE, on lit ainsi qu'« il convient de ne pas confondre les monnaies virtuelles avec la monnaie électronique au sens de l'article 2, point 2), de la directive 2009/110/CE du Parlement européen et du Conseil, ni avec la notion plus large de "fonds", définie à l'article 4, point 25), de la directive (UE) 2015/2366 du Parlement européen et du Conseil, ni avec la valeur monétaire stockée sur des instruments relevant des exclusions spécifiées à l'article 3, points k) et l), de la directive (UE) 2015/2366, ni avec les monnaies de jeu pouvant être uniquement utilisées dans un environnement donné de jeu. Bien que les monnaies virtuelles puissent souvent servir de moyens de paiement, elles pourraient également être utilisées à d'autres fins et trouver des applications plus larges telles que servir de moyens d'échange, d'instruments d'investissement, de réserves de valeur ou être utilisées dans les casinos en ligne. La présente directive vise à englober l'ensemble des utilisations possibles des monnaies virtuelles ».
(134) C.J.U.E., 22 octobre 2015, *Skatteverket*, C-264/14, point 12.
(135) *Ibidem*, points 24 et s.
(136) *Ibidem*, point 57.
(137) Le Bulletin d'information des SDA de janvier 2018 (https://www.ruling.be/sites/default/files/content/download/files/nieuwsbrief_sda_3_fr.pdf) donne ainsi l'exemple d'un étudiant qui a conçu une application informatique pour acheter et vendre des bitcoins de manière automatique. À cet égard, « le SDA a décidé que les plus-values que le demandeur réalise sur la vente de Bitcoins au moyen d'une application qu'il a lui-même développée, ne doivent pas être considérées comme des revenus professionnels au sens de l'article 23 du C.I.R. 92, mais vu le caractère spéculatif, sont imposables à titre de revenus divers conformément à l'article 90, 1o, du C.I.R. 92 ».
(138) Pour l'établir, le Service des Décisions Anticipées du SPF Finances a ainsi conçu et diffusé une liste de 17 questions dont les réponses lui permettront d'établir le régime fiscal applicable. La liste des questions est accessible en ligne : https://www.ruling.be/sites/default/files/content/download/files/liste_de_questions_crypto-monnaies_0.pdf. Sur ce point, voy. aussi « Comment déclarer vos plus-values sur le bitcoin ? », *L'Écho*, 22 mai 2018.
(139) https://tropbeaupouretre-vrai.be/.
(140) Celui-ci désigne l'« entité fournissant des services de conservation de clés cryptographiques privées pour le compte de ses clients à des fins de détention, de stockage et de transfert de monnaies virtuelles » (article 2, 19o, de la 4e directive AML).

simulant les transferts ou en bénéficiant d'un certain degré d'anonymat sur ces plates-formes. Il est dès lors indispensable d'étendre le champ d'application de la directive (UE) 2015/849 afin d'inclure les prestataires de services d'échange entre monnaies virtuelles et monnaies légales ainsi que les prestataires de services de portefeuilles de conservation. Aux fins de la lutte contre le blanchiment de capitaux et le financement du terrorisme, les autorités compétentes devraient pouvoir, par le biais d'entités assujetties, surveiller l'utilisation des monnaies virtuelles. Cette surveillance permettrait d'adopter une approche équilibrée et proportionnelle, préservant les progrès techniques et le haut degré de transparence atteints dans le domaine de la finance de substitution et de l'entrepreneuriat social ». Les prestataires de services de portefeuille de conservation ainsi que les prestataires de services d'échange de monnaies virtuelles sont ainsi tenus à une obligation d'immatriculation[141], et ils figurent dans la liste des entités assujetties[142], tenues notamment à des obligations de vigilance à l'égard des opérations et de la clientèle.

Ces mesures vont assurément dans le bon sens, même si elles ne permettront pas de garantir une transparence totale, ce dont le législateur est d'ailleurs conscient[143].

42. *Initial Coins Offerings* (ICO). — Les ICO — *Initial Coins Offerings*[144] — constituent une autre application de la technologie blockchain, dans le domaine financier. L'opération consiste à émettre des *tokens* (jetons) pour lever des fonds auprès du public. Le modèle connaît un succès grandissant puisqu'on évalue à plus de trois milliards de dollars les fonds récoltés par ce biais.

Au lieu de s'adresser aux institutions financières classiques, les start-ups ou autres porteurs de projets innovants, généralement actifs dans l'environnement de la blockchain et des crypto-monnaies, élaborent un document présentant leur projet (on parle de *white paper*), auquel des *advisors* — professionnels de la finance, du droit, des technologies innovantes — apportent leur soutien. Ces informations sont largement diffusées à travers les réseaux sociaux ; elles visent à convaincre le public de souscrire à l'émission de *tokens*, en échange des fonds investis le plus souvent en monnaie virtuelle. Les *tokens* font l'objet d'un *smart contract*, généralement déployé à travers la blockchain Ethereum. Comme le note un auteur, les *tokens* peuvent « représenter différents actifs numériques auxquels sont associés des droits financiers (*security tokens*), politiques, de propriété ou d'utilisation du bien ou service financé (*utility tokens*). Souscrire à un *token*, c'est ainsi souscrire à la prévente de services. Il peut s'agir de droits dans la gouvernance ou de droits à participation dans les bénéfices (*equity tokens*). Il peut aussi s'agir de *tokens* assis sur des actifs sous-jacents (*asset tokens*) »[145].

Comme dans les projets classiques de *crowdfunding*, les investisseurs bénéficient ainsi d'un accès privilégié au service, tout en détenant des *tokens* dont la valeur peut augmenter (laissant entrevoir d'intéressantes plus-values en cas de revente ultérieure)[146]. Si les avantages existent et sont bien réels, les risques le sont tout autant : au-delà des escroqueries pures et simples, les ICO restent des produits d'investissement : en y souscrivant, le consommateur doit accepter le risque de perdre la totalité du montant investi.

Ce risque est d'autant plus élevé, en l'espèce, qu'il s'agit de produits complexes (qui reposent sur des composantes — blockchain, crypto-monnaies, *smart contracts*, etc. — dont les caractéristiques sont rarement maîtrisées), extrêmement variés, et dont la soumission à la règlementation financière applicable reste discutée. Comme tout autre produit issu de la pratique, les ICO ne font pas (encore) l'objet de dispositions légales ou réglementaires spécifiques, même si, en fonction de leur structuration et de leurs caractéristiques, on ne peut pas exclure l'application de certaines règlementations ressortissant au droit financier (ce qui doit être vérifié au cas par cas). L'Autorité belge des Services et marchés financiers l'a ainsi rappelé dans une communication du 13 novembre 2017, citant notamment le règlement de la FSMA du 3 avril 2014 concernant l'interdiction de commercialisation de certains produits financiers auprès des clients de détail, la loi du 16 juin 2006 relative aux offres publiques d'instruments de placement et aux admissions d'instruments de placement à la négociation sur des marchés réglementés ou la loi du 18 décembre 2016 organisant la reconnaissance et l'encadrement du *crowdfunding* et portant des dispositions diverses en matière de finance[147]. À l'attention des consommateurs, elle rappelle d'ailleurs que les ICO peuvent échapper à tout encadrement normatif, susceptible de priver le consommateur/investisseur de toute protection. Parmi d'autres éléments, la FSMA pointe aussi les risques de fraude, le fait que les start-ups restent des entreprises à risques, le caractère subjectif et arbitraire de la valorisation de l'ICO par ses développeurs ou les risques spécifiques des crypto-monnaies. Elle souligne aussi que « les informations souvent sommaires, non standardisées, opaques, subjectives et non auditées fournies au sujet des ICO font qu'il est bien difficile d'estimer les risques qui y sont liés. Pour les personnes qui ne connaissent pas bien les technologies en ligne, les informations techniques et détaillées relatives à une ICO peuvent être incompréhensibles »[148] ; tout en rappelant qu'« il n'est nullement garanti que le projet sera effectivement mis sur le marché ni qu'il existe un marché pour cette technologie bien précise »[149]. À bon entendeur, ...

2. La blockchain comme technologie sous-jacente dans les *smart contracts*

43. De quoi le *smart contract* est-il le nom ? — L'expression *smart contract*, que l'on pourrait traduire en français par « contrat intelligent », est assurément ambiguë, dès lors qu'à l'analyse, il ne s'agit pas d'un « contrat » au sens juridique du terme et qu'il est loin d'être « intelligent ».

Le *smart contract* est un programme informatique dont l'exécution est automatisée, conformément aux instructions logicielles et algorithmiques inscrites dans la chaîne de blocs, et dont la fonction consiste à accomplir, sans intervention humaine, certaines opérations en lien avec l'exécution ou la dissolution d'un contrat, suivant la structure *if this... then that...*[150]. C'est à Nick Szabo que l'on attribue, dans les

(141) Article 47 de la 4e directive AML.
(142) Article 2, § 1er, g) et h), de la 4e directive AML.
(143) *Cfr* le considérant no 8 de la directive 2018/843/UE : « L'anonymat des monnaies virtuelles est susceptible de favoriser leur utilisation à des fins criminelles. L'inclusion des prestataires de services d'échange entre monnaies virtuelles et monnaies légales ainsi que des prestataires de services de portefeuilles de conservation ne résoudra pas complètement le problème de l'anonymat lié aux transactions en monnaies virtuelles, étant donné qu'une grande partie de l'environnement des monnaies virtuelles restera anonyme puisque les utilisateurs peuvent également effectuer des transactions sans passer par de tels prestataires. Pour lutter contre les risques liés à l'anonymat, les cellules de renseignement financier (CRF) nationales devraient être en mesure d'obtenir des informations leur permettant d'associer les adresses correspondant à la monnaie virtuelle à l'identité du propriétaire de la monnaie virtuelle. En outre, il convient d'examiner plus avant la possibilité de permettre aux utilisateurs de procéder à une auto-déclaration auprès des autorités désignées sur une base volontaire ».
(144) Il est aussi question de « Initial Token Sales », « Initial Token Offerings » ou « Crowdsales ».
(145) D. Legeais, « Regards sur une opération juridique non identifiée : les ICOs », *Dalloz IP/IT*, 2018, pp. 114-115. Voy. aussi la description donnée par le rapport du Groupe FinTech (*op. cit.*, p. 23) : « Depuis déjà plusieurs mois, fleurissent aux États Unis ou ailleurs des offres publiques d'une nature nouvelle,... parce qu'elles s'effectuent sous forme de crypto-monnaies, comme le Bitcoin (BTC) ou l'Ether (ETH). D'où leur nom : Initial Coin Offering (ICO), en référence aux Initial Public Offering (IPO). Ces opérations sont un mode de financement rapide —il faut de quelques jours à quelques heures pour lever les fonds — pour des entrepreneurs dans le monde de la DLT (Distributed Ledger Technology) leur permettant de tester leurs projets ou idées auprès de la communauté d'experts ».
(146) D. Legeais, « Regards sur une opération juridique non identifiée : les ICOs », *Dalloz IP/IT*, 2018, p. 115.
(147) FSMA, « "Initial Coins Offerings" (ICO) », communication FSMA_2017_20 du 13 novembre 2017, pp. 2-3.
(148) *Ibidem*, pp. 3-4.
(149) *Ibidem*.
(150) Pour une définition du *smart contract*, voy. J.-Ch. Roda, « Smart contracts, dumb contracts ? », *Dalloz IP-IT*, 2018, pp. 397 et s. (« les *smart contracts* sont présentés comme des programmes informatiques permettant d'exécuter automatiquement les termes du contrat »). Sur la notion et ses caractéristiques, voy. aussi M. Mekki, « Le contrat, objet des *smart contracts* (partie 1) », *Dalloz IP/IT*, 2018, pp. 409 et s. ou G. Guerlin, « Considérations sur les *smart contracts* », *Dalloz IP/IT*, 2017, pp. 512 et s. (« le *smart contract* est un programme informatique dont la fonction consiste à former, exécuter ou éteindre automatiquement un contrat qui, en toute hypothèse, ne se confond pas avec lui ») ; M. Raskin, « The Law and Legality of Smart Contracts », *Geo. L. Tech. Rev.*, 2017, p. 306 et pp. 309 et s. (*smart contracts are designed to ensure performance without recourse to the courts. Automation ensures performance, for better or worse, by excising human discretion from contract execution*).

années 1990, la paternité de l'expression *smart contract*[151], pour désigner la technologie permettant de sécuriser des échanges contractuels noués entre des parties qui ne se connaissent pas et, dès lors, ne se font pas confiance *a priori*. Le mécanisme n'est toutefois pas neuf[152]. Ce qui l'est, c'est d'inscrire le code dans la blockchain, pour renforcer la confiance. En pratique, les *smart contracts* peuvent par exemple être conçus dans la blockchain Ethereum, moyennant le recours au code Solidity[153].

44. Focus sur deux éléments caractéristiques des *smart contracts* et exemples. — Deux éléments caractérisent le *smart contract*.

On constate d'abord que le *smart contract* a souvent pour objet la phase d'exécution du contrat, rarement sa formation[154]. Deux exemples, souvent repris dans la littérature, permettent de l'illustrer : premier exemple, après un sinistre (une sécheresse exceptionnelle), attesté par un oracle (le service météo national), l'instruction est automatiquement donnée de verser l'indemnisation contractuellement prévue à l'agriculteur assuré ; deuxième exemple, moyennant le paiement convenu au titre de la location de l'appartement de vacances, le locataire reçoit le code permettant de déverrouiller la porte pendant la durée prévue. L'instruction peut également avoir pour objet de mettre en œuvre une sanction contractuelle en cas de non-respect, par l'une des parties, des obligations contractuelles qui lui incombent : on songe ici à l'immobilisation automatique d'un véhicule, l'échéance du leasing n'ayant pas été acquittée.

Dans ces diverses hypothèses, on suppose donc qu'au préalable, les volontés respectives des parties — ou leurs consentements — se sont rencontrées pour former valablement le contrat. Le *smart contract* n'est donc pas, à proprement parler, un contrat[155] : c'est davantage un moyen permettant de garantir son exécution (conformément aux termes convenus) — en privant les parties de toute intervention par laquelle elles pourraient refuser l'exécution, voire procéder à une exécution défectueuse ou tardive — ou de sanctionner son inexécution.

L'automatisation porte sur une instruction donnée par un programme d'ordinateur ou un algorithme, indépendamment de toute intervention humaine à cette étape du processus (c'est le second élément). Il s'agit donc de traduire en langage informatique les obligations des parties, de sorte qu'à un terme convenu, lors de la survenance d'un événement donné, voire sur confirmation d'un tiers (on parlera alors d'un oracle), la machine exécute automatiquement (et sans que les humains puissent *a priori* s'y opposer) ce que les parties avaient convenu. À cet égard, un auteur indique que « cette exécution peut être extrêmement complexe, et il n'existe en théorie pas de limitation technique à l'expressivité des conditions du contrat, dès lors que l'on peut les traduire en langage informatique »[156]. La nécessaire intervention de la machine tend néanmoins à limiter les hypothèses de *smart contracts* : s'il semble particulièrement indiqué pour initier des ordres de paiement, générer des commandes ou faire tout autre processus totalement dématérialisé, on le conçoit plus difficilement dans des circonstances requérant, matériellement, l'intervention d'une personne physique. Les progrès de l'intelligence artificielle ou de la robotique pourraient toutefois remettre en cause cette conclusion à moyen ou long terme.

Pour garantir l'intégrité des instructions exécutées automatiquement par la machine, indépendamment de toute intervention humaine, celles-ci sont stockées dans la blockchain. À la différence du bitcoin, pour lequel on enregistre dans la blockchain qu'« Alice a versé 1 BTC à Bob le 15 mai 2018 à 8 h 30 », il s'agira ici d'une instruction un peu plus complexe, et généralement conditionnelle (*if... then...*) : « *si* Alice a versé 100 EUR à Bob le 14 mai 2018, *alors* l'appartement XYZ sera déverrouillé et accessible à Alice du 15 mai 2018 au 20 mai 2018 ».

Les contrats qui s'exécutent de manière automatique, moyennant l'intervention d'une application d'intelligence artificielle (mais sans blockchain), sont nombreux en pratique[157]. Il faut toutefois avoir confiance en son cocontractant (et l'algorithme qu'il utilise), et espérer pour le reste que l'exécution aura lieu comme convenu. Une autre option est de faire intervenir un intermédiaire, jouant le rôle de tiers de confiance et censé rassurer les parties. La blockchain présente l'avantage de susciter la confiance, sans que l'intervention d'un tiers soit requise (la confiance résultant du recours à un système de registre distribué, dont la sécurité est garantie par le recours à la cryptographie asymétrique et un processus de validation)[158].

On comprend donc, en définitive, que le terme *smart* — intelligent — est un peu galvaudé[159] (ne l'est-il pas également quand on parle de smartphone, de smart TV ou de smart city ?) : l'exécution est automatique certes mais la machine ne fait que suivre les instructions données de manière totalement servile. En ce sens, elle ne fera que ce qui a été programmé par les parties, ni plus ni moins ; comme le pointe un auteur, « le *smart contract* ne gère ni l'imprévu, ni l'imprévision »[160].

45. Enjeux des *smart contracts* au moment de la formation des contrats. — Parmi les conditions de validité des conventions, listées à l'article 1108 du Code civil, figurent « le consentement de la partie qui s'oblige ; sa capacité de contracter ; un objet certain qui forme la matière de l'engagement ; une cause licite dans l'obligation ».

Dès lors que l'intervention automatique de la machine intervient au stade de l'exécution du contrat, et pas au moment de sa formation, le recours à la *blockchain* pour formaliser un *smart contract* ne soulève pas de difficulté particulière pour ce qui relève de la conclusion du contrat. On suppose en effet que les conditions de l'article 1108 du Code civil ont été observées (et donc, notamment, que les parties sont capables de contracter et que l'objet du contrat est parfaitement licite). Des difficultés pourraient survenir si des robots ou des applications d'intelligence artificielle interviennent également au moment de la conclusion du contrat. Cette éventualité n'est cependant pas propre à la blockchain, en ce sens que les mêmes questions se posent pour

(151) N. Szabo, « Smart Contracts : Formalizing and Securing Public Networks », First Monday, septembre 1997, n° 9 : « smart contracts combine protocols with user interfaces to formalize and secure relationships over computer networks. Objectives and principles for the design of these systems are derived from legal principles, economic theory, and theories of reliable and secure protocols ».
(152) Dans une version certes simplifiée, les distributeurs automatiques de boissons ou de friandises sont des exemples répandus de programmes qui s'auto-exécutent sans intervention humaine : si la somme requise est introduite dans la machine, celle-ci délivre le produit demandé, ce qui constitue l'exécution d'un contrat conclu entre l'utilisateur et la personne qui exploite la machine. Pour des réflexions en ce sens (en lien avec les *smart contracts*, voy. M. Raskin, « The Law and Legality of Smart Contracts », *Geo. L. Tech. Rev.*, 2017, pp. 315 et s.).
(153) https://solidity.readthedocs.io/en/v0.4.24/.
(154) Des auteurs pointent cependant que la technologie pourrait être utilisée pour optimiser la phase de formation du contrat, spécialement lorsque les parties doivent s'échanger divers documents contractuels (dans le domaine immobilier, la présentation de certificats de propriété, de documents notariés, etc., par exemple) : on peut en effet s'assurer que les documents requis ont été produits, et à quel moment (M. Mekki, « Le contrat, objet des *smart contracts* (partie 1) », *Dalloz IP/IT*, 2018, pp. 409 et s.). Il nous paraît toutefois que c'est davantage la fonction de « registre » qui est mobilisée ici, et pas le caractère auto-exécutant du *smart contract* (même en considérant que le contrat se forme automatiquement lorsque certains documents ont été produits, il s'agira d'une convention conclue sous condition suspensive de production de documents définis, dans laquelle il y aura en tout état de cause un échange préalable de consentements entre les parties).
(155) Voy. J.-Ch. Roda, « Smart contracts, dumb contracts ? », *Dalloz IP-IT*, 2018, pp. 397 et s. ; M. Mekki, « Le contrat, objet des *smart contracts* (partie 1) », *Dalloz IP/IT*, 2018, pp. 409 et s. (l'auteur note très justement que « le *smart contract* ne s'est pas substitué au contrat mais il s'est superposé à lui pour en optimiser la conclusion ou l'exécution ») ; G. Guerlin, « Considérations sur les *smart contracts* », *Dalloz IP/IT*, 2017, p. 514.
(156) J. Gossa, « Les blockchains et *smart contracts* pour les juristes », *Dalloz IT/IT*, 2018, pp. 393 et s.
(157) Outre l'hypothèse, précitée, du distributeur automatique de boissons ou de friandises, on peut donner l'exemple des sites internet de commerce électronique, qui valident automatiquement — et sans intervention humaine systématique — les commandes des utilisateurs lorsque des conditions prédéfinies ont été satisfaites (paiement reçu et biens en stock, par exemple).
(158) Cela ne signifie toutefois pas qu'il faut basculer, de manière générale et sans discernement, vers un système de blockchain : comme l'indique un auteur, « les blockchains permettent de recréer cette confiance, mais avec des coûts techniques, organisationnels, financiers et environnementaux non négligeables : les performances, notamment en termes de temps de traitement des transactions, seront toujours inférieures à celles d'un système traditionnel, et il faudra toujours trouver un moyen de motiver des pairs à investir dans le processus de minage » (J. Gossa, « Les blockchains et *smart contracts* pour les juristes », *Dalloz IT/IT*, 2018, pp. 393 et s.).
(159) Dans le même sens, M. van der Linden, « Het recht geketend : Smart Contracts : de oplossing voor gezeur, gedoe en onzekerheid ? », *Tijdschrift voor Internetsrecht*, 2018, p. 59 : « Smart Contracts : de oplossing voor alle problement ? ... "Als oudere jongere neig ik naar dat laatste ; bekijk dit ssort nieuwe ontwuikkelingen met de nodige skepsis. Lijkt het niet verdacht veel op oude wijn in nieuwe zakken ?" ».
(160) M. Mekki, « Le contrat, objet des *smart contracts* (partie 1) », *Dalloz IP/IT*, 2018, pp. 409 et s.

toute conclusion d'une convention à l'occasion de laquelle des machines sont intervenues (que le code soit ensuite inscrit dans une blockchain ou pas). On pourra en effet se poser la question de l'existence d'un consentement valable, tout en mobilisant divers mécanismes juridiques susceptibles de renforcer la sécurité juridique (la théorie de l'apparence, par exemple)[161].

En réalité, c'est surtout au moment de traduire la volonté des parties dans le code informatique que des problèmes pourraient être rencontrés[162]. Problèmes par ailleurs exacerbés par le fait que ce code deviendra la loi des parties (*code is law*, pour reprendre la formule de Lessig). L'une des parties pourrait ainsi être la victime d'un vice du consentement — l'erreur, voire le dol, en cas de manœuvres du cocontractant — susceptible de donner lieu à l'annulation du contrat. En cas de litige, il faudra analyser les circonstances de fait, pour décider si l'erreur était effectivement substantielle, commune et excusable.

Du reste, rien n'empêche aux parties de s'adresser au juge pour postuler la nullité de la convention. Reprenons l'exemple de la location d'un appartement de vacances. Suite au paiement, la serrure a été automatiquement débloquée à distance mais, lorsqu'il pénètre dans les lieux, le locataire considère que cela ne correspond pas à la description et qu'il a par conséquent été victime d'une erreur, voire d'un dol de la part du cocontractant[163].

46. Enjeux des *smart contracts* au moment de l'exécution des contrats. — Avec le *smart contract*, l'exécution du contrat devient automatique puisqu'elle résulte de la seule intervention d'un logiciel.

Le principe de la convention-loi — déposé à l'article 1134, alinéa 1er, du Code civil : « les conventions légalement formées tiennent lieu de loi à ceux qui les ont faites » — est ainsi consacré de manière quasi absolue. Si les conditions prédéfinies sont satisfaites, la machine procédera automatiquement à l'exécution des instructions convenues.

C'est assurément l'un des principaux avantages du *smart contract* : en pratique, il n'est en effet pas rare qu'un litige naisse entre les parties parce que l'une d'elles n'a pas exécuté les obligations qui lui incombaient conventionnellement. Aussi son cocontractant doit-il mobiliser les mécanismes que le droit met à sa disposition pour obtenir gain de cause, sans recourir au juge *a priori* (remplacement unilatéral, résolution unilatérale, exception d'inexécution), ou moyennant une intervention préalable de celui-ci (exécution forcée, le cas échéant sous astreinte, résolution judiciaire, exécution par équivalent). Avec le *smart contract*, on a normalement l'assurance que certaines obligations seront nécessairement exécutées, conformément à ce qui était prévu. C'est ainsi une manière d'en assurer l'exécution *ex ante*, pour éviter les coûts — probablement lourds — qu'impliquerait un recours en justice[164]. Pour le créancier de l'obligation formalisée dans le *smart contract*, le niveau de sécurité juridique est très élevé, en termes d'exécution, par son débiteur, de ladite obligation. Pour le dire autrement, le débiteur ne pourra normalement pas s'opposer à cette exécution, puisqu'elle ne dépendra pas de lui mais d'un logiciel qui donnera les instructions convenues.

L'avantage retiré par le créancier est, corrélativement, l'inconvénient majeur du débiteur. Sauf exception[165], c'est seulement *a posteriori* qu'il pourra se plaindre de l'exécution qui a été faite, en s'adressant aux cours et tribunaux, et en cherchant à obtenir la réparation du préjudice subi. L'exécution automatisée — et, en quelque sorte, aveugle de la machine — empêche en effet d'apprécier les circonstances de fait susceptibles d'être invoquées par l'une des parties pour s'opposer à celle-ci ou demander au juge des délais de grâce et, elles interdisent toute discussion sur la portée de tel ou tel terme (par exemple, l'expression « moyennant paiement attesté dans les 10 jours » renvoie-t-elle à 10 jours calendrier ou ouvrables ?). Or, la pratique montre justement que les cas d'espèce qui surviennent sont rarement d'une clarté limpide, excluant toute appréciation en fait ou toute interprétation en droit. On rappellera également que le principe de la convention-loi est loin d'être absolu, puisqu'il est assorti de limitations d'origine légale ou judiciaire[166]. Ainsi, si les termes d'un contrat constituent des clauses abusives au sens de l'article VI.83 du Code de droit économique, ou contreviennent à une disposition impérative ou d'ordre public (ressortissant par exemple au droit de la consommation), un magistrat saisi du litige pourra difficilement donner effet à de telles clauses par application du principe de la convention-loi.

Parmi les éléments qui peuvent être avancés par l'une des parties pour s'opposer à l'exécution du contrat conformément aux instructions écrites dans le code de la blockchain figure également la bonne foi, consacrée à l'article 1134, alinéa 3, du Code civil. C'est sur ce principe que la jurisprudence a construit la prohibition de l'abus de droit, en mobilisant la fonction modératrice de la bonne foi[167]. Les instructions contractuelles inscrites dans le code informatique pourraient en effet constituer un abus de droit : si c'est le cas, et comme l'a rappelé la Cour de cassation dans un arrêt récent du 2 février 2018, « la sanction en cas d'abus de droit lors de l'exercice de droits contractuels consiste à imposer l'exercice normal de ces droits ou à réparer le dommage résultant de cet abus. Lorsque l'exercice abusif de droits concerne l'application d'une clause contractuelle, la réparation peut consister à priver le créancier du droit de se prévaloir de la clause »[168].

Comme on l'imagine, ces limitations s'accommodent mal de la rigidité de la blockchain. Sauf à concevoir un code qui tient compte de celles-ci, les parties devront saisir les juridictions compétentes *a posteriori* pour être reconnues dans leurs droits et, le cas échéant, obtenir la réparation du préjudice subi.

Cette rigidité est par contre plus en phase avec le rejet actuel de la fonction adaptatrice de la bonne foi par la jurisprudence et — pour le moment en tout cas — de la théorie de l'imprévision[169]. À moins de traduire en code informatique les principes d'une clause de *hardship*, les parties seront confrontées à de réelles difficultés en cas de modification des circonstances postérieurement à la conclusion du contrat.

47. Enjeux des *smart contracts* comme sanction de l'inexécution des obligations contractuelles. — Le *smart contract* est également déployé pour y inscrire des sanctions de l'inexécution, par l'une des parties, de ses obligations contractuelles. On songe à une suspension des services en cas de non-paiement de ceux-ci, ou à la mise en œuvre automatique d'une clause pénale.

Ici aussi, le caractère automatique et, en principe irréversible, des instructions inscrites dans la blockchain s'accommode mal de la flexibilité que consacre le droit des obligations contemporain. Il est en effet douteux que certaines exigences — de nature plus subjective — comme le principe de proportionnalité, puissent être intégrées dans le code[170]. Imaginons que, suite à une erreur matérielle, le débiteur

(161) À ce sujet, voy. H. Jacquemin, « Comment lever l'insécurité juridique engendrée par le recours à l'intelligence artificielle lors du processus de formation du contrat ? », *in Droit, normes et libertés dans le cybermonde, Liber amicorum Yves Poullet*, Bruxelles, Larcier, 2018, pp. 141 et s. ; Y. Poullet, « Conclude a contract through electronic agents ? », *Electronic Commerce-Der Abschlub von Verträgen im Internet*, Baden-Baden, Nomos Verlagsgesellschaft, 2003, pp. 65-84.
(162) M. Raskin, « The Law and Legality of Smart Contracts », *Geo. L. Tech. Rev.*, 2017, pp. 326 et s. (l'auteur signale très opportunément que « the history of computing shows that programs do not always operate as their designers expect, but when the code is executed, the code does operate) ».
(163) On observe d'ailleurs que, dans le contexte de la *sharing economy*, l'intervention d'un prestataire intermédiaire (Uber, AirBnB, etc.) peut contribuer à la protection des parties. Elles pourront en effet s'adresser à lui en cas de souci, et bénéficier, le cas échéant, des services de médiation ou des assurances qu'il propose. Avec la blockchain, un tel intermédiaire n'existe plus ni, *a fortiori*, les services additionnels.
(164) M. Raskin, « The Law and Legality of Smart Contracts », *Geo. L. Tech. Rev.*, 2017, pp. 311-312.
(165) Pour les paiements, on pourrait en effet imaginer que le débiteur organise son insolvabilité en empêchant tout autre retrait sur le compte de paiement qui a été désigné.
(166) À ce sujet, voy. P. Wéry, *Droit des obligations*, vol. 1, *Théorie générale du contrat*, 2e éd., Bruxelles, Larcier, 2011, pp. 132 et s.
(167) Cass., 19 septembre 1983, *Pas.*, 1984, I, p. 55 : « le principe de l'exécution de bonne foi des conventions, consacré par l'article 1134 du Code civil, interdit à une partie à un contrat d'abuser des droits que lui confère celui-ci ».
(168) Cass., 2 mars 2018, *J.T.*, 2018, p. 462, note F. Glansdorff.
(169) On peut la définir comme « un concept qui autorise la révision du contrat en cas de survenance, postérieurement à la conclusion du contrat, de circonstances présentant les caractéristiques suivantes : être non imputables à la partie qui s'en prévaut ; être imprévisibles ; avoir pour effet le bouleversement de l'économie contractuelle » (D. Philippe, « L'imprévision », *J.T.*, 2007, p. 738).
(170) Voy. J.-Ch. Roda, « Smart contracts, dumb contracts ? », *Dalloz IP-IT*, 2018, pp. 397 et s., qui ajoute à cet égard que « la volonté affichée d'évincer le juge apparaît en opposition avec les tendances protectrices du droit contemporain » ; G. Guerlin, « Considérations sur les *smart contracts* », *Dalloz IP/IT*, 2017, p. 516.

d'un leasing pour une voiture ne paie pas les 550,50 EUR mensuels convenus, mais seulement 550 EUR. S'il est prévu de bloquer l'utilisation du véhicule en cas de non-paiement de la somme convenue (ce qui constitue une mise en œuvre, par le créancier, de l'exception d'inexécution), celle-ci devra normalement intervenir, le logiciel n'étant pas nécessairement en mesure d'apprécier le caractère disproportionné de la sanction, pour une différence de 0,50 EUR (en l'occurrence, nous postulons qu'il n'a pas été programmé en ce sens, ce qui aurait pu survenir). Or, l'exigence de proportionnalité constitue une condition d'application de l'exception d'inexécution. En cas de litige ultérieur, soumis aux cours et tribunaux, la juridiction saisie pourrait décider que la mesure mise en œuvre par le débiteur n'était pas conforme au prescrit légal et, par exemple, prononcer la résolution du contrat aux torts du créancier, ainsi que sa condamnation au paiement de dommages-intérêts, pour réparer le préjudice subi par le débiteur.

Une telle intervention *a posteriori* pourrait également survenir si la clause pénale constitue une clause abusive[171] ou si son caractère comminatoire est sanctionné par le juge conformément à l'article 1231 du Code civil.

Le *smart contract* traduit ainsi une vision ultralibérale des relations contractuelles, dans un but de réduction des coûts et de tout aléa engendré par l'intervention humaine[172]. Une telle conception est sans doute plus facilement acceptée en droit anglo-saxon que dans notre droit continental des contrats, où le législateur et la jurisprudence font la part belle à la protection du cocontractant le plus faible et au pouvoir d'appréciation et d'interprétation du juge.

48. Le mécanisme est-il si révolutionnaire ? — Les besoins de *stakeholders*, spécialement en droit économique, ont pu conduire par le passé (et conduisent encore, du reste) à la création de mécanismes originaux par les praticiens, que le droit a dû appréhender et intégrer, bon an, mal an, dans le système juridique.

Certains d'entre eux poursuivent des fonctionnalités similaires aux *smart contracts*, dont l'objectif est de revêtir l'obligation du débiteur d'une force obligatoire quasi absolue, de sorte qu'elle ne souffre en principe d'aucune discussion. On songe en particulier aux mécanismes du crédit documentaire ou de la garantie documentaire[173]. En ce qui concerne le crédit documentaire, l'objectif de ce moyen de paiement, utilisé dans le contexte des relations internationales, est de rassurer des parties (importateur/exportateur) qui ne se connaissent pas et nourrissent une méfiance réciproque, en faisant intervenir un tiers — une banque — qui procédera au paiement convenu moyennant la production de documents déterminés au préalable par la convention des parties. En principe, l'exécution de l'obligation de paiement de l'importateur ne souffrira aucune discussion : l'exportateur est ainsi rassuré, comme peut l'être le créancier qui se repose sur la blockchain pour garantir l'exécution automatique de l'engagement de son débiteur. L'intervention de la banque contribue également à assurer un niveau de confiance élevé des parties, eu égard au rôle neutre qu'elle accepte de jouer et à la crédibilité dont elle bénéficie[174]. La banque n'accepte cependant d'intervenir qu'à la condition de voir son rôle précisément circonscrit (vérifier des documents) et sans être prise à partie pour des discussions tenant à l'opération de base (la marchandise a-t-elle été livrée ? est-elle conforme ?). En ce sens, on insiste généralement sur le caractère littéral, autonome et abstrait de l'engagement pris par le banquier dans le crédit documentaire, par rapport au contrat sous-jacent[175]. Le donneur d'ordre ne pourrait donc pas lui opposer des exceptions tirées du contrat sous-jacent pour s'opposer au paiement. Seule une fraude évidente dans le chef du bénéficiaire, démontrée par le donneur d'ordre, pourrait conduire à la suspension du paiement. Avec la blockchain, c'est la technologie qui permet d'atteindre ces fonctions d'autonomie, d'abstraction et d'indépendance dans l'exécution de l'opération convenue. On pourrait d'ailleurs imaginer que la technologie blockchain, avec un *smart contract*, soit utilisée dans l'hypothèse d'un crédit documentaire. Quoi qu'il en soit la validité de l'opération de crédit documentaire est confirmée en droit, conformément au principe de la convention-loi, et rien n'empêche dès lors, *mutatis mutandis*, de reconnaître également la validité du *smart contract*. On relève néanmoins que le mécanisme est davantage mobilisé dans les relations entre professionnels.

On trouve un autre exemple d'opération automatisée, cette fois large public, semblable à la blockchain dans ses caractéristiques, avec le paiement par domiciliation[176]. Le mécanisme est bien connu : même si le montant n'est pas connu à l'avance, le titulaire du compte accepte que celui-ci soit débité à intervalle régulier de la somme demandée par le bénéficiaire, eu égard au contrat sous-jacent. Le risque existe néanmoins que le créancier — bénéficiaire — demande un paiement supérieur à celui qui est prévu contractuellement. Plusieurs garanties sont par conséquent introduites par le livre VII du Code de droit économique[177], de manière à protéger les intérêts du payeur. Le mandat donné par le payeur est ainsi soumis à des conditions de forme spécifiques (consentement exprès, signature, support durable, information sur le contrat sous-jacent[178]). *A posteriori*, le nouvel article VII.46, § 1er, du C.D.E. prévoit que « le prestataire de services de paiement du payeur doit rembourser au payeur une opération de paiement autorisée, initiée par ou via le bénéficiaire, qui a déjà été exécutée, pour autant que les deux conditions suivantes soient remplies : 1° l'autorisation n'indique pas le montant exact de l'opération de paiement lorsqu'elle a été donnée ; 2° le montant de l'opération de paiement dépasse le montant auquel le payeur peut raisonnablement s'attendre en tenant compte du profil de ses dépenses passées, des conditions prévues par son contrat-cadre et des circonstances pertinentes de l'affaire ». Il s'agit donc d'introduire un mécanisme correctif permettant au payeur d'être rétabli dans la situation antérieure. Des correctifs similaires pourraient être mis en œuvre dans l'environnement blockchain, pour permettre aux parties au *smart contract* d'obtenir un retour au *statu quo ante* en cas d'exécution automatisée dépassant manifestement ce qu'elles pouvaient légitimement attendre.

(171) Article VI.83, 13°, du C.D.E.
(172) M. Mekki, « Le contrat, objet des *smart contracts* (partie 1) », *Dalloz IP/IT*, 2018, pp. 409 et s. (l'auteur indique que « la philosophie de la blockchain, sur laquelle repose les *smart contracts*, est une philosophie libertaire qui prétend développer un monde sans État et sans droit étatique, un ordre juridique autonome, avec ses propres valeurs, ses propres principes et ses propres règles »).
(173) Il s'agit de « l'opération par laquelle la banque dite "émettrice" intervenant sur l'ordre d'un importateur pour le règlement financier d'une opération commerciale, le plus souvent internationale, s'engage à payer l'exportateur (ou son banquier qui peut intervenir comme banque "notificatrice" ou "confirmatrice") et ce, contre remise de documents dont la nature et le contenu sont en relation avec l'opération d'exportation (ainsi, les documents de transport, des certificats de qualité de la marchandise, la description et la quantité de produits, etc.) » (Y. De Cordt, C. Delforge, H. Jacquemin, Th. Léonard et Y. Poullet, *Manuel du droit de l'entreprise*, 3e éd., Limal, Anthemis, 2015, p. 286 ; *cfr* aussi D. Blommaert, « Les opérations de crédit », *in Traité pratique de droit commercial*, t. 5, *Droit bancaire et financier*, Diegem, Kluwer, 2016, pp. 403 et s.
(174) Sur ce besoin de confiance à la base des deux mécanismes bancaires, lire Y. Poullet, « Les garanties contractuelles dans le commerce international », *Droit et Pratique du Commerce International*, 1977, pp. 387-442.
(175) En ce sens, voy. notamment Gand, 24 juin 2009, *Bank Fin. R.*, 2010/4, p. 265 ; *NjW*, 2010, p. 672, note R. Steennot : « De verbintenis van KBC tot betaling aan de begunstigde van het documentair krediet heeft een onafhankelijk karakter. Deze onafhankelijkheid resulteert enerzijds uit het abstract karakter van de verbintenis van de bank ten aanzien van de overeenkomst tussen de koper-op-drachtgever en de bank, en anderzijds uit hetzelfstandig of niet-accessoir karakter van de verbintenis van de bank ten aanzien van de overeenkomst tussen de koper en de verkoper. [...] De verbintenis van de bank staat aldus autonoom ten opzichte van de onderliggende overeenkomst en van de verhouding tussen de betrokkene en de bank ». Voy. aussi Y. De Cordt, C. Delforge, H. Jacquemin, Th. Léonard et Y. Poullet, *Manuel du droit de l'entreprise*, 3e éd., Limal, Anthemis, 2015, p. 290 ; *cfr* aussi D. Blommaert, « Les opérations de crédit », *in Traité pratique de droit commercial*, t. 5, *Droit bancaire et financier*, Diegem, Kluwer, 2016, p. 405.
(176) Voy. la définition figurant à l'article I.9, 13°, du C.D.E. (« un service de paiement visant à débiter le compte de paiement d'un payeur, lorsqu'une opération de paiement est initiée par le bénéficiaire sur la base du consentement donné par le payeur au bénéficiaire, au prestataire de services de paiement du bénéficiaire ou au propre prestataire de services de paiement du payeur »).
(177) Ces dispositions ont été modifiées par une récente loi du 19 juillet 2018 portant modification et insertion de dispositions en matière de services de paiement dans différents livres du Code de droit économique, *M.B.*, 30 juillet 2018. Nous nous référons uniquement aux nouvelles dispositions (et à la nouvelle numérotation).
(178) Nouvel article VII.33, § 2, du C.D.E.

Conclusion : comment réguler la blockchain ?

49. Blockchain : une révolution ? une révolution du Droit ? — Notre introduction posait la question suivante : la blockchain et ses nombreuses applications constituent-elles une révolution pour la société et le Droit ? À l'heure où ces lignes sont écrites, la blockchain constitue une innovation qui cherche encore ses méthodes, ses applications et, en tout cas, à stabiliser celles qui sont à peine émergentes, comme le montre l'exemple du bitcoin. La question de l'interopérabilité entre les différents réseaux est soulevée et nécessitera une réponse rapide, faute de quoi les utilisateurs fuiront cette technologie qui les emprisonne dans un réseau[179]. Quoi qu'il en soit, la blockchain évoque le vieux rêve des bâtisseurs de l'internet, à savoir l'utilisation d'un réseau qui permettrait à chaque citoyen d'exercer ses libertés sans le contrôle d'une autorité centrale et, en particulier, de l'État (*supra*, n° 7). Certaines applications permettent d'envisager cet *empowerment* des citoyens vis-à-vis de l'État (*supra*, n° 18), des artistes vis-à-vis des sociétés de gestion des droits d'auteurs (*supra*, n° 14), etc., ou de se passer de certains intermédiaires (Uber, notaires, services de certification agréé, etc.) mais, comme l'ont montré les blockchains privées ou l'intervention des oracles, ces intermédiaires sont loin d'avoir disparu. Nos réflexions sur l'état des lieux témoignent cependant d'une récupération de la technologie, d'une part, par les pouvoirs privés, forts de l'argument de la globalisation, d'autre part, par l'État ; sans doute, est-ce dans le débat entre eux que l'avenir de cette technologie se joue. L'État, comme le montrent ses efforts en matière fiscale et financière (*supra*, n°s 39 et 40), souhaite reprendre le contrôle, non de la technologie, mais des opérations qui s'y jouent, du moins dans leurs aspects financiers et économiques.

50. Vers une nouvelle « *lex technologica* » ? — Au-delà, assiste-t-on, avec la technologie de la blockchain combinée à celle du *smart contract*, à la consécration de la *lex technologica* ou, comme certains auteurs la qualifient, de la *lex cryptographia*[180] ?

Le bilan de nos réflexions nous amène à en douter. Comme nous l'avons dit, à y regarder de près, si l'utilisation de la technologie exige une interprétation pas toujours aisée des textes législatifs existants comme le RGPD, ceux sur le droit d'auteur ou le règlement eIDAS, il n'y a pas, loin s'en faut, révolution. La figure présentée comme révolutionnaire du *smart contract*, elle-même, s'évanouit. La technologie ne remplace pas l'accord des parties, elle permet de mieux en garantir l'exécution dans un monde où la confiance ne s'obtient pas autrement. Il y a tout au plus sécurisation de l'exécution des contrats et, indéniablement — et sans doute cela pose question — renforcement de la force exécutoire des conventions (*supra*, n° 47).

Le mot « confiance » est le leitmotiv tant de l'intervention du droit que de sa non-intervention ; ainsi, lorsque la technologie de la blockchain crée un risque pour les citoyens comme en matière d'ICO (*supra*, n° 42), celui-ci intervient au nom de la nécessité de leur protection. À cet égard, nous avons souligné que l'absence de réponse adéquate en ce qui concerne la responsabilité des « acteurs » multiples de la blockchain constituait un obstacle sérieux à la confiance des utilisateurs (*supra*, n° 33).

Seconde question, faut-il, dès lors, réguler, de manière spécifique et sans attendre, ce phénomène de la blockchain ou le Droit et ses concepts peuvent-ils, à défaut de trouver dès maintenant des solutions, s'octroyer du temps pour prendre quelque recul devant ces innovations ?

À ce propos, deux réflexions : la première est de saluer la démarche de *Technology Assessment*, pratiquée par la STOA à la demande du Parlement européen. Il importe que nos législateurs prennent le temps du recul et analysent de manière multidisciplinaire la technologie, ses applications, son impact sociétaire, ses acteurs et les solutions envisageables, le cas échéant. Au-delà et précisément sur la base de cet état des lieux, il importe d'agir avec prudence. Le plaidoyer de nombre d'auteurs, à propos de la réglementation de la blockchain, pour des législations, qu'ils qualifient de législations « bac à sable »[181], nous apparaît fondé. Il s'agit, en ayant une vue positive de l'innovation, d'en favoriser certaines applications tout en encadrant celles-ci d'une réglementation purement provisoire soumise à évaluation. C'est à travers ces expérimentations et leurs évaluations, si possible menées au niveau européen, que doivent s'envisager l'évolution — et non la révolution — du, ou plutôt, des droits, que nécessite la blockchain.

Yves POULLET
Professeur ordinaire émérite à l'UNamur (CRIDS), co-président du NADI (Namur Digital Institute), membre de l'Académie royale de Belgique
Hervé JACQUEMIN
Chargé de cours à l'UNamur (CRIDS), membre du NADI, avocat au barreau de Bruxelles

(179) Sur cette question et l'avancement des travaux en cours en la matière, lire A. BRIDGWATER, « Blockchains Are Verticalizing, So We Need Interoperability », février 2018, disponible à l'adresse https://www.forbes.com/sites/adrianbridgwater/2018/02/07/blockchains-are-verticalizing-so-we-needinteroperability/#508687c87ab9.

(180) A. WRIGHT et P. DE FILIPPI, « Decentralized Blockchain Technology and the rise of Lex Cryptographia », Working paper, 2015, pp. 11-12, disponible sur http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664.

(181) Sur cette manière de procéder face à une innovation dont on a quelque peine à juger des risques et bénéfices et son application à la blockchain, lire l'excellent *paper* de M. FINCK, « Blockchain Regulation », Max Planck Institute for innovation and Competition Research Paper, n° 17-13, 2017. Lire également les réflexions de J. MAUPIN, « Mapping the Global Legal Landscape of Blockchain and Other Distributed Ledger Technologies », CIGI (Center for international Innovation Governance), Paper n° 149, octobre 2017 : *The term sandbox here takes its cue from the Financial Conduct Authority's (FCA's) recent initiative to set up a UK regulatory sandbox : a safe space in which fintech companies targeting UK markets can test out new technologies within a "light touch" regulatory environment under close government supervision and for a defined period*. En langue française, même réflexions, *in* N. DEVILLER, « Jouer dans le "bac à sable" réglementaire pour réguler l'innovation disruptive : le cas de la technologie de la chaîne des blocs », *R.T.D. com.*, 2017, pp. 1037 et s. ; T. VERBIEST, « Technologie de registres distribués : premières pistes de régulation », *R.L.D.I.*, 2016, n° 129, p. 52. ; L. DE MENEVAL et S. POIROT, « La blockchain, un nouveau paradigme pour le numérique », *Expertises*, 2017, pp. 51 et s.