

# Introduction

## Les aspects juridiques de la blockchain et de ses applications

Antoine VANDENBULKE

*Professeur (chargé de cours) à l'Université de Mons*

### Propos introductifs

1. Le présent ouvrage vise à proposer une analyse juridique de la blockchain et de ses applications. Ce phénomène, relativement récent, fait, en effet, encore peu l'objet d'études doctrinales, en tout cas en droit belge<sup>1</sup>.

L'ambition n'est pas de proposer une description approfondie de cette technologie<sup>2</sup>, mais d'appréhender juridiquement une réalité nouvelle. Cet ouvrage est principalement destiné aux juristes ou à toute autre personne intéressée par ces aspects juridiques, quelles que soient leurs compétences dans le domaine des technologies. L'objectif est de proposer une analyse suffisamment complète des questions posées, tout en restant accessible aux profanes de l'économie numérique.

2. Sur le plan de la réglementation, le droit a cette capacité hégémonique d'appréhender toute réalité nouvelle. À cette fin, deux méthodes semblent se dégager : soit le législateur décide de modifier le droit existant pour l'adapter aux technologies émergentes en élaborant des outils qui visent de manière spécifique le phénomène nouveau<sup>3</sup> ; soit le droit en vigueur dispose déjà des outils nécessaires, il suffit alors

---

<sup>1</sup> En langue française, on peut toutefois citer l'ouvrage collectif : H. JACQUEMIN, A. COTIGA et Y. POULLET, *Les blockchains et les smart contracts à l'épreuve du droit*, Bruxelles, Larcier, 2020 ; ou encore A. BEELEN, *Tout sur la blockchain et ses applications*, Limal, Anthemis, 2021, mais ce dernier traite plus des aspects techniques que des aspects juridiques à proprement parler. En langue néerlandaise, voy. not. M. DELANOTE et P. WAETERINCKX, *Cryptomunten juridisch ontsloten*, Mortsel, Intersentia, 2020 ; P.-J. AERTS, F. HOOGENDIJK et N. VANDEZANDE (éd.), *Smart contracts. Een overzicht vanuit juridisch perspectief*, Mortsel, Intersentia, 2020. En droit étranger, en revanche, cette problématique a déjà fait l'objet d'analyses juridiques approfondies ; voy. par exemple F. MARMOZ (éd.), *Blockchain et droit*, Paris, Dalloz, 2018 ; W. AZAN et G. CAVALIER (éd.), *Des systèmes d'information aux blockchains. Convergence en sciences juridiques et fiscales, économiques et de gestion*, Bruxelles, Bruylant, 2021 ; M. ARTZT et T. RICHTER (éd.), *Handbook of Blockchain Law*, Alphen aan den Rijn, Wolters Kluwer, 2020 ; A. GRINHAUS, *A Practical Guide to Smart Contracts and Blockchain Law*, Toronto, LexisNexis, 2019 ; A. BARBET-MASSIN et al., *Droit des crypto-actifs et de la blockchain*, Paris, LexisNexis, 2020 ; O. POLLICINO et G. DE GREGORIO (éd.), *Blockchain and Public Law. Global Challenges in the Era of Decentralisation*, Cheltenham-Northampton, Edward Elgar Publishing, 2021 ; L. JOLLY, *La réglementation des cryptomonnaies*, Bruxelles, Larcier, 2022 ; J. DE WERRA (éd.), *Propriété intellectuelle à l'ère du Big Data et de la Blockchain*, Genève, Schulthess, 2020. On notera, enfin, la création d'une revue américaine spécialement consacrée au droit des blockchains : la *Stanford Journal of Blockchain Law & Policy*.

<sup>2</sup> Un récent ouvrage, édité sous les auspices de notre même maison d'édition, a récemment été publié à ce propos : A. BEELEN, *Tout sur la blockchain et ses applications*, op. cit.

<sup>3</sup> Afin de le réguler ou, dans les cas les plus « extrêmes », de l'interdire.

de classer ce phénomène dans les catégories existantes, le cas échéant, grâce à une interprétation souple de la jurisprudence. Dans la plupart des cas toutefois, c'est un entremêlement de ces deux approches qui s'opère. Nous verrons en effet que, selon les matières et les aspects de droit, des dispositifs spécifiques ont été mis en place (ou seraient les bienvenus), alors que, pour bien d'autres aspects, les règles juridiques en vigueur semblent satisfaisantes.

Sous cet angle, l'ouvrage est également susceptible d'intéresser les décideurs politiques – la matière étant, jusqu'ici, encore peu réglementée. Il n'est toutefois nullement question de formuler des propositions concrètes, mais d'analyser la blockchain et ses applications au regard des dispositifs juridiques existants et d'en souligner, le cas échéant, leur (in)adéquation.

3. Le but de cette introduction est d'abord d'expliquer brièvement la technologie de la blockchain et les principales applications qui en sont faites, en accordant une attention toute particulière aux cryptomonnaies (section 1). Nous esquisserons ensuite les rapports entre le droit et la blockchain, en exposant les principales réglementations prises en droits belge et européen, puis en nous interrogeant sur les possibles conséquences que pourrait avoir la blockchain sur le droit et sur les métiers du droit (section 2). De premières conclusions viendront synthétiser ces éléments d'introduction (section 3), avant d'établir le plan de l'ouvrage. Chaque chapitre est consacré à une branche ou discipline spécifique du droit : contractuelle, intellectuelle, fiscale, publique et relative aux données personnelles (section 4).

## Section 1. Qu'est-ce que la blockchain ?

4. Bien que les questions qui seront abordées soient essentiellement juridiques, il est toutefois nécessaire de décrire et de comprendre la réalité traitée. Nous tenterons d'abord de définir la blockchain (§ 1), avant d'exposer – sans toutefois nous égarer dans des considérations trop techniques – le fonctionnement de cette technologie (§ 2). Nous évoquerons ensuite les principales applications de la blockchain (§ 3).

### § 1. Essai de définition

5. Littéralement, la blockchain peut être traduite par « chaîne de blocs ». Cette dénomination reprend l'essence de cette technologie, puisqu'elle consiste à enregistrer des données dans des blocs (sortes de « conteneur numérique »<sup>4</sup>), qui forment donc une chaîne. La blockchain est en effet une technologie de stockage d'informations, où les différentes transactions sont inscrites dans des blocs liés (enchaînés) les uns aux autres. Ces blocs ont pour particularité d'être en principe lisibles par tous ; la blockchain est donc *transparente*, ce qui permet de remonter la chaîne et les informations qu'elle contient<sup>5</sup>. La blockchain est souvent comparée à un grand *registre* informatisé, dont chaque page correspond à un bloc. Elle s'assimile en effet à une « chaîne de livres de comptes

---

<sup>4</sup> O. LASMOLES, « La difficile appréhension des blockchains par le droit », *R.I.D.E.*, 2018, n° 4, p. 454.

<sup>5</sup> R. BARON, « Aspects techniques de la technologie blockchain », in *Blockchain et droit*, Paris, Dalloz, 2018, p. 9.

virtuels retraçant l'ensemble des transactions effectuées, ces dernières pouvant être monétaires, juridiques ou de simples échanges de données »<sup>6</sup>. En somme, il s'agit d'une technologie de stockage qui permet de certifier les transactions et, plus généralement, les flux d'informations.

6. Sa grande spécificité est que les données sont stockées et certifiées par les utilisateurs eux-mêmes, les *pairs* (on parle de système *peer-to-peer* ou pair-à-pair<sup>7</sup>). Cette décentralisation est de deux ordres. Elle concerne d'abord le *stockage*, puisque les bases de données ne sont pas concentrées sur un serveur centralisé, mais sont « distribuées », c'est-à-dire répliquées sur des dispositifs électroniques divers (ordinateurs, téléphones portables, etc.), le cas échéant en très grand nombre, qui constituent les *nœuds* du réseau. Chaque nœud possède, en théorie, une copie du registre, ce qui garantit sa pérennité<sup>8</sup>. Il s'agit d'un argument de poids avancé par les défenseurs de la blockchain : les risques de perte d'informations ou de piratage du système sont fortement réduits, puisque tous les utilisateurs possèdent théoriquement une copie de la chaîne. On notera toutefois que si les risques de piratage sont moins élevés au niveau *macro*, ils restent importants au niveau *micro* : les utilisateurs risquent en effet de se voir subtiliser leur clé privée<sup>9</sup> et, par exemple, de perdre l'accès à leurs cryptomonnaies<sup>10</sup>.

7. La décentralisation s'opère ensuite au niveau de la *validation* des transactions effectuées. Il s'agit, ici, de l'idée véritablement révolutionnaire, « disruptive »<sup>11</sup>, de la blockchain<sup>12</sup>. Ce sont les pairs qui certifient les transactions, généralement par la technique dite du « minage ». Ceci permet de se passer d'un organe central de contrôle, d'un « tiers de confiance ». Dans le cadre de la blockchain en effet, ce n'est plus à la banque ou au notaire de certifier une opération, mais à la communauté des utilisateurs qui s'assure elle-même de l'exactitude des informations. Comme l'exprimait le journal *The Economist* dans un article remarqué, la blockchain joue le rôle d'une « machine créatrice de confiance »<sup>13</sup>.

8. En guise de résumé, nous pouvons nous référer à la définition proposée par l'Office parlementaire français d'évaluation des choix scientifiques et technologiques

<sup>6</sup> N. BARBAROUX, « Un exemple de blockchain à la frontière du droit et de l'économie : Bitcoin », in *Blockchain et droit*, op. cit., p. 20.

<sup>7</sup> Le *peer-to-peer* prend donc une autre dimension que celle, bien connue, de partage de fichiers audio ou vidéo, puisque son but est ici de faire fonctionner un système (par exemple, monétaire).

<sup>8</sup> B. MICHAUX et F. JACQUES, « La blockchain est-elle ou non une véritable base de données, protégeable par la propriété intellectuelle ? », in *Les blockchains et les smart contracts à l'épreuve du droit*, op. cit., p. 247.

<sup>9</sup> Cf. *infra*, § 15.

<sup>10</sup> Ce problème est de surcroît amplifié par le « pseudonymat » qui règne actuellement dans le monde de la *blockchain* et qui fait obstacle à la réattribution de clés perdues.

<sup>11</sup> Pour reprendre un terme à la mode dans le jargon numérique.

<sup>12</sup> Comme nous le verrons dans la section suivante, la technologie blockchain ne mobilise pas de techniques informatiques nouvelles, puisqu'elle se fonde principalement sur la cryptographie (plus précisément, la cryptographie « asymétrique »), mais l'ingéniosité repose sur la décentralisation de la validation des transactions.

<sup>13</sup> « *Simply put, it is a machine for creating trust* » (*The Economist*, « The trust machine. The technology behind bitcoin could transform how the economy works », 31 octobre 2015). En somme, des utilisateurs « qui ne se font pas mutuellement confiance peuvent entrer en relation sans avoir recours à un intermédiaire de confiance » (M. LOGNOUL, « La blockchain comme outil de protection et de gestion des actifs de propriété intellectuelle », in *Les blockchains et les smart contracts à l'épreuve du droit*, op. cit., p. 288). La confiance est donc placée « dans la technologie, plutôt que dans un intermédiaire » (Y. PUILLET et H. JACQUEMIN, « Blockchain : une révolution pour le droit ? », *J.T.*, 2018, p. 803).

(l'« OPECST »), qui définit les blockchains comme des « technologies de stockage et de transmission d'informations, permettant la constitution de registres répliqués et distribués (*distributed ledgers*), sans organe central de contrôle, sécurisées grâce à la cryptographie, et structurées par des blocs liés les uns aux autres »<sup>14</sup>.

Nous retiendrons plus généralement que la blockchain se caractérise par son caractère *décentralisé* (tant pour le stockage que pour la certification des données), par sa *transparence* (elle est généralement lisible par tous) et par son *immuabilité* (les blocs ainsi que leur séquence sont en principe protégés contre toute modification<sup>15</sup>).

9. Les flux d'informations concernés peuvent porter sur des choses très diverses. La blockchain permet d'abord d'enregistrer des transactions portant sur des actifs numériques. Ceux-ci peuvent être fongibles, comme pour les cryptomonnaies (par exemple, un bitcoin est interchangeable avec un autre bitcoin), ou non. Dans cette seconde hypothèse, on parle de NFT : *Non-fungible tokens*. L'une des illustrations les plus notoires concerne les œuvres numériques. Grâce à la blockchain en effet, de telles œuvres, pourtant reproductibles à l'infini, se voient revêtir une forme d'unicité (la blockchain permet de déterminer qui est le « propriétaire » de l'image – à distinguer de son auteur<sup>16</sup>).

La blockchain permet également de stocker et de certifier des informations portant sur des objets non numériques. Ceux-ci peuvent être *tangibles* : la blockchain permet, par exemple, de tracer les transactions immobilières, l'origine d'un produit alimentaire ou d'une marchandise (jouant le rôle de *supply chain*), voire d'assurer la traçabilité de l'énergie<sup>17</sup> ; ou *intangibles* : lorsqu'elle certifie les transferts d'actifs financiers, de droits de propriété intellectuelle ou encore l'octroi d'un diplôme<sup>18</sup>.

Enfin, la blockchain peut également héberger des *smart contracts* : elle sert alors à enregistrer des informations qui déclenchent l'application de clauses contractuelles et qui peuvent, par exemple, entraîner un paiement automatique en cryptomonnaies.

## § 2. Explication sommaire de la technologie blockchain

10. Afin d'affiner l'essai de définition, il nous paraît nécessaire d'exposer brièvement le fonctionnement de cette technologie. Notons que si nous parlons de la technologie blockchain au singulier, il existe en réalité une multitude de blockchains, fonctionnant selon des règles différentes définies dans un *protocole*<sup>19</sup>

<sup>14</sup> V. FAURE-MUNTIAN, C. DE GANAY et R. LE GLEUT, *Comprendre les blockchains : fonctionnement et enjeux de ces nouvelles technologies*, Paris, Office parlementaire d'évaluation des choix scientifiques et technologiques, 2018, p. 13, disponible sur [https://www.assemblee-nationale.fr/dyn/15/rapports/ots/115b1092\\_rapport-information](https://www.assemblee-nationale.fr/dyn/15/rapports/ots/115b1092_rapport-information).

<sup>15</sup> F. MARMOZ, « Propos introductif », in *Blockchain et droit*, *op. cit.*, p. 2.

<sup>16</sup> Voy. le chapitre « Aspects généraux de droits intellectuels et application spécifique : les NFT artistiques face au droit d'auteur », pp. 67 et s.

<sup>17</sup> En assumant que l'énergie soit un bien tangible. Voy., par exemple, J. GOUDRON, « La "blockchain" ouvre le champ des possibles pour la "smart city" », *Le Monde*, 27 septembre 2017, disponible sur [https://www.lemonde.fr/smart-cities/article/2017/09/27/la-blockchain-ouvre-le-champ-des-possibles-pour-la-smart-city\\_5192463\\_4811534.html](https://www.lemonde.fr/smart-cities/article/2017/09/27/la-blockchain-ouvre-le-champ-des-possibles-pour-la-smart-city_5192463_4811534.html).

<sup>18</sup> Puisque ce dernier bien est toutefois incessible (il n'est – n'en déplaie à certains – pas encore possible de vendre ou de transmettre un diplôme obtenu), une seule transaction est enregistrée par la *blockchain* : la délivrance du diplôme par l'institution au diplômé.

<sup>19</sup> Par « protocole », dans son sens informatique, il faut entendre l'« ensemble des règles qui permettent à un utilisateur de se connecter sur un réseau ou à diverses parties de ce réseau de communiquer entre elles » (Centre national de ressources textuelles et lexicales).

propre à chacune. Parmi les plus célèbres, on peut citer la blockchain liée au bitcoin, ou bien la blockchain Ethereum qui a aussi vocation à enregistrer des *smart contracts*.

Si certaines règles peuvent donc varier (par exemple, comment valider un bloc de la chaîne), les caractéristiques évoquées ci-dessous restent globalement similaires. Par ailleurs, le protocole du bitcoin a servi d'exemple pour la création d'autres blockchains et reste l'une des principales références.

**11.** Parmi les principales variantes, on distingue les blockchains dites *publiques*, qui sont ouvertes à tous, sans contrôle à l'entrée, des blockchains *privées* ou *de consortium*, réservées à certains membres et, donc, susceptibles d'un contrôle *a priori*<sup>20</sup>.

**12.** Comme évoqué précédemment<sup>21</sup>, la blockchain est une technique qui repose en grande partie sur des procédés connus, à savoir la cryptographie asymétrique et la transmission d'informations par blocs. Elle se distingue toutefois des réseaux traditionnels par son caractère décentralisé et par sa validation de la chaîne *via* la technique du minage<sup>22</sup> – cette dernière technique, d'abord associée au bitcoin, n'est toutefois pas utilisée dans toutes les blockchains (d'autres méthodes de validation ont en effet vu le jour<sup>23</sup>).

**13.** Encore fallait-il rassembler ces différentes technologies, ce qu'a réalisé Satoshi Nakamoto (il s'agit en réalité d'un pseudonyme, cachant une personne ou un groupe de personnes<sup>24</sup>). Il a expliqué le fonctionnement du protocole bitcoin dans un article du 31 octobre 2008 – soit dans la prolongation de la crise financière – intitulé : « Bitcoin: A Peer-to-Peer Electronic Cash System »<sup>25</sup> (qualifié de « livre blanc » du bitcoin). Le bitcoin sera ensuite lancé dans la foulée, en janvier 2009.

**14.** Dans ce papier, Nakamoto propose une solution permettant de payer directement une autre personne sans passer par une institution financière. Si la signature électronique offrait déjà une partie de la solution, encore fallait-il passer par un tiers de confiance pour éviter la « double dépense » (c'est-à-dire le risque qu'une personne paie deux fois avec le même jeton numérique) ; or c'est de ce tiers de confiance que le créateur du bitcoin propose de se passer, grâce à un réseau *peer-to-peer* qui valide les transactions par la technique du minage. Une fois ancrée dans la chaîne, la somme transmise ne peut pas être réutilisée pour effectuer une seconde transaction, puisque la première transaction est visible aux yeux de tous et que les blocs s'enchaînent.

**15.** La cryptographie permettait déjà de transférer de la monnaie numérique de A à B. Il s'agit en effet d'une technique d'écriture qui permet d'assurer, outre la confidentialité d'un message, son authenticité et son intégrité. Alors que

<sup>20</sup> R. BARON, « Aspects techniques de la technologie blockchain », *op. cit.*, p. 8. Dans le secteur bancaire, on peut, par exemple, citer le consortium R3 qui vise à rassembler les principales institutions.

<sup>21</sup> Cf. *supra*, note 12.

<sup>22</sup> H. CROZE, « Aspects juridiques de la blockchain », in *Blockchain et droit*, *op. cit.*, p. 42.

<sup>23</sup> Cf. *infra*, note 32.

<sup>24</sup> Cette figure mythique, quasi christique, de l'univers des cryptomonnaies continue à entretenir le mystère. Elle a annoncé quitter le projet Bitcoin fin 2010, transmettant la clé d'alerte du protocole à son successeur, laquelle permet d'envoyer un même message simultanément à tous les nœuds du système (A. BEELEN, *Tout sur la Blockchain et ses applications*, *op. cit.*, p. 27).

<sup>25</sup> Disponible sur <https://bitcoin.org/bitcoin.pdf>.

la cryptographie classique (symétrique) nécessite une clé pour lire un message ou une information chiffrée, la cryptographie asymétrique fonctionne avec deux clés : une publique, accessible à tous, et une privée, connue du possesseur de la clé seulement<sup>26</sup>.

L'exemple classique pour expliquer la cryptographie consiste à parler d'Alice et de Bob (A et B). Dans le cadre des cryptomonnaies, si Alice veut transférer un certain montant à Bob, elle va signer la transaction grâce à sa clé privée et utiliser la clé publique de Bob pour pouvoir l'identifier (la clé publique sert donc, en quelque sorte, de numéro de compte<sup>27</sup>). La transaction est communiquée au réseau qui doit la valider et l'intégrer dans un bloc de la chaîne (grâce au mécanisme du minage<sup>28</sup>). Le destinataire, Bob, doit ensuite utiliser sa clé privée (dont il a seul la connaissance) pour déchiffrer la transaction et accéder à la cryptomonnaie reçue (qu'il pourra à nouveau transférer selon le même processus).

**16.** La validation de la transaction, donc son inscription dans un bloc de la chaîne, est, comme nous l'avons souligné, réalisée par les pairs de manière décentralisée. Dans le cadre du protocole bitcoin – protocole de référence –, la certification des transactions s'opère par la technique du *minage*<sup>29</sup>. Les *mineurs* vont devoir valider la transaction en l'inscrivant dans un bloc de la chaîne, qui ne pourra en principe plus être modifiée par la suite.

Le minage consiste en la réalisation d'un calcul complexe, visant à obtenir un code spécifique, dont l'obtention est le produit du hasard. Pour résoudre ce calcul, il faut multiplier les essais, de telle sorte que sa résolution dépend essentiellement de la puissance de calcul des machines utilisées : plus elle est élevée, plus les chances sont grandes. Ceci a mené certains investisseurs à concentrer un nombre important d'ordinateurs, spécifiquement conçus pour ce type de calcul, dans de grands hangars climatisés, que l'on appelle « fermes » de minage. La dépense énergétique (et l'empreinte écologique) est très élevée, de telle sorte que la plupart de ces fermes sont situées dans des régions où le prix de l'électricité est très bas<sup>30</sup>.

Miner n'est pas sans intérêt : les mineurs qui résolvent le calcul sont en effet récompensés en bitcoins. Un mineur qui valide un bloc et qui l'inscrit dans la chaîne reçoit un certain montant de bitcoins. Le montant de la récompense est divisé par deux tous les quatre ans. Ces récompenses représentent les seuls jetons nouvellement émis ; le nombre de bitcoins est par ailleurs limité à 21 millions d'unités (on estime que les derniers bitcoins seront créés en 2140<sup>31</sup>). La mise en place d'une récompense vise à s'assurer que les utilisateurs contribuent au fonctionnement du système (qu'il puisse fonctionner sans autorité de contrôle).

---

<sup>26</sup> R. BARON, « Aspects techniques de la technologie blockchain », *op. cit.*, p. 10.

<sup>27</sup> Lorsque la cryptographie asymétrique est utilisée de manière plus classique afin d'envoyer des messages, la clé publique s'apparente plutôt à une forme de boîte aux lettres ou à une adresse e-mail.

<sup>28</sup> Cf. *infra*, n° 16.

<sup>29</sup> Le champ lexical utilisé, qui rappelle la recherche de métaux précieux, contraste avec la dimension éminemment virtuelle des cryptomonnaies.

<sup>30</sup> Les plus petits mineurs ont, quant à eux, tendance à se rassembler sous une forme de coopérative, dans laquelle les bénéfices obtenus sont partagés entre les membres (on parle de « *pool* » de minage).

<sup>31</sup> R. BARON, « Aspects techniques de la technologie blockchain », *op. cit.*, p. 17.

17. Pour valider un bloc, il faut donc résoudre un calcul complexe. Il s'agit d'un système de validation par « preuve de travail » (*Proof of Work – PoW*)<sup>32</sup>. La raison qui sous-tend la mise en place d'une telle épreuve est de laisser un certain laps de temps entre la validation des différents blocs. Sans une telle exigence, les blocs pourraient être validés instantanément, les chaînes se multiplieraient et le système courrait à sa perte. Grâce à la preuve de travail, les blocs de la blockchain sont créés à intervalles réguliers (pour le bitcoin, par exemple, de nouveaux blocs sont créés environ toutes les dix minutes<sup>33</sup>).

18. Quel est ce problème calculatoire complexe ? Pour valider un bloc, les mineurs doivent trouver un *hash* particulier grâce à la fonction de hachage. Une fonction de hachage consiste à transformer une information (par exemple, une phrase ou, dans notre cas, un ensemble de transactions) en un code de soixante-quatre caractères<sup>34</sup>, que l'on qualifie d'*empreinte* ou de *hash*. Deux informations différentes ne donneront jamais<sup>35</sup> la même empreinte (il suffit d'une infime modification et l'empreinte change complètement<sup>36</sup>), tandis qu'une même information donnera toujours la même empreinte<sup>37</sup>. Il s'agit, en quelque sorte, d'une empreinte digitale numérique.

*A priori*, le hachage ne pose pas de difficulté : vous inscrivez vos informations dans un logiciel destiné à cette fin<sup>38</sup> et vous obtenez directement le *hash*. Puisque chaque bloc comprend une série de transactions et l'empreinte du bloc précédent (afin de constituer la chaîne<sup>39</sup>), il suffirait d'inscrire ces données, on obtiendrait directement l'empreinte et le bloc serait créé. Afin de complexifier la chose (et de ralentir la création de blocs), le protocole va exiger que chaque *hash* commence par un certain nombre de 0. Il s'agit d'une convention artificielle visant à complexifier le calcul. Il est alors nécessaire d'ajouter des informations (concrètement, des suites de chiffres et lettres diverses) aux données du bloc pour arriver à ce résultat. Les machines vont donc multiplier les essais pour y arriver et, une fois atteint, le nouveau bloc est créé.

<sup>32</sup> D'autres systèmes ont également été envisagés, à l'instar du *Proof of Stake (PoS)*, dans lequel les utilisateurs mettent en jeu certains jetons de cryptomonnaie et espèrent être tirés au sort pour valider le bloc. Un tel mécanisme a pour avantage d'être moins énergivore et donc plus respectueux de l'écologie. Il est toutefois moins sécurisé et ébranle en partie l'objectif de décentralisation poursuivi par les cryptomonnaies fondatrices, puisqu'en l'espèce, les plus grands détenteurs de *tokens* sont les plus susceptibles de s'enrichir (A. BEELEN, *Tout sur la Blockchain et ses applications*, op. cit., pp. 57 et s.). La blockchain Ethereum est par exemple récemment passée d'un fonctionnement fondé sur la *Proof of Work* à la *Proof of Stake*.

<sup>33</sup> Plus les mineurs sont nombreux, plus le calcul à résoudre est complexe, afin de garder cet intervalle régulier de création de blocs.

<sup>34</sup> Par exemple, la phrase « Les aspects juridiques de la blockchain » devient « 5AC84451755E1B999A60451988E3C7C5971D83D2564D0C6522C0742DE6E554F2 ».

<sup>35</sup> Même si cela n'a pas encore été prouvé.

<sup>36</sup> Un seul bit d'information est modifié et le résultat est radicalement différent. Par exemple, « Les aspects juridiques des blockchains » devient : « 4B60A2B859ECC7A0447EEB85D5D27E3499C1C44726F56B8484F309085DDA4E5C ».

<sup>37</sup> Cette fonction a de nombreuses utilités. Très pragmatiquement, elle peut, par exemple, être utilisée pour vérifier si deux textes sont exactement les mêmes (ils auront en effet la même empreinte).

<sup>38</sup> Voy. par exemple le site suivant : <https://www.convertstring.com/fr/Hash/SHA256>.

<sup>39</sup> Puisque chaque bloc comprend l'empreinte du bloc précédent, cela permet de constituer une chaîne dans laquelle chaque maillon se suit dans l'ordre chronologique de sa création.

### § 3. Les applications de la blockchain

19. Les applications de la blockchain sont très nombreuses. De nouvelles idées continuent à éclore régulièrement. Sans nous aventurer dans un panorama exhaustif (qui serait difficilement réalisable et rapidement obsolète), nous allons brièvement évoquer ses principales applications – celles qui feront d’ailleurs l’objet d’analyses juridiques dans le présent ouvrage.

#### A. Les cryptomonnaies

20. Dès sa conception, la blockchain fut appliquée à un cas particulier : celui du bitcoin, la première forme de cryptomonnaie. L’invention de cette technologie est donc concomitante à une application particulière (contrairement à d’autres technologies inventées sans application concrète, mais faisant ensuite l’objet d’utilisations pratiques<sup>40</sup>). Désormais, les cryptomonnaies sont multiples (on en compte actuellement plus de dix-huit mille<sup>41</sup>), même si le bitcoin reste la plus importante en termes de capitalisation (*market cap*), représentant plus de 40 % du total des capitalisations de cryptomonnaies<sup>42</sup>.

21. Une question non directement juridique se pose instinctivement lorsque l’on évoque ce sujet : les cryptomonnaies sont-elles des monnaies ? Sur le plan économique, il n’y a pas d’unanimité sur la question, même si la majorité des économistes tendent à considérer qu’elles ne répondent pas aux fonctions essentielles d’une monnaie.

22. Encore faut-il s’entendre sur la définition d’une monnaie. Il est cependant généralement admis que la monnaie doit répondre à trois fonctions : celles d’instrument de paiement, d’unité de compte et de réserve de valeur<sup>43</sup>. Or, en l’état actuel, il semble difficile d’admettre que toutes ces fonctions sont remplies. Certes, on peut considérer que certaines cryptomonnaies, à l’instar du bitcoin, peuvent servir de moyen d’échange<sup>44</sup> et donc répondre à la première fonction, mais leur extrême volatilité ne permet pas de satisfaire les deux autres conditions. Elles ne peuvent ni être acceptées par les agents privés comme « numéraire de référence pour exprimer et comparer des prix de biens et services »<sup>45</sup> (*unité de compte*) ni constituer une réserve permettant à son détenteur « de reporter la consommation à une date future incertaine sans perdre trop de valeur »<sup>46</sup> (*réserve de valeur*). En outre, les cryptomonnaies ne jouent aucun rôle

<sup>40</sup> On pense à l’exemple du Post-it, souvent invoqué pour enseigner le droit des brevets : alors qu’une chimiste de l’entreprise 3M avait découvert la formule d’une colle repositionnable, son utilité pratique ne fut trouvée que bien après.

<sup>41</sup> Le site *CoinMarketCap* en comptait 20.394 au 29 juillet 2022.

<sup>42</sup> Selon ce même site d’information *CoinMarketCap* et à la même date, la capitalisation du bitcoin équivalait à 450 milliards USD, pour une capitalisation totale de 1 082 milliards USD (ce qui correspond à 41,5 % des valeurs additionnées de toutes les cryptomonnaies). En guise de comparaison, on notera que le PIB de la Belgique s’élevait, en 2021, à 560 milliards USD (source : Banque mondiale).

<sup>43</sup> N. BARBAROUX, « Un exemple de blockchain à la frontière du droit et de l’économie : Bitcoin », *op. cit.*, p. 30.

<sup>44</sup> En guise d’anecdote, la première transaction en cryptomonnaies a permis d’acheter une pizza pour 10.000 bitcoins.

<sup>45</sup> M. DAI et M. SIDIROPOULOS, « Le bitcoin est-il une monnaie », *Bulletin de l’Observatoire des politiques économiques en Europe*, 2017, vol. 37, p. 9.

<sup>46</sup> *Ibid.*, p. 10.

dans la stabilisation économique et financière, qui est parfois considérée comme une quatrième fonction nécessaire à la définition d'une monnaie dans nos économies modernes<sup>47</sup>. Les autorités publiques préfèrent d'ailleurs utiliser le terme « cryptoactif » à celui de cryptomonnaie.

**23.** Si peu admettent qu'il s'agit d'une monnaie, ils sont encore moins à considérer qu'il s'agit d'une « bonne » monnaie<sup>48</sup>, principalement en raison de la volatilité évoquée. Pour prendre l'exemple du bitcoin, sa valeur a atteint 64.400 USD le 12 novembre 2021 et est descendue à 18.948 USD le 17 juin 2022, soit une perte de valeur de plus de 70 % en seulement sept mois. L'absence d'autorité politique de contrôle (rôle pris en charge par les banques centrales pour les monnaies officielles) laisse la voie libre à ces fluctuations, qui dépendent dès lors exclusivement des interactions de l'offre et de la demande<sup>49</sup>.

On notera par ailleurs que si les cryptomonnaies devenaient un vrai moyen de paiement, une valeur d'échange, et non un simple outil de spéculation, on ne voit pas l'intérêt de la multiplicité des monnaies ; or, rappelons-le, il en existe actuellement plus de vingt mille<sup>50</sup>.

Par ailleurs, on peut également se demander si, en tant que valeur d'échange, l'intérêt premier des cryptomonnaies n'est pas la confidentialité qui les caractérise. Or une telle confidentialité a, parmi ses avantages, celui d'échapper au contrôle des autorités publiques, qu'il s'agisse de l'administration fiscale ou de la sécurité publique, dans l'hypothèse où les cryptomonnaies seraient utilisées pour blanchir de l'argent provenant d'activités illégales ou pour financer de telles activités (l'exemple paroxystique étant celui du financement du terrorisme)<sup>51</sup>. Alors que les États multiplient les efforts pour lever le secret bancaire et restreindre l'évasion fiscale *via* les paradis fiscaux, que les législations se multiplient pour éviter le blanchiment d'argent, les cryptomonnaies ouvrent de nouvelles voies que les monnaies traditionnelles ont de plus en plus de difficultés à emprunter. Comme nous le verrons d'ailleurs dans la prochaine section, la majorité des dispositions étatiques qui ont été adoptées jusqu'ici visent à lutter contre la fraude et le blanchiment d'argent.

**24.** Si la qualification des cryptomonnaies reste contestée économiquement, la question est bien plus simple juridiquement, puisqu'il suffit de vérifier si les autorités publiques ont admis une forme de cryptomonnaie comme monnaie officielle<sup>52</sup>. Or, au sein de la zone euro, l'euro est la seule monnaie officielle. En réalité, les reconnaissances étatiques sont tout à fait exceptionnelles : seuls le Salvador et la

<sup>47</sup> *Ibid.*, p. 11.

<sup>48</sup> N. BARBAROUX, « Un exemple de blockchain à la frontière du droit et de l'économie : Bitcoin », *op. cit.*, p. 31.

<sup>49</sup> Pour le bitcoin, il faut en outre rappeler que son nombre d'émission est limité à 21 millions, ce qui devrait être atteint en 2140, et est décroissant (le montant de la récompense est divisé par deux tous les quatre ans), de telle sorte que « [l]e système ne peut donc faire face à un surcroît – ou une baisse – de la demande en vue de réguler son prix (c'est-à-dire son cours de change exprimé en une devise officielle). Ceci explique donc la montée spéculative et les fortes fluctuations du cours du bitcoin » (*Ibid.*).

<sup>50</sup> *Cf. supra*, note 41.

<sup>51</sup> *Cf. infra*, note 88.

<sup>52</sup> On notera toutefois qu'il n'existe pas d'étanchéité totale entre l'appréciation économique et le champ juridique, puisque plus une cryptomonnaie répond aux fonctions classiques de la monnaie, plus elle est susceptible – outre de nombreuses autres considérations politiques – de reconnaissance publique.

Centrafrique ont officiellement reconnu le bitcoin comme devise officielle<sup>53</sup>. Bien entendu, l'absence de reconnaissance officielle ne correspond pas à une interdiction ; à l'inverse, le paiement par bitcoins ou autres cryptomonnaies est toléré par la plupart des États, et même reconnu indirectement. Par ailleurs, l'idée de monnaies officielles numériques, à l'instar d'un euro numérique<sup>54</sup>, est de plus en plus évoquée.

## B. Les *smart contracts*

25. L'une des autres illustrations les plus marquantes est le *smart contract* (littéralement, « contrat intelligent »), lequel ne consiste pas en un contrat à proprement parler, mais en l'exécution automatique d'un contrat ou d'une de ses clauses lors de la survenance d'un événement. Le *smart contract* est la codification d'un contrat (ou de certaines de ses clauses) et non sa conclusion ; « programmer un *smart contract*, ce n'est pas le conclure ; c'est seulement mettre en place le cadre d'un éventuel contrat (et non un contrat-cadre) qui s'apparente à une sorte de formulaire à disposition des futurs contractants »<sup>55</sup>. Il vise en effet à automatiser l'exécution d'une disposition contractuelle, lors de la survenance d'un événement donné<sup>56/57</sup>.

Cela permettrait par exemple d'automatiser la responsabilité contractuelle, dont le montant serait prévu par une clause pénale, ou l'exigibilité, voire l'extinction d'une obligation à l'arrivée du terme. Une illustration souvent citée est l'indemnisation d'un client en cas de retard ou d'annulation d'un vol d'avion, grâce à un outil de suivi des vols.

26. Fondamentalement, ces *smart contracts* ne bouleversent pas le droit des contrats, même s'ils sont susceptibles de complexifier certaines situations. Ils ne soulèvent pas moins de réelles questions juridiques<sup>58</sup>.

De tels *smart contracts* risquent principalement de poser des questions juridiques quant à leur exécution. La rigidité produite par l'automatisation exclut en effet « toute appréciation en fait ou toute interprétation en droit »<sup>59</sup> et est donc susceptible d'engendrer des contestations. Des questions peuvent par exemple se poser au regard du principe d'exécution de bonne foi, qui a valeur d'ordre public. La bonne foi est en effet présumée ; or l'automatisme de la sanction fait fi de ces considérations<sup>60</sup>. Il en va de même de la prise en compte du principe de proportionnalité, par exemple, dans l'application de l'exception d'inexécution<sup>61</sup>. Au niveau de la formation du contrat

<sup>53</sup> Dans le cadre du conflit russo-ukrainien, la possibilité de payer le gaz russe en bitcoins a été évoquée par le Kremlin (« L'éventualité de payer le gaz russe en bitcoin fait bondir le cours de la cryptomonnaie », *La Libre Belgique*, 25 mars 2022).

<sup>54</sup> Banque centrale européenne, *Report on a Digital Euro*, octobre 2020, disponible sur [https://www.ecb.europa.eu/pub/pdf/other/Report\\_on\\_a\\_digital\\_euro~4d7268b458.fr.pdf](https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.fr.pdf).

<sup>55</sup> H. CROZE, « Les smart contracts sont-ils des objets juridiques », in *Blockchain et droit*, *op. cit.*, p. 51.

<sup>56</sup> De tels événements peuvent être confirmés par un tiers, qualifié d'« oracle ».

<sup>57</sup> Comme l'expriment Y. POULLET et H. JACQUEMIN, « le terme *smart* – intelligent – est un peu galvaudé [...] : l'exécution est automatique certes, mais la machine ne fait que suivre les instructions données de manière totalement servile » (« Blockchain : une révolution pour le droit ? », *op. cit.*, p. 816).

<sup>58</sup> En droit belge, voy. not. H. JACQUEMIN, A. COTIGA et Y. POULLET, *Les blockchains et les smart contracts à l'épreuve du droit*, *op. cit.* ; ainsi que le chapitre de cet ouvrage « Chaîne de blocs et contrats intelligents ou blockchain et *smart contracts* », pp. 25 et s.

<sup>59</sup> Y. POULLET et H. JACQUEMIN, « Blockchain : une révolution pour le droit ? », *op. cit.*, p. 817.

<sup>60</sup> O. LASMOLES, « La difficile appréhension des blockchains par le droit », *op. cit.*, p. 463.

<sup>61</sup> Y. POULLET et H. JACQUEMIN, « Blockchain : une révolution pour le droit ? », *op. cit.*, p. 818.

en revanche, peu de questions nouvelles émergent, si ce n'est à propos de la traduction de la volonté des parties dans un code informatique<sup>62</sup>.

27. La blockchain la plus populaire sur laquelle reposent des *smart contracts* est Ethereum. Leur existence est toutefois bien antérieure à cette technologie, puisqu'ils ont été théorisés par N. Szabo en 1996 dans un article remarqué : « Smart contracts: Building blocs for digital markets »<sup>63</sup>. Si le dispositif n'est pas nouveau, son inscription dans la blockchain permet de garantir son intégrité, sans passer par un tiers de confiance.

### C. Les *Non-fungible tokens* (NFT)

28. Enfin, une application récente et très remarquée de la technologie blockchain est l'apparition des *Non-fungible tokens*, plus connus sous leur sigle NFT. Dans le domaine de l'art numérique en particulier, la blockchain bouscule les pratiques, puisqu'elle permet de créer la rareté d'une image numérique, *a priori* reproductible indéfiniment. Il est en effet possible de s'approprier une œuvre numérique, grâce à un certificat ancré dans la chaîne<sup>64</sup>. S'il n'est pas à exclure qu'un tel phénomène se révèle finalement être une « bulle », elle bouscule actuellement le marché de l'art<sup>65</sup>.

Précisons toutefois que la « révolution » porte sur la possibilité d'identifier un « propriétaire » d'une œuvre (ou d'un autre objet, le cas échéant non numérique), mais ne concerne pas la création.

### D. Autres applications

29. Plus généralement, ce dispositif est susceptible d'être mobilisé dans de nombreux domaines grâce à sa fonction d'authentification : par exemple, pour la certification de diplômes ou d'autres informations administratives, voire de brevets. La sécurisation des données est souvent évoquée dans le domaine de la santé<sup>66</sup>. Sa fonction de traçabilité peut aussi être utilisée en *supply chain* (circulation de marchandises), pour suivre l'origine d'un produit alimentaire ou encore de l'énergie.

30. Enfin, la *tokenisation*, mobilisée dans le cadre des NFT, peut également être employée pour contribuer au développement d'une finance décentralisée (on parle de « DeFi » dans le jargon, soit de « *Decentralized Finance* »). Il est en effet possible de *tokeniser* des titres de sociétés ou d'autres titres de propriété – le cas échéant peu liquides – afin de les échanger sur le marché sans passer par les intermédiaires traditionnels<sup>67</sup>.

<sup>62</sup> *Ibid.*, p. 817.

<sup>63</sup> N. SZABO, « Smart contracts: Building blocks for digital free markets », *Extropy Journal of Transhuman Thought*, 1996, n° 16.

<sup>64</sup> Sur cette question, voy. le chapitre « Aspects généraux de droits intellectuels et application spécifique : les NFT artistiques face au droit d'auteur », pp. 67 et s.

<sup>65</sup> En droit français, la loi n° 2022-267 du 28 février 2022 visant à moderniser la régulation du marché de l'art (*J.O.R.F.*, 1<sup>er</sup> mars 2022) a, par exemple, modifié le Code de commerce afin d'ouvrir les ventes aux enchères publiques aux NFT.

<sup>66</sup> Voy. I. MOTZI-OMOIJADE et A. KHARLAMOV, « Blockchain for healthcare applications and use cases », in *Blockchain and Public Law. Global Challenges in the Era of Decentralisation*, *op. cit.*, pp. 157 et s.

<sup>67</sup> P. DE FILIPPI, *Blockchain et cryptomonnaies*, 2<sup>e</sup> éd., Paris, PUF, 2022, p. 89.

## Section 2. Blockchain et droit

31. Les rapports entre la blockchain et le droit sont doubles. D'une part, de manière assez évidente, le droit tend à réglementer cette technologie et ses applications (§ 1). D'autre part, la blockchain est elle-même en mesure d'affecter certaines institutions juridiques ainsi que certains métiers du droit (§ 2).

### § 1. L'appréhension de la blockchain par le droit

32. Outre les règles juridiques susceptibles de s'appliquer à la blockchain et ses applications qui feront l'objet d'une analyse approfondie dans le présent ouvrage, le législateur et le gouvernement belges ont également adopté quelques réglementations spécifiques (que nous allons brièvement exposer dans cette introduction), bien qu'elles soient encore rares en l'état. Ce n'est d'ailleurs pas tant la technique elle-même qui fait l'objet de régulation, mais bien les activités menées par cette technique<sup>68</sup>, en particulier les cryptomonnaies.

33. En droit belge, l'intervention fut tardive et reste très limitée. Du reste, l'essentiel de la réglementation interne est le produit de la transposition de dispositions européennes – plus spécifiquement, de la cinquième directive antiblanchiment n° 2018/843 du 30 mai 2018<sup>69</sup>. 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<sup>70</sup> a en effet été modifiée par une loi du 20 juillet 2020<sup>71</sup>, puis par une loi du 1<sup>er</sup> février 2022<sup>72</sup>, afin d'étendre ses obligations aux prestataires de services de portefeuille<sup>73</sup> ainsi qu'aux services d'échange entre monnaies virtuelles et monnaies légales<sup>74</sup> établis sur le territoire belge<sup>75</sup>. Ceux-ci doivent donc être inscrits à

<sup>68</sup> E. TROPPEZ, « Quelle régulation internationale pour la blockchain ? *Code is Law v. Law will become Code* », in *Blockchain et droit*, op. cit., p. 62.

<sup>69</sup> 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, *J.O.U.E.*, 19 juin 2018.

<sup>70</sup> *M.B.*, 6 octobre 2017 ; ci-après, « loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux ».

<sup>71</sup> Loi du 20 juillet 2020 portant des dispositions diverses relatives à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces, *M.B.*, 5 août 2020.

<sup>72</sup> Loi du 1<sup>er</sup> février 2022 modifiant 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 afin d'introduire des dispositions relatives au statut et au contrôle des prestataires de services d'échange entre monnaies virtuelles et monnaies légales et des prestataires de services de portefeuilles de conservation, *M.B.*, 11 février 2022.

<sup>73</sup> L'expression exacte énoncée par la loi est « prestataire de services de portefeuille de conservation », qu'elle définit comme toute « 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 » (art. 4, al. 1<sup>er</sup>, 35°/2, de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux).

<sup>74</sup> C'est-à-dire ceux qui consistent à « effectuer des opérations d'achat ou de vente de monnaies virtuelles en contrepartie de monnaies légales ou de monnaies légales en contrepartie de monnaies virtuelles, en utilisant des capitaux détenus en propre » (art. 4, al. 1<sup>er</sup>, 35°/3, de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux).

<sup>75</sup> Pour ces opérateurs, l'installation d'une « infrastructure électronique par le biais [de laquelle] ils offrent [leurs] services » constitue un établissement au sens de la loi (art. 5, § 1<sup>er</sup>, al. 2, de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux). En d'autres termes est également visée l'installation de

la FSMA (l'Autorité des services et marchés financiers<sup>76</sup>) pour exercer leur activité ; l'autorité financière est ensuite chargée de contrôler si ces prestataires respectent les dispositions de la loi<sup>77</sup>. Les règles relatives à l'inscription auprès de la FSMA, ainsi que celles relatives à l'exercice de ces prestataires, ont été établies par le récent arrêté du 8 février 2022<sup>78</sup>. Le prestataire doit ainsi respecter une série de conditions<sup>79</sup> pour pouvoir être inscrit au registre pertinent (soit le registre des prestataires de services d'échange entre monnaies virtuelles et monnaies légales, soit le registre des prestataires de services de portefeuilles de conservation) et pour conserver cette inscription – en cas de non-respect des dispositions légales et réglementaires, la FSMA peut en effet radier le prestataire du registre, ce qui entraîne une interdiction d'exercer l'activité<sup>80</sup>. Un prestataire qui exercerait son activité sans être inscrit est, de surcroît, susceptible de sanctions pénales<sup>81</sup> (qui s'ajoutent aux sanctions administratives prévues par l'article 86bis de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers).

**34.** Par ailleurs, le législateur édicte une interdiction générale à l'égard des opérateurs qui relèvent d'un État hors de l'Espace économique européen. L'article 5, § 1<sup>er</sup>, alinéa 3, énonce en effet qu'« [i]l est interdit aux personnes physiques ou morales relevant du droit d'un pays tiers<sup>82</sup> d'offrir ou de fournir, sur le territoire belge, à titre d'activité professionnelle habituelle, même complémentaire ou accessoire, des services d'échange entre monnaies virtuelles et monnaies légales ou des services de portefeuilles de conservation ». Pour fournir de tels services, il est donc nécessaire de créer une personne morale dans un des États membres de l'Espace économique européen<sup>83</sup>.

---

distributeurs automatiques (« *Automated Teller Machines* » en anglais, mieux connues sous le sigle « ATM ») en Belgique, qui permettent l'échange de monnaies virtuelles contre des monnaies légales (qualifiées de monnaies « fiat » dans le jargon) et inversement (rapport du gouvernement pour l'adoption de l'arrêté royal du 8 février 2022 relatif au statut et au contrôle des prestataires de services d'échange entre monnaies virtuelles et monnaies légales et des prestataires de services de portefeuilles de conservation).

<sup>76</sup> « FSMA » étant l'acronyme de « *Financial Services and Markets Authority* ».

<sup>77</sup> L'article 45, § 1<sup>er</sup>, alinéa 1<sup>er</sup>, 2<sup>o</sup>, de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers (M.B., 4 septembre 2002) a été modifié par loi du 4 juillet 2021 portant transposition de directives et mise en œuvre de règlements européens en matière financière (M.B., 13 juillet 2021) afin de préciser que la FSMA a pour mission de contrôler les prestataires de services d'échange entre monnaies virtuelles et monnaies légales et des prestataires de services de portefeuilles de conservation.

<sup>78</sup> Arrêté royal du 8 février 2022 relatif au statut et au contrôle des prestataires de services d'échange entre monnaies virtuelles et monnaies légales et des prestataires de services de portefeuilles de conservation, M.B., 23 février 2022 (ci-après, « arrêté royal du 8 février 2022 »).

<sup>79</sup> Celles-ci sont détaillées à l'article 5 de l'arrêté royal du 8 février 2022. Parmi celles-ci, le prestataire doit, par exemple, être constitué sous une forme sociétaire déterminée (société coopérative, société anonyme, société européenne ou société coopérative européenne), dont le capital, entièrement libéré, doit être de minimum 50.000 euros.

<sup>80</sup> Art. 15, § 2, de l'arrêté royal du 8 février 2022.

<sup>81</sup> Art. 136, al. 2, de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux.

<sup>82</sup> Par « pays tiers », il faut, en effet, entendre « un État qui n'est pas partie à l'Accord sur l'Espace économique européen » (art. 4, al. 1<sup>er</sup>, 8<sup>o</sup>, de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux).

<sup>83</sup> Au commentaire du Conseil d'État qui, dans son avis, jugeait l'interdiction disproportionnée au regard des objectifs poursuivis, le gouvernement répond que, « [s]'il est exact que ces prestataires pourraient être soumis au contrôle de la FSMA s'ils étaient établis sur le territoire belge, l'absence d'une société établie [dans le sens « constituée », N.d.A.] en Belgique, ou à tout le moins dans l'Union européenne est de nature à porter préjudice à l'effectivité d'un tel contrôle (notamment dans le cadre de l'exercice des pouvoirs d'investigation de la FSMA), ainsi que des mesures coercitives qui pourraient en découler. Il n'est en effet pas crédible de considérer qu'un

**35.** En résumé, seuls les prestataires qui relèvent du droit d'un des États membres de l'EEE peuvent fournir de tels services en Belgique. Doivent s'inscrire à la FSMA les sociétés de droit belge, ainsi que les sociétés non belges qui relèvent d'un autre État membre de l'EEE et qui sont établies en Belgique – c'est-à-dire celles qui, de manière classique, installent une succursale ou un autre établissement stable sur le territoire belge, mais également celles qui, en vertu de l'article 5, § 1<sup>er</sup>, alinéa 2, de la loi du 18 septembre 2017, y ont installé des distributeurs automatiques<sup>84</sup>. Les sociétés étrangères relevant d'un État de l'EEE qui ne disposent pas d'un tel établissement ne sont donc pas soumises à l'obligation d'inscription.

**36.** On notera également que la loi du 18 septembre 2017 exige que la direction effective de l'entreprise soit assurée par des personnes qui possèdent « l'honorabilité professionnelle nécessaire et l'expertise adéquate pour exercer leurs activités »<sup>85</sup> et que l'inscription doit être refusée si « les personnes qui détiennent directement ou indirectement dans le capital de la société une participation, conférant le droit de vote ou non, de cinq pour cent au moins, ne présentent pas les qualités nécessaires au regard du besoin de garantir une *gestion saine et prudente*<sup>86</sup> de la société »<sup>87</sup>.

**37.** C'est donc dans un contexte de méfiance que les dispositions spécifiquement adoptées pour encadrer les cryptomonnaies ont été adoptées<sup>88</sup>. En droit belge, la première réglementation suivait déjà cette ligne, puisqu'il s'agissait d'un arrêté d'interdiction. L'arrêté royal du 24 avril 2014<sup>89</sup> a en effet approuvé un règlement de la

---

tel contrôle puisse être exercé, et que de tels pouvoirs et mesures puissent être appliqués, depuis le territoire belge, à l'égard d'une entité étrangère, de la même manière qu'à l'égard d'une entité relevant du droit d'un autre État membre, soumise à une législation harmonisée. En autorisant des entités étrangères, qui ne sont potentiellement soumises, dans l'État tiers dont elles relèvent, à aucune réglementation en matière de prévention du blanchiment de capitaux et de financement du terrorisme, et sans être assuré, de ce fait, de pouvoir compter sur un contrôle équivalent dans le pays tiers concerné, le gouvernement ferait courir à la Belgique des risques accrus de blanchiment de capitaux et de financement du terrorisme, dans un secteur par ailleurs reconnu comme étant particulièrement risqué en la matière. Pour ces raisons, le gouvernement estime que l'interdiction est proportionnée et qu'elle doit être maintenue » (projet de loi modifiant la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux, *Doc. parl.*, Ch. repr., 2021-2022, n° 2383/001, pp. 7-8). Le gouvernement rappelle en outre qu'un raisonnement similaire est suivi au niveau européen, qu'une telle interdiction est envisagée dans le cadre des discussions sur le projet de règlement MiCa (*cf. infra*, n° 38) et qu'une telle interdiction est également mise en place aux Pays-Bas (*ibid.*, p. 8).

<sup>84</sup> *Cf. supra*, note 75.

<sup>85</sup> Art. 5, § 1<sup>er</sup>, al. 5, de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux.

<sup>86</sup> C'est nous qui soulignons.

<sup>87</sup> Art. 5, § 1<sup>er</sup>, al. 7, de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux. Il s'agit d'obligations imposées par l'article 47, § 2, de la directive 015/849. Ces obligations font l'objet de précisions à l'article 5 de l'arrêté royal du 8 février 2022.

<sup>88</sup> Le considérant 8 de la directive 2018/843 énonçait, par exemple, que « [l]es groupes terroristes peuvent [...] 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 dissimulant les transferts ou en bénéficiant d'un certain degré d'anonymat sur ces plateformes. 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 ». Le considérant 9 précisait, quant à lui, que « [l]'anonymat des monnaies virtuelles est susceptible de favoriser leur utilisation à des fins criminelles » et qu'il est donc nécessaire que les cellules nationales de renseignements financiers soient « 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 ».

<sup>89</sup> Arrêté royal du 24 avril 2014 portant approbation du règlement de l'Autorité des services et marchés financiers concernant l'interdiction de commercialisation de certains produits financiers auprès des clients de détail, *M.B.*, 20 mai 2014.

FSMA<sup>90</sup> qui interdit de commercialiser en Belgique, à titre professionnel, auprès d'un ou de plusieurs clients de détail, des produits financiers dont le rendement dépend directement ou indirectement d'une monnaie virtuelle<sup>91</sup> (définie comme « toute forme de monnaie digitale non réglementée qui n'a pas cours légal »<sup>92</sup>).

**38.** Une réglementation bien plus complète des prestataires de services et, plus généralement, du marché des cryptoactifs est actuellement en cours de discussions au niveau européen. Une proposition de règlement a en effet été déposée en ce sens le 24 septembre 2020 : il s'agit du règlement « MiCa » (« *Market in crypto assets* »)<sup>93</sup>, dont le premier objectif est de mettre en place un cadre juridique clair applicable à tous les cryptoactifs qui ne sont pas couverts par les législations financières existantes ; il s'appliquera tant aux prestataires qu'aux émetteurs de cryptoactifs. Parallèlement, une proposition de règlement a également été déposée sur un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués<sup>94</sup>, qui vise à fixer des exigences uniformes pour l'exploitation de telles infrastructures<sup>95</sup> (ces propositions s'intègrent dans un ensemble de mesures visant à renforcer la finance numérique<sup>96</sup>). Il faudra donc rester attentif à l'adoption prochaine de nouvelles règles visant à réguler les applications de la blockchain, en particulier les cryptoactifs.

## § 2. La (potentielle) influence de la blockchain sur le droit

**39.** En sens inverse, la blockchain est elle-même susceptible d'avoir une certaine influence sur le droit et, plus spécifiquement, sur la pratique des métiers du droit. Si la première vocation de la blockchain était de se substituer au banquier (grâce à une décentralisation du contrôle des transactions)<sup>97</sup>, voire aux banques centrales (par une

<sup>90</sup> Règlement de l'Autorité des services et marchés financiers concernant l'interdiction de commercialisation de certains produits financiers auprès des clients de détail. L'article 30bis de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers (adopté à la suite de la crise financière de 2007) habilite en effet le comité de direction de la FSMA à adopter des règlements pouvant aller jusqu'à l'interdiction de la commercialisation de certains produits financiers auprès des clients de détail.

<sup>91</sup> Art. 2, al. 1<sup>er</sup>, 2<sup>o</sup>, du règlement précité. Les risques avancés pour justifier une telle interdiction étaient : « le risque qu'une plateforme de négociation ou un porte-monnaie digital soient piratés et que le propriétaire voie son argent virtuel dérobé ; le risque opérationnel lié aux systèmes utilisés, lequel n'a pas encore été évalué de manière formelle par les autorités de contrôle ; le risque de change ; le risque découlant du fait qu'il n'existe pas pour l'argent virtuel de garantie légale qu'il puisse être échangé à sa valeur initiale et du fait qu'il n'a pas cours légal » (note explicative jointe au règlement).

<sup>92</sup> Art. 1<sup>er</sup>, al. 1<sup>er</sup>, 6<sup>o</sup>, du règlement précité.

<sup>93</sup> Proposition de règlement du Parlement européen et du Conseil sur les marchés de cryptoactifs et modifiant la directive (UE) 2019/1937, COM(2020) 593 final 2020/0265(COD).

<sup>94</sup> Proposition du Parlement européen et du Conseil du 24 septembre 2020, COM(2020) 594 final 2020/0267(COD).

<sup>95</sup> Comme son nom l'indique, il s'agit d'un régime pilote qui devra être évalué après cinq années après l'entrée en vigueur du règlement, afin de décider s'il doit être maintenu en l'état, s'il doit être aménagé ou bien abandonné.

<sup>96</sup> Sur ce point, voy. la communication de la Commission « Une stratégie en matière de finance numérique pour l'UE », 23 septembre 2020, COM(2020) 591.

<sup>97</sup> Dans le cadre des cryptomonnaies, les machines jouent en effet « le même rôle que les (anciennes) banques : à savoir collecte des ordres de paiement, vérification des informations tant du côté de l'acheteur que du côté du vendeur, débit du compte des débiteurs et crédit du compte des créanciers » (N. BARBAROUX, « Un exemple de blockchain à la frontière du droit et de l'économie : Bitcoin », *op. cit.*, p. 24).

émission de monnaie nouvelle limitée à la seule récompense de ceux qui contribuent à l'efficacité du système en certifiant les transactions), qui ne sont pas étrangers au milieu du droit, des professions « strictement » juridiques sont également susceptibles de voir leurs tâches<sup>98</sup> bousculées par la blockchain.

**40.** C'est principalement sur le rôle de la *preuve* que cette technologie est susceptible d'avoir un impact. La blockchain pourrait notamment être utilisée pour certifier les transferts de biens immobiliers, ce qui aurait des conséquences sur la profession de notaire<sup>99</sup>. Le Ghana a par exemple mis en place un cadastre *via* la technologie blockchain afin d'authentifier les transactions immobilières<sup>100</sup>. La situation n'est pas comparable aux systèmes et institutions juridiques belges, ni même européens, mais cette illustration souligne néanmoins que l'idée n'est pas complètement fantasque.

Rappelons toutefois que, sur le plan juridique, il faut encore pouvoir s'assurer que le premier vendeur dont la transaction a été certifiée par la blockchain était bien propriétaire du bien (problème classique de la *probatio diabolica*). La propriété est alors établie par la prescription acquisitive (position paisible trentenaire en additionnant les possessions des propriétaires successifs) et non par la chaîne des contrats<sup>101</sup>. En matière de biens mobiliers, la question se pose moins puisqu'en fait de meubles, la possession vaut titre ; mais la possession, purement matérielle, est étrangère à la blockchain<sup>102</sup>. Il faudrait en outre régler le problème du « pseudonimat » actuel des blockchains<sup>103</sup>.

Plus généralement, c'est aussi se priver d'un acteur dont le rôle de conseil est essentiel. C'est toutefois la philosophie poursuivie par la blockchain, qui envisage la fin des tiers de confiance traditionnels<sup>104</sup>. Y compris dans l'hypothèse où une blockchain spécifique destinée à enregistrer ce type de transactions serait instituée et encadrée par des autorités publiques et que la finalité annoncée soit le renforcement de l'efficacité, cette initiative entraînerait nécessairement un mouvement de décentralisation dont il faut avoir conscience politiquement.

**41.** Dans une moindre mesure – mais de manière plus réaliste –, la blockchain permettrait de suppléer les professionnels du droit pour d'autres tâches « mécaniques »<sup>105</sup>, notamment par le biais des *smart contracts* qui, on l'a vu, entraînent une forme d'automatisation. Reste, bien entendu, la confection de tels contrats, ainsi que leur contrôle *a posteriori*, de telle sorte que les changements seraient mineurs en l'espèce. Par ailleurs, la conformité de telles automatisations au regard du droit créerait de nouvelles questions auxquelles devront répondre les juristes.

---

<sup>98</sup> Les plus radicaux diront leur « fonction ».

<sup>99</sup> Voy. not. B. BARRAUD, « Les blockchains et le droit », *Revue Lamy Droit de l'immatériel*, 2018, pp. 48 et s.

<sup>100</sup> Y. BISMUTH, « Blockchain : les périls attendus pour les professionnels du droit », in *Blockchain et droit*, *op. cit.*, p. 80.

<sup>101</sup> H. CROZE, « Aspects juridiques de la blockchain », *op. cit.*, p. 40.

<sup>102</sup> *Ibid.*, p. 41.

<sup>103</sup> O. LASMOLES, « La difficile appréhension des blockchains par le droit », *op. cit.*, p. 461.

<sup>104</sup> Y. BISMUTH, « Blockchain : les périls attendus pour les professionnels du droit », *op. cit.*, p. 79.

<sup>105</sup> *Ibid.*

### Section 3. Premières conclusions

42. En conclusion, la technologie blockchain a de réelles implications sur le monde juridique, tant sur l'influence qu'elle peut avoir comme outil au service du droit qu'en tant que phénomène nouveau faisant l'objet de nouvelles régulations et interrogeant les règles juridiques existantes. L'ouvrage tentera d'apporter des réponses à ces questions.

43. Comme nous l'avons vu, les applications de la blockchain ne se limitent pas aux cryptomonnaies, mais sont multiples et variées. Les dénominateurs communs qui sous-tendent ces applications sont la robustesse de la base de données (qui permet de certifier les informations qu'elle contient) et le caractère décentralisé du mécanisme<sup>106</sup>.

44. Or cette décentralisation n'est pas neutre politiquement. À l'inverse, la promotion de la blockchain est axiologiquement chargée. Elle s'ancre en effet dans une philosophie libertarienne, où les autorités de confiance – à l'exception de la machine – n'ont plus de légitimité<sup>107</sup>. La blockchain permet alors de faire fonctionner une institution par l'ensemble de ses membres (sans besoin d'autorité centrale, donc), tout en évitant les travers de l'anarchie.

L'idée de départ s'inscrivait elle-même dans une idéologie libertaire, puisque le fondateur du bitcoin, Satoshi Nakamoto, souhaitait créer une monnaie fonctionnant en dehors des circuits étatiques<sup>108</sup>. Il était donc question de démonter l'un des derniers monopoles publics, jusqu'ici encore considéré comme une fonction régalienn<sup>109</sup> : l'émission monétaire<sup>110</sup>. L'un des premiers auteurs à avoir théorisé la possibilité d'une monnaie non étatique est d'ailleurs Friedrich A. Hayek<sup>111</sup>, figure emblématique du libéralisme économique au xx<sup>e</sup> siècle. Or cette décentralisation conduit à la perte totale du pouvoir politique sur l'économie *via* la monnaie. C'est la disparition même de la politique monétaire qui est visée, en faveur d'une politique libertaire laissant cours aux seules interactions du marché.

45. Finalement, la blockchain revient aux premiers idéaux d'Internet<sup>112</sup>, monde virtuel de libertés, qui a peu à peu fait l'objet de réglementations publiques. Elle s'accorde par exemple très bien au mouvement cyberpunk<sup>113</sup>. Très vite toutefois,

<sup>106</sup> Qui peut toutefois se perdre dans le cadre de certaines blockchains privées. On peut alors se demander si la blockchain ne perd pas une part importante de sa spécificité, voire, dans certains cas, de son intérêt.

<sup>107</sup> L'utilité de la blockchain se manifeste dès lors en cas de déficit démocratique ou d'absence de confiance dans les institutions en place (D. KRAUS et C. SCHAUB, « Blockchain et propriété intellectuelle », *in Propriété intellectuelle à l'ère du Big Data et de la Blockchain, op. cit.*, p. 137).

<sup>108</sup> On notera d'ailleurs que le bloc initial du bitcoin contient un titre de journal du *Times* du 3 janvier 2009 : « *Chancellor on brink of second bailout for banks* » (« Le Chancelier sur le point d'accorder un second plan de sauvetage des banques » [traduction libre]) ; qui, outre la fonction d'horodatage (le premier bloc est nécessairement postérieur à cette date), annonce la couleur idéologique.

<sup>109</sup> À côté de la justice, de la police et de l'armée.

<sup>110</sup> Sur ce point, voy. le chapitre « Blockchain et droit public. Menace et/ou atout pour l'État ? », pp. 127 et s.

<sup>111</sup> F. A. HAYEK, *Denationalisation of Money*, Lancing, The Institute of Economic Affairs, 1976.

<sup>112</sup> La blockchain se veut être une « résurrection des utopies originelles de l'Internet et du Web » (B. CHRISTOPHE, « Du capitalisme sémantique aux NFT », *Psychanalyse YETU*, 2022, n° 1, p. 168).

<sup>113</sup> Dans un bref texte de 1988 qualifié de *Manifeste du crypto-anarchisme (The Crypto Anarchist Manifesto)*, Timothy C. May, informaticien, énonçait : « [c]omputer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive rerouting of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect

les États et les grands consortiums privés se sont emparés de cette technologie, d'un côté, pour la réguler, de l'autre, pour en faire des profits, de telle sorte que l'idéal libertaire commence à s'essouffler.

En outre, l'accroissement de blockchains privées et le développement de nouvelles techniques de validation des données (autres que le minage par preuve de travail) tendent à nous éloigner des caractéristiques initiales (et disruptives) de la blockchain. Face à l'émergence de blockchains « centralisées », c'est une analyse plus technique des coûts-bénéfices qui devra être opérée pour déceler l'utilité réelle de cette technologie nouvelle.

## Section 4. Plan de l'ouvrage

**46.** Le présent ouvrage est composé de cinq chapitres. Chacun traite de la blockchain et de ses applications (en particulier les cryptomonnaies, les *smart contracts* et les NFT) au regard d'une branche du droit ou discipline juridique.

D'abord, différentes questions *contractuelles* seront abordées (chapitre 1). Ensuite, les questions que suscite la blockchain au regard du *droit des données personnelles* seront analysées (chapitre 2).

Dans un troisième temps, nous observerons les questions qui se posent en matière de *droits intellectuels*. Il s'agira d'abord de déterminer si cette technologie peut faire l'objet d'une protection juridique, avant d'observer dans quelle mesure la blockchain peut elle-même avoir un impact sur les différents droits de la propriété intellectuelle. Une attention toute particulière sera ensuite attachée à une application spécifique de la blockchain : les NFT artistiques ; et les questions qu'ils posent en droit d'auteur (chapitre 3).

Dans un quatrième temps seront étudiés les aspects fiscaux des applications de la blockchain. Les auteurs aborderont en particulier le régime fiscal des investissements réalisés dans les cryptomonnaies. La fiscalité directe des plus-values réalisées grâce à la vente des NFT sera également évoquée (chapitre 4).

Enfin, la dernière partie de l'ouvrage sera consacrée à l'appréhension de la blockchain sous l'angle du droit public au sens strict (chapitre 5). À cet égard, la blockchain constitue à la fois une menace envers la souveraineté des États, mais également un outil sur lequel les États pourraient s'appuyer afin d'exercer certaines de leurs prérogatives.

---

*assurance against any tampering [...]. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation ».*