Les blockchains et les smart contracts en droit belge des obligations

Jacquemin, Herve; Cassart, Alexandre

Published in:
Les blockchains et les smart contracts à l'épreuve du droit

Publication date:
2020

Document Version
le PDF de l'éditeur

Les blockchains et les smart contracts en droit belge des obligations

Hervé Jacquemin

Professeur à l'Université de Namur (CRIDS – NaDI), avocat au barreau de Bruxelles

et

Alexandre Cassart

Avocat au barreau de Liège

Introduction

1. Enjeux de la blockchain et des smart contracts en droit des obligations. De manière schématique, la blockchain est une base de données dont la fonction principale est de créer la confiance des utilisateurs sans autorité centrale, en garantissant l'intégrité, la conservation à long terme et, dans une certaine mesure, la transparence des informations stockées. Cet objectif est atteint par la mise en place d'un registre distribué, le recours à la cryptographie asymétrique, ainsi que le respect de règles de consensus et de processus de validation pouvant impliquer des tiers (de type *proof of work*, par exemple). On précise immédiatement qu'à proprement parler, il n'existe pas une et une seule blockchain, mais plusieurs variétés de blockchains. Une distinction peut ainsi être faite entre les blockchains publiques (comme Ethereum ou Bitcoin) et les blockchains privées (ou de consortium), où un nombre limité d'acteurs définit les règles, spécialement en ce qui concerne l'accès à la chaîne des blocs et le processus de validation de ceux-ci[1].

[1] Pour une présentation technique de la blockchain, voy. la contribution de J.-N. Colin, dans le présent ouvrage. De manière générale, voy. aussi Y. Poullet et H. Jacquemin,

Si la blockchain offre des opportunités intéressantes dans de nombreux secteurs, elle est généralement citée comme technologie sous-jacente dans deux domaines clés : d'une part, en matière financière, avec les transactions réalisées en cryptomonnaies ou l'émission de jetons (tokens) pour lever des fonds auprès du public, d'autre part, avec les smart contracts, qui permettent d'automatiser certaines opérations en lien avec la formation, l'exécution ou la dissolution du contrat, sur la base d'instructions inscrites dans la chaîne des blocs.

La blockchain présente plusieurs caractéristiques qui constituent autant d'enjeux en droit des obligations : (i) il s'agit d'une technologie complexe ; (ii) les parties impliquées sont nombreuses et appelées à jouer des rôles différents et spécifiques ; (iii) les données figurant dans la blockchain présentent un caractère immuable et infalsifiable, empêchant normalement toute modification ultérieure, et permettant corrélativement une exécution automatique des instructions figurant dans le smart contract. Nous examinons ces trois éléments dans les paragraphes qui suivent.

2. Complexité de la technologie blockchain. À l'instar de l'informatique, de l'internet, du *cloud computing* ou de l'intelligence artificielle, la technologie blockchain est complexe et son recours croissant, dans de nombreux secteurs, suscite des interrogations – voire des craintes – légitimes de la part des personnes censées l'utiliser.

La blockchain est complexe en raison de la multiplicité des acteurs impliqués à des degrés divers (*cf. infra*, n° 3).

On doit aussi avoir égard à la variété des blockchains susceptibles d'être mises en place, ou à leur fonctionnement technique, qui peut exiger de recourir à des mécanismes complexes (comme la cryptographie asymétrique) ou à des règles de validation nouvelles et souvent mal connues (comme la *proof of work*). Le domaine dans lequel la blockchain est déployée peut encore creuser le déséquilibre – en termes informationnels,

---

« Blockchain : une révolution pour le droit ? », *J.T.*, 2018, pp. 801 et s. ; 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. ; 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 the 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*, https://blockchainfrance.net, 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.

notamment – entre les parties : on songe par exemple au secteur financier et aux risques associés aux transactions en Bitcoin ou aux investissements dans des ICOs.

Le cloud, l'IA ou l'informatique en général, supposent l'implication de plusieurs acteurs dont le niveau de connaissance et de maîtrise de la technologie en question varie sensiblement. On peut ainsi distinguer, d'une part, l'utilisateur, qui souffre généralement d'un manque de connaissance sur les caractéristiques du produit et les risques que son utilisation peut impliquer, sur le plan technique ou juridique (peu importe, du reste, que le client soit un professionnel ou un consommateur), d'autre part, un fournisseur de technologie, qui normalement connaît celle-ci et les risques associés, risques qu'il veille par ailleurs à limiter autant que possible, avec des clauses limitatives ou exonératoires de responsabilité dans les conditions contractuelles.

Avec la blockchain, le schéma est un peu plus compliqué (outre qu'il diffère suivant le type de blockchain). Prenons l'exemple du Bitcoin. On peut supposer que l'utilisateur reste généralement dans la même position de faiblesse caractérisée par un manque de connaissance sur des éléments de fait ou de droit de la technologie employée. Pour les autres acteurs, un examen au cas par cas est requis. Dans le cas de la *proof of work*, les mineurs possèdent des compétences et des moyens techniques importants (en termes de puissance de calcul) pour résoudre des problèmes mathématiques complexes grâce auxquels les blocs seront définitivement validés. Quant aux nœuds, sans lesquels la décentralisation de la blockchain ne serait pas possible, ils semblent intervenir de manière plus superficielle, en mettant à disposition de l'espace sur leurs serveurs (mais sans intervenir activement dans le fonctionnement de la chaîne des blocs).

Le droit – et spécialement le droit des obligations – a notamment pour objet de mettre en place des mécanismes préventifs et curatifs, en vue de garantir un niveau élevé de sécurité au bénéfice des parties impliquées. On songe aux obligations d'informations ou aux exigences de sécurité qui reposent sur le professionnel (pour le volet préventif), aux règles de responsabilité, ou de garanties, en cas d'inexécution des obligations convenues (pour le volet curatif). On examinera si ces régimes répondent adéquatement aux enjeux posés par la blockchain.

3. Intervention de nombreuses parties impliquées à des degrés divers. Les parties potentiellement impliquées dans la blockchain, et les transactions opérées à travers celles-ci, sont nombreuses. Par ailleurs, le rôle qu'elles sont appelées à jouer peut être délicat à caractériser, et à qualifier sur le plan juridique.

Dans l'exemple d'un paiement en Bitcoin, pour le volet « utilisateur », il faut ainsi avoir égard aux parties à la transaction (Alice qui verse 1 BTC à Bob), au prestataire qui génère le couple de clés cryptographiques, au prestataire qui fournit le service de wallet (et/ou le hardware associé, en cas de *cold wallet*, sur une clé USB), à la plateforme qui permet d'acquérir des Bitcoins contre des euros (par exemple), et de l'échanger ensuite, etc. Dans le volet « infrastructure blockchain », on pense 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 notamment en vue de concevoir des smart contracts. Ethereum veille d'ailleurs à s'identifier – Ethereum Fondation, relevant du droit suisse[2]. 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).

L'examen est sans doute plus simple dans l'hypothèse d'une blockchain privée ou de consortium, dès lors qu'un acteur donné (ou un groupe d'acteurs, issus du monde bancaire, par exemple) se détache plus précisément, et fixe des règles claires. Il faudra toutefois tenir compte de l'intervention éventuelle d'un fournisseur de technologie, qui a développé celle-ci en amont ou s'engage à le faire, sur mesure, à la demande des acteurs impliqués.

Le cas échéant, la qualité des parties peut justifier l'application de règles complémentaires. Tel est le cas si l'une d'elles est un consommateur. Des exigences additionnelles, censées protéger ce dernier, supposé en situation de vulnérabilité, devront en effet être observées. On précise que, dans la présente contribution, l'analyse se fait en droit des obligations classique, sans examiner de manière systématique les règles de protection des consommateurs.

Dès lors que chacune des parties impliquées dans un schéma blockchain peut prendre des engagements envers l'un ou l'autre des intervenants, on examinera s'il est raisonnable de considérer que des contrats bi- ou, plus probablement, multipartites sont conclus entre les acteurs, ou si un autre modèle devrait trouver à s'appliquer, pour rendre compte plus fidèlement de la spécificité des relations nouées entre les *stakeholders*.

[2] https://www.ethereum.org/foundation.

4. Caractère immuable et infalsifiable des données enregistrées dans la chaîne des blocs. Si la blockchain parvient à créer la confiance des utilisateurs en l'absence d'autorité centrale, c'est notamment parce qu'elle garantit que les données inscrites dans la chaîne ne pourront pas être modifiées, ni par les parties à la transaction, ni par des tiers. Elles sont normalement immuables et infalsifiables.

Cet avantage peut devenir un inconvénient s'il s'avère que, par dol ou simple négligence, les informations enregistrées sont erronées, ou que les parties poursuivent un objectif contraire à l'ordre public ou à certaines dispositions impératives. De même, dans l'hypothèse des smart contracts, l'instruction inscrite dans la blockchain s'exécutera automatiquement, en déclenchant un paiement en cryptomonnaies, par exemple. Peu importe que cette instruction soit par ailleurs illicite ou manifestement contraire à certaines exigences de droit des obligations contractuelles (une exception d'inexécution mise en œuvre en violation de l'exigence de proportionnalité, par exemple).

Comme on le verra, les règles de droit des obligations sont généralement caractérisées par une certaine flexibilité ; aussi faudra-t-il établir si elles peuvent s'accommoder de la rigidité et de l'immutabilité des informations enregistrées dans la blockchain.

5. Plan et limites de la présente contribution. Dans un premier temps, on veille à qualifier les opérations réalisées dans le cadre de ces technologies, afin d'identifier certaines règles matérielles susceptibles de s'appliquer (chapitre 1).

On examine ensuite les enjeux juridiques posés par la blockchain et les smart contracts à l'aune des règles à observer en matière de conclusion (chapitre 2) ou d'exécution des contrats, en ce compris les sanctions susceptibles d'être appliquées en cas d'inexécution (chapitre 3).

Enfin, on présente brièvement les régimes de responsabilité susceptibles de s'appliquer en cas de dommages résultant de l'utilisation de la blockchain ou des smart contracts (chapitre 4).

L'analyse est faite en droit belge des obligations. À certains égards, le résultat peut donc se révéler artificiel : vu le caractère transfrontalier des blockchains, on peut en effet s'attendre à ce que d'autres lois soient potentiellement applicables, conformément aux règles de droit international privé[3].

[3] Sur cette question, voy. la contribution d'A. COTIGA, dans le présent ouvrage.

CHAPITRE 1. Enjeux des qualification et règles applicables

6. Exercice de qualification. Pour la blockchain et les smart contracts, comme pour d'autres technologies émergentes, le juriste doit d'abord se prêter à un exercice de qualification, consistant à identifier les éléments pertinents de l'opération et, sur cette base, à classer celle-ci dans une catégorie déterminée (voire dans plusieurs catégories).

C'est en effet à l'aune du cadre normatif ainsi identifié que l'on pourra déterminer si les parties ont respecté les obligations qui leur incombent, à toutes les étapes du processus contractuel, ainsi que les sanctions susceptibles d'être prononcées en cas de manquement de l'une d'elles, tout en tenant compte des éventuelles limitations de responsabilité établies par ailleurs.

7. Plan du chapitre 1. Pour procéder à l'exercice de qualification, une distinction est faite entre les blockchains privées et les blockchains publiques, pour lesquelles les enjeux juridiques sont différents (section 1). On étudie ensuite les smart contracts en tant que tels (section 2).

SECTION 1. – Qualification des opérations réalisées dans le cadre de la blockchain

§ 1. Blockchain publique

8. Blockchain publique. Par souci de clarté, dans les lignes qui suivent, on prend l'exemple de la blockchain publique Bitcoin[4].

Dans cette blockchain publique, une distinction doit être faite entre les simples utilisateurs de la cryptomonnaie et ceux qui participent activement à son fonctionnement de la blockchain (celle-ci étant vue comme un système à part entière).

[4] Le cas échéant, un exercice similaire, avec une analyse au cas par cas, devrait être fait pour les autres blockchains publiques, dans la mesure où des variantes pourraient être observées ici ou là.

9. Relations impliquant les utilisateurs de cryptomonnaies. Les utilisateurs ont *d'abord* créé un portefeuille (wallet), en s'adressant à un prestataire spécifique. Plusieurs modèles existent, suivant que les clés privées sont stockées sur un périphérique externe (comme une clé USB spécifique), sur un ordinateur portable ou un smartphone, voire sur le web. On parlera de « cold » ou de « hot wallet » suivant que le portefeuille est respectivement hors ligne ou en ligne et, dès lors, plus vulnérable aux attaques éventuelles. Le portefeuille externe offre un niveau de sécurité plus élevé mais il présente l'inconvénient d'être plus complexe à utiliser et plus coûteux, puisqu'il faut acheter le matériel. Pour la création de leur portefeuille, les utilisateurs ont normalement dû se soumettre à des procédures de vérification de leur identité (KYC), conformément à 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 : celle-ci définit en effet les « monnaies virtuelles »[5], ainsi que les « prestataires de services de portefeuilles de conservation »[6]. On précise qu'en dépit de la terminologie utilisée, le wallet ne stocke en réalité aucun BTC : seule la clé privée est stockée dans le wallet. Les opérations relatives aux BTC sont enregistrées dans la blockchain Bitcoin et associées à une clé publique, accessible à tous. C'est en utilisant la clé privée stockée dans son wallet que l'utilisateur peut disposer de ses BTC et effectuer des transactions avec ceux-ci.

D'un point de vue contractuel, il s'agit de relations assez classiques entre un client-utilisateur, consommateur ou professionnel, et un prestataire qui fournit des services (la fourniture d'un wallet) ou des biens (le support USB permettant de stocker les clés privées, par exemple)[7]. On appliquera donc la théorie générale des contrats et des obligations[8], ainsi que les règles spécifiques aux contrats conclus à distance et par voie

[5] On vise 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 » (art. 4, 35°/1, de la loi).

[6] On vise 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 » (art. 4, 35°/2, de la loi).

[7] Il peut s'agir de prestataires distincts.

[8] *Cf.* le Code civil (règles générales et, le cas échéant, dispositions applicables aux contrats nommés, spécialement la vente et le louage d'ouvrage) et le livre VI du Code de droit économique (qui contient des règles spécifiques de protection au bénéfice des consommateurs et des entreprises).

électronique[9]. Si le client est un consommateur, on devra observer le cadre normatif spécifique établi en faveur de ce dernier[10], en particulier l'interdiction des clauses abusives[11] ou des pratiques commerciales déloyales[12], outre les obligations d'informations (assorties, le cas échéant, de formes corrélatives)[13], l'octroi d'une garantie pour les biens de consommation[14], des règles d'interprétations préférentielles[15] ou certaines interdictions[16]. On rappelle que, même entre professionnels, des régimes similaires ont été introduits : interdiction des clauses abusives[17], d'une part (inapplicables aux services financiers[18], cependant) et interdiction des pratiques du marché déloyales, en raison de leur caractère trompeur[19] ou agressif[20], et sur la base de la norme générale de loyauté[21]. Le cas échéant, des législations spécifiques ressortissant au domaine financier doivent également être observées. En pratique, des conditions générales et une charte vie privée *ad hoc* sont établis par le prestataire et une procédure plus ou moins développée est mise en place pour s'assurer de leur force obligatoire à l'égard du client.

Les utilisateurs se connectent ensuite à une plateforme à travers laquelle il est possible d'acheter et de vendre du Bitcoin (BTC). À ce stade également, une relation contractuelle est nouée entre l'intermédiaire et le client-utilisateur ; des conditions générales et une charte vie privée établissent les droits et les obligations des parties. Le cadre normatif évoqué précédemment peut également trouver à s'appliquer à cette relation. L'objet du service fourni diffère cependant : le prestataire joue davantage un rôle d'intermédiaire, qui se rapproche à de nombreux égards de celui d'un courtier, pour permettre à l'utilisateur d'effectuer des transactions en

[9] *Cf.* livre XII C.D.E., art. XII.6 à XII.11 et, si le client est un consommateur, les règles figurant aux articles VI.45/1 et s. (contrats à distance ne portant pas sur des services financiers, pour la clé USB, par exemple) et VI.54 et s. (contrats à distance portant sur des services financiers, pour le service de portefeuille en tant que tel).

[10] Outre les dispositions citées, on devra aussi tenir compte des dispositions visant à transposer la directive (UE) 2019/770 du Parlement européen et du Conseil du 20 mai 2019 relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques, *J.O.*, L136, 22 mai 2019.

[11] Art. VI.82 et s. C.D.E.

[12] Art. VI.92 et s. C.D.E.

[13] Art. VI.2 ou VI.45 C.D.E.

[14] Art. 1649*bis* C. civ.

[15] Art. VI.37 C.D.E.

[16] Art. VI.41 et s. C.D.E.

[17] Art. VI.91/1 et s. C.D.E.

[18] Art. VI.91/1, § 1er, C.D.E.

[19] Art. VI.105 à VI.109 C.D.E.

[20] Art. VI.109/1 à VI.109/3 C.D.E.

[21] Art. VI.104 C.D.E.

BTC. On observe que, dans certains cas, cette même plateforme se charge également de créer et de gérer le portefeuille du client ; le niveau de sécurité est donc assez faible, puisque l'utilisateur n'a pas une maîtrise totale et exclusive de son portefeuille.

Muni de ses BTC (ou d'une fraction de ceux-ci), le client a plusieurs options. À des fins d'investissement, il peut attendre que la valeur du BTC augmente, pour les échanger contre des euros ou des dollars, voire d'autres cryptomonnaies, et réaliser une plus-value[22]. Il peut également transférer tout ou partie de ses BTC à un tiers, à titre gratuit ou moyennant une contrepartie éventuelle, en utilisant la clé publique de celui-ci. Ce tiers doit donc également posséder un portefeuille BTC. Enfin, même si les hypothèses restent assez limitées, en tout cas en Europe, il pourrait acquérir des biens ou des services en les payant en BTC. Dans tous les cas, il devra faire appel à un intermédiaire qui se chargera d'inscrire l'opération dans la blockchain Bitcoin. Souvent, il s'agira du même prestataire que celui qui propose des services d'achat/vente de BTC. Ici aussi, un contrat est noué entre le prestataire et le client, régi par des conditions générales et une charte vie privée *ad hoc*, et soumis par ailleurs aux dispositions légales ou réglementaires applicables.

En principe, les relations contractuelles nouées entre les utilisateurs et les prestataires impliqués dans la fourniture de services en lien avec la blockchain publique peuvent être identifiées sans trop de difficultés. Il s'agit de contrats d'adhésion, régis par des conditions contractuelles établies par le prestataire, sans préjudice des règles applicables par ailleurs.

Par contre, aucun contrat spécifique n'est apparemment conclu entre l'utilisateur et la blockchain Bitcoin en tant que telle. On se heurte en effet à une difficulté de taille, consistant à identifier le cocontractant de l'utilisateur. La blockchain Bitcoin est en effet une communauté d'utilisateurs, qui ne possède pas la personnalité juridique, et n'est pas représentée par une personne physique identifiée ou identifiable (à noter que la situation pourrait être sensiblement différente pour d'autres blockchains). Du reste, au moment d'acheter la cryptomonnaie à travers la plateforme d'échanges, l'utilisateur n'est pas amené à accepter des T&C spécifiques – à supposer qu'ils existent – qui présenteraient les règles de fonctionnement de la blockchain ou les droits et les obligations des parties dans ce cadre. Il est par ailleurs possible de trouver des informations sur la blockchain Bitcoin et sur la cryptomonnaie éponyme[23]. Aussi incombe-t-il à l'utilisateur de se renseigner. Comme indiqué dans les conditions

[22] Le cas échéant, il peut également les échanger alors que la valeur a diminué par rapport au moment de leur acquisition, et subir ainsi une perte plus ou moins importante.

[23] Voy. not. le site bitcoin.org.

générales des intermédiaires, l'acquisition de cryptomonnaies présente des risques. En pratique, la situation est comparable à celle d'un investisseur qui décide d'acheter des actions d'une entreprise cotée en bourse sur un marché réglementé. À la différence de la blockchain BTC néanmoins, cette entreprise est une personne morale, qui existe, et contre laquelle il sera possible d'agir le cas échéant.

10. Personnes intervenant dans le système blockchain (et participant à son fonctionnement). Le fonctionnement d'une blockchain publique requiert l'intervention de plusieurs personnes.

Dans l'exemple de la blockchain Bitcoin, on distingue principalement les nœuds, qui mettent à disposition des ressources informatiques sur lesquelles les informations sont répliquées (c'est la fonction de registre distribué), et les mineurs, qui participent au processus de validation des blocs.

On doit également ajouter les programmeurs, qui contribuent à l'évolution de la blockchain. Elle suppose en effet la création d'un software, appelé à évoluer en continu (notamment pour répondre aux exigences de sécurité). La liste de ceux-ci est librement accessible.

Le site bitcoin.org contient diverses informations à l'attention de chaque catégorie d'intervenants[24]. Il aurait été créé à l'origine par Satoshi Nakamoto and Martti Malmi. Désormais, il se décrit comme un projet open source indépendant. Il indique également que « *Bitcoin.org is not Bitcoin's official website. Just like nobody owns the email technology, nobody owns the Bitcoin network. As such, nobody can speak with authority in the name of Bitcoin* »[25]. La blockchain appartiendrait donc à la communauté de ses utilisateurs, qui seraient libres de faire évoluer le logiciel, suivant le modèle du consensus.

La question se pose de l'existence d'un éventuel contrat conclu entre ces intervenants (nœuds, mineurs et programmeurs) et la blockchain Bitcoin.

Lorsqu'elles contribuent au fonctionnement de la blockchain, dans leurs rôles respectifs, ces personnes doivent respecter des protocoles et des règles techniques très précises. Ces exigences sont pour la plupart détaillées sur le site bitcoin.org. On peut les voir comme des obligations qui incombent aux participants. À certains égards, la relation devient synallagmatique, avec des droits et des obligations dans le chef du participant et dans celui de la blockchain : lorsqu'un mineur remporte le *proof of work*

[24] https://bitcoin.org/en/support-bitcoin.
[25] https://bitcoin.org/en/about-us#own.

et valide le bloc, il est récompensé en BTC (c'est du reste ce qui motive son intervention).

Peut-on considérer que les participants concluent un contrat – au sens de *negotium* – avec la blockchain Bitcoin ? On doute sérieusement que tel soit le cas, dans la mesure où cette blockchain n'est pas une entité dotée de la personnalité juridique et qu'aucun représentant n'est identifié. Il n'y a donc pas de cocontractant.

Tout au plus pourrait-on considérer la blockchain publique comme une association de fait rassemblant toute la communauté Bitcoin. L'hypothèse du contrat multipartites pourrait aussi être avancée mais elle paraît peu opérationnelle sur le plan pratique. Dans les deux cas, il semble très difficile, voire impossible, d'identifier précisément toutes les personnes physiques ou morales membres de cette communauté, éparpillée aux quatre coins du monde, soumis à des systèmes juridiques divers et variés, et dont le nombre est appelé à évoluer en permanence.

Un autre modèle – *sui generis* – devrait donc être construit, sur le plan juridique, pour comprendre correctement cette réalité. Le droit des sociétés pourrait utilement servir de source d'inspiration. À l'origine, il a en effet été créé parce que la théorie contractuelle ne permettait pas d'expliquer de manière satisfaisante les mécanismes développés dans le cadre des sociétés commerciales dotées de la personnalité juridique (comme la personnalité morale, par exemple)[26].

§ 2. Blockchain privée

11. Modèle contractuel adapté au cas par cas. Le modèle contractuel applicable aux blockchains privées se prête plus facilement à l'analyse : on part en effet du postulat qu'un acteur ou un groupe d'acteurs décide de constituer une blockchain dont il(s) maîtrise(nt) l'accès (on parle généralement de *permissioned blockchain*), en termes d'écriture et de lecture, ainsi que les règles de validation (généralement plus simples). Un nombre plus limité de nœuds est nécessaire et, globalement, les règles de gouvernance et de consensus sont normalement plus simples. Au final, les transactions sont validées plus rapidement que dans le cadre d'une blockchain publique.

À l'heure actuelle, il semble que le secteur financier – banques et assurances, principalement – soit particulièrement intéressé par la technologie,

[26] Voy. H. Culot, Y. De Cordt, H. Jacquemin et Th. Léonard, *Manuel du droit de l'entreprise*, Limal, Anthemis, 2019, pp. 100-101.

même si d'autres domaines sont également concernés, comme la *supply chain* ou l'énergie.

D'un point de vue contractuel, plusieurs aspects peuvent être distingués. On les analyse successivement. Par souci de clarté, on prend l'exemple d'une blockchain développée par des distributeurs dans le secteur de l'alimentation, en vue de permettre aux consommateurs de connaître et tracer l'origine de certains produits vendus en magasins[27]. Le potentiel des blockchains privées est important et d'autres modèles sont envisageables, avec des variantes plus ou moins substantielles. Le cas échéant, l'analyse devrait donc être répétée au cas par cas.

12. Relation entre les entités à l'origine de la blockchain. Si plusieurs acteurs décident de s'associer pour lancer une blockchain privée, il convient dans un premier temps d'organiser leur modèle de coopération. Dans l'exemple précité, on songe à de grands acteurs de la distribution, dans le secteur alimentaire.

Plusieurs possibilités existent.

Ils peuvent ainsi opter pour une *joint venture* ou un consortium (l'expression blockchain de consortium est d'ailleurs fréquemment utilisée). Le premier modèle ne fait pas l'objet d'une définition légale ou d'un régime juridique propre. On vise « le contrat de coopération à long terme conclu entre deux (ou plus) d'entreprises juridiquement et économiquement indépendantes et ayant pour objet la mise en commun de moyens en vue de la réalisation d'un projet conjoint prédéfini (élaboration d'un prototype, fabrication d'un produit, construction d'un grand ensemble immobilier, etc.) »[28]. Sa particularité est, en général, de reposer sur une double structure, contractuelle (avec la conclusion d'un accord de coopération) et sociétale (avec la constitution d'une filiale commune)[29]. Le consortium est quant à lui visé à l'article 1:19, § 1er, du Code des sociétés et associations, qui désigne « la situation dans laquelle une société, d'une part, et une ou plusieurs autres sociétés de droit belge ou étranger, d'autre part, qui ne sont ni filiales les unes des autres, ni filiales d'une même société, sont placées sous une direction unique ». Le paragraphe 2 de la disposition énonce ensuite les circonstances permettant de présumer, de manière irréfragable ou pas, si les sociétés sont placées sous une direction

[27] L'exemple s'inspire librement de la blockchain développée par Carrefour pour assurer la transparence de certains produits spécifiques (https://actforfood.carrefour.eu/fr/nos-actions/Acte-19).

[28] H. Culot, Y. De Cordt, H. Jacquemin et Th. Léonard, *Manuel du droit de l'entreprise*, *op. cit.*, pp. 306-307.

[29] *Ibid.*, p. 307.

unique. À ce niveau également, le droit des obligations contractuelles et le droit des sociétés sont mobilisés pour encadrer les échanges et définir la meilleure option de gouvernance.

Mis à part ces deux hypothèses, les parties peuvent aussi concevoir un contrat multipartite original, ou recourir à des formes de sociétés plus ou moins élaborées. On songe à la société simple, sans personnalité juridique (et assez facile à mettre en place), ou à la société coopérative par exemple (plus complexe sur le plan de la constitution, mais avec une certaine flexibilité dans la gestion).

De manière générale, on observe que la régulation dans le domaine reste très réduite, ce qui permet aux parties de concevoir le système avec une grande autonomie, par application de leur liberté contractuelle[30].

13. Relation avec un fournisseur de technologie. Les acteurs à l'initiative de la blockchain peuvent évidemment compter sur leurs propres ressources, en interne, pour développer la blockchain sur le plan technique.

Le plus souvent, un contrat sera conclu avec un prestataire IT spécialisé, chargé de concevoir les aspects techniques de la blockchain. Des acteurs comme IBM, par exemple, proposent ce type de prestation : il est possible d'utiliser une solution standard ou, au contraire, de postuler la conception et le développement d'un produit sur mesure.

La convention ainsi conclue devrait globalement contenir les clauses figurant en général dans un contrat de l'informatique[31]. Une attention

[30] Sans recevoir de consécration légale expresse dans le Code civil, il n'est pas contesté qu'il s'agit d'un principe fondamental du droit des contrats, qui permet aux parties de conclure (ou de ne pas conclure) le contrat, de choisir librement leur cocontractant, ainsi que la figure contractuelle retenue et son contenu (en ce sens, P. Wéry, *Droit des obligations*, vol. 1, *Théorie générale du contrat,* 2e éd., Bruxelles, Larcier, 2011, pp. 124 et s. ; P. Van Ommeslaghe, *Droit des obligations,* t. 1, Bruxelles, Bruylant, 2010, pp. 152 et s.).

[31] Aussi peut-on se référer, pour l'essentiel, aux développements réalisés depuis près de quarante ans, dans le domaine des contrats de l'informatique. Voy. F. George, J.-B. Hubin, N. Gillard et H. Jacquemin, « Contrats de l'informatique et commerce électronique. Chronique de jurisprudence en droit des technologies de l'information 2015-2017 », *R.D.T.I.*, 2017/68-69, pp. 9 et s. ; H. Jacquemin, « Contrats informatiques. Chronique de jurisprudence en droit des technologies de l'information (2002-2008) », *R.D.T.I.*, n° 35, 2009, pp. 29-41 ; J.-P. Triaille et R. Robert, « Titre VII. Les contrats informatiques », in Ch. Jassogne (dir.), *Traité pratique de droit commercial*, t. 1, 2e éd., Bruxelles, Kluwer, 2009, pp. 1077 à 1157 ; E. Montero, *Les contrats de l'informatique et de l'internet,* Tiré à part du Répertoire notarial, Bruxelles, Larcier, 2005 ; Ch. Steyaert, « Droit des obligations – Contrats », *Droit de l'informatique et des technologies de l'information. Chronique de jurisprudence (1995-2001)*, Les dossiers du Journal des tribunaux, n° 41, Bruxelles, Larcier, 2003, pp. 11 et s. ; J.-P. Buyle, L. Lanoye, Y. Poullet et V. Willems, « Chronique de jurisprudence : L'informatique (1987-1994) », *J.T.*, 1996, pp. 205 et s. ; J.-P. Buyle, L. Lanoye, et A. Willems, « Chronique de jurisprudence : L'informatique (1976-1986) », *J.T.*, 1988, pp. 93 et s.

spécifique devra être portée aux questions de responsabilité, de confidentialité (et de protection des données), ainsi qu'aux prestations complémentaires dans le cadre de la maintenance et de l'évolution continue du système mis en place.

14. Relation avec les utilisateurs. Dans l'exemple présenté en fil rouge de ce paragraphe 2, deux catégories d'utilisateurs de la blockchain peuvent être identifiées.

D'une part, les producteurs de denrées alimentaires – agriculteurs, éleveurs, etc. – qui enregistrent les informations utiles dans la blockchain à des fins de traçabilité ultérieure. Ceux-ci devraient veiller à s'identifier. Ils pourraient également jouer le rôle de nœud. Dans ce cadre, une procédure devrait être mise en place pour s'assurer qu'ils concluent un contrat avec l'acteur à l'initiative de la blockchain privée (ou le consortium ou la JV ou tout autre modèle constitué), dans lequel les obligations des uns et des autres seraient précisées.

D'autre part, les consommateurs qui, par le biais d'une application dédiée, pourront accéder aux informations stockées dans la blockchain en vue de connaître l'origine des produits qu'ils souhaitent acheter (par exemple en scannant un QR Code). À ce niveau également, rien n'empêche de séquencer le processus contractuel, pour s'assurer que les consommateurs aient l'occasion de prendre connaissance et d'accepter les conditions générales d'utilisation du service avant d'y accéder (comme pour toute autre application mobile ou site internet).

SECTION 2. – Qualification des opérations réalisées au moyen de smart contracts

§ 1. Le smart contract est-il un contrat ?[32]

15. Notion de smart contract et exemples. Le smart contract est un programme informatique dont l'exécution est automatisée, conformément aux instructions logicielles et algorithmiques inscrites dans la chaîne de blocs. Il a pour fonction d'accomplir, sans intervention humaine, certaines opérations en lien avec l'exécution ou la dissolution d'un contrat

[32] À ce propos, voy. notre analyse dans Y. POULLET et H. JACQUEMIN, « Blockchain : une révolution pour le droit ? », *op. cit.*, pp. 801 et s., dont les numéros qui suivent sont repris en partie.

(voire, plus rarement, avec sa formation). On considère généralement que le smart contract est conçu suivant la structure « *if this... then that...* »[33].

En pratique, les smart contracts peuvent par exemple être conçus dans la blockchain Ethereum, moyennant le recours au code *Solidity*[34].

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 8h30 », 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 2020, *alors* l'appartement XYZ sera déverrouillé et accessible à Alice du 15 mai 2020 au 20 mai 2020 ».

L'événement susceptible de déclencher l'opération de manière automatisée peut être certain (une date, par exemple) ou incertain (une tempête ayant dévasté les récoltes, par exemple). Cet événement peut être indépendant de la volonté des parties ou résulter du non-respect, par l'une d'elles, de ses obligations, volontairement ou par négligence. Dans l'hypothèse de l'événement incertain, les parties peuvent convenir de faire appel à un tiers de confiance pour confirmer sa survenance. On parle d'« oracle » (à ce sujet, voy. aussi *infra*, n° 18). Son intervention est normalement indispensable pour faire le lien entre la blockchain et un événement extérieur à celle-ci, tout en préservant la confiance des utilisateurs. Il s'agit *a priori* du maillon faible du système puisque, si on doute de la

[33] 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) », *op. cit.*, 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 », *op. cit.*, p. 306 et pp. 309 et s. (« *smart contracts are defined as agreements wherein execution is automated, usually by computers. Such 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* »). Voy. aussi E. Melchior, « Réflexions juridiques autour de la blockchain : analyse sous l'angle du droit des contrats », *R.D.T.I.*, 2018/3, pp. 52 et s. ; K. Verslype et B. Verheye, « Smart contracts », *Blockchain en smart contracts*, Gand, Larcier, 2019, pp. 72 et s. ; A. Cassart, « FinTech : l'art délicat de la disruption », in *Le droit des MachinTech (FinTech, LegalTech, MedTech...)*, Bruxelles, Larcier, 2018, pp. 79-99 ; Ch. Boillot, « Le « contrat » intelligent dit smart contract », in *La Blockchain saisie par le droit,* vol. 1, Paris, IRJS Edition, 2019, pp. 24 et s.

[34] https://solidity.readthedocs.io/en/v0.7.1/.

fiabilité de l'information clé fournie par l'oracle (elle est clé en ce sens qu'elle déclenche l'exécution du smart contract), le système blockchain ne convaincra pas.

Plusieurs exemples, souvent cités par la littérature, permettent d'illustrer le mécanisme.

La vente d'un immeuble peut être assortie d'une ou de plusieurs conditions suspensives : obtention d'un financement, confirmation que le bien ne fait pas l'objet d'infractions urbanistiques ou qu'il n'est grevé d'aucune charge, dette ou privilège, etc. On pourrait recourir au smart contract pour exécuter automatiquement le paiement d'un acompte ou de la totalité du prix, si les événements futurs et incertains se réalisent. Par exemple, si le financement est obtenu, le contrat est valablement conclu et doit être exécuté, ce qui engendre, dans le chef de l'acheteur, l'obligation de verser un acompte de 10 % du prix, par exemple. Concrètement, un oracle (le notaire instrumentant, par exemple) pourrait confirmer la réalisation des conditions, déclenchant automatiquement, et sans opposition possible des parties, le paiement en cryptomonnaies. En appliquant le mécanisme à toutes les vérifications que les notaires sont tenus d'effectuer, cela peut conduire à remplacer leur intervention par le recours à la blockchain (en tout cas pour ce volet de la vente – la chaîne des blocs n'étant pas encore capable de conseiller les parties en fonction des spécificités du cas d'espèce). Dans cette illustration, le smart contract est utilisé en marge de la *conclusion* des contrats.

Il peut l'être également au stade de leur *exécution*. Ainsi, après un sinistre tel qu'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. On peut aussi citer l'exemple du paiement convenu au titre de la location de l'appartement de vacances, qui déclenche la transmission au locataire d'un code lui permettant de déverrouiller la porte pendant la durée du bail.

Enfin, l'instruction déposée dans la blockchain peut avoir pour objet de mettre en œuvre une *sanction contractuelle* en cas de non-respect, par l'une des parties, des obligations qui lui incombent : on songe ici à l'immobilisation automatique d'un véhicule, l'échéance du leasing n'ayant pas été acquittée, ou au versement du montant prévu au titre de la clause pénale, en cas d'exécution tardive ou défectueuse (ledit défaut étant confirmé par un oracle, par exemple).

16. Origine (et nouveauté ?). C'est à Nick Szabo que l'on attribue, dans les années 1990, la paternité de l'expression « smart contract »[35], 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. 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[36]. Les contrats qui s'exécutent de manière automatique, moyennant l'intervention d'une application d'intelligence artificielle faible (mais sans blockchain) sont nombreux en pratique[37]. 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 précisément l'avantage de susciter la confiance, sans que l'intervention d'un tiers soit requise (la confiance résultant du système de registre distribué, dont la sécurité est garantie par le recours à la cryptographie asymétrique et à un processus de validation)[38].

L'intervention de la technologie pour créer la confiance pose des limites logiques lorsque l'opération implique une interaction avec l'environnement

---

[35] 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* ».

[36] Pour des réflexions en ce sens (en lien avec les smart contracts, voy. M. Raskin, « The Law and Legality of Smart Contracts », *op. cit.*, pp. 315 et s.).

[37] Outre l'exemple, précité, 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 – les commandes des utilisateurs lorsque des conditions prédéfinies ont été satisfaites (paiement reçu et biens en stock, par exemple).

[38] 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 », *op. cit.*, pp. 393 et s.).

« réel » : si le paiement du loyer entraine automatiquement la transmission du code permettant de déverrouiller la porte de l'appartement loué, rien n'empêche au propriétaire d'ajouter une nouvelle serrure, empêchant *de facto* au locataire de pénétrer dans l'appartement. L'efficacité du mécanisme aura donc tendance à se réduire dès l'instant où des interactions avec le réel sont nécessaires, soit en amont (pour déclencher l'exécution), soit en aval (pour mettre en œuvre ladite exécution). C'est d'ailleurs pour pallier cet inconvénient que le mécanisme de l'oracle a été conçu (*cf. infra*, n° 18).

17. En définitive, s'agit-il vraiment d'un contrat ? et est-il si *smart* ? Dans les hypothèses mentionnées au point précédent, 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[39] : 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.

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. 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 (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 »[40]. 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

[39] Voy. J.-Ch. Roda, « Smart contracts, dumb contracts ? », *op. cit.*, pp. 397 et s. ; M. Mekki, « Le contrat, objet des smart contracts (partie 1) », *op. cit.*, 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 », *op. cit.*, p. 514 ; Ch. Boillot, « Le « contrat » intelligent dit smart contract », *op. cit.*, p. 28.

[40] J. Gossa, « Les blockchains et smart contracts pour les juristes », *op. cit.*, pp. 393 et s.

l'intelligence artificielle ou de la robotique pourraient toutefois remettre en cause cette conclusion à moyen ou long terme.

On comprend donc, en définitive, que le terme « *smart* » - intelligent – est un peu galvaudé[41] (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 »[42].

§ 2. L'oracle

a) Présentation du rôle joué par l'oracle

18. À quoi sert l'oracle dans les smart contracts ? Les oracles établissent des liens entre le smart contract et le monde réel[43]. En effet, pour qu'un smart contract puisse intégrer des éléments extérieurs à sa propre blockchain, il doit disposer d'une source fiable de renseignements.

Les conditions d'exécution du contrat peuvent dépendre d'écritures dans le smart contract lui-même[44] ou bien d'indicateurs temporels pouvant être fournis informatiquement. Il n'y aura, dans cette hypothèse, pas de difficulté dans la vérification des conditions d'exécution, « puisque le contrat est programmé pour vérifier que ces conditions existent »[45] et qu'il dispose par lui-même de l'information requise.

Au contraire, il se peut que les conditions d'exécution dépendent d'autres facteurs, externes au smart contract. Qu'il s'agisse de la température d'un camion frigo, de l'évolution d'un indice financier, du chargement d'un colis dans un navire... Des capteurs, voire des personnes, vont

---

[41] 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* ? ».

[42] M. MEKKI, « Le contrat, objet des smart contracts (partie 1) », *op. cit.*, pp. 409 et s.

[43] « How do oracle services work under the hood ? », ETHEREUM STACK EXCHANGE, https://ethereum.stackexchange.com/questions/11589/how-do-oracle-services-work-underthe-hood.

[44] Des smart contracts peuvent évidemment uniquement intégrer des informations internes à leur propre exécution, et se déclencher en fonction de l'ajout d'un bloc particulier par exemple.

[45] E. MELCHIOR, « Réflexions juridiques autour de la blockchain: analyse sous l'angle du droit des contrats », *op. cit.*, n° 72, p. 52.

fournir une information, une donnée au smart contract pour que celui-ci puisse s'exécuter, ou pour qu'une condition précise soit vérifiée.

Ces systèmes ou ces personnes sont appelés les oracles. On distingue les oracles entrants – qui fournissent des informations – et les oracles sortants – qui agissent sur le monde réel en fonction du résultat du smart contract.

19. Diversité des oracles. Les oracles présentent une grande diversité. Ils peuvent être centralisés ou décentralisés, physiques ou informatiques, rémunérés en token ou en monnaies « réelles »...

Si l'oracle est centralisé, une entreprise ou une source en particulier, comme un service d'information météorologique, fournira l'information requise. Le plus souvent, l'oracle sera décentralisé, c'est-à-dire intégrant lui-même une chaîne de blocs. Dans ce cas, l'information devra être validée par les différents nœuds avant d'être communiquée au smart contract.

Ils peuvent également être purement logiciels ou partiellement physiques. Un oracle peut tout aussi bien être un script surveillant l'évolution d'un mot-clef sur Twitter, un capteur RFID dans un camion frigo, qu'un gardien dans sa guérite à l'entrée d'une usine comptant les camions.

Leur méthode de rémunération peut également varier, même si l'oracle – ou les opérateurs de nœuds en cas d'oracle décentralisé – est le plus souvent payé au moyen d'un token.

20. Cybersécurité. Étant les yeux et les oreilles des smart contracts, les oracles sont autant de points faibles en ce qui concerne la cybersécurité. Aussi créent-ils d'importantes exigences en termes de confiance.

Des solutions techniques sont donc mises en place pour pallier les potentielles failles de sécurité et augmenter la confiance, afin de vérifier, par exemple en multipliant les sources, la fiabilité des informations fournies.

Les oracles décentralisés permettent, par la validation de l'information par une majorité de nœuds, d'augmenter la sécurité. Cela étant, un oracle décentralisé doit atteindre une certaine masse critique pour éviter d'être manipulé trop aisément ou de subir certaines attaques informatiques. Par ailleurs, l'obtention de certaines informations ne se prête pas à un tel recoupement. Lorsqu'il s'agit de vérifier un paramètre spécifique par le recours à un capteur, il sera souvent peu économique de multiplier ces capteurs. La validation ultérieure d'une information déjà fournie par un capteur unique aurait en effet peu de sens.

Par ailleurs, la complexité d'un système est parfois impossible[46] à appréhender pour un logiciel. Il est alors nécessaire de faire appel à un être humain, avec tous les aléas et biais que cela implique.

Cette limitation pratique des oracles plaide pour une utilisation raisonnée et raisonnable des smart contracts. Cette technologie n'est, en effet, pas toujours la plus appropriée à l'usage projeté. Le recours à une base de données classique pourrait souvent constituer une option plus efficiente.

21. Tiers de confiance. Paradoxalement, les oracles conjurent le retour d'un semblant de tiers de confiance, là où la blockchain avait justement pour objet de remplacer les acteurs de la confiance (en créant celle-ci par la seule technologie).

Les oracles tels que compris ici ne rentrent *a priori* pas dans la définition de service de confiance fournie par l'article 3, 16°, du règlement eIDAS. Cette définition vise en effet « les services électroniques normalement fournis 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 ».

Dans certains aspects annexes de leur fonctionnement, les oracles peuvent – mais ce n'est pas obligatoire[47] – faire appel à des services de confiance, voire être considérés comme tels : signatures électroniques, horodatage...

Leur objet n'est toutefois pas de fournir de tels services contre rémunération, mais d'apporter une information, laquelle est éventuellement validée ou sécurisée au moyen d'un service de confiance.

A priori, aucune des obligations prévues par le règlement eIDAS ne s'applique donc aux oracles. Les garanties de fiabilité souhaitées par les parties utilisant le smart contract devront être trouvées dans un autre instrument juridique, qu'il s'agisse d'un contrat avec l'oracle ou dans les règles de gouvernance de celui-ci.

De lege ferenda, la question se pose néanmoins de l'encadrement – par exemple dans le règlement eIDAS – d'un nouveau service de confiance, dont les finalités pourraient correspondre à celles qui sont attendues de

[46] Ou très coûteuse.

[47] Sauf dans certains cas particuliers, comme en matière financière, voy. Y. POULLET et H. JACQUEMIN, « Blockchain : une révolution pour le droit ? », *op. cit.*, n° 6748, p. 812.

l'oracle (ou de certains oracles), dans la blockchain. Nous sommes favorables à l'adoption de telles règles, dont l'application reposerait sur une base volontaire, et qui seraient de nature à renforcer la confiance dans les processus envisagés. Comme indiqué précédemment, l'oracle – spécialement s'il implique une intervention humaine – est en effet le maillon faible du smart contract. Si son rôle est encadré, on peut réduire le risque corrélatif.

b) Qualification juridique de la relation avec l'oracle

22. Comment qualifier le rôle d'un oracle ? Si on considère que l'oracle est un service extérieur au système informatique permettant l'exécution du smart contract, comment qualifier juridiquement cette relation ?

Les hypothèses sont légion en fonction de la construction technologique et juridique adoptée par le service.

L'hypothèse principale étant une société identifiée offrant l'intégration de services d'oracles[48], ou une organisation décentralisée (de type DAO[49]).

23. Est-il possible de conclure une convention avec un oracle décentralisé ? Il convient tout d'abord de s'interroger sur la possibilité de nouer un contrat avec l'oracle. Est-il possible de conclure un contrat qui soit effectivement liant alors que les cocontractants sont une masse de personnes réparties dans le monde entier uniquement « identifiables » par une suite de signe, comme une adresse Bitcoin ? Un oracle prenant la forme d'un DAO (*Distributed Autonomous Organisation*[50]*), soit un service totalement décentralisé dans lequel les personnes physiques ou morales derrière les opérateurs de nœuds restent largement anonymes et les décisions prises en*

[48] Comme https://provable.xyz/ ou https://chain.link/ (cette dernière société étant basée dans les îles Cayman, son identification effective est probablement impossible. Cela démontre l'opacité de nombreux acteurs du secteur).

[49] Pour l'analyse d'un exemple concret de DAO, voy. Securities And Exchange Commission Securities Exchange Act Of 1934 Release No. 81207 / July 25, 2017 Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 : The DAO, https://www.sec.gov/litigation/investreport/34-81207.pdf. Voy. égal. D. Yermack, « Corporate Governance and Blockchains », *Review of Finance*, novembre 2016, working paper disponible sur https://ssrn.com/abstract=2700475. Voy. égal. du même auteur, https://corpgov.law.harvard.edu/2016/01/06/corporate-governance-and-Blockchains/.

[50] Y. Poullet et H. Jacquemin, « Blockchain : une révolution pour le droit ? », *op. cit.*, n° 6748, pp. 801-819.

fonction de « governance framework »[51], dispose-t-il d'une personnalité juridique en tant que telle ? *A priori* non[52], à défaut de rentrer dans l'une des catégories donnant droit à la personnalité juridique. Au mieux, la communauté dans son ensemble peut être considérée comme une association de fait, sans toutefois que cette qualification ne donne la moindre prise concrète à une personne souhaitant introduire une action en responsabilité contractuelle.

En l'état, le recours à des oracles décentralisés n'offre que très peu de garanties juridiques. Les clients de ces oracles ne pourront guère compter que sur les règles de gouvernance interne de l'oracle et la discipline de ses membres.

24. Contrat d'entreprise. La prestation de l'oracle se réalisera le plus souvent dans les liens d'un contrat d'entreprise. Si l'oracle est une société plus classique, identifiée et disposant de la personnalité juridique, cette société pourrait intervenir comme un sous-traitant de l'entreprise fournissant le logiciel de smart contract ou directement comme prestataire de services pour les parties au smart contract. Cette solution est bien plus simple juridiquement, mais ne plaira sans doute guère aux *geeks,* adeptes de la décentralisation.

L'oracle interviendra alors dans le cadre d'un contrat d'entreprise.

La doctrine et la jurisprudence définissent habituellement le contrat d'entreprise comme « la convention par laquelle une personne, l'entrepreneur, s'engage envers une autre, le maître de l'ouvrage, à effectuer, moyennant le paiement d'un prix, un travail ou un service déterminé, sans aliéner son indépendance dans l'exécution matérielle de ses engagements ni disposer d'un pouvoir de représentation »[53].

Le cas échéant, mais moins souvent qu'en présence d'oracles décentralisés, le paiement du prix pourra se faire au moyen d'un token.

Si l'oracle est choisi par le fournisseur du système de smart contract et intervient comme son sous-traitant, l'entrepreneur principal devra vérifier l'indépendance de l'oracle, et si le degré de fiabilité de l'oracle était

[51] Ou Whitepaper. Pour les défis liés à la gouvernance de ce type d'organisation, voy. P. De Filippi et B. Loveluck, « The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure », *Internet Policy Review*, 5(3), 2016, https://policyreview.info/articles/analysis/invisible-politics-bitcoin-governance-crisis-decentralised-infrastructure.

[52] Certains États réfléchissent à fournir cette possibilité, sans doute afin d'attirer les entrepreneurs, comme Malte : https://www.mondaq.com/fin-tech/707696/legal-personality-for-blockchains-daos-and-smart-contracts.

[53] Cass., 3 octobre 1961, *Pas.*, 1962, I, p. 142; Bruxelles, 19 décembre 2002, *Res jur. imm.*, 2003, p. 138 cités par B. Kohl, *Contrat d'entreprise*, Bruxelles, Bruylant, 2016, pt 6, p. 22.

pertinent par rapport aux besoins exprimés des parties. Il sera en outre responsable[54] des éventuels manquements de l'oracle, son sous-traitant, conformément aux principes bien connus.

Si l'oracle est choisi directement par les parties, il sera tenu, à l'instar des autres fournisseurs informatiques, d'un devoir de conseil en proportion du degré d'expertise technologique des parties[55].

25. L'oracle peut agir comme mandataire, voire comme tiers décideur. Si la prestation attendue de l'oracle sortant implique la réalisation d'un acte juridique au nom et pour le compte d'une des parties au smart contract, le contrat entre l'oracle et les parties pourrait être qualifié de contrat de mandat.

L'oracle sortant interviendra donc en tant que mandataire de l'une ou de l'autre partie au smart contract.

Étant donné l'importance de l'apport d'information pour la vérification des conditions prévues dans le smart contract et donc son exécution, on pourrait envisager de qualifier les oracles de tiers décideurs. En fonction de leur apport d'information, le contrat s'exécutera en effet différemment.

La plupart des oracles apportent toutefois uniquement une information qui est confrontée à la condition prévue dans le smart contract. La teneur de cette condition n'est pas connue de l'oracle.

La décision sera prise alors automatiquement par le smart contract sur base de l'information fournie par l'oracle et des critères définis par les parties. L'oracle ne prend alors lui-même aucune décision[56].

c) Conclusions sur le recours aux oracles

26. Quelles règles pour encadrer l'intervention des oracles ? Pour autant que l'oracle dispose de la personnalité juridique, il sera généralement qualifié de prestataire de service informatique, qui interviendra dans le cadre d'un contrat d'entreprise et sera tenu des obligations classiques d'un entrepreneur, ou d'un sous-traitant.

---

[54] Sous réserve qu'il ne puisse pas bénéficier de l'exemption de responsabilité ouverte aux prestataires intermédiaires de services de la société de l'information, établie aux articles XII.15 et suivants du Code de droit économique, voy. H. JACQUEMIN et Y. POULLET, « Blockchain : une révolution pour le droit ? », *op. cit.*, n° 6748, pp. 810-811.

[55] Voy. not. à ce sujet E. MONTERO, « Les contrats de l'informatique et de l'internet », *Rép. not.*, t. IX, l. IX, Bruxelles, Larcier, 2004, ou B. DOCQUIR, *Droit du numérique*, Bruxelles, Larcier, 2018, pp. 22-33.

[56] Il est bien sûr envisageable de charger un oracle de répondre à une question. Sa réponse aura alors la valeur contractuelle que les parties auront bien voulu lui reconnaître.

Par ailleurs, quand bien même les exigences en matière de fiabilité de l'oracle seront très importantes pour la bonne exécution du smart contract, celui-ci échappera aux règles applicables aux services de confiance. Les parties devront donc être particulièrement attentives, lors de la mise au point de leur smart contract, aux oracles qu'elles choisissent[57] et aux garanties qu'elles peuvent en tirer.

En conclusion sur ce point, les parties doivent tenir compte des limites du recours aux oracles, tant en termes de fiabilité qu'en termes de pertinence par rapport à l'information utile à obtenir, lors de leur réflexion sur le choix d'utiliser un smart contract. L'utilisation d'un smart contract plutôt qu'un contrat traditionnel appuyé sur des technologies classiques peut s'avérer bien plus pertinente que de succomber à l'effet de mode des smart contracts.

CHAPITRE 2. La blockchain et les smart contracts à l'épreuve des conditions de formation des contrats

SECTION 1. – Obligations contemporaines à la formation des contrats

27. D'un point de vue statique, conditions de validité 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 ».

Comme on l'a vu, la technologie est complexe, et certains intervenants difficiles à identifier. Aussi peut-on se demander si ces conditions sont observées lors de l'utilisation de la technologie blockchain ou de smart contracts. On examine les obligations d'information au stade précontractuel, l'interdiction des pratiques commerciales (ou du marché) déloyales, ainsi que les vices du consentement et la cause.

28. Obligation d'information au stade précontractuel. Le consentement doit être libre et éclairé. De nombreuses dispositions légales ou

[57] Ou aux critères de sélection si un oracle est choisi en cours d'exécution du smart contract.

réglementaires – en droit de la consommation notamment – imposent ainsi à la partie théoriquement la mieux renseignée d'informer le cocontractant potentiel (voy. *infra*, n° 29).

Parallèlement, la doctrine et la jurisprudence ont dégagé diverses obligations d'information (à charge de l'une des parties ou des deux parties) visant précisément à permettre à chaque cocontractant de consentir en pleine connaissance de cause[58]. Elles trouvent leur source dans l'exigence de bonne foi[59], qui s'impose à toutes les étapes du processus contractuel.

Par identité de motifs, on peut d'ailleurs s'appuyer sur la jurisprudence rendue dans le domaine des contrats de l'informatique, qui s'est révélée un terreau fertile[60]. Les cours et tribunaux ont ainsi précisé les contours de cette obligation d'information, tout en veillant à sanctionner sa méconnaissance de manière adéquate[61]. De manière générale, le prestataire doit ainsi informer le client sur les éléments caractéristiques du matériel fourni ou du logiciel installé. Il doit le conseiller ou le mettre en garde, à la lumière de ses attentes ou besoins concrets[62]. Cette obligation d'information lui impose également de se renseigner[63]. Parallèlement, le client a l'obligation de collaborer de bonne foi à la définition du projet, en lui communiquant les informations demandées.

La technologie blockchain (et les smart contracts intégrés dans celle-ci, le cas échéant) est assurément complexe, ce qui peut présenter des risques pour la sécurité des utilisateurs ou des tiers.

Aussi sommes-nous d'avis qu'une obligation d'information devrait normalement reposer sur les prestataires impliqués dans la fourniture d'une application blockchain, pour présenter ses caractéristiques,

---

[58] À ce sujet, voy. P. Wéry, *Droit des obligations*, vol. 1, *Théorie générale du contrat,* 2e éd., *op. cit.*, pp. 151 et s. ; P. Van Ommeslaghe, *Droit des obligations*, t. 1, *op. cit.*, pp. 534 et s.

[59] Art. 1134, al. 3, C. civ.

[60] On ne s'en étonne guère, eu égard à l'objet de la prestation, par nature très technique, et au déséquilibre généralement constaté entre les parties, en particulier sur le plan des connaissances.

[61] Le non-respect de l'obligation d'information visant à protéger le consentement des parties est généralement sanctionné sur le fondement des articles 1382 et 1383 du Code civil. Une faute, en lien de causalité avec un dommage, doit ainsi être démontrée. Le client pourrait également arguer que son consentement a été vicié, à la suite d'une erreur, et demander en conséquence l'annulation du contrat.

[62] Soulignant l'obligation d'information du fournisseur au moment de la commande, voy. Liège, 19 février 2002, *Entr. Dr.*, 2003, p. 133.

[63] Bruxelles, 11 décembre 2007, inédit, 2007/AR/2207 : « c'est à la SA I., spécialiste en la matière, qu'il incombait de s'informer précisément des exigences et espérances du client, du matériel dont il disposait et du hardware et du software dont il aurait besoin pour atteindre le résultat souhaité ».

fonctionnalités, ainsi que les risques qu'elle peut présenter (indépendamment du respect des normes techniques applicables par ailleurs).

Des obligations d'information spécifiques figurent également dans les règles générales de protection des consommateurs[64], et les règles sectorielles spécifiques, notamment dans le secteur financier[65].

L'existence d'un cadre normatif protecteur pourrait toutefois rester lettre morte si le débiteur de l'obligation est difficile, voire impossible, à identifier. Comme on l'a vu, tel pourrait être le cas dans l'hypothèse d'une blockchain publique, la blockchain en tant que telle n'ayant pas la personnalité juridique et n'étant pas représentée par une personne physique ou morale identifiable.

29. Interdiction des pratiques commerciales (ou du marché) déloyales. Aux termes de l'article VI.95 du Code de droit économique, « les pratiques commerciales déloyales des entreprises à l'égard des consommateurs sont interdites ». La notion de « pratique commerciale » est définie largement[66]. Pour qualifier une pratique de déloyale, il faut d'abord vérifier si elle figure dans la liste des pratiques jugées trompeuses ou agressives en toutes circonstances[67]. Dans un deuxième temps, le caractère déloyal de la pratique doit s'apprécier à l'aune de la norme semi-générale. Le C.D.E. interdit en effet les pratiques trompeuses, par action ou par omission[68], ainsi que les pratiques agressives[69]. En dehors des deux hypothèses précitées, la pratique commerciale ne peut être considérée comme étant déloyale, et donc interdite, que si « a) elle est contraire aux exigences de la diligence professionnelle et b) elle altère ou est susceptible d'altérer de manière substantielle le comportement économique, par rapport au produit, du consommateur moyen qu'elle touche ou auquel elle s'adresse, ou du membre moyen du groupe lorsqu'une pratique commerciale est ciblée vers un groupe particulier de consommateurs »[70] (norme générale).

Sans que ce soit imposé par le droit de l'Union, le législateur belge a introduit un régime similaire dans les relations entre entreprises. Plus précisément, l'interdiction des pratiques trompeuses et agressives, suivant la norme semi-générale, a été reprise et, sous réserve de modifications

[64] On songe aux obligations relatives aux principales caractéristiques des biens ou des services, ou aux fonctionnalités des contenus numériques (art. VI.45, § 1er, 1° et 18°, C.D.E.).

[65] Voy. les contributions de D. Szafran et M. Defosse, dans le présent ouvrage.

[66] Art. I.8, 23°, C.D.E.

[67] Art. VI.100 et VI.103 C.D.E.

[68] Art. VI.97-VI.99 C.D.E.

[69] Art. VI.101-VI.102 C.D.E.

[70] Art. VI.93 C.D.E.

mineures, appliquée aux entreprises[71]. Par ailleurs, l'interdiction des actes contraires aux pratiques honnêtes du marché reste d'application et peut être vue comme la norme générale à respecter dans les relations B2B.

Une pratique est ainsi trompeuse lorsqu'elle peut induire en erreur sur les « caractéristiques principales du produit, telles que [...] les risques qu'il présente, [...] son aptitude à l'usage, son utilisation, [...] ses spécifications, son origine géographique ou commerciale ou les résultats qui peuvent être attendus de son utilisation, ou les résultats et les caractéristiques essentielles des tests ou contrôles effectués sur celui-ci »[72]. La Commission européenne a par ailleurs considéré que la complexité du produit impliquait de communiquer davantage d'information à son propos[73]. La technologie blockchain, en ce compris les smart contracts, constitue assurément un produit complexe, pour lequel une obligation d'information renforcée devrait reposer sur le prestataire qui intervient dans sa fourniture. Cela étant, et comme déjà indiqué, encore faut-il identifier ce dernier... Si cela semble normalement possible dans le cadre d'une blockchain privée ou de consortium, des difficultés seront rencontrées pour les blockchains publiques.

30. Un consentement exempt de vice en matière de blockchain et de smart contracts. Le manque d'information évoqué au point précédent pourrait également donner lieu à un vice de consentement dans le chef du cocontractant (erreur ou dol). L'erreur pourrait ainsi porter sur l'objet même du contrat (par exemple parce que les risques engendrés par l'utilisation d'une blockchain n'avaient pas été suffisamment compris) ou sur la personne du cocontractant. Cette dernière hypothèse pourrait notamment se rencontrer dans les blockchains publiques, où les parties sont identifiées au moyen d'une clé publique.

Par ailleurs, s'agissant des smart contracts, c'est surtout au moment de traduire la volonté des parties dans le code informatique que des problèmes pourraient survenir[74]. 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

[71] Art. VI.105-VI.109 C.D.E. pour les pratiques trompeuses ; art. VI.109/1-VI.109/3 pour les pratiques agressives.

[72] Art. VI.97 et VI.105 C.D.E.

[73] Commission européenne, « Document de travail des services de la Commission – Orientations pour la mise en œuvre et l'application de la directive 2005/29/CE sur les pratiques commerciales déloyales », 3 décembre 2009, SEC(2009) 1666.

[74] M. Raskin, « The Law and Legality of Smart Contracts », *op. cit.*, 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* »).

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.

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[75]. L'exception de nullité paraît par contre plus délicate à invoquer par le débiteur, dans l'hypothèse où le créancier lui demanderait l'exécution de la convention. Par définition, cette exécution ne relève plus du contrôle des parties.

31. La cause en cas de recours à certaines blockchains publiques et cryptomonnaies. Même si on peut le regretter, de nombreuses personnes procèdent à des transactions en cryptomonnaies en raison de l'anonymat (ou du pseudonymat, le cas échéant) que la blockchain leur procure. En effet, dans le registre, seule leur clé publique est mentionnée. En dépit des obligations qui pèsent désormais, en droit de l'Union et dans les États membres, sur les « prestataires de services de portefeuille de conservation » conformément à 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, on peut craindre qu'il reste difficile d'identifier certains titulaires de clés privées.

À supposer que cette identification soit possible, la question se pose de la validité du contrat conclu avec les prestataires intervenant dans le cadre de la blockchain, s'il apparaît que le mobile de la création du portefeuille, de l'acquisition de cryptomonnaies auprès d'une plateforme d'échanges et, ensuite, du transfert de ces cryptomonnaies à un tiers, résidait dans la volonté de blanchir des capitaux, d'éluder l'impôt ou de rémunérer une activité illicite.

On pourrait en effet considérer que les conventions conclues à cette fin sont affectées d'une cause illicite. L'article 1131 du Code civil énonce que l'obligation « sur une cause illicite [...] ne peut avoir aucun effet ».

[75] 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.

À l'article 1133 du même Code, il est précisé que « la cause est illicite, quand elle est prohibée par la loi, quand elle est contraire aux bonnes mœurs ou à l'ordre public ». Si la cause comme condition de validité des conventions fait débat en doctrine et en jurisprudence, notamment quant à l'acception qu'il convient de lui donner, il semble admis, de manière générale, que lorsque l'une des parties est animée de mobiles illicites, la convention doit être frappée de nullité absolue[76]. La jurisprudence a appliqué la règle à des conventions visant à éluder l'impôt en organisant une fraude au carrousel TVA. La Cour de cassation a ainsi jugé qu'« une convention qui a pour but d'organiser une fraude envers des tiers dont les droits sont protégés par une législation d'ordre public, a une cause illicite et est frappée de nullité absolue »[77]. Elle précise par ailleurs que, « s'agissant de l'intérêt général, il suffit que l'une des parties ait contracté à des fins illicites et qu'il n'est pas nécessaire que ces fins soient connues du cocontractant ». Nonobstant certaines critiques doctrinales, le mobile illicite unilatéral est ainsi accepté par la jurisprudence.

En l'occurrence, et par identité de motifs, on devrait considérer qu'est illicite le mobile qui anime la personne qui ouvre un portefeuille auprès d'un prestataire, acquiert des cryptomonnaies auprès d'une plateforme et les transmet ensuite à un tiers pour financer des activités illicites ou blanchir de l'argent. En pratique, on se heurtera toutefois à plusieurs difficultés, tenant d'abord à l'identification de la personne concernée et à la démonstration de son mobile illicite. À supposer que ce soit acquis, si les conventions avec les intermédiaires – fournisseur de portefeuille et plateforme d'échange – peuvent être théoriquement annulées, les opérations inscrites dans la blockchain Bitcoin (notamment le transfert des BTC de A à B) ne pourront pas être supprimées. Le cas échéant, on pourrait toutefois envisager de corriger celles-ci ultérieurement, par exemple en imposant un transfert équivalent de B à A.

SECTION 2. – *De lege ferenda*, consécration de principes de non-discrimination et de présomptions

32. Le recours à la blockchain ou aux smart contracts pourrait-il être vu comme un obstacle à la conclusion des contrats ? Comme pour

[76] P. Wéry, *Droit des obligations*, vol. 1, *Théorie générale du contrat*, 2e éd., *op. cit.*, pp. 290 et s.

[77] Cass., 12 octobre 2000, *R.C.J.B.*, 2003, p. 73, note P. Wéry.

d'autres technologies auparavant, d'aucuns pourraient considérer que le régime juridique actuellement applicable ne permet pas de recourir à la technologie blockchain ou aux smart contracts pour conclure des contrats. À tout le moins, même si le cadre normatif n'interdit pas le recours à de tels procédés, la sécurité juridique pourrait être affectée.

De même, la recevabilité et la force (ou la valeur) probante des moyens de preuve tirés de la blockchain pourraient être contestées ; les effets juridiques attachés aux smart contracts pourraient par ailleurs être refusés en cas de litige.

33. Pistes de solutions. Conformément l'article 9, § 1er, de la directive sur le commerce électronique[78], « les États membres veillent à ce que leur système juridique rende possible la conclusion des contrats par voie électronique. Les États membres veillent notamment à ce que le régime juridique applicable au processus contractuel ne fasse pas obstacle à l'utilisation des contrats électroniques ni ne conduise à priver d'effet et de validité juridiques de tels contrats pour le motif qu'ils sont passés par voie électronique ». Si cette disposition visait les exigences de forme (comme l'écrit ou la signature, par exemple), d'autres obstacles étaient également envisagés[79]. Dès lors que la blockchain et les smart contacts impliquent le recours à des moyens électroniques, nous sommes d'avis que l'obligation figurant à l'article 9 de la directive devrait s'appliquer à cette hypothèse.

Le législateur est déjà intervenu pour lever les obstacles à l'accomplissement des exigences de forme dans un environnement dématérialisé. Les principales règles en la matière se trouvent dans le (nouveau) Code civil (livre 8) et à l'article XII.15 du Code de droit économique. En droit de l'Union, il faut avoir égard au règlement eIDAS[80]. Ces dispositions

[78] Dir. 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »), *J.O.*, L 178, 17 juillet 2000.

[79] Voy. le considérant n° 34 de la directive, « chaque État membre doit ajuster sa législation qui contient des exigences, notamment de forme, susceptibles de gêner le recours à des contrats par voie électronique. Il convient que l'examen des législations nécessitant cet ajustement se fasse systématiquement et porte sur l'ensemble des étapes et des actes nécessaires au processus contractuel, y compris l'archivage du contrat. Il convient que le résultat de cet ajustement soit de rendre réalisables les contrats conclus par voie électronique [...] ». Des obstacles étrangers aux règles de forme pourraient également être rencontrés (à ce sujet, voy. M. Demoulin et E. Montero, « Le formalisme contractuel à l'heure du commerce électronique », in *Commerce électronique : de la théorie à la pratique*, Cahier du CRID, n° 23, Bruxelles, Bruylant, 2003, pp. 160-161).

[80] Règl. (UE) n° 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

consacrent notamment deux principes directeurs pour lever les obstacles formels : un principe de non-discrimination et un principe d'assimilation (ou une présomption).

De lege ferenda, nous sommes d'avis que, pour assurer un niveau élevé de sécurité juridique, de tels principes devraient également être consacrés pour le recours à la technologie blockchain ou aux smart contracts (à ce sujet, voy. *infra*, n^os^ 34-35).

Nous avions déjà plaidé en ce sens concernant le recours aux applications d'intelligence artificielle dans le processus contractuel[81]. Idéalement, les modifications normatives devraient être conçues de manière suffisamment large – et neutre sur le plan technologique – pour viser ces deux technologies, de préférence en identifiant des éléments communs (comme le caractère automatique ou autonome). La directive sur le commerce électronique est en cours de révision et devrait être remplacée par un *Digital Services Act*. Celui-ci pourrait par exemple consacrer de telles clauses transversales de non-discrimination et d'assimilation au profit des applications d'intelligence artificielle et de blockchain.

Indépendamment (et dans l'attente) de cette intervention normative, les parties peuvent renforcer la sécurité juridique en convenant, contractuellement, que l'une d'elles (ou les deux) pourront recourir à la blockchain ou aux smart contracts à l'occasion du processus de formation des contrats. Les parties formaliseront ainsi l'acceptation du recours à ce type de technologie, tout, en lui donnant des effets juridiques similaires à un contrat « traditionnel ».

34. Principe de non-discrimination. Le règlement eIDAS applique le principe de non-discrimination au document électronique, en énonçant que « l'effet juridique et la recevabilité d'un document électronique comme preuve en justice ne peuvent être refusés au seul motif que ce document se présente sous une forme électronique »[82]. Il en va de même pour la signature électronique[83], le cachet électronique[84], l'horodatage électronique[85], les données envoyées et reçues à l'aide d'un service d'envoi

au sein du marché intérieur et abrogeant la directive 1999/93/CE, *J.O.*, L 257, 28 août 2014.

[81] H. Jacquemin et J.-B. Hubin, « Aspects contractuels et de responsabilité civile en matière d'intelligence artificielle », in *L'intelligence artificielle et le droit*, coll. du CRIDS, Bruxelles, Larcier, 2017, pp. 105 et s.

[82] Art. 46 règl. eIDAS.

[83] Art. 25, § 1^er^, règl. eIDAS.

[84] Art. 35, § 1^er^, règl. eIDAS.

[85] Art. 41, § 1^er^, règl. eIDAS.

recommandé électronique[86], ainsi que l'archivage électronique[87]. Pour les services de confiance, l'interdiction de toute discrimination est double, en ce qu'elle s'applique, d'une part, au bénéfice d'un service de confiance non-qualifié (par rapport à un service qualifié), d'autre part, au bénéfice d'un service de confiance – par définition de nature électronique – par rapport à un procédé correspondant dans l'environnement papier (une signature manuscrite par exemple). S'agissant du document électronique, seule cette seconde interdiction existe.

Avec ce principe, c'est la dématérialisation des échanges, et le recours aux technologies de l'information et de la communication dans les transactions électroniques, que le législateur entend défendre. Les règles adoptées perdraient tout effet utile si, en cas de litige, la juridiction pouvait tout simplement refuser d'examiner le procédé (un procédé de signature électronique appliqué à un courriel, par exemple) au seul motif qu'il est électronique.

La technologie blockchain et les smart contracts devraient également bénéficier de ce principe. Il faut en effet éviter que lorsqu'il y recourt, l'un des cocontractants puisse échapper à ses obligations sous prétexte que les moyens de preuve dont l'autre partie entend se prévaloir sont tirés de la blockchain ou que l'automatisation – au moment de la formation du contrat, de son exécution ou de la sanction en cas d'inexécution – résulte du recours à un smart contract.

À tout le moins, la juridiction saisie du litige ne pourrait donc pas écarter la technologie à laquelle les parties ont décidé de recourir sous prétexte qu'elle s'appuie sur la blockchain ou les smart contracts.

35. Présomption. Lorsqu'il lève les obstacles à l'accomplissement des formes dans l'environnement numérique, le législateur complète généralement la règle de non-discrimination d'une règle d'assimilation, ou d'une présomption, qui mobilise le principe d'équivalence fonctionnelle[88]. Par

[86] Art. 43, § 1er, règl. eIDAS.

[87] Art. XII.25, § 4, C.D.E.

[88] Ce principe part du constat que les procédés mis en œuvre dans l'environnement papier pour accomplir les formes prescrites ne peuvent être reproduits comme tels lorsque le contrat est conclu par voie électronique. Si l'on souhaite que des rapports contractuels puissent être noués par ce biais, il doit être possible d'identifier les procédés à mettre en œuvre dans l'environnement numérique. Suivant la théorie des équivalents fonctionnels, on ne définit pas une exigence de forme par référence à un procédé technique particulier (le support papier pour l'écrit, le graphisme personnel et manuscrit apposé directement sur le support pour la signature, etc.) mais à la lumière des fonctions qu'elle permet de remplir (garantir la lisibilité, la pérennité, voire l'intégrité de l'information, pour l'écrit, par exemple). Deux procédés accomplis respectivement dans l'environnement traditionnel (le support papier pour l'écrit, par exemple) et dans l'environnement numérique (un document au

exemple, l'article 25, § 2, du règlement eIDAS énonce que « l'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite »[89].

Nous sommes d'avis qu'une présomption pourrait également être établie dans le domaine de la blockchain, eu égard aux fonctions que la technologie permet de préserver. À tout le moins, il semble en effet admis que la blockchain garantit l'intégrité des informations inscrites dans la chaîne, ainsi que leur chronologie. Une telle présomption présenterait un intérêt certain si la technologie est par ailleurs utilisée en matière d'archivage électronique ou pour certaines activités dans le cadre desquelles ces fonctionnalités sont importantes.

On pourrait donc présumer que ces fonctions sont atteintes lorsqu'une blockchain est utilisée, ce qui est notamment utile pour démontrer que certaines exigences de forme ont été valablement accomplies.

En introduisant une présomption, on renverse la charge de la preuve en faveur du cocontractant. Cette présomption devrait toutefois être réfragable.

CHAPITRE 3. Le smart contract comme moyen d'automatiser l'exécution du contrat

36. Fonction d'automatisation. La technologie permet déjà depuis plusieurs années l'exécution mécanique et rapide de contrats. Pensons au

format pdf enregistré sur un CD-ROM pour l'écrit, par exemple) sont alors jugés équivalents s'ils permettent de remplir les fonctions minimales reconnues à la formalité (l'écrit, en l'occurrence). Cette équivalence entre les procédés signifie que, sur le plan juridique, ils ont les mêmes effets et sont interchangeables. Autrement dit, la formalité prescrite est valablement accomplie dans l'environnement numérique lorsque le procédé choisi permet d'atteindre les fonctions reconnues à l'exigence. En droit belge, ce principe est consacré à l'article XII.15, § 1er, du Code de droit économique, aux termes duquel « toute exigence légale ou réglementaire de forme relative au processus contractuel est réputée satisfaite à l'égard d'un contrat par voie électronique lorsque les qualités fonctionnelles de cette exigence sont préservées ». À propos de ce principe, voy. E. Caprioli et R. Sorieul, « Le commerce international électronique : vers l'émergence de règles juridiques transnationales », *J.D.I.*, 2, 1997, p. 382 ; M. Demoulin, *Droit du commerce électronique et équivalents fonctionnels. Théorie critique*, coll. du CRIDS, Bruxelles, Larcier, 2014.

[89] Voy. aussi les présomptions figurant aux articles 35, § 2 (cachet électronique), 41, § 2 (horodatage électronique), et 43, § 2 (service d'envoi recommandé électronique), règl. eIDAS.

trading à haute fréquence[90] ou, plus anciennement, au recours à l'EDI[91] afin d'automatiser les échanges de documents commerciaux. Ces techniques ont généralement pour objectif d'accélérer des processus contractuels assez simples[92], d'achat-vente par exemple, au sein d'environnements particuliers et codifiés, comme la bourse ou les relations entre les acteurs de la grande distribution.

Les smart contracts diffèrent de ces technologies en ce qu'ils promettent non seulement d'être plus sûrs grâce à l'ajout de blockchain[93], mais également d'être plus versatiles en acceptant des consignes plus complexes et des inputs de la part d'intervenants extérieurs, les oracles.

Comme on l'a vu, la terminologie ne doit pas induire le lecteur en erreur. Il n'est ici pas véritablement question de contrat, mais de programmes informatiques exécutant une suite d'instructions et vérifiant certaines conditions. L'accord de volonté des parties réside dans la rédaction de ces instructions et la détermination de ces conditions.

Le smart contract pourra parfois s'appliquer à l'intégralité des opérations contractuelles visées, si celles-ci sont toutes virtuelles, par exemple un transfert financier automatique à la suite du téléchargement d'un fichier. Mais le smart contract pourra aussi être mixte et permettre l'accomplissement d'une partie d'un contrat global.

Pour assurer cet accomplissement, le smart contract doit parfois obtenir des données provenant du monde physique, afin de vérifier si une condition est remplie, ou pas. Dans ce cas, le smart contract fera appel à un « oracle », généralement un autre logiciel, qui lui fournira l'information demandée (*supra*, n° 18).

Dans le présent chapitre, on se penchera sur la manière dont l'exécution automatisée des smart contracts peut – ou non – s'accommoder des

---

[90] Voy. not. M. Lewis, *Flash Boys : A Wall Street Revolt*, W.W. Norton & Company, 2014 ; B. Biais, T. Foucault, F. Abergel, C.-A. Lehalle et M. Rosenbaum, « Trading haute fréquence, liquidité et stabilité du marché », *Opinions & Débats*, n° 2, novembre 2013, https://www.louisbachelier.org/trading-haute-frequence-liquidite-et-stabilite-du-marche/.

[91] Échange de Données Informatisées. À cet égard, voy. la recommandation 94/820/CE de la Commission, du 19 octobre 1994, concernant les aspects juridiques de l'échange de données informatisées, *J.O.*, L 338, 28 décembre 1994.

[92] Les algorithmes de trading à haute fréquence peuvent présenter un haut degré de complexité, mais ils ne sont pas adossés à une blockchain.

[93] L. Leloup, *Blockchain, la révolution de la confiance*, Paris, Eyrolles, 2017 ; M. Pilkington, « Blockchain technology : principles and applications », in F. Olleros et M. Zhegu (ed.), *Research handbook on Digital Transformations*, Montréal, Edward Elgar Publishing, 2016, pp. 225 et s.

incidents susceptibles d'émailler la vie du contrat sous-jacent[94]. En effet, l'automatisation permise par le smart contract est à la fois une fonctionnalité recherchée par les parties, mais peut s'avérer être une arme à double tranchant en rendant *de facto* impossible le recours aux mécanismes protecteurs traditionnels du droit des contrats.

37. Automatisation. Les smart contracts promettent une sécurité renforcée grâce à la blockchain et aux garanties cryptographiques qu'elle intègre. L'autre argument intéressant généralement les parties au smart contract est l'automatisation : une fois le smart contract lancé, celui-ci exécutera froidement la suite d'instructions qui lui a été soumise et effectuera ce pour quoi il a été programmé, peu importent les circonstances non prévues dans son code.

L'automatisation est un avantage indéniable pour le créancier d'une obligation puisqu'elle lui assure l'exécution de la part du débiteur. Le débiteur, lui, ne pourra guère qu'agir *a posteriori* s'il s'estime lésé par l'exécution du smart contract.

Entrer dans les liens d'un smart contract est donc particulièrement risqué pour le débiteur des obligations. Eu égard à la difficulté concrète éventuelle d'identification du cocontractant ou de l'opérateur technique sous-jacent, aux questions de preuve générées par le recours à une technologie complexe qui peut s'avérer une vraie boîte noire, les recours concrets du débiteur lésé peuvent être sévèrement restreints.

Par ailleurs, les deux parties peuvent être préjudiciées par un évènement imprévu modifiant les circonstances dans lesquels le smart contract doit s'exécuter.

Tous ces éléments rendent cruciale la préparation, en amont, de l'accord à traduire dans le smart contract.

38. La préparation du smart contract, une étape cruciale pour intégrer les aléas de l'exécution. Le smart contract renforce le principe de convention loi, tout en supprimant les tempéraments à la rigueur de ce principe, comme l'application des lois impératives[95], le principe d'exécution de bonne foi, ou les marges de manœuvre issues de l'interprétation des conventions.

[94] Le smart contract étant compris comme la technologie permettant l'exécution, automatisée et sécurisée au moyen d'une blockchain, d'un contrat « traditionnel » conclu entre les parties.

[95] Si elles ne sont pas prévues par les parties dans leur accord préalable.

Le smart contract s'exécute froidement, nonobstant les changements de circonstance : « le smart contract ne gère ni l'imprévu, ni l'imprévision »[96].

En conséquence, les parties devraient réserver le smart contract à quelques opérations très spécifiques, relativement simples à conceptualiser. Les parties devraient également tenter d'intégrer ces tempéraments dans leur accord préalable.

39. Force majeure et imprévision. La théorie de l'imprévision implique la possibilité de modifier ou de résilier une convention lorsque des circonstances inexistantes au moment de la conclusion du contrat, imprévisibles par les parties, surviennent et modifient l'équilibre des prestations réciproques des parties, rendant l'exécution de la convention, sinon impossible, particulièrement lourde, nonobstant toute faute des parties elles-mêmes[97].

Cette théorie est rejetée par la Cour de cassation en droit belge[98].

Il est toutefois loisible aux parties de prévoir des clauses dites de *hardship*, relativement courantes dans les contrats commerciaux internationaux[99].

Les smart contracts pourraient être un terreau fertile pour des clauses de ce type puisqu'il s'agirait de prévoir un certain nombre de critères à surveiller tout au long de l'exécution du contrat, ce pour quoi un smart contract ayant recours à un service d'oracle est parfaitement équipé. Si un de ces critères venait à dépasser un seuil fixé (l'évolution du prix d'une matière première par exemple), le smart contract adapterait automatiquement les conditions d'exécution du contrat ou en stopperait tout aussi automatiquement l'exécution avec les conséquences à prévoir par les parties.

La force majeure est une notion proche de l'imprévision, mais qui implique une impossibilité d'exécution de la convention.

Dans cette acception, les cas de force majeure pourraient être gérés par les parties en prévoyant simplement une procédure à suivre si le smart contract se trouvait confronté à l'impossibilité de s'exécuter. Le cas de force majeure pourrait toutefois affecter un autre élément du monde réel sur lequel le smart contract n'aurait pas de prise. Si l'on prend l'exemple d'un verrou électronique sur la porte d'une chambre d'hôtel, le smart contract pourrait ouvrir le verrou alors que l'immeuble a été victime d'une inondation et est inaccessible aux voyageurs. Le recours à différents

---

[96] M. Mekki, « Le contrat, objet des smart contracts (partie 1) », *op. cit.*, pp. 409 et s.

[97] P. Van Ommeslaghe, *Droit des obligations*, t. 1, *op. cit.*, 530.

[98] Cass., 14 avril 1994, *Pas.*, I, 365.

[99] P. Van Ommeslaghe, « Les clauses de hardship dans les contrats internationaux », *Rev. Dr. Int. Et Comp.*, 1980, p. 7.

oracles sera donc nécessaire pour vérifier que les critères et conditions prévues par les parties pour s'assurer de la possibilité d'exécution sont toujours remplis.

Qu'il s'agisse d'imprévision ou de force majeure, il sera toutefois nécessaire que les parties s'accordent au préalable sur les paramètres. Or, par définition, imprévision et force majeure visent des circonstances qui sont normalement imprévisibles. Techniquement, il faudrait donc prévoir des mécanismes de « *fail safe* » qui permettront au smart contract de réagir de manière conservatoire à n'importe quel type d'imprévu.

40. L'exception d'inexécution, inhérente à l'automatisation. L'exception d'inexécution permet à une partie de suspendre l'exécution de ses obligations lorsque son cocontractant est en défaut d'exécuter les siennes. L'exception d'inexécution se comprend dans un rapport synallagmatique et suppose des prestations réciproques[100]. L'exception d'inexécution doit être appliquée de bonne foi et dans le respect du principe de proportionnalité.

Le smart contract est *a priori* l'expression ultime de *l'exceptio non adimpleti contractu*, puisqu'il ne s'exécutera que si la condition prévue – soit généralement la vérification de la bonne exécution de l'obligation réciproque – est remplie. Cette vérification pourra se faire par le biais d'un oracle.

Comme dans un contrat classique, les parties peuvent convenir dans leur accord préalable au smart contract des modalités de l'exception d'inexécution, les dispositions du Code civil y relatives étant supplétives.

Elles peuvent même déroger complètement au principe, sauf législation impérative protégeant spécifiquement une partie réputée faible.

L'accord coulé dans le smart contract peut donc prévoir une large gamme d'hypothèses en fonction des conditions et critères.

Le smart contract – ou l'oracle – pourrait toutefois difficilement appréhender les subtilités, aléas, incohérences de certaines situations, impossibles à modéliser pour une machine. Certaines hypothèses qui pourraient justifier une application d'une exception d'inexécution dans un contrat classique pourraient donc ne pas être prises en compte dans un smart contract.

De même, le smart contract ne pourra pas intégrer une notion aussi ouverte et floue que la bonne foi avec laquelle l'exception d'inexécution doit être appliquée. Les parties ne pourront donc bénéficier de la

[100] P. Wéry, *Droit des obligations*, vol. 1, *Théorie générale du contrat*, 2e éd., *op. cit.*, pp. 881-893.

protection offerte par le principe d'exécution de bonne foi qu'*a posteriori*, après avoir saisi un magistrat. Le recours au smart contract pourrait donc privilégier le cocontractant qui entend éventuellement agir de mauvaise foi.

41. Conclusions sur l'exécution des smart contracts. Certains peuvent voir dans le renforcement du principe de convention loi, et dans l'automatisation des smart contracts un avantage et un gain d'efficacité important, par rapport aux aléas de l'interprétation humaine des notions ouvertes.

La froideur logique de la machine contre l'incohérence poétique des juristes.

La logique de la machine peut faire parfois merveille. Mais le logiciel ne permettra pas d'atteindre la même versatilité qu'un esprit humain lorsqu'il s'agira d'appréhender les subtilités d'un système complexe, difficile à modéliser.

Cette fonctionnalité du smart contract doit simplement être vue comme un élément factuel inhérent au choix technologique opéré. Les parties, lorsqu'elles font le choix d'utiliser un smart contract pour exécuter leur accord, doivent avoir conscience de cette fonctionnalité, ou de cette limitation selon le point de vue.

Le smart contract ne pourra pas s'appliquer à des situations trop complexes, échappant à l'algorithme et nécessitant des interprétations en fait ou en droit. Il sera également limité par l'application de législations impératives, même si certaines pourront sans doute être factorisées dans l'algorithme.

En conclusion sur ce point, l'automatisation, ses limites et ses désavantages sont autant d'arguments démontrant que le recours au smart contract est loin d'être la panacée. Il s'agit d'un outil sans doute particulièrement efficace pour quelques applications précises, mais dont le coût d'une préparation adéquate en amont le rend impraticable dans de nombreux cas.

CHAPITRE 4. Blockchain et responsabilités

42. Une activité génératrice de risques et, potentiellement, de responsabilités. Comme toute autre technologie (ou toute activité humaine, du reste), la blockchain est génératrice de risques, pour ses utilisateurs et,

le cas échéant, pour la société dans son ensemble. Des erreurs de programmation peuvent en effet être commises[101], sans compter les atteintes à la sécurité, les fraudes, les attaques informatiques[102] ou les mobiles illicites animant certains utilisateurs intéressés par l'anonymat relatif de la clé publique. Corrélativement, des dommages peuvent être subis par certains utilisateurs de la blockchain ou des tiers.

Le droit de la responsabilité civile a précisément pour objet de permettre aux victimes d'obtenir la réparation du préjudice subi, en veillant – en principe – à une distribution des risques juste et équilibrée. Comme on le verra, son application à la blockchain peut poser certaines difficultés et être source d'insécurité juridique[103].

En théorie, moyennant la démonstration d'une faute, d'un dommage, et d'un lien de causalité entre les deux, la réparation intégrale est normalement garantie.

Ce schéma général est complété par des régimes spécifiques de responsabilités établis par la loi ou consacrés par la jurisprudence à la faveur d'une interprétation de certaines dispositions particulières. Dans ces régimes, les victimes bénéficient généralement d'un allègement de la charge de la preuve, grâce à des présomptions ou à l'établissement d'une responsabilité objective, qui peut par ailleurs canaliser l'obligation de réparer sur un débiteur facilement identifiable et normalement solvable (et/ou assuré)[104].

---

[101] 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 best practices 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/).

[102] Ou d'une exploitation opportune de certaines failles du code informatique, comme avec *The DAO* d'Ethereum en 2016.

[103] À ce sujet, voy. les réflexions de L. Buonanno, « La responsabilité civile à l'heure des nouvelles technologies : l'influence de la blockchain », *DAOR*, 2020/1, pp. 30-38 ; Y. Poullet et H. Jacquemin, « Blockchain : une révolution pour le droit ? », *op. cit.*, pp. 801 et s., nos 31 et s. ; 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.

[104] Voy. par ex. la présomption de responsabilité du fait des choses (art. 1384, al. 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 (art. 24) et entraînant un renversement de la charge de la preuve.

Parallèlement, il faut aussi avoir égard aux limitations – voire aux exonérations – de responsabilité dont certains acteurs peuvent bénéficier, conformément à la loi ou moyennant des clauses contractuelles *ad hoc*.

43. Application des régimes classiques de responsabilité à la blockchain. Suivant le cas de figure rencontré, les règles de la responsabilité contractuelle ou extracontractuelle devront être mobilisées[105].

On observe que, dans les deux cas, il convient d'identifier une personne physique ou morale auprès de laquelle l'indemnisation du dommage peut être postulée. C'est l'un des principaux écueils en matière de blockchain, spécialement dans les blockchains publiques[106] : les utilisateurs sont identifiés par leur clé publique (qu'il pourrait être très difficile, voire impossible, de lier à une personne déterminée) ; quant à la blockchain en tant que telle (comme la blockchain Bitcoin), elle n'a pas de personnalité juridique et se revendique comme étant une « communauté d'utilisateurs » (dont l'identification est un problème). Aucun recours utile ne semble donc possible en pratique, ce qui empêche toute réparation au bénéfice de la victime (et lui fait donc supporter la totalité du risque encouru). Pour pallier cet inconvénient, deux correctifs pourraient être mis en place. D'abord, il faut s'assurer que les utilisateurs de ce type de blockchain sont parfaitement informés du risque pris et qu'ils acceptent, en pleine connaissance de cause, de les assumer le cas échéant. Ensuite, des mécanismes assurantiels devraient être promus (et, le cas échéant, imposés), pour réduire la charge financière susceptible d'être supportée par les victimes de dommages.

Comme on l'a vu, les systèmes de blockchains publiques ou privées sont au cœur d'un écheveau de contrats, qui peuvent prévoir des obligations à charge de l'une ou l'autre des parties. En cas d'inexécution, par l'une des parties, de ses obligations, sa responsabilité contractuelle pourra, le cas échéant, être engagée (moyennant la démonstration d'une faute, en lien de causalité avec le dommage subi)[107]. On aura principalement égard aux dispositions de la convention, à l'existence éventuelle d'obligations de résultat (donnant lieu à un renversement de la charge de la preuve au

[105] Pour une application de ces régimes à l'intelligence artificielle et aux robots (qui présentent un certain nombre de points communs avec la technologie blockchain), voy. H. JACQUEMIN et J.-B. HUBIN, « Aspects contractuels et de responsabilité civile en matière d'intelligence artificielle », *op. cit.*, pp. 112 et s.

[106] En principe, dans les blockchains privées ou de consortium, les participants sont préalablement identifiés (et acceptés), de même que les personnes à l'initiative du système.

[107] On note que l'inexécution, par une partie, de ses obligations contractuelles, peut également conduire à d'autres mesures, comme l'exception d'inexécution, l'exécution en nature ou la résolution du contrat.

profit du créancier)[108] et aux clauses limitatives ou exonératoires de responsabilité (sur ce point, voy. *infra*, n° 44).

Sous réserve de l'hypothèse du concours de responsabilités, les règles de la responsabilité extracontractuelle seront d'application en l'absence de contrat conclu entre la victime et l'auteur du dommage, notamment en cas de manquement à l'obligation d'information au stade précontractuel[109] (tirée de l'obligation de bonne foi de l'article 1134, alinéa 3, du Code civil). Si les conditions de l'article 1382 du Code civil sont réunies, une indemnisation pourra normalement être obtenue.

L'application de la loi du 25 février 1991 relative à la responsabilité du fait des produits défectueux peut également être envisagée, même si elle ne nous paraît guère prometteuse en l'espèce (en tout cas si on se place du point de vue de la victime). L'article 1er de la loi énonce que « le producteur est responsable du dommage causé par un défaut de son produit ». Cette loi établit un régime de responsabilité objective : si la personne lésée démontre que le produit – ici, la blockchain ou le smart contract – est affecté d'un défaut et que celui-ci est en lien avec le dommage subi, le producteur sera responsable et devra indemniser la victime dans les limites prévues par la loi. L'application de cette loi présente plusieurs difficultés dans l'hypothèse qui nous occupe. En admettant qu'une solution technologique comme la blockchain (combinant algorithmes, logiciels et base de données) constitue un produit, encore faut-il démontrer qu'elle est affectée d'un défaut. En outre, seuls certains dommages peuvent être réparés : les dommages aux personnes et, sous déduction d'une franchise de 500 euros, les dommages aux biens « qui sont d'un type normalement destiné à l'usage ou à la consommation privés et ont été utilisés par la victime principalement pour son usage ou sa consommation privés »[110]. On peut douter que ce type de préjudices soit rencontré. En outre, plusieurs causes d'exonérations pourraient être utilement invoquées, conformément à l'article 8 de la loi[111].

Dans le domaine de l'intelligence artificielle, des discussions sont en cours, notamment au niveau de la Commission européenne, pour revoir

[108] En pratique, les conditions contractuelles applicables indiqueront expressément au contraire que les obligations du prestataire sont de moyens, précisément pour éviter un tel renversement de la charge de la preuve.

[109] Sur ce point, voy. *supra*, n° 28.

[110] Art. 11, § 2, de la loi du 25 février 1991.

[111] Ainsi, le producteur n'est pas responsable, si démontre que « b) que, compte tenu des circonstances, il y a lieu d'estimer que le défaut ayant causé le dommage n'existait pas au moment où le produit a été mis en circulation par lui ou que ce défaut est né postérieurement » ou que « e) que l'état des connaissances scientifiques et techniques au moment de la mise en circulation du produit par lui ne permettait pas de déceler l'existence du défaut ».

le cadre normatif actuel et s'assurer qu'il réponde aux enjeux de l'IA, spécialement en matière de responsabilité[112]. Dès lors que la blockchain présente de nombreux points communs avec l'IA, au moment d'appliquer les régimes de responsabilité, on peut normalement espérer que les nouvelles règles lèvent également certaines incertitudes dans le domaine de la blockchain.

44. Exonération et limitations de responsabilité mobilisées par certains acteurs, sur une base conventionnelle. Moyennant le respect de certaines conditions, le droit belge des obligations reconnaît la validité des clauses limitatives ou exonératoires de responsabilité.

Lorsqu'un contrat est conclu entre un utilisateur de la blockchain et un prestataire, de telles clauses sont généralement insérées dans les conditions générales d'utilisation.

À titre d'illustration, la clause suivante figure dans les conditions générales d'une plateforme d'échange de cryptomonnaies (qui fournit par ailleurs un service de portefeuille électronique) : « La responsabilité de B. vis-à-vis des CLIENTS qui n'agissent pas en tant que CONSOMMATEURS sera seulement engagée dans le cas d'une faute lourde de B., et sera en tout cas limitée au SOLDE disponible sur les WALLETS du CLIENT au moment de la faute, avec un maximum de 25 000 EUR »[113]. On constate donc une double limitation de responsabilité, avec la fixation d'un cap (plafond) de responsabilité et la seule réparation des préjudices résultant de fautes lourdes ou de dol du prestataire. En pratique, cela rend la possible indemnisation très théorique. Il est également prévu que « B. ne pourrait être tenu responsable de l'apparition d'une fourche sur la chaîne

[112] Expert Group on Liability and New Technologies, *Liability for Artificial Intelligence and other emerging digital technologies*, 2019, disponible sur https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608. Ce rapport fait d'ailleurs référence à la blockchain. Voy. aussi le Rapport de la Commission au Parlement européen, au Conseil et au Comité économique et social sur les conséquences de l'intelligence artificielle, de l'internet des objets et de la robotique sur la sécurité et la responsabilité, COM(2020) 64 final.

[113] Dans les relations avec les consommateurs, les clauses d'exonération sont un peu plus favorables à ces derniers :

« la responsabilité de B. vis-à-vis des CLIENTS qui agissent en tant que CONSOMMATEURS est limitée comme suit : o Pour l'inexécution d'une obligation consistant en une des prestations principales du contrat, la responsabilité de B. sera limitée jusqu'au SOLDE disponible sur les WALLETS du CLIENT au moment de l'inexécution, avec un maximum de 25 000 EUR ; o Pour l'inexécution d'une obligation consistant en une des prestations non principales du contrat, la responsabilité de B. sera seulement engagée dans le cas d'une faute lourde de B. ou de celle de ses préposés ou mandataires, et sera en tout cas limitée au SOLDE disponible sur les WALLETS du CLIENT au moment de l'inexécution, avec un maximum de 25 000 EUR ».

de blocs de la CRYPTOMMONAIE en question et qui invaliderait certaines transactions passées ».

On peut aussi reprendre la clause suivante, tirée des conditions générales d'une autre plateforme :

« C. is committed to a high standard of data security and precision. However, C. shall not be liable for any loss that you may incur as a result of malfunctions, errors, security breaches or any other reason.
C. will not be responsible or liable to you for any loss and take no responsibility for and will not be liable to you for any use of our Services and/or solutions, including but not limited to any losses, damages or claims arising from:
User error such as forgotten passwords, incorrectly constructed transactions, or mistyped virtual currency addresses or similar;
Server failure or data loss;
Corrupted Wallet files;
Unauthorized access to applications;
Any unauthorized third party activities, including without limitation the use of viruses, phishing or other means of attack against the C. website or C. services or solutions.
Once you create your C. account, you are responsible for the activities performed. Likewise, it is solely your responsibility to guard your password, and track any activity that occur with the use of your password and/or in your account. Please notify us immediately if you suspect any security breach, caused by you or other parties. C. cannot be held responsible or liable for losses or damages relating to account settings, or security breaches caused by you.
C. shall not be liable for your or other users'content. If you come across content that is not correct, offensive or against the Terms, you should report this to C. (compliance@C..com) immediately. C. reserves the right to delete content at any time it deems necessary.
In no event shall C. be liable for indirect losses and/or an amount larger than the amount you have paid to C. ».

Dans cette hypothèse également, les limitations de responsabilité sont telles qu'en pratique, il sera très difficile, voire impossible, d'obtenir une indemnisation substantielle de la part du prestataire.

On peut d'ailleurs s'interroger sur leur conformité au droit applicable (spécialement à partir du 1er décembre 2020 dans les relations B2B).

On rappelle en effet que la validité des clauses limitatives ou exonératoires de responsabilité est soumise aux règles de droit commun. On considère ainsi que ces clauses ne peuvent pas porter atteinte à une

obligation essentielle du contrat et sont inapplicables en cas de dol. On interdit également qu'elles portent atteinte à une disposition légale impérative ou d'ordre public.

Par ailleurs, entre une entreprise et un consommateur, les clauses abusives sont prohibées (et nulles) : si la clause en question ne figure pas dans la liste noire des clauses abusives en toutes circonstances au sens de l'article VI.83 du Code de droit économique[114], il faut avoir égard à la définition générale de la clause abusive, et s'assurer qu'elle ne crée pas « un déséquilibre manifeste entre les droits et les obligations des parties au détriment du consommateur »[115].

En Belgique, à partir du 1er décembre 2020, ce même critère sera également d'application pour déterminer si une clause est abusive dans les relations entre entreprises[116]. Préalablement, on devra s'assurer qu'elle ne figure, ni dans la liste noire (clauses abusives en tout état de cause)[117], ni dans la liste grise (clauses présumées abusives sauf preuve contraire)[118]. C'est en effet dans cette dernière liste que figure l'interdiction des clauses ayant pour objet de « libérer l'entreprise de sa responsabilité du fait de son dol, de sa faute grave ou de celle de ses préposés ou, sauf en cas de force majeure, du fait de toute inexécution des engagements essentiels qui font l'objet du contrat »[119]. On souligne néanmoins que l'interdiction des clauses abusives dans les relations entre entreprises ne s'applique pas aux services financiers[120].

45. Exonération de responsabilité des prestataires intermédiaires de la société de l'information. Les articles XII.17 et suivants du Code de droit économique établissent une exonération de responsabilité (civile et pénale) au bénéfice des prestataires de la société de l'information[121]. Elle est toutefois circonscrite à certaines de leurs activités : le simple transport, le stockage sous forme de cache et l'hébergement[122].

---

[114] Voy. en particulier l'art. VI.83, 13°, C.D.E. : est interdite la clause ayant pour objet de « libérer l'entreprise de sa responsabilité du fait de son dol, de sa faute lourde ou de celle de ses préposés ou mandataires, ou, sauf en cas de force majeure, du fait de toute inexécution d'une obligation consistant en une des prestations principales du contrat ».

[115] Voy. la définition de la clause abusive figurant à l'art. I.8, 22°, C.D.E.

[116] Art. VI.91/3 C.D.E.

[117] Art. VI.91/4 C.D.E.

[118] Art. VI.91/5 C.D.E.

[119] Art. VI.91/5, 6°, C.D.E.

[120] Art. VI.91/1 C.D.E.

[121] À noter que ce régime devrait faire l'objet de modifications à l'occasion de la révision de la directive sur le commerce électronique et son remplacement par un *Digital Services Act*.

[122] À ce propos, voy. par ex. H. JACQUEMIN, « Le régime d'exonération de responsabilité des prestataires intermédiaires : état des lieux et perspectives », in *Responsabilités et*

La question se pose de savoir si certaines blockchains, publiques ou privées (voire de consortium) pourraient se prévaloir de cette exonération de responsabilité, dans l'hypothèse où, à la suite d'actes illicites commis à travers ces blockchains, la victime cherche à engager la responsabilité de celles-ci (l'auteur de l'acte étant plus difficile à identifier, localisé dans un États tiers ou peu solvable).

Dans ce cadre également, il faudra identifier une personne physique ou morale susceptible de répondre, en qualité d'intermédiaire, des actes illicites commis à travers la blockchain.

En admettant que cet écueil soit dépassé, l'exonération ne lui sera applicable que si elle s'est comportée 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 » »[123]. Ce n'est donc 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 « prestataire intermédiaire » et bénéficier de l'exonération de responsabilité (pour autant que les conditions soient, le cas échéant, satisfaites, *cf. infra*). La Cour confirme sa jurisprudence dans l'affaire *Mc Fadden*, où elle y voit un point commun entre les services des FAI et des hébergeurs, qui « n'ont ni la connaissance, ni le contrôle des informations [...] transmises ou stockées »[124]. Il appartient évidemment aux juridictions nationales d'apprécier, en l'espèce, si le critère est satisfait ou pas à la lumière des exemples donnés par la Cour de justice[125]. Qualifier une blockchain d'intermédiaire, au sens de la jurisprudence de la Cour de justice nous paraît douteux lorsque, pour valider les blocs, les données figurant dans la blockchain doivent être traitées et, le cas échéant vérifiées (pour s'assurer par exemple qu'Alice disposait bien de 1 BTC avant de le transmettre à Bob).

---

numérique, Limal, Anthemis, 2018, pp. 63-99 ; F. JONGEN et A. STROWEL (avec la coll. de E. CRUYSMANS), *Droit des médias et de la communication,* Bruxelles, Larcier, 2017, pp. 781 et s. ; Th. LÉONARD, « Les réseaux sociaux face à l'exonération de responsabilité des intermédiaires de l'internet : une application délicate », *Les réseaux sociaux et le droit,* Conférence du Jeune barreau, Bruxelles, Larcier, 2014, pp. 125 et s.

[123] 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.

[124] C.J.U.E., 15 septembre 2016, *Mc Fadden,* aff. C-484/14, § 61.

[125] C.J.U.E., 23 mars 2010, *Google France et Google,* aff. jointes C-236/08 à C-238/08, §§ 115-118 ; C.J.U.E., 12 juillet 2011, *L'Oréal e.a. c. eBay*, aff. C-324/09, §§ 114-116. Voy. aussi C.J.U.E., 11 septembre 2014, *Papasavvas,* aff. C-291/13, §§ 42-44.

À supposer même que ce soit le cas, il faudrait ensuite appliquer les conditions propres au régime d'hébergement : suivant celles-ci, le prestataire ne peut en effet bénéficier de l'exonération de responsabilité pour les informations qu'il stocke que dans l'une ou l'autre des hypothèses visées par la loi. Soit, et c'est le premier cas de figure, il n'a pas « une connaissance effective de l'activité ou de l'information illicite, ou, en ce qui concerne une action civile en réparation, [il n'a pas] connaissance de faits ou de circonstances laissant apparaître le caractère illicite de l'activité ou de l'information ». Dans ce cas, il bénéficie de l'exonération de responsabilité. Soit, et c'est le second cas de figure, le prestataire a une telle connaissance et, pour conserver le bénéfice de l'exonération, il doit agir « promptement pour retirer les informations ou rendre l'accès à celles-ci impossible », dans le respect de la procédure visée à l'article XII.19, § 3, du Code de droit économique. Dans l'hypothèse de la blockchain, l'intégrité de l'information enregistrée dans les blocs ne peut pas être compromise : le prestataire sera normalement dans l'impossibilité de retirer les informations ou de rendre l'accès à celles-ci impossible. Aussi devrait-il perdre le bénéfice de l'exonération de responsabilité.

Conclusion

46. Pas de révolution pour le droit des obligations. En analysant les blockchains et les smart contracts à travers le prisme du droit belge des obligations, on constate que les règles actuellement applicables sont, pour l'essentiel, suffisamment flexibles pour s'appliquer à ces technologies, et répondre aux principaux enjeux qu'elles posent (en termes de complexité, de pluralité d'intervenants, etc.).

Des difficultés pratiques pourraient néanmoins être rencontrées, eu égard aux caractéristiques de la blockchain (anonymat, absence de personne représentant la blockchain publique, caractère irréversible des informations inscrites dans la chaîne, etc.). On aurait toutefois tort de les considérer nécessairement comme des obstacles bloquants : au contraire, elles invitent le juriste à faire preuve de créativité en vue de trouver des solutions pragmatiques (en s'inspirant par exemple du droit de sociétés ou, par identité de motifs, en apportant des réponses communes à l'IA et à la blockchain, par exemple).

47. Des défis à relever pour le législateur ou les *stakeholders*. La blockchain et les smart contracts présentent en effet d'intéressants défis, qu'il incombe aux législateurs nationaux (ou européen, dans la mesure du possible) et aux *stakeholders* de relever. Ponctuellement, et de manière ciblée, des modifications législatives devraient en effet être introduites, pour assurer un niveau élevé de sécurité juridique. Parallèlement, les parties doivent quant à elles veiller à la conclusion de contrats équilibrés, qui respectent les intérêts de chaque cocontractant (à défaut, les régimes d'interdiction des clauses abusives doivent être appliqués).

De cette manière, et pour autant que la technologie présente objectivement une plus-value par rapport à d'autres moyens, les parties pourront recourir à la blockchain et aux smart contracts en toute confiance.