

## **Un travail écrit : "Enjeux juridiques et impacts de la Blockchain pour le notariat et le secteur bancaire belge"**

**Auteur** : Hiéronimus, Fanny

**Promoteur(s)** : Partsch, Philippe-Emmanuel

**Faculté** : Faculté de Droit, de Science Politique et de Criminologie

**Diplôme** : Master en droit, à finalité spécialisée en gestion

**Année académique** : 2017-2018

**URI/URL** : <http://hdl.handle.net/2268.2/4867>

---

### *Avertissement à l'attention des usagers :*

*Tous les documents placés en accès ouvert sur le site le site MatheO sont protégés par le droit d'auteur. Conformément aux principes énoncés par la "Budapest Open Access Initiative"(BOAI, 2002), l'utilisateur du site peut lire, télécharger, copier, transmettre, imprimer, chercher ou faire un lien vers le texte intégral de ces documents, les disséquer pour les indexer, s'en servir de données pour un logiciel, ou s'en servir à toute autre fin légale (ou prévue par la réglementation relative au droit d'auteur). Toute utilisation du document à des fins commerciales est strictement interdite.*

*Par ailleurs, l'utilisateur s'engage à respecter les droits moraux de l'auteur, principalement le droit à l'intégrité de l'oeuvre et le droit de paternité et ce dans toute utilisation que l'utilisateur entreprend. Ainsi, à titre d'exemple, lorsqu'il reproduira un document par extrait ou dans son intégralité, l'utilisateur citera de manière complète les sources telles que mentionnées ci-dessus. Toute utilisation non explicitement autorisée ci-avant (telle que par exemple, la modification du document ou son résumé) nécessite l'autorisation préalable et expresse des auteurs ou de leurs ayants droit.*

---

# **Enjeux juridiques et impacts de la *Blockchain* pour le notariat et le secteur bancaire belge**

**Fanny HIERONIMUS**

## **Jury**

Promoteur :

Philippe-Emmanuel PARTSCH, avocat  
partner chez Arendt & Medernach et chargé  
de cours à l'Université de Liège

Année académique 2017-2018

Lecteurs :

Michael SCHYNS, directeur académique des  
études et chargé de cours à HEC Liège

Jean CATTARUZZA, chef du département  
légal chez ING Belgique

Mémoire présenté en vue de  
l'obtention du diplôme de  
Master en droit, à finalité  
spécialisée en gestion



## ABSTRACT

À travers ce travail de fin d'études, nous nous intéressons aux importantes évolutions technologiques auxquelles nous sommes soumis. Nous traitons plus particulièrement du phénomène de la *Blockchain* directement lié à un concept plus connu, celui du *Bitcoin*. Aucun secteur n'y échappe, ce qui nous a permis de proposer une approche à la fois juridique et économique du problème.

Il faut cependant avant toute chose mettre en garde le lecteur. L'intérêt autour de la *Blockchain* est un phénomène fort récent. Les analyses faites à son sujet sont encore assez limitées et sont susceptibles de changer très rapidement.

Nous tenterons dès lors à travers cet exposé de répondre à deux questions. Premièrement, nous nous demanderons quels seraient les enjeux d'un point de vue juridique si l'utilisation de la technologie *Blockchain* venait à véritablement s'implanter en Belgique. Deuxièmement, nous nous interrogerons sur les conséquences d'une telle implantation dans le domaine du notariat ainsi que le secteur bancaire belge. Nous avons choisi d'analyser la *Blockchain* à travers ces deux secteurs, car ce sont pour nous ceux qui seraient les plus impactés si l'utilisation de cette technologie venait à se répandre chez nous.

Ce travail est divisé en quatre parties principales. La première consiste en un bref exposé de la *Blockchain* et de ses applications. Nous ne faisons en aucun cas l'apologie de celle-ci mais cette partie servira à expliquer clairement ce concept jusqu'alors peu connu du grand public, ce qui permet de mieux comprendre les enjeux de sa réception dans l'ordre juridique belge. La deuxième consiste à établir un état des lieux sur le plan juridique de ce phénomène. La troisième a trait aux avantages et inconvénients de l'utilisation de la *Blockchain* dans le secteur du notariat belge, et ensuite dans le secteur bancaire belge. La quatrième consiste en une brève réflexion sur le rôle qu'il reste à l'État dans un tel système.

Cette étude nous permet de mettre en lumière le fait que, malgré des tentatives de réglementation de la part des législateurs européen et national autour des nouvelles technologies, le cadre juridique de la *Blockchain* reste insuffisant voire inexistant à ce jour. Ceci nous amène alors à poser quelques pistes de régulation nécessaires dans un État de droit comme la Belgique.

À la suite de ces différentes parties, nous concluons que la *Blockchain* nécessite des aménagements tant d'un point de vue juridique qu'économique. Cependant, elle ne doit pas être vue comme un danger mais plutôt comme une opportunité d'amélioration pour les secteurs qui décideront de l'utiliser.

## ABSTRACT

In this dissertation, we are interested in important technological developments to which we are subjected. We are addressing the Blockchain phenomenon, which is directly connected to the better-known concept of Bitcoin. No sector has been spared, which has allowed us to propose a legal and economic approach to the problem.

However, we caution readers that the interest around Blockchain is a very recent phenomenon. There are a limited number of studies on the topic and they are likely to evolve quickly.

Therefore, we aim to answer two questions in this study. First, what would be the legal issues if the Blockchain technology were to be set up in Belgium? Second, what would be the consequences of such implementation in the Belgian notary and banking sector? We chose to analyze Blockchain in these two sectors, as they are the ones that would be the most impacted if the use of this technology were to spread in our country.

This work is divided into four main parts. The first part consists of a brief introduction to Blockchain and its applications. We do not in any way advocate that technology; the main purpose of that section is to explain clearly a concept still relatively unknown to the public, which allows a better understanding of the stakes of its implementation. The second part aims to establish an overview of the legal context surrounding that phenomenon. The third part discusses the advantages and disadvantages of using Blockchain in the Belgian notary, and in the Belgian banking sector thereafter. The fourth part consists of a brief reflection on the remaining role of the State in such a system.

This study allows us to highlight that despite attempts by European and Belgian legislators to regulate new technologies, the legal framework for the use of Blockchain remains insufficient or even inexistent. Then, this enables us to suggest a few necessary regulatory measures in a State governed by the rule of law, such as Belgium.

Following these different parts, we conclude that Blockchain requires adjustments from both a legal and an economic point of view. However, that technology should not be seen as a threat but rather as an opportunity for improvement in the sectors willing to use it.



## **REMERCIEMENTS**

Je remercie mon promoteur, Monsieur Philippe-Emmanuel Partsch, ainsi que mon premier lecteur, Monsieur Michael Schyns, pour avoir accepté d'encadrer mon travail ainsi que pour leurs précieux conseils.

Je remercie également Monsieur Jean Cattaruzza pour l'intérêt qu'il a porté à mon sujet en acceptant d'être mon second lecteur.

Je remercie tout particulièrement Christian Luyten, directeur du département communication à la Fédération Royale du Notariat belge, et Olivier Duron, analyste des affaires prudentielles et comptabilité chez Febelfin, pour avoir pris le temps de m'aider ainsi que pour leurs conseils.





## TABLE DES MATIERES

|   |           |
|---|-----------|
| <b>INTRODUCTION.....</b>  | <b>5</b>  |
| <b>I.- PRESENTATION DE LA <i>BLOCKCHAIN</i> .....</b>                                 | <b>6</b>  |
| <b>A.- DEFINITION DE LA <i>BLOCKCHAIN</i> .....</b>                                   | <b>6</b>  |
| <b>B.- FONCTIONNEMENT DE LA <i>BLOCKCHAIN</i> .....</b>                               | <b>8</b>  |
| <b>C.- CARACTERISTIQUES DE LA <i>BLOCKCHAIN</i>.....</b>                              | <b>10</b> |
| 1) La décentralisation.....   | 10        |
| 2) Un consensus .....   | 11        |
| 3) Le caractère distribué.....  | 11        |
| 4) La transparence.....   | 11        |
| 5) Le caractère immuable.....   | 11        |
| <b>D.- <i>BLOCKCHAIN</i> PRIVEE ET PUBLIQUE : DISTINCTION.....</b>                    | <b>12</b> |
| <b>E.- FAIBLESSES DE LA <i>BLOCKCHAIN</i> .....</b>                                   | <b>13</b> |
| 1) Coût énergétique.....  | 13        |
| 2) Limites techniques .....   | 14        |
| 3) Anonymat .....   | 14        |
| 4) L'absence de régulation.....   | 15        |
| <b>F.- APPLICATIONS DE LA <i>BLOCKCHAIN</i> .....</b>                                 | <b>15</b> |
| 1) Listes non exhaustives .....   | 16        |
| 2) Le <i>Bitcoin</i> .....  | 16        |
| 3) Les <i>Smart contracts</i> .....   | 20        |
| <b>II.- CADRE JURIDIQUE APPLICABLE.....</b>   | <b>22</b> |
| <b>A.- LE DROIT COMMUN DES CONTRATS .....</b>   | <b>22</b> |
| 1) Définition.....  | 23        |
| 2) Formation des contrats conclus par voie électronique.....                          | 23        |
| 3) Grands principes du droit des contrats.....  | 24        |
| a) <i>Autonomie de la volonté</i> .....   | 24        |
| b) <i>Le consensualisme</i> .....   | 24        |
| c) <i>Le principe de convention-loi</i> .....   | 25        |
| 4) La formation du contrat à proprement parler.....                                   | 26        |
| a) <i>Les conditions de validité du contrat</i> .....                                 | 26        |
| b) <i>Absence de sanction adéquate</i> .....  | 28        |
| 5) Problèmes transfrontaliers .....   | 28        |
| 6) Application du droit international privé.....                                      | 28        |
| a) <i>Juridiction compétente</i> .....  | 29        |
| b) <i>Loi applicable</i> .....  | 29        |
| 7) Conclusion : faiblesses des <i>Smart contracts</i> face au droit des contrats..... | 30        |
| <b>B.- LE DROIT DE LA PREUVE .....</b>  | <b>32</b> |
| 1) Introduction .....   | 32        |
| 2) Contexte.....  | 33        |

|    |   |    |
|----|---|----|
| 3) | Règlement eIDAS .....   | 33 |
| a) | <i>Apports du règlement</i> .....                                     | 34 |
| b) | <i>Définition de la signature électronique</i> .....                  | 34 |
| c) | <i>Trois types de signatures électroniques</i> .....                  | 35 |
| d) | <i>Intérêt de la distinction</i> .....                                | 36 |
| e) | <i>Cachet électronique</i> .....                                      | 36 |
| f) | <i>Horodatage</i> .....   | 37 |
| 4) | Droit national belge .....  | 38 |
| a) | <i>Introduction de la signature électronique en droit belge</i> ..... | 38 |
| b) | <i>Service d'archivage électronique</i> .....                         | 40 |
| 5) | Conclusion : règlement eIDAS et <i>Blockchain</i> .....               | 41 |

### **III.- ANALYSE DE L'IMPACT DE L'IMPLANTATION DE LA BLOCKCHAIN DANS DES SECTEURS ECONOMIQUES ..... 43**

|            |  |           |
|------------|--|-----------|
| <b>A.-</b> | <b>LE SECTEUR DU NOTARIAT.....</b>                         | <b>43</b> |
| 1)         | Introduction .....   | 43        |
| 2)         | Définition .....   | 44        |
| 3)         | Rôle du notaire .....                                      | 44        |
| 4)         | <i>Blockchain</i> et secteur notarié .....                 | 44        |
| a)         | <i>Les actes notariés</i> .....                            | 45        |
| 1.         | Date certaine .....  | 45        |
| 2.         | Force probante .....                                       | 45        |
| 3.         | Force exécutoire .....                                     | 46        |
| 4.         | Conservation en minute .....                               | 46        |
| b)         | <i>La Blockchain et les actes authentiques</i> .....       | 46        |
| 1.         | Horodatage .....   | 46        |
| 2.         | Force probante limitée .....                               | 47        |
| 3.         | Absence de force exécutoire .....                          | 47        |
| 4.         | Conservation .....   | 47        |
| 5.         | Formation de l'acte authentique et <i>Blockchain</i> ..... | 47        |
| c)         | <i>Mission du notaire</i> .....                            | 49        |
| 1.         | Avantages .....  | 49        |
| a.         | Diminution des délais .....                                | 49        |
| b.         | Diminution des coûts .....                                 | 51        |
| c.         | Facilité administrative .....                              | 51        |
| 2.         | Inconvénients .....  | 52        |
| a.         | Vraisemblance des informations .....                       | 52        |
| b.         | La responsabilité du notaire .....                         | 52        |
| c.         | Confidentialité .....                                      | 53        |
| 3.         | Suppression du notaire tiers de confiance ? .....          | 53        |
| <b>B.-</b> | <b>LE SECTEUR BANCAIRE .....</b>                           | <b>54</b> |
| 1)         | Introduction .....   | 54        |
| 2)         | Rôle du banquier .....                                     | 55        |
| 3)         | Conditions d'établissement .....                           | 55        |
| a)         | <i>Avantages</i> .....                                     | 55        |

|             |   |           |
|-------------|---|-----------|
| 1.          | Diminution des coûts.....   | 55        |
| 2.          | Diminution des risques de défaut de paiement et sécurité des transactions financières ..... | 56        |
| 3.          | Diminution des délais.....  | 57        |
| 4.          | Double dépense .....  | 58        |
| 5.          | Registre uniformisé .....   | 58        |
| b)          | <i>Inconvénients</i> .....  | 59        |
| 1.          | Limite d'ordre technique .....  | 59        |
| 2.          | « Attaque des 51 % ».....   | 60        |
| 3.          | Risque de fraude.....   | 60        |
| 4.          | Problème d'identification.....  | 60        |
| 5.          | Le consortium R3 .....  | 62        |
| c)          | <i>La Blockchain, un danger pour les banques ?</i> .....                                    | 62        |
| <b>IV.-</b> | <b>ROLE DE L'ÉTAT.....</b>  | <b>63</b> |
|             | <b>CONCLUSION.....</b>  | <b>64</b> |



# INTRODUCTION

Nous vivons dans un monde de plus en plus soumis à la technologie et aucun secteur n'y échappe. Le domaine du droit est depuis quelques années soumis aux contrats conclus par voie électronique, ce qui a amené le législateur national à adopter la loi sur la signature électronique du 21 juillet 2016<sup>1</sup>. Cette loi a été prise afin de mettre en œuvre le règlement eIDAS adopté par l'Union européenne le 23 juillet 2014 et portant sur l'identification électronique et les services de confiance<sup>2</sup>. Ce règlement vient remplacer la directive 1999/93/CE qui avait pour but d'instaurer un cadre communautaire pour l'utilisation de la signature électronique. Ce dernier constitua cependant un échec de la part du législateur européen comme nous le verrons<sup>3</sup>.

Dans le secteur économique aussi cette expansion de la technologie fait peur. Ainsi, le secteur du notariat et le secteur bancaire tentent de réagir à ce phénomène en l'utilisant dans leur façon de travailler. Le but est d'éviter d'être remplacé par la technologie et de privilégier un vivre ensemble.

La technologie *Blockchain* repose sur deux éléments principaux autour desquels nous avons inscrit notre travail. Tout d'abord, la *Blockchain* se sert d'un système de cryptographie asymétrique afin de sécuriser ses transactions<sup>4</sup>. Ce qui nous amène directement au mécanisme de signature électronique. En effet, le mécanisme de cryptographie asymétrique est l'un des mécanismes visés par la législation sur la signature électronique<sup>5</sup>. C'est pour cette raison qu'il nous paraît être le plus approprié dans un objectif de régulation de la *Blockchain*. Deuxième élément, la *Blockchain* repose sur un réseau décentralisé<sup>6</sup>. Les opérations ne passent plus par un organe centralisé et donc les utilisateurs interagissent directement entre eux<sup>7</sup>. Ceci diffère du schéma classique dans lequel nous avons besoin d'intermédiaires de confiance comme les banquiers ou les notaires pour effectuer diverses opérations dans la vie de tous les jours<sup>8</sup>. Nous verrons alors dans quelle mesure exactement la place de ces tiers intermédiaires va être remise en cause.

---

<sup>1</sup> Loi du 21 juillet 2016 mettant en œuvre et complétant le règlement (UE) 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII " Droit de l'économie électronique " du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique, *M.B.*, 28 septembre 2016, p. 67478.

<sup>2</sup> Règlement (UE) 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, *J.O.U.E.*, L 257, 28 août 2014.

<sup>3</sup> Directive (UE) 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, *J.O.C.E.*, L 13, 19 janvier 2000.

<sup>4</sup> A. TORDEURS, « Une approche pédagogique de la Blockchain » in *Revue internationale des services financiers / International Journal for Financial Services*, Bruylant, 2017, p. 11.

<sup>5</sup> H. JACQUEMIN, *L'identification électronique et les services de confiance depuis le règlement eIDAS*, Bruxelles, Larcier, 2016, p. 7. ; Loi du 21 juillet 2016. ; Règlement (UE) 910/2014.

<sup>6</sup> A. TORDEURS, « Une approche pédagogique de la Blockchain », *op. cit.*, p. 9.

<sup>7</sup> M. GUERINEAU, « Blockchain : l'ère de la transparence ? » in *Revue internationale des services financiers / International Journal for Financial Services*, Bruylant, 2016, p. 78.

<sup>8</sup> *Ibid.*, p. 78.

A travers cet exposé, l'objectif est double. Premièrement, nous déterminerons les enjeux juridiques que pourrait amener l'utilisation de la *Blockchain* en Belgique. Deuxièmement, nous pointerons les dangers mais également les opportunités d'une telle implantation dans les secteurs qui nous paraissent susceptibles d'être les plus impactés par cette technologie, à savoir notariat belge et le secteur bancaire belge.

Pour ce faire, nous avons divisé notre travail en quatre parties principales. La première partie consiste en un exposé de la *Blockchain*. La deuxième partie dresse un état des lieux juridique de ce phénomène. La troisième partie vise à analyser les impacts tant positifs que négatifs de l'utilisation de la technologie *Blockchain* dans le secteur bancaire et dans le notariat. Enfin, la quatrième partie consiste en une brève réflexion sur le rôle qu'il reste à l'État dans un système dominé de plus en plus par la technologie.

## **I.- PRÉSENTATION DE LA *BLOCKCHAIN***

Avant de nous consacrer à l'analyse des conséquences juridiques et économiques de l'implantation de la *Blockchain* en Belgique, il convient de définir cette notion et d'en exposer quelque peu les caractéristiques. Cette étape est essentielle pour la suite du travail car cela permettra de comprendre au mieux les enjeux que représente cette technologie quant à son implantation. La particularité de ce travail est que l'analyse qui est faite de chaque caractéristique de la *Blockchain* permet de trouver les problématiques ou les opportunités qui en découlent.

### **A.- DÉFINITION DE LA *BLOCKCHAIN***

La *Blockchain*, encore appelée « chaîne des blocs », est une technologie apparue en 2009 avec la monnaie virtuelle *Bitcoin*<sup>9</sup>. Elle a émergé à la suite de la crise de confiance de 2008 dirigée contre les institutions financières et plus largement contre l'État<sup>10</sup>. Ce qui explique son intérêt pour le secteur bancaire et plus précisément, pour les établissements de paiement. Si, à l'origine, la *Blockchain* a été créée pour faire fonctionner le système de paiement en *Bitcoin*, il existe désormais de nombreux autres cas d'application, dont un qui nous intéressera particulièrement pour son aspect juridique, celui des *Smart contracts* ou « contrats intelligents ».

---

<sup>9</sup> C. HOUSSA et L. STANDAERT, « La « Nouvelle frontière » de la finance » *in X.*, 2016, p. 187.

<sup>10</sup> D. GEIBEN, O. JEAN-MARIE, T. VERBIEST et J-F. VILOTTE, *Bitcoin et Blockchain. Vers un nouveau paradigme de la confiance numérique ?*, RB édition, 2016, p. 42.

La *Blockchain* peut être définie comme étant « une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle »<sup>11</sup>. Cette technologie permet d'accomplir et d'enregistrer n'importe quel type d'opérations de façon transparente et sécurisée<sup>12</sup>. Elle constitue dès lors une immense base de données sécurisée tenant compte de toutes les transactions effectuées par les différents utilisateurs depuis sa création<sup>13</sup>.

Beaucoup d'auteurs la comparent à un grand livre comptable, car toutes les transactions sont enregistrées les unes à la suite des autres de façon infalsifiable<sup>14</sup>. Pour Jean-Paul Delahaye il faut imaginer un « très grand cahier, que tout le monde peut lire librement, gratuitement, sur lequel tout le monde peut écrire, qui est impossible à effacer et indestructible »<sup>15</sup>.

Il en existe un grand nombre de définitions. Nous avons choisi plus largement comme référence la définition donnée par Laurent Leloup. Elle est selon nous la plus complète, puisqu'elle permet de comprendre ce qu'est la *Blockchain*, la façon dont elle fonctionne, ainsi que ses différentes caractéristiques.

Pour lui, la *Blockchain* est « une base de données transactionnelle distribuée, comparable à un grand livre comptable décentralisé et partagé, qui stocke et transfère de la valeur ou des données via Internet, de façon transparente, sécurisée et autonome, car sans organe central de contrôle. Ce registre est actif, chronologique, distribué, vérifiable et protégé contre la falsification par un système de confiance répartie (consensus) entre les membres ou participants (nœuds). Chaque membre du réseau possède une copie à jour du grand livre (en temps quasi réel) et le contenu est toujours en phase avec l'ensemble des participants »<sup>16</sup>.

Ainsi, nous retrouvons les trois principaux piliers de la *Blockchain*, à savoir l'automatisation des transactions à travers la suppression des tiers de confiance, un système de consensus qui se situe à la base du fonctionnement par cryptographie asymétrique, enfin, une infrastructure décentralisée et distribuée<sup>17</sup>. C'est à travers ces trois piliers que se développera l'essentiel de la réflexion de notre travail.

---

<sup>11</sup> C. HOUSSA et L. STANDAERT, *La « Nouvelle frontière » de la finance*, op. cit., p. 187.

<sup>12</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, Paris, Eyrolles, 2017, p. 13.

<sup>13</sup> C. HOUSSA et L. STANDAERT, *La « Nouvelle frontière » de la finance*, op. cit., p. 187.

<sup>14</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p. 13.

<sup>15</sup> J. P. DELAHAYE, « Les blockchains, clefs d'un nouveau monde » in *Logique et calcul*, mars 2015, p. 81.

<sup>16</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p. 14.

<sup>17</sup> *Ibid.*, p. 14.

## B.- FONCTIONNEMENT DE LA *BLOCKCHAIN*

Le fonctionnement de la *Blockchain* est un processus informatique complexe. C'est pourquoi nous avons choisi de l'expliquer de façon assez synthétique, ce qui est toutefois suffisant pour comprendre l'exposé. Son fonctionnement peut s'expliquer par un processus en plusieurs étapes. Nous nous aidons d'un schéma sur le fonctionnement de la *Blockchain* reproduit ci-dessous afin d'illustrer nos propos.

Les utilisateurs voulant opérer une transaction ou échanger une information sur la *Blockchain*, vont traduire leur accord dans un code informatique et soumettre leur demande de transaction à l'ensemble du réseau<sup>18</sup>. La *Blockchain* fonctionne sur la base d'un consensus entre les individus qui l'utilisent. Ce consensus se traduit à travers un système de cryptographie asymétrique<sup>19</sup>. Pour fonctionner, ce système aura besoin de deux fonctions. Nous avons une première fonction appelée « clé publique » qui sert d'adresse dans la *Blockchain*, et une seconde nommée « clé privée » qui permet d'initier une transaction et de décrypter le message<sup>20</sup>. Ainsi, l'utilisateur qui souhaite envoyer un message utilise la clé publique du destinataire pour encoder ce message. Seul le destinataire en possession de la clé privée pourra le décoder<sup>21</sup>. Si le message est intercepté par quelqu'un qui ne possède pas la clé privée, cela sera tout simplement incompréhensible<sup>22</sup>.

Avant de pouvoir être exécutée, la transaction doit être vérifiée par les membres du réseau. Il s'agit de l'étape quatre sur notre schéma. Il existe plusieurs moyens de valider une transaction. Le plus connu est la preuve de travail<sup>23</sup>. Dans ce système, chaque nouvelle écriture sera contrôlée par des mineurs<sup>24</sup>. Les mineurs sont des membres du réseau qui ont décidé de participer au processus de construction de la *Blockchain* en validant les transactions<sup>25</sup>. Ils vont regrouper plusieurs transactions au sein d'un même bloc afin de vérifier et valider ce bloc<sup>26</sup>. Tant que les transactions à l'intérieur d'un bloc ne sont pas validées, le bloc reste en attente et n'est pas incorporé à la *Blockchain*<sup>27</sup>. Ce n'est qu'à partir du moment où les transactions sont vérifiées et que le bloc est validé par un mineur, que la transaction sera exécutée. Le rôle des mineurs est donc de vérifier la légitimité des transactions soumises sur la *Blockchain*. Par exemple, lors d'un transfert d'argent, ils vont vérifier que l'individu a bien les fonds nécessaires à la transaction et donc qu'il ne les a pas déjà dépensés<sup>28</sup>. Il s'agit d'une fonction dont le but est

---

<sup>18</sup> T. CAMBRAI, *Tout comprendre sur la Blockchain. Une technologie révolutionnaire au cœur du système économique de demain*, 2017, p. 7.

<sup>19</sup> P. HERLIN, *La fin des banques ?*, Paris, Eyrolles, 2015, p. 76.

<sup>20</sup> *Ibid.*, p. 76.

<sup>21</sup> *Ibid.*, p. 76.

<sup>22</sup> A. TORDEURS, « Une approche pédagogique de la Blockchain », *op. cit.*, p. 128.

<sup>23</sup> I. PAVEL, « La blockchain - Les défis de son implémentation » in *réalités industrielles*, août 2017, p. 20.

<sup>24</sup> *Ibid.*, p. 20.

<sup>25</sup> T. CAMBRAI, *Tout comprendre sur la Blockchain. Une technologie révolutionnaire au cœur du système économique de demain*, *op. cit.*, p. 7.

<sup>26</sup> *Ibid.*, p. 7.

<sup>27</sup> *Ibid.*, p. 7.

<sup>28</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, *op. cit.*, p. 17.



de faire résoudre par le mineur à l'aide de son ordinateur une énigme complexe<sup>29</sup>. Pour parler en des termes plus simples et de façon plus imagée, le travail des mineurs consistera à remonter très loin dans la chaîne de transactions afin de vérifier la source des fonds demandés, trouver le montant qu'il reste de ces fonds ainsi que toutes les informations nécessaires pour pouvoir valider la nouvelle transaction. Le premier mineur à avoir résolu cette énigme valide la transaction et est rémunéré pour son travail<sup>30</sup>. L'assurance d'une validation correcte ne tient cependant pas du mineur en lui-même mais de la puissance de calcul nécessaire à son ordinateur afin de valider une transaction<sup>31</sup>. Ainsi, une fois que toutes les transactions comprises dans un bloc ont été vérifiées, le bloc est validé par le mineur, il est horodaté et ajouté définitivement au bloc qui le précède et ainsi de suite pour chaque transaction ce qui forme la « chaîne des blocs » ou la *Blockchain*<sup>32</sup>.

Enfin, ce registre est distribué à l'ensemble du réseau, ce qui permet la recherche des informations effectuée par les mineurs et la consultation par tous les participants à la chaîne<sup>33</sup>.

Nous l'avons dit, d'autres moyens de valider les blocs existent, le plus connu après la preuve de travail est la preuve d'enjeu. Ainsi, pour pouvoir valider un bloc de transactions, il faut prouver que nous possédons un certain montant de crypto-monnaies, ce qui nous donne une certaine importance dans la chaîne<sup>34</sup>.

#### Fonctionnement de la blockchain

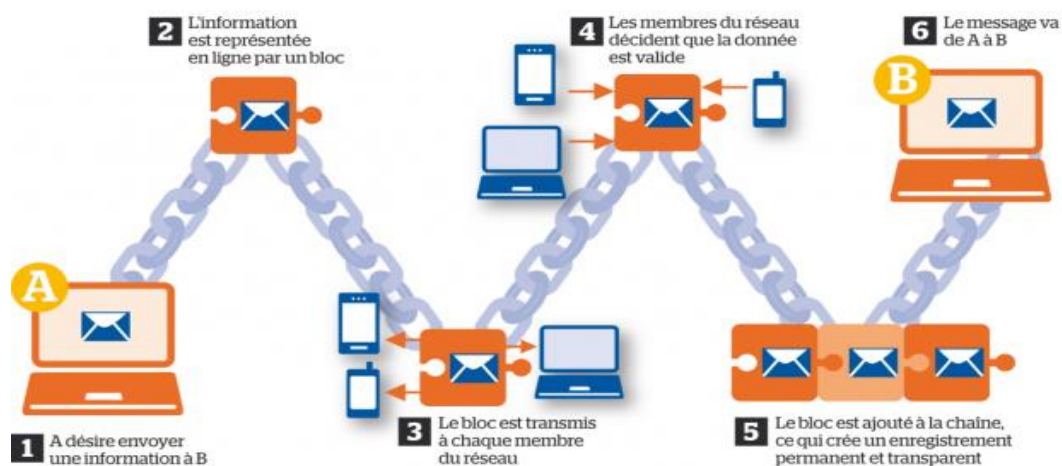


Schéma 1 : Schéma illustrant le fonctionnement de la *Blockchain*<sup>35</sup>. Source : Claire Dubos.

<sup>29</sup> P. RODRIGUEZ, *La révolution Blockchain. Algorithmes ou institutions, à qui donnerez-vous votre confiance ?*, Malakoff, Dunod, 2017, p. 129.

<sup>30</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p. 48.

<sup>31</sup> D. GEIBEN, O. JEAN-MARIE, T. VERBIEST et J-F. VILOTTE, *Bitcoin et Blockchain. Vers un nouveau paradigme de la confiance numérique ?*, op. cit., p. 117.

<sup>32</sup> *Ibid.*, pp. 17. et 173.

<sup>33</sup> T. CAMBRAI, *Tout comprendre sur la Blockchain. Une technologie révolutionnaire au cœur du système économique de demain*, op. cit., p. 7.

<sup>34</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p. 99.

<sup>35</sup> B. KIRALY, « Comment la blockchain va bousculer la construction », 3 mai 2016, disponible sur <https://www.lemoniteur.fr> (27 avril 2018).

## C.- CARACTERISTIQUES DE LA *BLOCKCHAIN*

Ce qui rend la *Blockchain* si attrayante, ce sont ses caractéristiques. En effet, chaque technologie est conçue pour accomplir une tâche précise. Dès lors, les caractéristiques de cette technologie découleront de l'usage que l'on veut en faire. En ce qui concerne la *Blockchain*, elle a été créée dans un but précis : pouvoir faire des transactions sans passer par des tiers intermédiaires. Pour ce faire, elle fonctionne à travers un réseau décentralisé et est caractérisée par un consensus distribué qui assure la transparence et l'immutabilité des opérations<sup>36</sup>.

### 1) *La décentralisation*

La caractéristique principale de la *Blockchain* est qu'elle est décentralisée<sup>37</sup>. Cela signifie que, contrairement à un réseau centralisé traditionnel dans lequel les informations passent toutes par un serveur unique, les informations sont ici distribuées entre plusieurs serveurs localisés dans des endroits géographiquement différents<sup>38</sup>. Les diverses opérations ne passent plus par des tiers mais sont gérées directement par les différents utilisateurs à partir de chez eux<sup>39</sup>.

Cette caractéristique présente tant un avantage qu'un inconvénient. Ce système présente une certaine sécurité, car il est plus résistant qu'un réseau centralisé. En effet, pour pouvoir mettre à mal le système, il faudrait attaquer plusieurs serveurs alors que, dans un réseau centralisé, il suffit de prendre le contrôle d'un seul<sup>40</sup>. De plus, contrairement au réseau centralisé, la défaillance d'un serveur n'empêche pas le réseau de fonctionner puisque les autres sont là pour prendre le relais<sup>41</sup>. Cependant, le fait que les données ne passent plus par un tiers ou par un serveur central mais sont échangées directement entre les utilisateurs ne permet aucun contrôle des informations qui sont partagées<sup>42</sup>.

---

<sup>36</sup> A. TORDEURS, « Une approche pédagogique de la Blockchain », *op. cit.*, p. 14.

<sup>37</sup> *Ibid.*, p. 9.

<sup>38</sup> *Ibid.*, p. 9.

<sup>39</sup> *Ibid.*, p. 9.

<sup>40</sup> *Ibid.*, p. 9.

<sup>41</sup> *Ibid.*, p. 9.

<sup>42</sup> *Ibid.*, p. 9.

## 2) *Un consensus*

Certains auteurs comme Laurent Leloup parlent de la *Blockchain* comme étant une « révolution de la confiance »<sup>43</sup>. En effet, cette technologie est basée sur un consensus quant à son utilisation<sup>44</sup>. L'acceptation ou le rejet d'une opération sur la *Blockchain* n'est dès lors plus le fruit d'une institution centralisée mais résulte d'un consensus entre les différents utilisateurs comme nous l'avons vu en analysant le fonctionnement de celle-ci<sup>45</sup>.

## 3) *Le caractère distribué*

La *Blockchain* est construite comme un grand livre comptable<sup>46</sup>. La comptabilité est en partie utile pour que les personnes extérieures à l'entreprise puissent s'informer sur l'état de celle-ci.

Dans le cadre de la *Blockchain*, il s'agit plus précisément d'un grand registre dans lequel toutes les opérations sont enregistrées. Ce registre est ensuite distribué à chaque utilisateur qui disposera dès lors d'une copie de celui-ci<sup>47</sup>.

## 4) *La transparence*

Il découle du caractère distribué de la *Blockchain* que tous les membres du réseau peuvent accéder au registre et prendre connaissance de n'importe quelle transaction existante jusqu'à la première transaction ayant été inscrite sur la *Blockchain*<sup>48</sup>.

Il faut cependant distinguer deux choses. Si les opérations effectuées sur la *Blockchain* sont visibles, leur contenu ne l'est pas et leurs auteurs sont anonymes<sup>49</sup>.

## 5) *Le caractère immuable*

Nous l'avons déjà dit, la *Blockchain* ressemble à un grand registre dans lequel sont ajoutées une à une chaque transaction après avoir été validée grâce à la cryptographie asymétrique<sup>50</sup>. Mais ce que nous n'avons pas encore précisé c'est que, une fois l'opération

---

<sup>43</sup> L. LELOUP, « *Blockchain : La révolution de la confiance* », *op. cit.*, p. 15.

<sup>44</sup> *Ibid.*, p. 15.

<sup>45</sup> *Ibid.*, p. 15.

<sup>46</sup> *Ibid.*, p. 13.

<sup>47</sup> A. TORDEURS, « Une approche pédagogique de la Blockchain », *op. cit.*, p. 10.

<sup>48</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, *op. cit.*, p. 126.

<sup>49</sup> I. PAVEL, « La blockchain - Les défis de son implémentation », *op. cit.*, p. 23.

<sup>50</sup> P. HERLIN, *La fin des banques ?*, *op. cit.*, p. 76.

enregistrée sur la *Blockchain*, il est impossible de la supprimer ou de la modifier<sup>51</sup>. Le registre étant distribué à l'ensemble du réseau, cela implique que, pour le falsifier, il faudrait modifier l'ensemble des copies appartenant aux différents membres<sup>52</sup>.

Le caractère immuable de la *Blockchain* peut cependant poser certains problèmes. Nous pouvons dès lors nous demander quelles solutions nous pourrions envisager dans l'hypothèse où une opération sur la *Blockchain* serait validée alors qu'elle était incorrecte ou encore, lorsque les parties qui ont conclu un accord sur la *Blockchain* décidaient finalement de revenir sur celui-ci ?

Un autre élément important qui découle de cet enregistrement est que, au moment où la transaction est validée et ajoutée à la chaîne, elle est horodatée<sup>53</sup>. Nous avons donc une preuve de la date et de l'heure à laquelle a été passée une transaction. Cet élément pourrait constituer un réel avantage pour le secteur du notariat dans la mesure où, comme nous le verrons, le notaire confère date certaine aux actes qu'il signe. Si l'acte authentique n'est pas daté, il ne sera pas valable<sup>54</sup>.

#### **D.- BLOCKCHAIN PRIVÉE ET PUBLIQUE : DISTINCTION**

Afin de bien comprendre ce qu'est la *Blockchain*, il convient de faire une dernière distinction. Il existe trois types de *Blockchain*<sup>55</sup>. Il faut distinguer selon que la *Blockchain* est ouverte à tout le monde, limitée à certaines personnes ou constitue un mélange des deux. Nous distinguons alors les *Blockchains* publiques, les *Blockchains* privées et les *Blockchains* de consortium. L'intérêt de cette distinction est apparu lorsque les institutions financières ont commencé à expérimenter diverses applications de la *Blockchain* mais de préférence de façon privée<sup>56</sup>.

Les *Blockchains* publiques sont des *Blockchains* ouvertes, dans lesquelles tout le monde peut lire des données, les écrire et participer au consensus<sup>57</sup>. C'est par exemple la technologie utilisée pour le *Bitcoin* ou *Ethereum*. Nous verrons plus tard de quoi il s'agit exactement.

---

<sup>51</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p. 126

<sup>52</sup> *Ibid.*, p. 17.

<sup>53</sup> *Ibid.*, p. 173.

<sup>54</sup> F. MOURLON BEERNAERT, « La preuve en matière civile et commerciale » in *pratique du droit*, 2<sup>e</sup> édition, Wolters Kluwer, p. 106.

<sup>55</sup> T. CAMBRAI, *Tout comprendre sur la Blockchain. Une technologie révolutionnaire au cœur du système économique de demain*, op. cit., p. 20.

<sup>56</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p. 93.

<sup>57</sup> T. CAMBRAI, *Tout comprendre sur la Blockchain. Une technologie révolutionnaire au cœur du système économique de demain*, op. cit. p. 21.

Ensuite, nous avons les *Blockchains* dites de consortium. Le processus d'approbation est effectué par un nombre restreint de personnes<sup>58</sup>. Elles peuvent cependant décider d'ouvrir la *Blockchain* à tous, de la garder privée ou d'en autoriser un accès limité<sup>59</sup>.

Enfin, dans les *Blockchains* privées, tant l'accès au processus de validation des transactions que leur lecture sont limités à quelques personnes déterminées<sup>60</sup>. Celles-ci nécessitent donc à la fois une permission pour écrire les données et pour les lire<sup>61</sup>.

## E.- FAIBLESSES DE LA *BLOCKCHAIN*

Malgré l'approche très attractive qui est faite de la *Blockchain* par ses défenseurs, nous ne devons pas oublier qu'elle comporte encore quelques faiblesses. Ces faiblesses doivent à notre avis être prises en considération dans l'implantation future de ce système chez nous.

### 1) *Coût énergétique*

La *Blockchain* a un coût énergétique très important. En effet, le calcul pour effectuer la preuve de travail entraîne une consommation énergétique énorme puisque des milliers d'ordinateurs tournent en même temps afin de valider une unique opération<sup>62</sup>. Une étude a d'ailleurs démontré que le réseau du *Bitcoin* avait en 2014 consommé entre 0.1 et 10 gigawatts, alors que l'application la plus performante du marché ne consommerait que 1300 watts<sup>63</sup>. Si nous prenons l'ensemble des mineurs sur la *Blockchain Bitcoin*, ils consomment en moyenne 400 mégawatts, ce qui équivaut en termes de puissance à la moitié d'une centrale nucléaire<sup>64</sup>.

De plus, le fait de récompenser les mineurs pour leur travail entraîne une augmentation du nombre de personnes voulant intégrer le réseau ainsi que l'utilisation d'ordinateurs de plus en plus puissants. Cela nous amène donc à nous interroger sur l'acceptabilité d'un point de vue écologique d'un tel système. D'un côté, plus le nombre de mineurs augmente, plus la protection contre une éventuelle attaque est forte mais d'un autre, la compétitivité qu'elle entraîne augmente très fortement la consommation énergétique également<sup>65</sup>.

---

<sup>58</sup> T. CAMBRAI, *Tout comprendre sur la Blockchain. Une technologie révolutionnaire au cœur du système économique de demain*, op. cit., p. 21.

<sup>59</sup> A. TORDEURS, « Une approche pédagogique de la Blockchain », op.cit., p. 18.

<sup>60</sup> *Ibid.*, p. 18.

<sup>61</sup> *Ibid.*, p. 18.

<sup>62</sup> T. CAMBRAI, *Tout comprendre sur la Blockchain. Une technologie révolutionnaire au cœur du système économique de demain*, op. cit., p. 7.

<sup>63</sup> Il s'agit de AntMiner S9 ; I. PAVEL, « La blockchain - Les défis de son implémentation », op. cit., p. 22.

<sup>64</sup> I. PAVEL, « La blockchain - Les défis de son implémentation », op. cit., p. 22.

<sup>65</sup> A. TORDEURS, « Une approche pédagogique de la Blockchain », op.cit., p. 16.

Une solution serait de favoriser la vérification des transactions par la preuve d'enjeu, qui est moins énergivore que la preuve de travail<sup>66</sup>. Le problème est qu'elle est aussi moins sécurisée, car la vérification n'est plus faite grâce à la puissance de calcul mais grâce aux parts de crypto-monnaie détenues par les membres du réseau<sup>67</sup>.

## 2) *Limites techniques*

Lorsque nous entendons dire que la *Blockchain* est sécurisée et infalsifiable, il faut plutôt entendre qu'elle est très difficile à attaquer. En effet, la taille des blocs a été limitée afin d'empêcher une prise de contrôle, ainsi les blocs sur la *Blockchain Bitcoin* par exemple ont une capacité maximum d'un méga-octet<sup>68</sup>. Cependant, aucun ordinateur n'est à l'abri d'une attaque ou d'une erreur technologique. Une personne ou un groupe de personnes pourrait très bien arriver à contrôler le réseau et ainsi décider seul de valider certaines opérations, de refuser d'en valider d'autres ou encore d'opérer des doubles dépenses, c'est-à-dire, d'utiliser plusieurs fois le même argent pour effectuer des transactions différentes<sup>69</sup>. Dans le cadre d'une *Blockchain*, c'est ce qui s'appelle « l'attaque des 51 % », car pour arriver à cela il faudrait arriver à prendre le contrôle de plus de la moitié de la puissance du minage. À nouveau, là où la *Blockchain* tire son avantage, c'est que plus le réseau s'agrandit, plus le nombre d'ordinateurs dont nous avons besoin pour prendre le contrôle augmente et donc plus cela deviendra coûteux et difficile d'y parvenir<sup>70</sup>.

De plus, comme nous le verrons dans l'analyse économique, cette limite peut poser problème quant à l'implantation de la *Blockchain* dans certains secteurs comme le secteur bancaire, car elle restreint fortement le nombre de transactions pouvant être opérées<sup>71</sup>. Ainsi, nous pouvons nous demander si une telle limitation de la capacité de la *Blockchain* comparé au coût énergétique qu'elle représente fait vraiment d'elle la meilleure solution pour révolutionner le domaine de la technologie.

## 3) *Anonymat*

La sécurité des transactions passe par l'identification de ses auteurs<sup>72</sup>. Or, la *Blockchain* ne permet pas d'être sûr de l'identité de la personne avec laquelle nous sommes en train de communiquer.

---

<sup>66</sup> D. GEIBEN, O. JEAN-MARIE, T. VERBIEST et J-F. VILOTTE, *Bitcoin et Blockchain. Vers un nouveau paradigme de la confiance numérique ?*, op. cit., p. 42.

<sup>67</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p. 98.

<sup>68</sup> I. PAVEL, « La blockchain - Les défis de son implémentation », op. cit., p. 20.

<sup>69</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p. 49.

<sup>70</sup> A. TORDEURS, « Une approche pédagogique de la Blockchain », op. cit., p. 17.

<sup>71</sup> I. PAVEL, « La blockchain - Les défis de son implémentation », op. cit., p. 21.

<sup>72</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p. 25.

Cela s'explique tout d'abord parce qu'il n'y a rien qui force les individus à divulguer des informations personnelles quant à leur identité sur la *Blockchain*<sup>73</sup>. Ainsi, beaucoup recourent à des pseudonymes<sup>74</sup>.

Ensuite, parce que pour participer à la *Blockchain* les utilisateurs possèdent des clés comme nous l'avons vu *supra*, cependant une telle clé peut être volée, perdue et donc nous pouvons très bien conclure une opération avec une personne qui n'est pas celle avec qui nous avons l'intention de traiter<sup>75</sup>.

#### 4) *L'absence de régulation*

Enfin, la *Blockchain* étant un procédé informatique dont l'intérêt n'est que fort récent, il ne fait l'objet d'aucune réglementation. Une autre raison à cela est que les créateurs de cette technologie ont volontairement établi un système qui ne laisse aucune place aux intermédiaires de confiance, dont le premier est l'État<sup>76</sup>. Cette volonté traduit la perte de confiance envers les institutions après la crise de 2008<sup>77</sup>. Ces intermédiaires assurent pourtant une mission de sécurisation des opérations<sup>78</sup>.

Certes, la *Blockchain* instaure une certaine sécurité mais dans une mesure limitée. En effet, l'absence de cadre réglementaire ne permettra pas une viabilité à long terme de ce système. La preuve réside dans les diverses fraudes opérées à l'aide du *Bitcoin*. À titre d'exemple, en février 2014, pas moins de 774 000 *Bitcoins* pour une valeur de 409 millions de dollars avaient disparu de la plateforme d'échange MtGox<sup>79</sup>. Tout ceci a d'ailleurs amené les institutions de l'Union européenne à prendre différentes mesures afin d'encadrer l'utilisation du *Bitcoin*<sup>80</sup>.

### F.- APPLICATIONS DE LA *BLOCKCHAIN*

Bien que la *Blockchain* soit née avec le *Bitcoin*, nous nous sommes vite rendu compte que son potentiel allait bien au-delà d'une simple plateforme d'échanges de crypto-monnaie. En effet, certains voient en elle « l'émergence de nouveaux modèles économiques »<sup>81</sup>. Nous en

---

<sup>73</sup> I. PAVEL, « La blockchain - Les défis de son implémentation », *op. cit.*, p. 23.

<sup>74</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, *op. cit.*, p. 51.

<sup>75</sup> M. GUERINEAU, « Blockchain : l'ère de la transparence ? », *op. cit.*, p. 79.

<sup>76</sup> D. GEIBEN, O. JEAN-MARIE, T. VERBIEST et J-F. VILOTTE, *Bitcoin et Blockchain. Vers un nouveau paradigme de la confiance numérique ?*, *op. cit.*, p. 42.

<sup>77</sup> P. HERLIN, *La fin des banques ?*, *op. cit.*, p. 56.

<sup>78</sup> D. GEIBEN, O. JEAN-MARIE, T. VERBIEST et J-F. VILOTTE, *Bitcoin et Blockchain. Vers un nouveau paradigme de la confiance numérique ?*, *op. cit.*, p. 42.

<sup>79</sup> I. PAVEL, « La blockchain - Les défis de son implémentation », *op. cit.*, p. 23.

<sup>80</sup> Cf. *infra* section 2) Le *Bitcoin*, p. 16 du travail.

<sup>81</sup> D. GEIBEN, O. JEAN-MARIE, T. VERBIEST, et J-F VILOTTE, *Bitcoin et Blockchain. Vers un nouveau paradigme de la confiance numérique ?*, *op. cit.*, p. 41.

citerons quelques-uns avant de nous attarder plus longuement sur deux applications qui ont particulièrement retenu notre attention. Il s'agit du *Bitcoin* et des *Smart contracts*. Nous avons choisi de parler plus en profondeur de ces deux applications, car ce sont celles qui amènent les premières à une réflexion juridique.

### 1) *Listes non exhaustives*

Citons tout d'abord les *wallets*. Ce sont des plateformes permettant de stocker et d'échanger des *Bitcoins* comme moyen de paiement<sup>82</sup>.

Une autre application a été la création du programme Monegraph. Basé sur le principe de la *Blockchain*, il permet de tracer toutes les données relatives aux œuvres digitales et plus particulièrement leurs licences<sup>83</sup>.

La *Blockchain* sert également à la gestion cadastrale. En effet, certains pays comme le Honduras et le Ghana mettent en place un outil de gestion du cadastre numérique basé sur le protocole de la *Blockchain* qui reprend par exemple toutes les hypothèques existantes sur le territoire<sup>84</sup>.

Nous pouvons également citer l'initiative prise à Dubaï en octobre 2016 afin de mettre en place sur la *Blockchain* un registre des visas permettant de faciliter leur vérification<sup>85</sup>. Le pays estimait alors une réduction du nombre d'heures de travail de la part des différents agents administratifs de l'ordre de 25,1 millions par an<sup>86</sup>.

Une autre application est le *trading* financier, dans lequel l'échange de titres se fait de façon sécurisée sur la base du processus de la *Blockchain*<sup>87</sup>.

Les domaines dans lesquels nous pouvons utiliser la *Blockchain* sont multiples et très divers. Nous pouvons encore citer le secteur des assurances, la gestion des dossiers médicaux, un registre pour les administrations et bien d'autres<sup>88</sup>.

### 2) *Le Bitcoin*

Nous ne pouvons pas parler de la *Blockchain* sans dire quelques mots à propos du *Bitcoin*. En effet, la *Blockchain* est « l'architecture sous-jacente au *Bitcoin* »<sup>89</sup>. C'est sur la base de cette technologie que fonctionne le système *Bitcoin*. Le *Bitcoin* est aussi l'application la plus

---

<sup>82</sup> D. GEIBEN, O. JEAN-MARIE, T. VERBIEST, et J-F VILOTTE, *Bitcoin et Blockchain. Vers un nouveau paradigme de la confiance numérique ?*, op. cit., p. 41.

<sup>83</sup> *Ibid.*, p. 43.

<sup>84</sup> *Ibid.*, p. 45.

<sup>85</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p. 141.

<sup>86</sup> *Ibid.*, p. 141.

<sup>87</sup> *Ibid.*, p. 45.

<sup>88</sup> *Ibid.*, p. 129.

<sup>89</sup> C. HOUSSA et L. STANDAERT, « La « Nouvelle frontière » de la finance », op. cit., p. 27.



célèbre de la *Blockchain*. Sa notoriété a d'ailleurs amené les institutions européennes à s'intéresser à son statut comme nous le verrons.

Thomas Cambrai définit le *Bitcoin* comme « un projet d'échange décentralisé et sécurisé d'argent virtuel »<sup>90</sup>. Le but principal est alors de se passer de ces intermédiaires de confiance dont le rôle est de certifier et d'enregistrer les diverses transactions monétaires de façon sécurisée<sup>91</sup>.

En pratique, cela fonctionne exactement comme nous l'avons vu plus haut<sup>92</sup>. Nous allons prendre un exemple concret pour faciliter la compréhension. Monsieur Dubois a prêté de l'argent à Madame Florelle<sup>93</sup>. Au moment du remboursement, Madame Florelle va saisir l'identifiant à l'aide de la clé publique de Monsieur Dubois et son mot de passe personnel, c'est-à-dire, sa clé privée afin de lui transférer l'argent qu'elle lui doit. De son côté, Monsieur Dubois sera averti du transfert et devra saisir à son tour son mot de passe à l'aide de sa clé privée pour bénéficier de ce transfert. Les mineurs vont entre-temps valider la transaction. Pour ce faire, ils vérifient si les adresses de Monsieur Dubois et de Madame Florelle sont correctes et si l'argent transféré n'a pas déjà été utilisé<sup>94</sup>. Une fois validée par les mineurs, la transaction est ajoutée à la chaîne des blocs et les mineurs seront rémunérés en *Bitcoin* pour leur travail<sup>95</sup>.

Nous sommes cependant amenés à nous demander quelle est la place d'un tel système dans un État comme le nôtre. Nous pourrions considérer le *Bitcoin* comme une monnaie complémentaire, une monnaie qui serait utilisée uniquement en complément de la monnaie officielle d'un pays sans pouvoir la remplacer. À la différence que le *Bitcoin* n'est pas limité à un territoire déterminé, ce qui le fait s'écarter de la notion de monnaies complémentaires traditionnelles<sup>96</sup>.

Le *Bitcoin* ne peut pas être considéré comme une monnaie fiduciaire étatique. En effet, la création et l'émission de monnaie fiduciaire est un monopole des banques nationales des États membres, ce qui permet d'apporter les garanties nécessaires au bon fonctionnement du système monétaire<sup>97</sup>. En Belgique, c'est la Banque nationale de Belgique qui tient ce rôle<sup>98</sup>. Pour ce qui est de la monnaie scripturale, elle est créée par les banques, par le biais d'octroi de crédit<sup>99</sup>.

De plus, si nous regardons la définition de la monnaie électronique telle que définie à l'article 2, 2) de la directive 2009/110/CE sur les établissements de monnaie électronique, le *Bitcoin* n'est pas non plus une monnaie électronique légale. Selon cette définition, la monnaie

---

<sup>90</sup> T. CAMBRAI, *Tout comprendre sur la Blockchain. Une technologie révolutionnaire au cœur du système économique de demain*, op. cit., p. 15.

<sup>91</sup> *Ibid.*, p. 15.

<sup>92</sup> Cf. *supra* B.-Fonctionnement, p. 8 du travail.

<sup>93</sup> D. GEIBEN, O. JEAN-MARIE, T. VERBIEST et J-F. VILOTTE, *Bitcoin et Blockchain. Vers un nouveau paradigme de la confiance numérique ?*, op. cit., p. 23.

<sup>94</sup> *Ibid.*, p. 23.

<sup>95</sup> *Ibid.*, p. 24.

<sup>96</sup> A-P. ANDRE-DUMONT, « Les services de paiement à l'épreuve des évolutions technologiques » in *La révolution digitale et les start-ups*, Larcier, 2016, p. 85.

<sup>97</sup> P. HERLIN, *La fin des banques ?*, op. cit., p. 47.

<sup>98</sup> NBB, « A quoi sert la Banque nationale ? », disponible sur <https://www.nbb.be/fr> (27 avril 2018).

<sup>99</sup> S. ADALID, « La naissance de la monnaie unique : naissance de consensus » in *La banque centrale européenne et l'Eurosystème*, Bruxelles, Bruylant, 2015, p. 14.

électronique est « une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement telles que définies à l'article 4, point 5), de la directive 2007/64/CE et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique »<sup>100</sup>.

Plusieurs éléments différencient le *Bitcoin* de la monnaie électronique étatique. La raison principale est que la monnaie électronique est émise par des institutions régulières et peut être à tout moment convertie en valeur nominale, en euros par exemple, ce qui n'est pas le cas du *Bitcoin*<sup>101</sup>. En effet, le *Bitcoin* est émis lors du processus de minage pour récompenser le travail des mineurs<sup>102</sup>. Ensuite, ces mineurs peuvent décider de vendre leurs *Bitcoins* à travers des plateformes créées à cet effet. Ainsi, n'importe quelle personne peut se rendre sur l'une de ces plateformes afin d'acheter ou vendre des *Bitcoins*<sup>103</sup>. Il existe également d'autres moyens pour acquérir des *Bitcoins*, comme les distributeurs automatiques permettant d'échanger des espèces contre des *Bitcoins*<sup>104</sup>. Le problème est que le *Bitcoin* est très volatile<sup>105</sup>. Sa valeur peut fortement augmenter ou diminuer du jour au lendemain. Il n'y a donc aucune garantie que le *Bitcoin* sera remboursé au pair, à tout moment et à sa valeur nominale<sup>106</sup>.

Le *Bitcoin* n'a pas non plus de cours légal<sup>107</sup>. Cela signifie que le débiteur « ne peut valablement se libérer d'une dette de somme à l'aide des signes monétaires caractérisés par ce cours »<sup>108</sup>.

Le *Bitcoin* n'étant pas une monnaie légale, cela a pour conséquence qu'il n'est pas soumis aux textes réglementant la monnaie électronique. Cela pose un certain nombre de difficultés. Le problème le plus important est celui de l'absence d'identification. Le *Bitcoin* se base sur l'anonymat des utilisateurs, ce qui ne permet pas d'écarter son utilisation à des fins criminelles comme le blanchiment d'argent ou le financement du terrorisme<sup>109</sup>. À titre d'exemple, nous pouvons citer l'affaire *Silk Road* qui s'est déroulée en 2013 aux États-Unis et dans le cadre de laquelle le *Bitcoin* avait été utilisé par des trafiquants de stupéfiants afin de

---

<sup>100</sup> Directive 2009/110/CE du Parlement européen et du Conseil du 16 septembre 2009 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, modifiant les directives 2005/60/CE et 2006/48/CE et abrogeant la directive 2000/46/CE, *J.O.C.E.*, L 267/7 du 10 octobre 2009.

<sup>101</sup> Question et réponse écrite n° 0762 de C. Gennez du 7 février 2014, Ch., 2014, QRVA 53 152 disponible sur <https://www.lachambre.be/kvvcr/index.cfm?language=fr> (Consulté le 27 avril 2018).

<sup>102</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, *op. cit.*, p. 37.

<sup>103</sup> À titre d'exemple, Paymium.com permet d'acheter et de vendre des *Bitcoins*. L. LELOUP, *Blockchain : La révolution de la confiance*, *op. cit.*, p. 36.

<sup>104</sup> D. GEIBEN, O. JEAN-MARIE, T. VERBIEST, et J-F. VILOTTE, *Bitcoin et Blockchain. Vers un nouveau paradigme de la confiance numérique ?*, *op. cit.*, p. 31.

<sup>105</sup> Rapport de la BCE, « virtual currency schemes - a further analysis », 2015, disponible sur <https://www.ecb.europa.eu>, p. 23.

<sup>106</sup> G. BEGUE, *Confidentialité et prévention de la criminalité financière - Étude de droit comparé*, Bruylant, 2017, p. 698.

<sup>107</sup> A-P. ANDRE-DUMONT, « Les services de paiement à l'épreuve des évolutions technologiques », *op. cit.*, p. 85.

<sup>108</sup> *Ibid.*, p. 85.

<sup>109</sup> D. GEIBEN, O. JEAN-MARIE, T. VERBIEST, et J-F. VILOTTE, *Bitcoin et Blockchain. Vers un nouveau paradigme de la confiance numérique ?*, *op. cit.*, p. 21.

blanchir le produit de leur vente<sup>110</sup>. Ceci a alors amené la Commission européenne à publier une communication recommandant la plus grande vigilance lors de l'utilisation de crypto-monnaies telle que le *Bitcoin*<sup>111</sup>.

Malgré ses faiblesses, le *Bitcoin* fascine et ses utilisations ne cessent de croître ce qui a amené l'intervention du législateur afin d'établir un cadre juridique autour du *Bitcoin*. La Cour de justice de l'Union européenne et la Banque centrale européenne se sont alors penchées sur la question afin de déterminer un embryon de statut du *Bitcoin*.

À l'origine, la Banque centrale européenne considérait le *Bitcoin* comme une monnaie virtuelle<sup>112</sup>. Elle définissait dès lors les monnaies virtuelles comme « un type de monnaie non régulée et digitale, qui est émise et généralement contrôlée par ses développeurs, et qui est utilisée et acceptée par les membres de communautés virtuelles spécifiques »<sup>113</sup>.

En Belgique, les monnaies virtuelles sont définies comme étant « toute forme de monnaie digitale non réglementée qui n'a pas cours légal »<sup>114</sup>. Ce qui rappelle bien l'idée d'une monnaie qui n'est pas légale.

En 2015, la Banque centrale européenne est cependant revenue sur sa définition pour supprimer la notion de monnaie<sup>115</sup>. Elle considère en effet que les monnaies virtuelles ne sont pas des actifs suffisamment liquides et qu'elles n'atteignent pas un niveau d'acceptation suffisant associé à l'argent<sup>116</sup>.

Par conséquent, la Banque centrale européenne définit les monnaies virtuelles comme des « représentations numériques d'une valeur qui ne sont émises ni par une banque centrale ni par une autorité publique, qui ne sont pas nécessairement liées non plus à une monnaie à cours forcé mais qui sont acceptées comme moyen de paiement par des personnes physiques ou morales et qui peuvent être transférées, stockées ou échangées par voie électronique »<sup>117</sup>.

Elle a d'ailleurs confirmé cette définition dans un avis du 12 octobre 2016 sur une proposition de directive modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du

---

<sup>110</sup> G. BEGUE, *Confidentialité et prévention de la criminalité financière - Étude de droit comparé*, *op. cit.*, p. 699.

<sup>111</sup> Communication de la Commission au Parlement européen et au Conseil relative à un plan d'action destiné à renforcer la lutte contre le financement du terrorisme, COM (2016) 50 final, février 2016.

<sup>112</sup> Rapport de la BCE, « virtual currency schemes », 2012, disponible sur <https://www.ecb.europa.eu>, p. 21.

<sup>113</sup> Traduction libre du rapport de la BCE, « virtual currency schemes », 2012, disponible sur <https://www.ecb.europa.eu>, p. 13. ; A-P. ANDRE-DUMONT, « Les services de paiement à l'épreuve des évolutions technologiques », *op. cit.*, p. 85.

<sup>114</sup> Règlement de l'Autorité des services et marchés financiers du 3 avril 2014 concernant l'interdiction de commercialisation de certains produits financiers auprès des clients de détail, *M.B.*, 20 mai 2014, p. 40096, article 1, 6°.

<sup>115</sup> A-P. ANDRE-DUMONT, « Les services de paiement à l'épreuve des évolutions technologiques », *op. cit.*, p. 85.

<sup>116</sup> Rapport de la BCE, « virtual currency schemes - a further analysis », 2015, disponible sur <https://www.ecb.europa.eu>, p. 23.

<sup>117</sup> Rapport de la BCE, « virtual currency schemes - a further analysis », 2015, disponible sur <https://www.ecb.europa.eu>, p. 23.

terrorisme<sup>118</sup>. L'objectif de la proposition de directive est d'amener un renforcement de la législation en vigueur dans l'Union européenne en matière de lutte contre le blanchiment des capitaux<sup>119</sup>.

À présent, la Banque centrale européenne ne parle plus du *Bitcoin* en termes de monnaie virtuelle mais de « devise virtuelle »<sup>120</sup>. Ceci évite la confusion avec la notion de monnaies étatiques.

La Cour de justice de l'Union européenne a même été un peu plus loin en considérant dans un arrêt du 22 octobre 2015 que « la devise virtuelle "Bitcoin" étant un moyen de paiement contractuel elle ne saurait, d'une part, être regardée ni comme un compte courant ni comme un dépôt de fonds, un paiement ou un virement. D'autre part, à la différence des créances, des chèques et des autres effets de commerce (...), elle constitue un moyen de règlement direct entre les opérateurs qui l'acceptent »<sup>121</sup>. Elle considère donc le *Bitcoin* comme un moyen de paiement, mais uniquement dans la mesure où les parties au transfert sont d'accord pour le considérer comme tel<sup>122</sup>.

### 3) *Les Smart contracts*

Les *Smart contracts* ou « contrats intelligents » sont, après le *Bitcoin*, l'application la plus célèbre de la technologie *Blockchain*. Il s'agit de contrats programmables qui s'exécutent automatiquement si certains événements ou certaines conditions se réalisent<sup>123</sup>. Il y a trois étapes lors de leur fonctionnement. Tout d'abord, les termes du contrat seront traduits en code informatique. Ensuite, les parties doivent marquer leur accord sur le code utilisé et enfin le code pourra être exécuté automatiquement et de manière fidèle à la volonté des parties<sup>124</sup>. À nouveau dans ce système, le mot d'ordre est la confiance. En effet, c'est le système informatisé qui garantit la fiabilité des transactions<sup>125</sup>.

---

<sup>118</sup> Avis de la Banque centrale européenne du 12 octobre 2016 sur une proposition de directive du Parlement européen et du Conseil modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme et modifiant la directive 2009/101/CE, *J.O.U.E*, C 459, 9 décembre 2016, point 1.1.3.

<sup>119</sup> Avis de la Banque centrale européenne du 12 octobre 2016 sur une proposition de directive du Parlement européen et du Conseil modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme et modifiant la directive 2009/101/CE, *J.O.U.E*, C 459, 9 décembre 2016.

<sup>120</sup> T. CREMERS, « La blockchain et les titres financiers : retour vers le futur » in *Bulletin Joly Bourse*, 1<sup>er</sup> Juin 2016, n°06, p. 1.

<sup>121</sup> C.J., arrêt *Skatteverket c. David Hedqvist*, 22 octobre 2015, C-264/14, EU:C:2015:718, point 42.

<sup>122</sup> B. SEGENDORF, « What is Bitcoin ? », in *Sveriges Riksbank Economic Review*, 2014, disponible sur <http://www.riksbank.se/>, p. 72.

<sup>123</sup> T. CAMBRAI, *Tout comprendre sur la Blockchain. Une technologie révolutionnaire au cœur du système économique de demain*, *op. cit.*, p. 31.

<sup>124</sup> *Ibid.*, p. 55.

<sup>125</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, *op. cit.*, p. 79.

Les applications des *Smart contracts* peuvent être nombreuses : prêts, locations, transferts de bien<sup>126</sup>. Un couple d'américains s'est même marié en novembre 2015 à l'aide d'un *Smart contract*<sup>127</sup>. Nous pourrions encore imaginer des contrats d'assurance dont les conditions sont préalablement définies et une fois les conditions de remboursement réunies, le contrat s'exécute automatiquement afin de verser l'indemnisation à l'assuré<sup>128</sup>. Nous ne voyons ici que quelques exemples mais ceux-ci sont multipliables à l'infini.

Les *Smart contracts* peuvent dès lors représenter un gain de temps important. Au lieu d'avoir une personne qui va venir vérifier que toutes les conditions pour l'exécution sont réunies, le système informatique s'en chargera pour lui et exécutera directement le contrat ce qui empêche les problèmes courants de non-exécution des contrats<sup>129</sup>. De plus, la confiance qu'ils apportent pourrait éviter de recourir à des garanties souvent très coûteuses comme les sûretés<sup>130</sup>. Mais le plus gros avantage des *Smart contracts* est le fait qu'est enregistrée sur la *Blockchain* la preuve de l'existence d'un document ou d'un contrat dans notre cas, horodaté de manière infalsifiable et irréfutable<sup>131</sup>.

Les *Smart contracts* sont vus comme une réelle possibilité de faciliter le droit des contrats<sup>132</sup>. De ce fait, une *Blockchain* dédiée aux *Smart contracts* a été créée, il s'agit d'Ethereum<sup>133</sup>. Ethereum est une *Blockchain* publique qui permet la création de *Smart contracts* par les utilisateurs<sup>134</sup>. Ils sont vérifiés et validés par les mineurs et sont ensuite ajoutés sur la *Blockchain* afin d'être exécutés et consultables publiquement<sup>135</sup>. La vérification porte sur la véracité des éléments contenus dans le contrat par rapport aux transactions antérieures. Par exemple, pour la vente d'une maison, les mineurs vérifient que le vendeur a bien une maison à vendre et que l'acheteur a bien les fonds nécessaires à cette transaction<sup>136</sup>. L'efficacité de l'opération réside dans le caractère informatisé du processus, qui exécutera automatiquement les conditions dès qu'elles auront été vérifiées par les mineurs<sup>137</sup>. À l'instar du *Bitcoin*, les individus qui valident les transactions sont rémunérés en *ether*, monnaie virtuelle de l'Ethereum<sup>138</sup>.

Même si les *Smart contracts* semblent être une solution très efficace pour l'avenir des contrats, ils posent encore certaines questions. Tout d'abord, le fait que les *Smart contracts* soient immuables, une fois qu'ils sont encodés, nous ne pouvons plus revenir en arrière pour

---

<sup>126</sup> D. GEIBEN, O. JEAN-MARIE, T. VERBIEST, et J-F. VILOTTE, *Bitcoin et Blockchain. Vers un nouveau paradigme de la confiance numérique ?*, op. cit., p. 92.

<sup>127</sup> *Ibid.*, p. 52.

<sup>128</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p. 80.

<sup>129</sup> C. HOUSSA et L. STANDAERT, *La « Nouvelle frontière » de la finance*, op. cit., p. 190.

<sup>130</sup> *Ibid.*, p. 190.

<sup>131</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p. 173.

<sup>132</sup> C. BARREAU, « La régulation des smart contracts et les smart contracts des régulateurs » in *réalités industrielles*, août 2017, p. 75.

<sup>133</sup> D. GEIBEN, O. JEAN-MARIE, T. VERBIEST, et J-F VILOTTE, *Bitcoin et Blockchain. Vers un nouveau paradigme de la confiance numérique ?*, op. cit., p. 92.

<sup>134</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p. 76.

<sup>135</sup> *Ibid.*, p. 76.

<sup>136</sup> *Ibid.*, p. 17.

<sup>137</sup> *Ibid.*, p. 79.

<sup>138</sup> D. GEIBEN, O. JEAN-MARIE, T. VERBIEST, et J-F. VILOTTE, *Bitcoin et Blockchain. Vers un nouveau paradigme de la confiance numérique ?*, op. cit., p. 93.

les modifier ou les supprimer<sup>139</sup>. Ceci pose des problèmes principalement dans le cadre du droit des contrats dans lequel la possibilité de pouvoir revenir sur ses engagements par exemple est primordiale.

Ensuite, l'exécution en pratique de ces « contrats » sera très difficile<sup>140</sup>. En effet, que fera un juge face à un litige découlant d'un tel accord ? Comment pourrait-il le lire ? Comment pourrait-il identifier toutes les parties en cause ? Comment les parties pourraient-elles modifier ou revenir sur leur accord ? Ainsi, si nous reprenons l'exemple du contrat de mariage, nous pouvons nous interroger sur la légalité d'un tel acte<sup>141</sup>.

Les *Smart contracts* seraient-ils donc véritablement des contrats au sens juridique du terme ou ne s'agirait-il pas seulement d'une modalité d'exécution de ceux-ci ? C'est à cette question que nous tenterons de répondre en premier lieu à travers la partie juridique de notre exposé.

## II.- CADRE JURIDIQUE APPLICABLE

Le but de ce chapitre est d'analyser quel cadre juridique nous pourrions appliquer à la *Blockchain* et plus précisément à ses applications. Tout d'abord, nous verrons dans quelle mesure le droit commun des contrats s'applique aux accords conclus sur la *Blockchain* et plus précisément aux *Smart Contracts*. Ensuite, nous analyserons le régime juridique de la signature électronique afin de voir si une inscription sur la *Blockchain* peut servir de preuve à un accord, un *Smart Contract* ou une transaction.

### A.- LE DROIT COMMUN DES CONTRATS

À travers cette section nous analyserons les *Smart contracts* à travers le droit commun des contrats afin de déterminer si les accords conclus sur la *Blockchain*, et plus précisément ce qu'on appelle des *Smart contracts*, sont de vrais contrats au sens juridique du terme et donc si ce cadre juridique est applicable à la *Blockchain*.

---

<sup>139</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p. 81.

<sup>140</sup> D. GEIBEN, O. JEAN-MARIE, T. VERBIEST, et J-F. VILOTTE, *Bitcoin et Blockchain. Vers un nouveau paradigme de la confiance numérique ?*, op. cit., p. 94.

<sup>141</sup> *Ibid.*, p. 52.

## 1) Définition

Nous ne pouvons pas analyser ce qu'est un contrat sans revoir les bases du droit commun des contrats. Dans ce cadre, un contrat se définit comme « un accord de volontés entre deux ou plusieurs personnes en vue de créer, d'éteindre, de transmettre ou de modifier des obligations juridiques »<sup>142</sup>. Lorsque nous parlons d'obligations juridiques, nous visons des engagements qui, lorsqu'ils ne sont pas respectés, pourront être sanctionnés si besoin par le recours à un juge<sup>143</sup>. Les *Smart contracts* ne rentrent pas dans cette définition, puisqu'il n'y a pas de sanctions prévues en cas de problème dans l'exécution du contrat. En effet, ce problème ne vient pas d'un comportement humain mais d'un système informatisé, ce qui rend le recours au droit des contrats très difficile.

Certes, les mineurs vérifient diverses informations avant de valider une transaction, ils vérifient le solde restant d'un individu par exemple, mais *quid* des éléments qu'ils n'avaient pas pris en compte lors de l'encodage ? Ces éléments ne seront alors pas du tout pris en compte lors de l'exécution du *Smart contract*. Il faudrait absolument tout prévoir à l'avance dans le codage, ce qui est extrêmement compliqué également.

## 2) Formation des contrats conclus par voie électronique

Les *Smart contracts* peuvent rentrer dans ce que nous appelons « le droit des contrats conclus par voie électronique »<sup>144</sup>. La conclusion de contrats par voie électronique n'est qu'un mode de formation des contrats, ce qui ne change pas leur qualification<sup>145</sup>. Ainsi, ces contrats restent soumis aux règles du Code civil et du droit commun des contrats<sup>146</sup>. Nous pouvons alors imaginer conclure un contrat pour s'abonner à un magazine sur internet, commander des vêtements en ligne, ou encore conclure un contrat de travail par voie électronique. Les contrats pouvant être conclus par voie électronique sont donc multiples.

Il existait autrefois des lois particulières sur les contrats conclus par voie électronique venant compléter le droit commun des contrats mais elles ont récemment été abrogées et leurs règles ont été insérées dans le Code de droit économique belge. Il s'agissait tout d'abord, de la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information, remplacée par la loi du 15 décembre 2013 portant insertion du Livre XII, « Droit de l'économie électronique » dans le Code de droit économique, portant insertion des définitions propres au Livre XII et des dispositions d'application de la loi propres au Livre XII, dans les Livres I et XV du Code de droit économique. Ensuite, il y avait la loi du 6 avril 2010 relative aux pratiques du marché et à la protection du consommateur, remplacée par la loi du 21 décembre 2013

---

<sup>142</sup> M. DUPONT, *Le b.a.-ba du contrat*, Liège, Edipro, 2013, p. 15.

<sup>143</sup> *Ibid.*, p. 15.

<sup>144</sup> C. ALTER, R. THUNGEN, P. VAN OMMESLAGHE, *Incidence des nouvelles technologies de la communication sur le droit commun des obligations*, Bruxelles, Bruylant, 2012, p. 43.

<sup>145</sup> F. DECHAMPS, L. VANCAELEMONT, « Les obligations contractuelles et Internet », in *Les obligations contractuelles en pratique : Questions choisies*, Limal, Anthemis, 2013, p. 75.

<sup>146</sup> *Ibid.*, p. 75.

portant insertion du titre VI « Pratiques du marché et protection du consommateur » dans le Code de droit économique et portant insertion des définitions propres au livre VI, et des dispositions d'application de la loi propres au livre VI, dans les Livres Ier et XV du Code de droit économique.

### 3) *Grands principes du droit des contrats*

Les contrats conclus par voie électronique, étant soumis aux règles du Code civil et au droit des contrats, doivent respecter les grands principes du droit des contrats<sup>147</sup>.

#### a) **Autonomie de la volonté**

Les parties qui concluent un contrat sont soumises au principe de l'autonomie de la volonté. Cela signifie qu'elles peuvent contracter avec qui elles veulent et contracter ce qu'elles veulent<sup>148</sup>. Ce principe n'est soumis qu'à de rares exceptions, à savoir le respect des règles d'ordre public et de bonnes mœurs ainsi que le respect des règles impératives<sup>149</sup>.

Ce principe se retrouve dans l'idée des *Smart contracts*. Le principe est que les *Smart contracts* peuvent avoir des objets multiples et tout le monde peut accéder à la plateforme pour en conclure un et ce, avec qui il veut<sup>150</sup>.

#### b) **Le consensualisme**

Le consensualisme vise la façon dont le contrat est conclu<sup>151</sup>. Ce principe veut qu'un contrat est valablement conclu par simple échange des consentements<sup>152</sup>. La loi impose cependant des exceptions. Dans certains cas, elle impose le respect de certaines formalités. Ainsi, les contrats solennels doivent être conclus selon un certain formalisme<sup>153</sup>. Par exemple, le contrat d'hypothèque doit obligatoirement être conclu par acte notarié. Les contrats réels aussi ne peuvent être valablement conclus sans la remise effective de la chose sur laquelle porte le contrat<sup>154</sup>.

Nous voyons bien la difficulté que représente cette condition pour l'application des *Smart contracts*. Ceux-ci ne posent dès lors pas de problème pour des contrats assez simples,

---

<sup>147</sup> C. ALTER, R. THUNGEN, P. VAN OMMESLAGHE, *Incidence des nouvelles technologies de la communication sur le droit commun des obligations*, op. cit., p. 42.

<sup>148</sup> M. DUPONT, *Le b.a.-ba du contrat*, op. cit., p. 21.

<sup>149</sup> *Ibid.*, p. 21.

<sup>150</sup> LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p. 76.

<sup>151</sup> M. DUPONT, *Le b.a.-ba du contrat*, op. cit., p. 22.

<sup>152</sup> *Ibid.*, p. 23.

<sup>153</sup> *Ibid.*, p. 23.

<sup>154</sup> *Ibid.*, p. 23.



mais dès qu'il s'agit d'un enjeu un peu plus important, il est nécessaire de respecter certaines formalités comme la signature d'un acte notarié, ce qui rend difficile l'application d'un *Smart contract*. La conséquence est pourtant fatale, si une telle formalité n'est pas respectée le contrat ne sera pas valablement conclu et les parties ne seront dès lors pas engagées juridiquement. De plus, le rôle du mineur n'a pas, comme nous pourrions l'imaginer, pour rôle de vérifier des conditions de validité du contrat. Il ne fait que vérifier si la transaction est possible d'un point de vue technique, c'est-à-dire, si les fonds sont suffisants pour exécuter la transaction par exemple<sup>155</sup>.

Cependant, même dans les cas où le contrat est valablement conclu par le simple échange des consentements, il reste le problème de l'opposabilité aux tiers. À titre d'exemple, la vente d'une maison peut se conclure à la suite d'un simple accord de volontés de la part des parties. Il s'agit donc d'un contrat consensuel. Pourtant, la loi impose l'intervention d'un notaire afin que la vente soit opposable aux tiers. À partir du moment où un accord est conclu à l'aide d'un *Smart contract*, le recours à un acte notarié est impossible et donc le contrat ne sera pas opposable aux tiers, ce qui peut avoir des conséquences très désagréables en pratique. Par exemple, si nous voulons faire un emprunt hypothécaire à la banque, il faudra amener la preuve que l'achat porte bien sur cet immeuble<sup>156</sup>.

Autrement dit, les *Smart contracts* ne font qu'enregistrer une transaction sur la *Blockchain* sans constituer la transaction en elle-même<sup>157</sup>. Cet enregistrement vaudra au mieux comme preuve de la propriété mais ne sera pas opposable aux tiers sans intervention du législateur pour le permettre<sup>158</sup>.

### c) Le principe de convention-loi

Le premier alinéa de l'article 1134 du Code civil dispose que : « les conventions légalement formées tiennent lieu de loi à ceux qui les ont faites ». Cela signifie que les engagements pris par les parties ont la même force que les obligations qui découlent de la loi. Si un engagement n'est pas respecté, les parties pourront aller devant les cours et tribunaux afin d'en faire exécuter les obligations<sup>159</sup>. À nouveau, une telle possibilité n'est pas prévue par les *Smart contracts*. Les utilisateurs n'ont aucune entité juridique vers laquelle se tourner en cas de problème, puisqu'il s'agit d'un système qui se veut totalement décentralisé<sup>160</sup>.

Ce principe est également assorti de certaines exceptions. Tout d'abord, le juge peut réviser un contrat lorsque l'équilibre de celui-ci a été rompu. Cela peut se traduire par exemple par un délai supplémentaire ou par une diminution du montant des dommages et intérêts prévus dans le contrat. Un tel aménagement n'est pas possible avec un *Smart contract* à cause de son

---

<sup>155</sup> LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p. 17.

<sup>156</sup> *Ibid.*, p. 23.

<sup>157</sup> *Ibid.*, p. 173.

<sup>158</sup> *Ibid.*, p. 173.

<sup>159</sup> M. DUPONT, *Le b.a.-ba du contrat*, op. cit., p. 24.

<sup>160</sup> D. GEIBEN, O. JEAN-MARIE, T. VERBIEST, et J-F. VILOTTE, *Bitcoin et Blockchain. Vers un nouveau paradigme de la confiance numérique ?*, op. cit., p. 94.

caractère immuable. Une fois les conditions du contrat déterminées et codées en langage informatique, nous ne pouvons plus revenir en arrière ni modifier cet accord<sup>161</sup>. Une possibilité est de prévoir toutes les hypothèses qui pourraient se produire dès la création du *Smart contract*, ce qui est extrêmement compliqué puisque certaines situations ne peuvent être prévues comme les cas de force majeure<sup>162</sup>.

Une autre possibilité serait alors d'envisager un mécanisme tel que celui de la contre-passation. La contre-passation est une méthode qui permet aux banquiers ou aux comptables, lorsqu'il y a eu une erreur dans l'inscription d'une opération, de procéder à une nouvelle inscription du même montant, en sens inverse, afin d'annuler l'opération erronée<sup>163</sup>.

Ensuite, les tribunaux ont développé une jurisprudence en ce qui concerne l'abus de droit<sup>164</sup>. Si un contrat est exécuté d'une façon qui nuit à autrui, les tribunaux doivent refuser de l'appliquer. À nouveau, cette exception ne peut pas être respectée dans un *Smart contract* puisqu'une fois les conditions de départ respectées, il s'exécute automatiquement, et un système informatique ne saurait avoir égard à un quelconque abus.

Nous voyons donc, dès à présent, que le recours à un juge est indispensable. Le juge doit pouvoir opérer un contrôle, lui permettant d'ordonner le cas échéant, une contre-passation ou une écriture en sens contraire.

#### **4) *La formation du contrat à proprement parler***

Les contrats conclus par voie électronique doivent également respecter les conditions de formation et de validité du droit commun des contrats<sup>165</sup>.

##### **a) Les conditions de validité du contrat**

Afin qu'un contrat soit valablement formé, il convient de vérifier que l'accord de volonté respecte certaines conditions. Ces conditions sont principalement motivées par deux raisons. D'abord, il faut être sûr qu'il y ait eu un consentement et ensuite, il faut que le contrat ne viole pas les règles impératives existantes<sup>166</sup>. Elles sont reprises à l'article 1108 du Code civil rédigé comme suit :

---

<sup>161</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p. 81.

<sup>162</sup> C. HOUSSA et L. STANDAERT, *La « Nouvelle frontière » de la finance*, op. cit., p. 192.

<sup>163</sup> C. ALTER, « Droit bancaire général - Réglementation - Devoirs du banquier - Comptes - Services de paiement », Rép. not., Tome IX, Contrats divers, Livre 11/1, Bruxelles, Larcier, 2010, n° 246.

<sup>164</sup> M. DUPONT, *Le b.a.-ba du contrat*, op. cit., p. 25.

<sup>165</sup> C. ALTER, R. THUNGEN, P. VAN OMMESLAGHE, *Incidence des nouvelles technologies de la communication sur le droit commun des obligations*, op. cit., p. 42.

<sup>166</sup> M. DUPONT, *Le b.a.-ba du contrat*, op. cit., p. 44.

« Quatre conditions sont essentielles pour la validité d'une convention :

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 »<sup>167</sup>.

Tout d'abord, il faut un consentement réciproque sur les éléments essentiels du contrat. Si une seule partie consent, le contrat n'est pas valablement formé<sup>168</sup>. Le consentement doit être réel, c'est-à-dire donné de façon consciente. Et enfin, le consentement ne doit pas être vicié. Cela signifie que le consentement doit avoir été donné librement et en pleine connaissance de cause, ce qui exclut donc l'erreur, le dol, la violence et la lésion<sup>169</sup>.

Ce consentement libre et éclairé doit avoir été donné par une personne ayant la capacité de s'engager<sup>170</sup>. Sauf exceptions, dans lesquelles nous ne rentrerons pas, les personnes qui ne sont pas capables juridiquement de conclure un contrat sont les mineurs, les interdits judiciaires, les faibles d'esprits et les prodiges<sup>171</sup>.

Ensuite, le contrat doit porter sur un objet déterminé ou déterminable, réalisable ou possible et surtout licite<sup>172</sup>. Ce dernier élément signifie que l'objet doit respecter les règles relatives à l'ordre public, aux bonnes mœurs et aux règles impératives<sup>173</sup>.

Enfin, il faut une cause licite<sup>174</sup>. L'intention des parties doit être conforme à l'ordre public et aux bonnes mœurs<sup>175</sup>.

La vérification de ces conditions pose de réels problèmes lorsqu'il s'agit de les appliquer au domaine des *Smart contracts*. La première raison est évidente, aucun recours devant un juge n'est prévu en cas de litige survenu à propos d'un *Smart contract*<sup>176</sup>. De plus, même en recourant à un juge, il reste toujours la barrière de la technologie. Les *Smart contracts* sont codés en langage informatique, ce qui est incompréhensible pour les tribunaux<sup>177</sup>. Il faudrait dès lors établir un système dans lequel le juge serait accompagné d'experts et dans lequel il pourrait forcer les parties à donner leurs clés. Cependant, dans la mesure où la *Blockchain* est anonyme, le juge ne pourrait pas être sûr que la clé qu'il a entre les mains correspond bien à la personne qui la lui présente. Il est impossible dans l'état actuel des choses de pouvoir vérifier avec certitude les conditions de consentement et de capacité dans le chef des parties<sup>178</sup>.

---

<sup>167</sup> C. civ., art. 1108.

<sup>168</sup> M. DUPONT, *Le b.a.-ba du contrat, op. cit.*, p. 44.

<sup>169</sup> C. civ., art. 1110 à 1116, 1674 et 1305.

<sup>170</sup> C. civ., art. 1108.

<sup>171</sup> M. DUPONT, *Le b.a.-ba du contrat, op. cit.*, p. 49.

<sup>172</sup> *Ibid.*, p. 50.

<sup>173</sup> *Ibid.*, p. 51.

<sup>174</sup> M. DUPONT, *Le b.a.-ba du contrat, op. cit.*, p. 52.

<sup>175</sup> C. civ., art. 1131.

<sup>176</sup> D. GEIBEN, O. JEAN-MARIE, T. VERBIEST et J-F. VILOTTE, *Bitcoin et Blockchain. Vers un nouveau paradigme de la confiance numérique ?*, *op. cit.*, p. 94.

<sup>177</sup> *Ibid.*, p. 94.

<sup>178</sup> I. PAVEL, « La blockchain - Les défis de son implémentation », *op. cit.*, p. 23.

## **b) Absence de sanction adéquate**

Même si nous rendions le recours devant un juge possible, nous aurions encore un problème au niveau des sanctions applicables à un *Smart contract* non valablement formé. En effet, le Code civil sanctionne le non-respect des conditions de validité par la nullité du contrat<sup>179</sup>. Il sera annulé et considéré comme n'ayant jamais existé<sup>180</sup>. Cependant, cette sanction prévue par le Code civil ne peut être appliquée au *Smart contract* dans la mesure où une des principales caractéristiques de la *Blockchain* est son caractère irréversible. Cela signifie qu'une fois que le *Smart contract* est enclenché, il sera très difficile de revenir sur l'accord passé<sup>181</sup>. À moins, d'établir un système semblable à celui de la contre-passation.

## **5) Problèmes transfrontaliers**

Le fait que la *Blockchain* soit décentralisée engendre comme conséquence que, même si un régime juridique clair venait un jour à encadrer cette technologie, cela n'empêchera pas les utilisateurs d'opérer à partir de pays où la réglementation leur paraîtra plus favorable. Donc, outre un régime juridique national, il convient également de trouver un régime ou un consensus international qui lui serait applicable<sup>182</sup>.

## **6) Application du droit international privé**

Un premier élément favorable à la dimension internationale de la *Blockchain* est le recours au droit international privé. En effet, les contrats ne se limitant pas aux frontières nationales, le législateur a prévu que, lorsque nous sommes face à un litige à ce sujet, nous devons généralement recourir au droit international privé. Nous devons dès lors différencier deux choses. Premièrement, nous devons déterminer quelle juridiction est compétente pour trancher le litige. Deuxièmement, nous devons déterminer à l'aide de quel droit cette juridiction devra trancher le litige.

---

<sup>179</sup> M. DUPONT, *Le b.a.-ba du contrat*, op. cit., p. 44.

<sup>180</sup> *Ibid.*, p. 53.

<sup>181</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p.175.

<sup>182</sup> D. GEIBEN, O. JEAN-MARIE, T. VERBIEST, et J-F. VILOTTE, *Bitcoin et Blockchain. Vers un nouveau paradigme de la confiance numérique ?* », op. cit., p. 70.

## a) Jurisdiction compétente

En ce qui concerne la juridiction compétente, nous devons distinguer deux situations. Tout d'abord, la situation dans laquelle le contrat a été conclu entre professionnels et, ensuite, la situation dans laquelle le contrat est conclu entre un professionnel et un consommateur<sup>183</sup>.

Dans le cas d'un contrat conclu entre des professionnels, si le défendeur est domicilié dans un État membre de l'Union européenne, alors, sauf exception, la juridiction compétente sera celle du domicile du défendeur<sup>184</sup>. Les exceptions concernent, tout d'abord, la possibilité de poursuivre le défendeur dans un autre État membre lorsqu'il y a une clause attributive de juridiction dans le contrat<sup>185</sup>. Ensuite, lorsque le « lieu d'exécution de l'obligation qui sert de base à la demande se situe dans un autre État membre », alors le défendeur sera poursuivi devant cet État membre<sup>186</sup>.

Si le défendeur n'a pas son domicile dans un État membre alors il faudra se référer aux règles déterminées par le droit de son lieu de domicile<sup>187</sup>. En Belgique, les juridictions sont compétentes si l'obligation est née ou exécutée en Belgique<sup>188</sup>.

Enfin, si le contrat est conclu avec un consommateur, le consommateur pourra choisir d'aller devant le tribunal du lieu du domicile du défendeur ou du lieu où il est lui-même domicilié<sup>189</sup>.

## b) Loi applicable

Pour ce qui est de la loi applicable, le Code de droit international privé belge renvoie au règlement (CE) 593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles appelé plus communément règlement « Rome I »<sup>190</sup>.

La première règle est la liberté de choix des parties<sup>191</sup>. Ce n'est que si les parties n'ont pas choisi de loi applicable qu'on se référera au règlement<sup>192</sup>. À titre d'exemple, l'article 4, § 1, du règlement précise qu'à défaut de choix des parties « le contrat de vente de biens est régi par la loi du pays dans lequel le vendeur a sa résidence habituelle ». Lorsque la situation du contrat n'est pas couverte par une des hypothèses reprises à l'article 4, § 1, le contrat sera régi

---

<sup>183</sup> F. DECHAMPS et L. VANCAELEMONT, « Les obligations contractuelles et Internet », *op. cit.*, p. 87.

<sup>184</sup> Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.U.E.*, L 119, 4 mai 2016, art. 4, § 1.

<sup>185</sup> Règlement (UE) 2016/679, art. 25.

<sup>186</sup> Règlement (UE) 2016/679, art. 7.

<sup>187</sup> Règlement (UE) 2016/679, art. 6, § 1.

<sup>188</sup> Code D.I.P., art. 96.

<sup>189</sup> Règlement (UE) 2016/679, art. 18, § 1.

<sup>190</sup> Code D.I.P., art. 96.

<sup>191</sup> Règlement (CE) 593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles (Rome I), *J.O.U.E.*, L 177, 4 juillet 2008, art. 3.

<sup>192</sup> F. DECHAMPS, L. VANCAELEMONT, « Les obligations contractuelles et Internet », *op. cit.*, p. 89.

« par la loi du pays dans lequel la partie qui doit fournir la prestation caractéristique du contrat a sa résidence habituelle »<sup>193</sup>. Il s'agit de l'article 4, § 2, du règlement. Enfin, lorsqu'il « résulte de l'ensemble des circonstances de la cause que le contrat présente des liens manifestement plus étroits avec un pays autre que celui visé au paragraphe 1 ou 2 » ou « lorsque la loi applicable ne peut être déterminée sur la base du paragraphe 1 ou 2 », alors « le contrat sera régi par la loi du pays avec lequel il a les liens les plus étroits »<sup>194</sup>.

Le législateur a à nouveau voulu protéger le consommateur, ce qui fait que, dans les contrats conclus avec des consommateurs, le libre choix des parties reste applicable mais « ce choix ne peut cependant avoir pour résultat de priver le consommateur de la protection que lui assurent les dispositions auxquelles il ne peut être dérogé par accord en vertu de la loi qui aurait été applicable, en l'absence de choix, sur la base du paragraphe 1 »<sup>195</sup>. Le paragraphe 1 de cet article vise l'application de « la loi du pays où le consommateur a sa résidence habituelle »<sup>196</sup>.

Cependant, nous nous retrouvons à nouveau face au problème de l'anonymat de la *Blockchain*. Nous voyons bien l'importance de pouvoir identifier les parties d'un accord pour pouvoir aller devant un juge afin de résoudre un litige, ce qui est très difficile en pratique avec la *Blockchain*. Il incombera alors au demandeur de prouver qu'il y a bien un contrat mais également d'en déterminer quelles sont les parties<sup>197</sup>.

## **7) Conclusion : faiblesses des Smart contracts face au droit des contrats**

Les *Smart contracts* posent en définitive deux problèmes essentiels. Tout d'abord, ils sont irréversibles. Dans un contrat ordinaire, si une partie a contracté sans en avoir la capacité juridique, les parties pourront aller devant un tribunal afin de faire annuler rétroactivement ce contrat. Cela signifie que, à partir de l'annulation, le contrat sera considéré comme n'ayant jamais existé<sup>198</sup>. Le caractère irréversible des *Smart contracts*, et plus précisément de la *Blockchain*, rend cette annulation très difficile pour un *Smart contract* puisque l'opération ne pourra pas être effacée. Il faudra dès lors passer par d'autre mécanisme comme celui de la contre-passation afin de rectifier l'opération.

Ce caractère irréversible pose encore d'autres problèmes. En effet, divers mécanismes ont été pris pour lutter contre les difficultés de mise en œuvre que peut représenter la conclusion de contrat par voie électronique. À titre d'exemple, nous pouvons citer l'article VI.47 du Code de droit économique rédigé de la manière suivante : « sans préjudice de l'article VI.53, le consommateur dispose d'un délai de 14 jours pour se rétracter d'un contrat à distance, sans avoir à motiver sa décision et sans encourir d'autres coûts que ceux prévus à l'article VI.50, § 2, et à

---

<sup>193</sup> F. DECHAMPS, L. VANCAELEMONT, « Les obligations contractuelles et Internet », *op. cit.*, p. 89.

<sup>194</sup> Règlement (CE) 593/2008, art. 4, §§ 3 et 4.

<sup>195</sup> Règlement (CE) 593/2008, art. 6, § 2.

<sup>196</sup> Règlement (CE) 593/2008, art. 6, § 1.

<sup>197</sup> C. civ., art. 1315 ; C. jud. 870.

<sup>198</sup> M. DUPONT, *Le b.a.-ba du contrat*, *op. cit.*, p. 53.

l'article VI.51 ». Cet article prévoit donc la possibilité pour un consommateur prenant part à un contrat conclu à distance de rompre son engagement dans un délai de quatorze jours, ce qui est logiquement impossible dans le cadre d'un *Smart contract* puisque l'opération a déjà été exécuté automatiquement<sup>199</sup>. Ainsi, nous pourrions imaginer un système de versement d'indemnités compensatoires afin de réparer le préjudice subi par l'exécution d'une opération annulée par la suite<sup>200</sup>.

Ensuite, le principe des *Smart contracts* est que leur exécution est infaillible puisqu'ils exécutent précisément les termes encodés. Cependant, les rédacteurs de ces codes ne sont pas des machines mais des êtres humains, qui, eux, n'ont rien d'infaillible. Les *Smart contracts* ne sont donc pas à l'abri d'une erreur dans l'encodage, ce qui entraîne une situation très embêtante puisque les parties seront face à un contrat exécuté qui ne correspond pas à leur volonté mais qu'ils ne peuvent pas modifier.

De plus, les personnes qui encodent les termes du contrat sont des informaticiens qui ne peuvent pas connaître toutes les subtilités du droit. Un juriste est donc nécessaire dans la phase d'encodage afin d'assister les développeurs. Nous voyons ici que l'aspect humain, nonobstant une fiabilité extrême de la *Blockchain*, reste indispensable.

Nous pourrions très bien imaginer la « correction » de ce genre d'erreur en créant un nouveau *Smart contract* qui, en quelque sorte, dirait l'inverse du précédent de façon à en annuler les effets. Cependant, nous ne pouvons pas faire cela sans l'accord des propriétaires des adresses concernées et il est fort probable que la personne ayant reçu l'argent par exemple ne soit pas disposée à procéder au remboursement sans un système l'y contraignant<sup>201</sup>. Le passage devant un juge serait dès lors indispensable afin d'obtenir l'exécution forcée de l'obligation de remboursement<sup>202</sup>. Nous verrons que le notaire joue un rôle également important dans ce domaine puisque ses actes sont revêtus de la force exécutoire<sup>203</sup>.

Les *Smart contracts* ne sont donc pas de vrais contrats<sup>204</sup>. Ils le seraient s'ils remplissaient les conditions de formation, à savoir : une offre suivie d'une acceptation, tout en respectant l'ensemble des conditions de validité des contrats. Nous avons bien vu que ce n'est pas le cas. Certains auteurs définissent alors le *Smart contract* comme une « modalité technique d'exécution » d'un contrat puisque la *Blockchain* ne fera qu'exécuter automatiquement un accord inscrit sur elle et validé par les mineurs<sup>205</sup>. Mais rien n'empêche de créer des contrats qui seraient à la fois des *Smart contracts* et des contrats traditionnels. Nous pourrions ainsi imaginer, un contrat rédigé par un juriste et soumis à la *Blockchain* afin d'en assurer l'exécution, l'opposabilité et la preuve. En effet, les *Smart contracts* représentent, outre un bon moyen d'assurer l'exécution des contrats, un moyen d'enregistrer ces contrats afin d'en assurer la conservation, ce qui permettrait également de répondre à certaines exigences de publicité

---

<sup>199</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p.175.

<sup>200</sup> C. BARREAU, « La régulation des smart contracts et les smart contracts des régulateurs », op. cit., p. 76.

<sup>201</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p.174.

<sup>202</sup> M. DUPONT, *Le b.a.-ba du contrat*, op. cit., p. 109.

<sup>203</sup> Loi du 25 ventôse an XI contenant organisation du notariat du 16 mars 1803, *M.B.*, 16 mars 1803, p. 0, art. 19.

<sup>204</sup> D. GEIBEN, O. JEAN-MARIE, T. VERBIEST et J-F. VILOTTE, *Bitcoin et Blockchain. Vers un nouveau paradigme de la confiance numérique ?*, op. cit., p. 94.

<sup>205</sup> *Ibid.*, p. 94.

déterminé par le législateur afin de rendre les contrats opposables aux tiers<sup>206</sup>. Enfin, les *Smart contracts* pourraient constituer un bon moyen de preuve, comme nous le verrons dans un instant.

Ainsi, il est indispensable, si nous voulons pouvoir travailler à l'aide de *Smart contracts*, de prévoir la réversibilité des accords, que les juristes et les développeurs puissent travailler ensemble, et de prévoir un recours devant le juge en cas de problème<sup>207</sup>.

## **B.- LE DROIT DE LA PREUVE**

Nous avons vu les conditions pour conclure valablement un contrat. Dans la mesure où les contrats sont consensuels, nous pouvons très bien imaginer des contrats assez simples conclus à travers le processus de la *Blockchain*. Cependant, une question demeure : dans quelle mesure un accord conclu sur la *Blockchain* pourrait-il servir de preuve à un engagement ?

A travers ce chapitre nous nous demanderons dès lors si le régime de la preuve de la signature électronique pourrait être applicable à la technologie *Blockchain*.

### ***1) Introduction***

En Belgique, le droit de la preuve fait une différence selon que nous nous trouvons en matière commerciale ou civile. En matière commerciale, à moins que la loi ne prévienne autre chose, les actes peuvent être prouvés par toute voie de droit<sup>208</sup>. En matière civile, il faut distinguer selon le montant de l'accord. Si l'accord porte sur une somme supérieure à 375 euros, la loi exige une preuve écrite et signée de cet accord<sup>209</sup>. En revanche, s'il s'agit d'un accord portant sur une somme d'un montant inférieur à 375 euros, la preuve est libre<sup>210</sup>.

Lorsque nous sommes face à une contestation quant à l'existence d'un contrat, le meilleur moyen de la prouver est donc d'avoir un écrit signé. Cependant, ce moyen de preuve est difficile à transposer à un contrat conclu par voie électronique. C'est pour cette raison que le législateur européen s'est emparé de la question et a instauré le régime de signature électronique. L'objectif principal de la signature électronique est de « garantir l'intégrité de l'acte » comme le fait un support écrit traditionnel sur lequel est apposée une signature manuscrite<sup>211</sup>. Mais elle a également pour but de faciliter la tâche du juge quant à l'appréciation de la valeur probante d'une preuve électronique présentée devant lui comme nous le verrons.

---

<sup>206</sup> P. WERY, « La théorie générale du contrat » in *Droit des obligations*, Bruxelles, Larcier, 2010, n° 923 et 924.

<sup>207</sup> F. STROUCKEN, M. OOSTERMEYER, "Gaat blockchain de juridische (notariële) wereld veranderen" in *Vastgoed Fiscaal & Civiël*, 22 juin 2017, p. 3.

<sup>208</sup> F. MOURLON BEERNAERT, « La preuve en matière civile et commerciale », *op. cit.*, p. 86.

<sup>209</sup> C. civ., art. 1341.

<sup>210</sup> F. MOURLON BEERNAERT, « La preuve en matière civile et commerciale », *op. cit.*, p. 81.

<sup>211</sup> F. DECHAMPS, L. VANCAELEMONT, « Les obligations contractuelles et Internet », *op. cit.*, p. 84.



La signature électronique a plus précisément trois fonctions essentielles. Tout d'abord, elle tient à l'identification de l'auteur de la signature. Ensuite, elle permet d'établir l'adhésion à l'acte de la part du signataire. Enfin, elle permet d'identifier le support sur lequel se trouve la signature afin de l'assimiler à un exemplaire original de l'acte<sup>212</sup>.

## 2) *Contexte*

Le cadre européen sur la signature électronique avait été amorcé avec la directive 1999/93/CE du Parlement et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques<sup>213</sup>. Cette directive fut cependant un échec. Tout d'abord parce qu'elle visait des applications qui n'étaient pas encore suffisamment définies<sup>214</sup>. Ensuite, parce qu'elle laissait aux États membres le soin de transposer le texte selon leur niveau de maturité face aux nouvelles technologies, ce qui empêchait un cadre communautaire uniforme<sup>215</sup>.

Cette directive a quand même eu une portée positive. Elle posa un principe fondamental, le principe de non-discrimination d'un écrit électronique par rapport à un écrit papier<sup>216</sup>. Ce qui signifie que l'écrit électronique a la même valeur que l'écrit papier et donc qu'une signature ne peut pas être refusée en justice pour le seul motif qu'elle se trouve sous forme électronique<sup>217</sup>.

## 3) *Règlement eIDAS*

Face à cet échec, le législateur européen a alors laissé du temps pour que les États acquièrent une certaine maturité quant aux échanges par voie électronique avant de légiférer à nouveau. Il aura attendu le 23 juillet 2014 pour adopter le règlement eIDAS relatif à l'identification électronique et aux services de confiance<sup>218</sup>. Ce règlement vient remplacer la directive 1999/93/CE.

---

<sup>212</sup> C. ALTER, R. THUNGEN, P. VAN OMMESLAGHE, *Incidence des nouvelles technologies de la communication sur le droit commun des obligations*, *op. cit.*, p. 31.

<sup>213</sup> Directive (UE) 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électronique, *J.O.C.E*, L 13, 19 janvier 2000.

<sup>214</sup> C.-E. ARMINGAUD, « La blockchain et l'espace de confiance électronique européen » in *Revue pratique de la prospective et de l'innovation*, n°1, janvier 2017, p. 1.

<sup>215</sup> *Ibid.*, p. 1.

<sup>216</sup> *Ibid.*, p. 1.

<sup>217</sup> H. JACQUEMIN, *L'identification électronique et les services de confiance depuis le règlement eIDAS*, *op. cit.* p. 158.

<sup>218</sup> Règlement (UE) 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, *J.O.U.E*, L 257, 28 août 2014.

## a) Apports du règlement

L'objectif principal du règlement eIDAS est de « mettre en place un cadre juridique en vue de susciter la confiance accrue dans les transactions électroniques au sein du marché intérieur »<sup>219</sup>.

Cet objectif traduit les trois apports principaux du règlement eIDAS par rapport à la directive de 1999. Tout d'abord, nous retrouvons la volonté non aboutie en 1999 d'un marché intérieur uniforme<sup>220</sup>. Ensuite, un apport essentiel de ce règlement est la notion de confiance<sup>221</sup>. Le règlement tend à accroître la confiance dans les diverses transactions électroniques. Enfin, il vise une augmentation de la sécurité juridique pour les prestataires de services électroniques ainsi que pour leurs utilisateurs<sup>222</sup>.

## b) Définition de la signature électronique

Le règlement eIDAS définit la signature électronique comme « des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer »<sup>223</sup>. Nous retrouvons dans cette définition l'importance de l'identification de l'auteur de la signature.

Nous pouvons alors dire que pour être considérées comme une signature, les données sous forme électronique doivent représenter un « lien matériel fort entre l'acte et la signature »<sup>224</sup>. Cette condition vient du fait que, contrairement à un écrit papier où la feuille de papier assure ce lien, l'environnement électronique ne le permet pas. Concrètement, cela signifie que les données ne doivent pas pouvoir être disjointes de l'acte<sup>225</sup>.

Ensuite, le signataire doit avoir la volonté de signer l'acte grâce à ces données électroniques<sup>226</sup>. Cependant, le législateur européen ne définit pas ce qu'il entend par le fait de signer mais laisse aux États membres le soin de le définir. En Belgique, la Cour de cassation a défini la signature comme « la marque manuscrite par laquelle le signataire révèle habituellement sa personnalité aux tiers »<sup>227</sup>. La doctrine a alors associé deux fonctions à la

---

<sup>219</sup> ECONOMIE, « Aspects juridiques et enjeux de la signature électronique », 9 février 2018, disponible sur <https://economie.fgov.be/fr> (9 avril 2018).

<sup>220</sup> ECONOMIE, « Signature électronique et autres services de confiance », 5 avril 2018, disponible sur <https://economie.fgov.be/fr> (9 avril 2018).

<sup>221</sup> *Ibid.*

<sup>222</sup> *Ibid.*

<sup>223</sup> Règlement (UE) 910/2014, art. 3, § 10.

<sup>224</sup> H. JACQUEMIN, *L'identification électronique et les services de confiance depuis le règlement eIDAS*, *op. cit.*, p. 160.

<sup>225</sup> *Ibid.*, p. 160.

<sup>226</sup> *Ibid.*, p. 160.

<sup>227</sup> Cass., 7 janvier 1995, *Pas.*, 1995, I, p. 456.

signature, tout d'abord une fonction d'identification de son auteur et ensuite une fonction d'appropriation du contenu par le signataire<sup>228</sup>.

La signature électronique vise tous types de signatures utilisés par voie électronique. Cela peut être tant une signature manuscrite scannée, qu'une reconnaissance grâce aux empreintes digitales ou à l'iris de l'œil, qu'un code de carte bancaire<sup>229</sup>.

### c) Trois types de signatures électroniques

Au-delà des signatures ordinaires telles que définies ci-dessus, il existe encore deux autres types de signatures électroniques, selon qu'elles respectent ou non un certain nombre de conditions. Il peut également s'agir d'une signature avancée ou d'une signature qualifiée<sup>230</sup>.

Pour qu'une signature soit dite avancée, elle doit répondre aux quatre conditions reprises dans l'article 26 du règlement, à savoir « a) être liée au signataire de manière univoque; b) permettre d'identifier le signataire; c) avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif; et d) être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable »<sup>231</sup>.

Une signature qualifiée est « une signature électronique avancée créée par un dispositif de création de signatures qualifiées et qui repose sur un certificat qualifié pour signature électronique »<sup>232</sup>. Dès lors, pour que la signature soit dite qualifiée, il faut, en plus de devoir remplir les conditions d'une signature avancée, qu'elle soit créée par un dispositif qui en assure la confidentialité ainsi que la fiabilité et qu'elle soit délivrée à l'aide d'un « certificat qualifié de signature électronique »<sup>233</sup>. L'idée est que, lorsque l'on utilise une signature qualifiée, il faut qu'elle soit sous-tendue par un processus extrêmement fiable<sup>234</sup>.

En effet, la distinction entre ces trois types de signatures dépend du degré de risque que comportent les documents qui y sont associés. Ainsi, pour un contrat de travail par exemple, une signature simple ou avancée suffira<sup>235</sup>. Alors que pour un contrat d'assurance, il faudra une signature électronique qualifiée<sup>236</sup>. Le but étant de favoriser l'utilisation d'un processus fiable lorsque l'enjeu est plus important ou plus risqué.

---

<sup>228</sup> H. JACQUEMIN, *L'identification électronique et les services de confiance depuis le règlement eIDAS*, op. cit., p. 161.

<sup>229</sup> ECONOMIE, « Signature électronique et autres services de confiance », 5 avril 2018, disponible sur <https://economie.fgov.be/fr> (28 avril 2018).

<sup>230</sup> *Ibid.*

<sup>231</sup> Règlement (UE) 910/2014, art. 26.

<sup>232</sup> Règlement (UE) 910/2014, art. 3, § 12.

<sup>233</sup> Règlement (UE) 910/2014, art. 3, § 12.

<sup>234</sup> H. JACQUEMIN, *L'identification électronique et les services de confiance depuis le règlement eIDAS*, op. cit., p. 128.

<sup>235</sup> *Ibid.*, p. 128.

<sup>236</sup> *Ibid.*, p. 128.

#### d) Intérêt de la distinction

La conséquence directe de cette distinction est que les signatures électroniques qualifiées bénéficient d'une présomption légale encore appelée « principe d'assimilation », alors que les signatures « non-qualifiées » restent soumises aux aléas de la preuve<sup>237</sup>.

La présomption légale des signatures qualifiées a pour effet de renverser la charge de la preuve, ce qui signifie qu'elles sont présumées valables et, que le juge n'aura pas de marge d'appréciation quant à l'assimilation de cette signature à une signature manuscrite<sup>238</sup>. On considère cependant, qu'il doit rester possible d'en apporter la preuve contraire<sup>239</sup>. Cette distinction ne permet donc pas de refuser une signature qui n'est pas qualifiée comme preuve en justice. Cela veut simplement dire que seule la signature qualifiée peut être assimilée à la signature manuscrite<sup>240</sup>.

En ce qui concerne les signatures dites « non-qualifiées », elles ne bénéficient pas de cette présomption. Cependant, afin d'éviter de méconnaître le principe de non-discrimination entre l'écrit électronique et papier, il est permis de démontrer au juge que la signature respecte les fonctions essentielles des signatures électroniques et mérite qu'on lui reconnaisse des effets juridiques ou plus précisément, qu'on lui confère une valeur probante<sup>241</sup>.

#### e) Cachet électronique

Il faut toutefois noter que, pour les personnes morales, on ne parlera pas de signature électronique mais de cachet électronique<sup>242</sup>. Le cachet a pour fonction de garantir « l'authentification de la personne morale et le maintien de l'intégrité des données auxquelles elle est liée »<sup>243</sup>. Donc, contrairement à la signature électronique qui a pour fonction l'identification de l'auteur et son adhésion à l'acte, le cachet électronique vise l'authentification de la personne morale qui l'utilise, ainsi que l'intégrité des données auxquelles le cachet est lié<sup>244</sup>.

Comme les signatures électroniques, le cachet peut être de trois types selon le niveau de sécurité requis<sup>245</sup>. Le cachet électronique peut être ordinaire, avancé ou qualifié<sup>246</sup>.

Le cachet électronique ordinaire est défini à l'article 3, § 25, du règlement comme étant un outil composé de « données sous forme électronique, qui sont jointes ou associées

---

<sup>237</sup> H. JACQUEMIN, *L'identification électronique et les services de confiance depuis le règlement eIDAS*, op. cit., p. 128.

<sup>238</sup> *Ibid.*, p. 134.

<sup>239</sup> *Ibid.*, p. 134.

<sup>240</sup> Règlement (UE) 910/2014, art. 25.

<sup>241</sup> H. JACQUEMIN, *L'identification électronique et les services de confiance depuis le règlement eIDAS*, op. cit., pp. 134 et 135.

<sup>242</sup> *Ibid.*, p. 160.

<sup>243</sup> *Ibid.*, p. 192.

<sup>244</sup> *Ibid.*, p. 192.

<sup>245</sup> *Ibid.*, p. 195.

<sup>246</sup> *Ibid.*, p. 195.

logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières »<sup>247</sup>. Il bénéficie seulement du principe de non-discrimination<sup>248</sup>. Ainsi, s'il est contesté, il faudra prouver que les conditions d'origine et d'intégrité sont remplies<sup>249</sup>.

Le cachet électronique avancé est celui qui répond aux exigences de l'article 36 du règlement, à savoir : « a) être lié au créateur du cachet de manière univoque; b) permettre d'identifier le créateur du cachet; c) avoir été créé à l'aide de données de création de cachet électronique que le créateur du cachet peut, avec un niveau de confiance élevé, utiliser sous son contrôle pour créer un cachet électronique; et d) être lié aux données auxquelles il est associé de telle sorte que toute modification ultérieure des données soit détectable »<sup>250</sup>. Outre le principe de non-discrimination, le législateur européen n'attache pas de valeur spécifique au cachet électronique avancé. Cependant, au regard de la lourdeur des conditions, nous nous attendons à ce que les juges soient plus cléments dans l'appréciation des conditions d'origine et d'intégrité<sup>251</sup>.

Seul le cachet électronique qualifié dispose « d'une présomption d'intégrité et d'exactitude de son origine »<sup>252</sup>. Le cachet électronique qualifié est « un cachet électronique avancé qui est créé à l'aide d'un dispositif de création de cachet électronique qualifié et qui repose sur un certificat qualifié de cachet électronique ». Cette présomption est réfragable<sup>253</sup>.

Donc, à l'instar de la signature électronique, le cachet électronique ne peut pas être refusé en justice sous prétexte qu'il est électronique. Seul le cachet électronique qualifié sera présumé venir de la personne morale qui a conçu ce cachet et sera présumé intègre<sup>254</sup>.

## f) Horodatage

Dans la mesure où la *Blockchain* permet d'horodater des opérations, il nous paraît intéressant de faire le point sur ce sujet au travers du règlement eIDAS<sup>255</sup>.

L'horodatage consiste à « procéder à une datation précise et à fixer la chronologie de la vie d'un document »<sup>256</sup>. L'horodatage est essentiel, car, bien que la signature électronique apporte la preuve de l'origine ainsi que de l'intégrité d'un document, elle n'apporte aucune

---

<sup>247</sup> H. JACQUEMIN, *L'identification électronique et les services de confiance depuis le règlement eIDAS*, op. cit., p. 191.

<sup>248</sup> *Ibid.*, p. 195.

<sup>249</sup> *Ibid.*, p. 195.

<sup>250</sup> Règlement (UE) 910/2014, art. 36.

<sup>251</sup> H. JACQUEMIN, *L'identification électronique et les services de confiance depuis le règlement eIDAS*, op. cit., p. 196.

<sup>252</sup> Règlement (UE) 910/2014, art. 35, § 2.

<sup>253</sup> H. JACQUEMIN, *L'identification électronique et les services de confiance depuis le règlement eIDAS*, op. cit., p. 196.

<sup>254</sup> *Ibid.*, p. 196.

<sup>255</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p. 173.

<sup>256</sup> H. JACQUEMIN, *L'identification électronique et les services de confiance depuis le règlement eIDAS*, op. cit., p. 205.

garantie quant à l'heure et la date à laquelle ce document a été créé<sup>257</sup>. Dans le contexte électronique, l'horodatage est un ensemble de « données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant »<sup>258</sup>.

Comme pour la signature et le cachet électronique qualifiés, l'horodatage qualifié bénéficie d'un statut privilégié de la part du législateur. Ce dernier lui attache une présomption d'exactitude quant à la date et l'heure qu'il indique ainsi que pour l'intégrité des données auxquelles elles se rapportent<sup>259</sup>. Pour ce faire, l'horodatage doit satisfaire à certaines exigences : il doit lier « la date et l'heure aux données de manière à raisonnablement exclure la possibilité de modification indétectable des données ; il est fondé sur une horloge exacte liée au temps universel coordonné ; et est signé au moyen d'une signature électronique avancée ou cacheté au moyen d'un cachet électronique avancé du prestataire de services de confiance qualifié, ou par une méthode équivalente »<sup>260</sup>. Cette présomption est également réfragable<sup>261</sup>.

#### **4) Droit national belge**

##### **a) Introduction de la signature électronique en droit belge**

L'influence du législateur européen de 1999 a d'abord amené le législateur belge à adopter la loi du 20 octobre 2000 introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire. Celle-ci a entraîné la modification du Code civil en son article 1322, alinéa 2, afin de reconnaître la signature électronique et rédigée comme telle : « Peut satisfaire à l'exigence d'une signature, pour l'application du présent article, un ensemble de données électroniques pouvant être imputées à une personne déterminée et établissant le maintien de l'intégrité du contenu de l'acte »<sup>262</sup>. Dans un contexte européen, nous avons vu que, pour avoir une signature, il faudra remplir deux conditions. La première est qu'il faut avoir la volonté de s'identifier à l'acte, et la deuxième est qu'il faut vouloir adhérer à l'acte et à son contenu<sup>263</sup>. Cependant, l'article 1322, alinéa 2, ajoute une condition. Selon cet article, pour qu'une signature par voie électronique soit assimilée à une signature manuscrite, il faudra également prouver que « l'ensemble de données

---

<sup>257</sup> H. JACQUEMIN, *L'identification électronique et les services de confiance depuis le règlement eIDAS*, op. cit., p. 205.

<sup>258</sup> Règlement (UE) 910/2014, art. 3, § 33.

<sup>259</sup> Règlement (UE) 910/2014, art. 41.

<sup>260</sup> Règlement (UE) 910/2014, art. 42.

<sup>261</sup> H. JACQUEMIN, *L'identification électronique et les services de confiance depuis le règlement eIDAS*, op. cit., p. 207.

<sup>262</sup> C. civ., art. 1322, al. 2.

<sup>263</sup> H. JACQUEMIN, *L'identification électronique et les services de confiance depuis le règlement eIDAS*, op. cit., p. 160.

électroniques maintienne le document intègre »<sup>264</sup>. L'intégrité de l'acte exprime l'idée que, une fois l'acte signé, il ne faut pas qu'il puisse être modifié<sup>265</sup>.

Ainsi, si cette signature vient à être contestée devant les juridictions belges il faudra dès lors démontrer que les conditions de l'article 1322, alinéa 2, sont remplies, à savoir l'identification de la personne qui signe, l'adhésion par rapport au contenu et l'intégrité de l'acte<sup>266</sup>. Bien qu'en pratique, le juge vérifiera cette dernière condition quant au support plutôt qu'à la signature en elle-même<sup>267</sup>.

L'article 1322, alinéa 2, du Code civil détermine donc dans quelle mesure un acte sous seing privé a une force probante. À l'origine, la doctrine considérait que cet article ne valait que pour le droit de la preuve<sup>268</sup>. Mais cette situation a changé avec l'insertion dans le Code de droit économique de l'article XII.15. Cet article dispose que :

« § 1er. 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.

§ 2. Pour l'application du § 1er, il y a lieu de considérer :

- que l'exigence d'un écrit est satisfaite par une suite de signes intelligibles et accessibles pour être consultés ultérieurement, quels que soient leur support et leurs modalités de transmission ;
- que l'exigence, expresse ou tacite, d'une signature est satisfaite dans les conditions prévues soit à l'article 1322, alinéa 2, du Code civil, [2 soit à l'article 3.12. du règlement 910/2014];
- que l'exigence d'une mention écrite de la main de celui qui s'oblige peut être satisfaite par tout procédé garantissant que la mention émane de ce dernier »<sup>269</sup>.

Ainsi, selon une certaine doctrine, cet article pose les conditions de validité dans lesquelles peuvent être conclus des actes juridiques par voie électronique<sup>270</sup>.

En ce qui concerne les actes notariés, il faut se référer à l'article 1317 du Code civil, qui dit que, pour pouvoir servir de preuve à un acte authentique, il faut une signature électronique qualifiée qui réponde aux conditions de l'article 3, § 12, du règlement 910/2014.

---

<sup>264</sup> H. JACQUEMIN, *L'identification électronique et les services de confiance depuis le règlement eIDAS*, op. cit., p. 161.

<sup>265</sup> *Ibid.*, p. 143.

<sup>266</sup> *Ibid.*, p. 143.

<sup>267</sup> *Ibid.*, p. 172.

<sup>268</sup> *Ibid.*, p. 144.

<sup>269</sup> C.D.E., art. XII.15.

<sup>270</sup> H. JACQUEMIN, *L'identification électronique et les services de confiance depuis le règlement eIDAS*, op. cit., p. 145.

## b) Service d'archivage électronique

Enfin, le législateur belge a adopté la loi du 21 juillet 2016 qui met en œuvre le règlement eIDAS et qui est applicable depuis le 1<sup>er</sup> juillet 2016<sup>271</sup>. La finalité de la loi est la même que celle du règlement, en ajoutant un élément que le législateur belge considérait essentiel et qui ne figurait pas dans le règlement. La loi belge instaure un cadre juridique complet quant à l'archivage électronique. Le but de la loi est de couvrir toutes les étapes du processus électronique de la conclusion de l'acte, jusqu'à l'archivage de ce dernier<sup>272</sup>.

En effet, nous déplorons que le législateur européen n'ait pas choisi de considérer l'archivage électronique comme un service de confiance au même titre que la signature électronique<sup>273</sup>. Le recours à des méthodes d'archivage électronique permet une diminution des coûts et de l'espace nécessaire au stockage traditionnel, un classement plus facile, une solution face aux risques de perte des documents papier et de leur dégradation, ainsi qu'un accès direct et plus facile à l'information<sup>274</sup>. Un exemple de son utilité est l'obligation pour les hôpitaux de conserver les dossiers médicaux pendant trente ans ou encore les factures pendant une durée de sept ans<sup>275</sup>. Ce qui nécessite des espaces de stockage considérables et représente un risque de perte important.

L'archivage électronique « consiste en la conservation de données électroniques ou la numérisation de documents papier, et qui est fourni par un prestataire de services de confiance au sens de l'article 3, paragraphe 19, du règlement 910/2014 ou qui est exploité pour son propre compte par un organisme du secteur public ou une personne physique ou morale »<sup>276</sup>.

Tant le service d'archivage qualifié que non qualifié bénéficie du principe de non-discrimination, ce qui signifie que l'archivage papier n'est plus le seul à pouvoir satisfaire à une obligation de conservation au sens de la loi<sup>277</sup>. Mais, à nouveau, seul un service d'archivage électronique qualifié bénéficie d'une présomption d'intégrité relatif au contenu des documents stockés grâce à un tel service<sup>278</sup>. Cette présomption est toutefois réfragable<sup>279</sup>. Mais, pour ce faire, il doit remplir différentes conditions, dont la plus importante est l'intervention d'un

---

<sup>271</sup> Loi du 21 juillet 2016 mettant en œuvre et complétant le règlement (UE) 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII " Droit de l'économie électronique " du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique, *M.B.*, 28 septembre 2016, p. 67478.

<sup>272</sup> ECONOMIE, « Aspects juridiques et enjeux de la signature électronique », 9 février 2018, disponible sur <https://economie.fgov.be/fr> (9 avril 2018).

<sup>273</sup> H. JACQUEMIN, *L'identification électronique et les services de confiance depuis le règlement eIDAS*, *op. cit.*, p. 216.

<sup>274</sup> *Ibid.*, p. 216.

<sup>275</sup> Arrêté royal du 3 mai 1999 déterminant les conditions générales minimales auxquelles le dossier médical, visé à l'article 15 de la loi sur les hôpitaux, coordonné le 7 août 1987, doit répondre, *M.B.*, 30 juillet 1999, p. 28462, art 1<sup>er</sup> § 3 et C.D.E, art. III. 86.

<sup>276</sup> Loi 21 juillet 2016, art. 2.

<sup>277</sup> H. JACQUEMIN, *L'identification électronique et les services de confiance depuis le règlement eIDAS*, *op. cit.*, p. 244.

<sup>278</sup> *Ibid.*, p. 245.

<sup>279</sup> *Ibid.*, p. 245.



prestataire de services de confiance<sup>280</sup>. Pour ce qui concerne les services d'archivage non-qualifiés, il faudra prouver qu'ils permettent bien de « conserver la lisibilité des données, de préserver l'intégrité et l'authenticité des données et d'éviter les modifications des données sous réserve de celles relatives à leur support ou leur format qui sont nécessaires pour l'accomplissement du service »<sup>281</sup>.

## 5) Conclusion : règlement eIDAS et Blockchain

Dans la mesure où la *Blockchain* n'est encadrée par aucune réglementation, il nous paraît légitime de nous demander si le cadre légal encadrant la signature électronique pourrait lui être appliqué et ainsi attribuer une certaine force probante à la *Blockchain*.

En effet, nous avons vu que les échanges basés sur la *Blockchain* s'opèrent au travers d'un système de cryptographie asymétrique qui fait que, lorsque nous effectuons une opération sur la *Blockchain*, l'utilisateur se voit attribuer une clé privée et une clé publique. La clé privée permet de signer la transaction afin de s'identifier sur la *Blockchain*. Ce procédé est également utilisé pour le fonctionnement de la signature électronique au sens juridique du terme<sup>282</sup>. D'ailleurs, les exigences techniques nécessaires pour qu'une signature électronique soit qualifiée sont très lourdes et il ressort à l'heure actuelle que seul le système de cryptographie asymétrique rencontre ces exigences en offrant un très haut niveau de sécurité<sup>283</sup>. À titre d'exemple, une signature électronique basée sur le certificat de signature des cartes d'identité électroniques belges remplit les exigences d'une telle signature<sup>284</sup>.

Mais il convient tout de même de se demander si cette signature sur la *Blockchain* pourrait être envisagée comme une signature électronique au sens de la loi. En effet, pour qu'une telle signature bénéficie d'une présomption de fiabilité il faut qu'elle soit qualifiée. Nous avons vu qu'il y avait des conditions à respecter pour qu'une signature électronique soit qualifiée. Tout d'abord, il faut respecter les quatre conditions de l'article 26 du règlement 910/2014. Pour rappel, il faut que la signature soit exclusivement liée au signataire, elle doit permettre son identification, elle doit être créée par des moyens qu'il peut garder sous son contrôle et enfin, il doit y avoir un lien entre la signature et l'acte auquel elle renvoie<sup>285</sup>. Même si ces conditions semblent pouvoir être remplies d'un point de vue technique par la *Blockchain*, nous pouvons quand même nous interroger sur la fiabilité de l'identification du signataire de l'acte. En effet, comment être sûr que la personne derrière son ordinateur est bien celle qu'elle prétend ? Cette incertitude constitue la première faiblesse de la *Blockchain* quant à l'application du système de signature électronique.

---

<sup>280</sup> H. JACQUEMIN, *L'identification électronique et les services de confiance depuis le règlement eIDAS*, op. cit., p. 250.

<sup>281</sup> *Ibid.*, p. 244.

<sup>282</sup> *Ibid.*, p. 10.

<sup>283</sup> *Ibid.*, p. 166.

<sup>284</sup> *Ibid.*, p. 166.

<sup>285</sup> Règlement (UE) 910/2014, art. 26.

De plus, pour être considérée comme une signature qualifiée et bénéficier de la présomption légale, il faut que la signature électronique résulte d'un procédé d'identification sécurisé pouvant être vérifié à l'aide d'un certificat établi par un prestataire de services de confiance agréé<sup>286</sup>. Ces formalités n'existent pas sur la *Blockchain* ce qui constitue sa deuxième faiblesse. En effet, les clés sur la *Blockchain* permettent de coder et déchiffrer les messages, mais elles n'assurent pas le lien entre la personne qui les utilisent et leurs propriétaires initiaux puisque de telles clés peuvent être volées par exemple<sup>287</sup>. La *Blockchain* est anonyme ou plutôt pseudonyme<sup>288</sup>. Le règlement n'empêche pas une signature pseudonyme mais il est important de savoir que, dans le cas du règlement, un prestataire de services de confiance reprend les données personnelles tenant à l'identification de la personne, ce qui est absent sur la *Blockchain*<sup>289</sup>. Un tel système serait d'ailleurs contraire au postulat qui veut que la *Blockchain* soit décentralisée et donc fonctionne sans intermédiaire.

Certes, nous ne pouvons pas considérer les opérations faites sur la *Blockchain* à l'aide de la cryptographie asymétrique comme ayant une présomption légale d'assimilation puisqu'elle ne répond pas aux conditions de la signature électronique qualifiée. Mais ne pouvons-nous pas parler d'une signature électronique avancée ou à tout le moins ordinaire ? Pour être considérée comme telle, nous avons vu que qu'il faut au moins remplir deux conditions. Tout d'abord, il faut pouvoir identifier l'auteur de la signature et ensuite il faut que l'auteur ait l'intention de s'approprier le contenu par le signataire<sup>290</sup>. Ce à quoi, en Belgique, l'article 1322, alinéa 2, du Code civil ajoute une condition. Il faut pouvoir garantir l'intégrité de l'acte. Un élément est cependant indéniable, c'est le fait que la *Blockchain* est tout à fait apte à garantir l'intégrité de l'acte grâce à son caractère immuable<sup>291</sup>. Cependant, en l'absence d'identification de l'auteur de l'acte avec certitude sur la *Blockchain*, nous pouvons craindre qu'elle ne soit pas considérée comme une signature électronique, même ordinaire.

Par conséquent, il paraît raisonnable de conclure que, à ce stade et sans intervention du législateur pour ouvrir le régime de la preuve par signature électronique à la *Blockchain*, celle-ci ne peut pas bénéficier de la présomption légale attachée à la signature électronique, au cachet ou à l'horodatage qualifié, en raison de l'absence de délivrance d'un certificat par un prestataire agréé. La cause principale reste le manque d'identification possible du signataire et l'absence de prestataire de services de confiance pour assurer cette identification. Dès lors, toute contestation portée devant un juge à ce sujet l'obligera à trancher à partir des différents moyens de preuve présentés par les parties afin de prouver la fiabilité du processus<sup>292</sup>. Il est cependant essentiel de noter que si le législateur intervient pour imposer à la *Blockchain* l'utilisation de certificats par un service agréé, son caractère inaltérable la placerait parmi les preuves les plus efficaces. En effet, elle répond déjà parfaitement à la condition de garantie d'intégrité de l'acte

---

<sup>286</sup> Règlement (UE) 910/2014, art. 3 § 15.

<sup>287</sup> M. GUERINEAU, « Blockchain : l'ère de la transparence ? », *op. cit.*, p. 79.

<sup>288</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, *op. cit.*, p.175.

<sup>289</sup> H. JACQUEMIN, *L'identification électronique et les services de confiance depuis le règlement eIDAS*, *op. cit.*, p. 167.

<sup>290</sup> *Ibid.*, p. 161.

<sup>291</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, *op. cit.*, p. 126.

<sup>292</sup> C.-E. ARMINGAUD, « La blockchain et l'espace de confiance électronique européen », *op. cit.*, p. 3.

tel que repris aux articles 26 du règlement eIDAS et 1322, alinéa 2, du Code civil belge, ce qui amènerait alors une révolution du système probatoire.

### **III.- ANALYSE DE L'IMPACT DE L'IMPLANTATION DE LA *BLOCKCHAIN* DANS DES SECTEURS ÉCONOMIQUES**

Nous nous sommes jusqu'à présent intéressés aux enjeux juridiques qui s'imposeraient au législateur belge si la *Blockchain* venait à être plus largement utilisée en Belgique. Nous nous demandons maintenant quels secteurs seraient les plus impactés par une telle implantation. L'importance de la question réside dans le caractère décentralisé de la *Blockchain*. Comme nous l'avons vu, elle a été conçue dans une idée de suppression du tiers de confiance, ce qui peut avoir des conséquences très importantes sur les métiers de conseillers comme les notaires, les avocats, les assureurs ou encore les banquiers. Nous avons choisi d'analyser plus spécifiquement deux secteurs, celui du notariat et le secteur bancaire, car ce sont les deux domaines les plus cités lorsque nous entendons parler de l'impact de la *Blockchain*. Nous tenterons alors d'analyser dans quelle mesure la place de ces tiers va être remise en cause.

#### **A.- LE SECTEUR DU NOTARIAT**

##### ***1) Introduction***

Outre les exemples bien connus du *Bitcoin* et des *Smart Contracts*, la *Blockchain* permet également de certifier et de stocker des documents et des opérations<sup>293</sup>. Cette nouvelle application de la *Blockchain* nous amène donc à nous interroger sur la place qu'il restera au notaire dans le processus de la *Blockchain*. En effet, puisque le but premier de la *Blockchain* est de supprimer les intermédiaires de confiance, il y a fort à penser que le notaire pourrait être évincé de ce processus.

---

<sup>293</sup> A.-L. JOUBAIRE, « Les notaires doivent-ils craindre la Blockchain ? », 11 juillet 2017, disponible sur <https://www.eliott-markus.com/> (7 avril 2018).

## 2) *Définition*

L'article 1, alinéa 1, de la loi du 25 ventôse an XI contenant organisation du notariat définit les notaires comme « les fonctionnaires publics établis pour recevoir tous les actes et contrats auxquels les parties doivent ou veulent faire donner le caractère d'authenticité attaché aux actes de l'autorité publique, et pour en assurer la date, en conserver le dépôt, en délivrer des grosses et expéditions ». Le notaire est donc un officier public qui a reçu pour mission de rédiger des actes et de leur conférer valeur authentique<sup>294</sup>.

## 3) *Rôle du notaire*

Le notaire est un officier public muni d'une double mission. Le notaire a avant tout un rôle de conseiller. Il informe ses clients sur leurs droits et leurs devoirs, ainsi que sur les conséquences juridiques de leurs engagements<sup>295</sup>. Nous mettons tous un jour les pieds dans une étude notariale, lors de l'achat d'une maison, lors de la rédaction d'un contrat de mariage, lors d'un divorce ou encore en vue de régler une succession<sup>296</sup>.

Ensuite, le notaire rédige des actes et sa signature permet d'authentifier ses actes<sup>297</sup>. Cette valeur authentique donne à ses actes une force probante importante dans la hiérarchie des preuves et une force exécutoire égale à celle conférée par un juge<sup>298</sup>.

Le notaire est également un officier public chargé de garantir la sécurité juridique<sup>299</sup>. Il opère une mission de justice préventive<sup>300</sup>. Son rôle n'est pas de régler un conflit mais de le prévenir à l'aide de ses conseils et des outils qu'il a à sa disposition<sup>301</sup>. À titre d'exemple, lorsqu'une personne achète une maison, elle aimerait logiquement que le contrat soit valable juridiquement afin d'éviter d'éventuels problèmes dans le futur.

## 4) *Blockchain et secteur notarié*

Lorsque nous analysons l'impact de l'implantation de la *Blockchain* dans le secteur du notariat dans l'optique de suppression des tiers de confiance, nous nous rendons vite compte que cette idée n'est pas vraie en pratique, et ce pour plusieurs raisons. Tout d'abord, nous

---

<sup>294</sup> R. CHARRAS, « Notaire vs. Blockchain : conflit d'authenticité », 19 juin 2016, disponible sur <http://jurischain.com> (7 avril 2018).

<sup>295</sup> NOTAIRE.BE, « Un notaire, pour quoi faire ? », disponible sur <https://www.notaire.be/> (7 avril 2018).

<sup>296</sup> *Ibid.*

<sup>297</sup> R. CHARRAS, « Notaire vs. Blockchain : conflit d'authenticité », 19 juin 2016, disponible sur <http://jurischain.com> (7 avril 2018).

<sup>298</sup> NOTAIRE.BE, « Un notaire, pour quoi faire ? », disponible sur <https://www.notaire.be/> (7 avril 2018).

<sup>299</sup> *Ibid.*

<sup>300</sup> R. CHARRAS, « Notaire vs. Blockchain : conflit d'authenticité », 19 juin 2016, disponible sur <http://jurischain.com> (7 avril 2018).

<sup>301</sup> *Ibid.*

verrons plus précisément le rôle du notaire en tant que garant des actes authentiques. Ces actes ont une place importante dans la hiérarchie des preuves en Belgique, ce qui ne peut être assuré par la *Blockchain*. Ensuite, nous verrons que le rôle de conseiller du notaire est essentiel, car l'intervention humaine apporte une grande valeur ajoutée à une transaction.

## a) Les actes notariés

Tout d'abord, nous avons vu que les actes passés par le notaire sont des actes notariés. Ces actes font partie de ce que nous appelons les actes authentiques. L'alinéa premier de l'article 1317 du Code civil définit l'acte authentique comme « celui qui a été reçu par officiers publics ayant le droit d'instrumenter dans le lieu où l'acte a été rédigé, et avec les solennités requises ».

Cette authenticité se traduit à travers des caractéristiques particulières. En effet, les actes passés par des officiers publics comme les notaires ont date certaine, force probante, force exécutoire et sont conservés par ces derniers<sup>302</sup>.

### 1. *Date certaine*

Les actes notariés ont date certaine<sup>303</sup>. Cela signifie que leur date fait foi à l'égard des parties et assure l'opposabilité vis-à-vis des tiers. C'est ce qui différencie un acte notarié d'un acte sous seing privé qui requiert dans certains cas l'accomplissement de formalités afin d'être opposable<sup>304</sup>.

### 2. *Force probante*

Les actes notariés ont force probante<sup>305</sup>. Cela signifie que ce que constate le notaire ne peut être remis en cause. Par exemple, si lors d'un contrat de vente, le notaire acte que le prix a été payé sur son compte, cette information fait foi à l'égard des tiers<sup>306</sup>.

---

<sup>302</sup> R. CHARRAS, « Notaire vs. Blockchain : conflit d'authenticité », 19 juin 2016, disponible sur <http://jurischain.com> (7 avril 2018).

<sup>303</sup> *Ibid.*

<sup>304</sup> *Ibid.*

<sup>305</sup> *Ibid.*

<sup>306</sup> *Ibid.*

### 3. *Force exécutoire*

Les actes établis par les notaires ont force exécutoire<sup>307</sup>. Cela permet aux parties de recourir directement à un huissier sans devoir passer préalablement devant un juge pour faire exécuter l'accord<sup>308</sup>.

### 4. *Conservation en minute*

En règle générale, la copie originale des actes notariés est conservée par le notaire. Ce dernier ne délivrera aux parties qu'une copie afin qu'elles puissent faire exécuter l'accord<sup>309</sup>.

## b) *La Blockchain et les actes authentiques*

Les caractéristiques de la *Blockchain* rappellent sensiblement celles des actes authentiques mais sans pour autant atteindre les mêmes vertus d'un point de vue juridique<sup>310</sup>. L'authenticité dans le processus de la *Blockchain* est vue comme « la situation dans laquelle un particulier pourrait utiliser la *Blockchain* afin de prouver la propriété de son document et son intégrité »<sup>311</sup>.

### 1. *Horodatage*

La *Blockchain* permet d'enregistrer et de stocker la preuve horodatée et indélébile de l'existence d'une transaction ou d'un document. Le registre étant public, tout le monde peut voir cette preuve, ce qui est un élément très avantageux de la *Blockchain*<sup>312</sup>. Cela permet tant aux parties de la transaction qu'aux tiers de connaître avec certitude la date à laquelle une transaction a été effectuée ou plus précisément la date à laquelle la transaction a été enregistrée sur la *Blockchain*.

---

<sup>307</sup> R. CHARRAS, « Notaire vs. Blockchain : conflit d'authenticité », 19 juin 2016, disponible sur <http://jurischain.com> (7 avril 2018).

<sup>308</sup> NOTAIRE.BE, « Un notaire, pour quoi faire ? », disponible sur <https://www.notaire.be/> (7 avril 2018).

<sup>309</sup> *Ibid.*

<sup>310</sup> R. CHARRAS, « Notaire vs. Blockchain : conflit d'authenticité », 19 juin 2016, disponible sur <http://jurischain.com> (7 avril 2018).

<sup>311</sup> *Ibid.*

<sup>312</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p.173.

## **2. Force probante limitée**

Cependant, en l'absence de décision de justice établissant le contraire, la *Blockchain* ne garantit pas la force probante du document.

Nous avons vu dans le chapitre précédent que la *Blockchain* ne permet pas de répondre suffisamment aux conditions d'une signature électronique au sens de la loi<sup>313</sup>. Elle ne bénéficie donc pas d'une force probante particulière en raison du manque d'identification possible sur la *Blockchain* et à l'absence de délivrance d'un certificat par un prestataire agréé. Dès lors, si une contestation vient à être portée devant un juge à ce sujet, ce dernier ne sera pas obligé d'accepter cette preuve en justice et, s'il l'accepte, les parties devront prouver que l'identification de l'auteur de l'acte est possible et établir la fiabilité du processus qu'elles apportent comme preuve<sup>314</sup>.

## **3. Absence de force exécutoire**

Bien qu'un accord conclu au moyen d'un *Smart contrat* est exécuté automatiquement, une transaction opérée et stockée sur la *Blockchain* ne possède pas de force exécutoire au sens juridique du terme. Dès lors, le passage devant un juge pour faire exécuter une obligation reste obligatoire<sup>315</sup>.

## **4. Conservation**

La *Blockchain* est un outil de stockage qui permet de stocker les différentes transactions opérées sur celle-ci<sup>316</sup>. Elle fonctionne comme un grand registre et les informations qu'elle contient sont sécurisées et infalsifiables<sup>317</sup>. Ce qui représente donc un intérêt pour le secteur notarié en raison du rôle attribué au notaire pour la conservation des actes notariés.

## **5. Formation de l'acte authentique et Blockchain**

L'article 1317, alinéa 2, du Code civil énonce que l'acte authentique « peut être dressé sur tout support s'il est établi et conservé dans des conditions fixées par la loi ou par le Roi, par arrêté délibéré en Conseil des Ministres ». Nous pourrions donc imaginer l'utilisation de la *Blockchain* comme support. Cependant, l'alinéa 3 vient compléter l'alinéa 2 en disant que, « sans préjudice des conditions prévues à l'alinéa 2, pour les actes authentiques établis, reçus

---

<sup>313</sup> Cf. *supra* 5) Conclusion : règlement eIDAS et *Blockchain*, p. 40 du travail.

<sup>314</sup> C.-E. ARMINGAUD, « La blockchain et l'espace de confiance électronique européen », *op. cit.*, p. 3.

<sup>315</sup> R. CHARRAS, « Notaire vs. Blockchain : conflit d'authenticité », 19 juin 2016, disponible sur <http://jurischain.com> (7 avril 2018).

<sup>316</sup> C. HOUSSA et L. STANDAERT, *La « Nouvelle frontière » de la finance*, *op. cit.*, p. 187.

<sup>317</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, *op. cit.*, p.173

ou signifiés sous forme dématérialisée par un fonctionnaire public, seule une signature électronique qualifiée, visée à l'article 3, § 12, du règlement (UE) 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, satisfait aux conditions d'une signature ». Nous retrouvons une nouvelle fois ici l'exigence d'une signature électronique qualifiée qui sous-tend l'importance de l'acte. Or, comme nous l'avons déjà démontré à plusieurs reprises, la *Blockchain* ne permet pas de répondre à cette exigence.

De plus, l'alinéa 4 réitère l'exigence de connaissance de l'identité de l'auteur de la signature. En effet, cet article dispose que « la qualité du signataire de l'acte authentique qui fait usage d'une signature électronique qualifiée doit toujours pouvoir être vérifiée au moyen d'une banque de données authentiques prévue par la loi »<sup>318</sup>.

Enfin, même dans l'hypothèse où la *Blockchain* viendrait à être acceptée par le législateur comme support pour un tel acte, il manquerait toujours la condition reprise à l'alinéa premier de l'article 1317 du Code civil. Cet acte doit en effet être dressé par un officier public, le notaire, afin d'avoir un caractère authentique.

Les actes opérés sur la *Blockchain* n'étant pas dressés par des officiers publics, ils ne possèdent donc pas de caractère authentique. La question autour du caractère authentique au sens légal du terme de la *Blockchain* a toute son importance. En effet, à partir du moment où les actes passés sur la *Blockchain* n'ont pas de valeur authentique, ils n'ont pas de force exécutoire ni de force probante. Ainsi, si un litige naît à la suite d'une transaction effectuée sur la *Blockchain*, les parties n'ont aucun moyen de se défendre.

Pour illustrer l'importance de ce débat, nous voulions expliquer une affaire qui s'est passée en 2016 en France. Une députée française avait proposé un amendement à la loi française sur la transparence de la vie publique pour que « les opérations effectuées au sein d'un système organisé selon un registre décentralisé permanent et infalsifiable de chaîne de blocs de transactions constituent des actes authentiques ». Cependant cette idée avait été très mal reçue par les notaires, qui considéraient que c'était un appel à la suppression de leur profession. Le député Jean-Jacques Urvoas avait dès lors répondu à cette proposition en disant que « cette technologie de stockage numérique et de transmission à coût minime n'est qu'une technique et ce n'est pas cela qui fait l'acte authentique »<sup>319</sup>. Cette réponse nous paraît intéressante dans le sens où elle rappelle bien le statut actuel de la *Blockchain* en tant que technologie et rien d'autre<sup>320</sup>.

Certains auteurs voient l'avenir avec un notaire qui serait toujours chargé de la rédaction des actes mais où ce serait la *Blockchain* qui en conférerait le caractère authentique<sup>321</sup>. En ce qui concerne les conditions de forme, elles seraient remplies par les *Smart contracts*<sup>322</sup>.

---

<sup>318</sup> C. civ., art. 1317, al. 4.

<sup>319</sup> A.-L. JOUBAIRE, « Les notaires doivent-ils craindre la Blockchain ? », 11 juillet 2017, disponible sur <https://www.eliott-markus.com/> (7 avril 2018).

<sup>320</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p. 172.

<sup>321</sup> R. CHARRAS, « Notaire vs. Blockchain : conflit d'authenticité », 19 juin 2016, disponible sur <http://jurischain.com> (7 avril 2018).

<sup>322</sup> *Ibid.*



Cependant, il faudra indispensablement une intervention du législateur si nous voulons pouvoir un jour conférer un caractère authentique aux actes inscrits sur la *Blockchain*.

### **c) Mission du notaire**

Nous parlerons dans cette section de l'importance du travail du notaire mais aussi de son rôle de conseiller auprès de ses clients. Nous verrons quel pourrait être l'impact positif ou négatif de l'implantation de la *Blockchain* dans la vie d'un notaire et l'impact que cela aurait sur l'efficacité de son travail. Nous analyserons l'impact en termes de coût, de délai et nous verrons si ce tiers de confiance qu'est le notaire est réellement voué à disparaître.

#### ***1. Avantages***

##### **a. Diminution des délais**

Afin de comprendre quelle serait la place du notaire dans le processus de la *Blockchain*, il est important de comprendre comment il travaille en pratique. Afin d'expliquer au mieux comment travaille le notaire, nous partirons d'un exemple qui constitue une tâche quotidienne du notaire : participer à l'achat d'une maison. Lorsqu'une personne se rend chez le notaire pour acheter une maison, ce dernier va commencer à récolter toutes les informations nécessaires à la conclusion de la vente. Ces informations seront nécessaires pour conseiller le client afin qu'il soit bien informé sur le bien qu'il compte acheter et enfin finaliser la transaction.

Le délai complet pour conclure définitivement une telle vente sera de trois à quatre mois<sup>323</sup>. Il s'agit d'un délai qui peut paraître très long et nous entendons d'ailleurs souvent les gens se plaindre de la « lenteur des notaires ». Or, avant de penser que les notaires sont lents, il convient de se demander quelle est la véritable raison de ce long délai. En effet, entre le compromis de vente et la signature de l'acte notarié, c'est-à-dire de l'acte authentique de vente, le notaire va devoir faire, comme nous l'avons dit, un grand nombre de recherches. Ces recherches auront, par exemple, pour but par exemple de vérifier que l'immeuble n'est pas grevé d'une hypothèque ou qu'il n'est pas grevé d'une servitude dont les futurs acheteurs n'étaient pas informés.

Cependant, le notaire n'a pas accès directement à toutes ces informations. Pour les avoir, il doit en faire la demande aux différentes administrations concernées<sup>324</sup>. Selon Christian Luyten, directeur du département communication à la Fédération Royale du Notariat belge, c'est à ce stade qu'il y a les plus grosses lacunes. Toutes ces administrations n'ont, dans la plupart des cas, pas de registre informatique et doivent donc chercher dans leurs archives papier ce qui peut prendre un temps très important au vu du nombre d'archives, de la grandeur des entrepôts et des informations parfois très anciennes à retrouver. Nous pouvons cependant nous interroger sur la plus-value que représenterait un registre sur la *Blockchain* pour les

---

<sup>323</sup> NOTAIRE.BE, « L'acte notarié », disponible sur <https://www.notaire.be/> (7 avril 2018).

<sup>324</sup> *Ibid.*

administrations par rapport à une simple digitalisation des documents. En effet, la *Blockchain* étant très énergivore, nous pouvons penser que ce n'est pas nécessairement la meilleure solution. Cependant, l'avantage de la *Blockchain* réside dans son caractère distribué qui permet une augmentation de la sécurité puisqu'il existe une copie des documents chez chaque membre du réseau<sup>325</sup>.

Nous voyons ici une réelle opportunité que peut constituer la *Blockchain*. Elle permettrait de réunir en un seul registre toutes les informations des différentes administrations<sup>326</sup>. Ainsi, le notaire pourrait directement rechercher l'information dont il a besoin sans passer par des démarches administratives longues et périlleuses afin d'obtenir toutes les informations nécessaires à la conclusion d'un acte. Ainsi, l'étape de recherche des informations nécessaires au processus de vente ne prendrait plus quelques mois mais quelques minutes. En effet, l'obtention d'une information sur la *Blockchain* prend généralement dix minutes<sup>327</sup>.

De plus, si un client se rend chez le notaire pour lui poser une question simple ou lui demander un conseil, il ne devra plus attendre plusieurs jours pour avoir sa réponse. Grâce à la *Blockchain*, le notaire pourra se renseigner directement sur le registre et répondre immédiatement à son client.

Nous avons déjà parlé de ce genre d'initiative dans notre travail. Par exemple, nous pouvons nous servir de la *Blockchain* pour établir un registre cadastral, ce qui permettrait d'enregistrer l'ensemble des actes fonciers sur une même base de données<sup>328</sup>. Cela constituerait un avantage pour l'État, car cela lui faciliterait la tâche dans sa mission d'établissement et de perception des impôts. Cela serait aussi avantageux pour les citoyens qui pourront prouver leur propriété sur tel ou tel terrain, et enfin cela constituerait un avantage pour les notaires et les administrations pour qui la recherche d'informations serait facilitée.

Cependant, cette totale informatisation à travers un réseau distribué peut nous amener à nous demander si le notaire est encore nécessaire dans ce schéma. En effet, nous pourrions très bien imaginer qu'un individu désirant acheter une maison déclenche le processus directement sur la *Blockchain*. Elle se chargerait alors des vérifications grâce aux données des administrations, et conclurait la vente automatiquement, sans devoir passer par un notaire.

Nous voyons cependant un désavantage à ce système. À partir du moment où toutes les informations utiles sont réunies rapidement et que la transaction peut être conclue en quelques jours, voire en quelques heures, nous pouvons nous demander ce qu'il reste aux parties comme temps de réflexion. Il nous semble en effet indispensable que les parties puissent prendre le temps de réfléchir aux conséquences des actes qu'elles veulent passer. Nous nous rendons généralement chez le notaire pour des événements importants de notre vie comme l'achat d'une maison, et il est impensable de pouvoir acheter une maison en un jour ou en quelques clics.

---

<sup>325</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p. 17.

<sup>326</sup> *Ibid.*, p. 13.

<sup>327</sup> T. CAMBRAI, *Tout comprendre sur la Blockchain. Une technologie révolutionnaire au cœur du système économique de demain*, op. cit., p. 31.

<sup>328</sup> D. GEIBEN, O. JEAN-MARIE, T. VERBIEST, et J-F VILOTTE, *Bitcoin et Blockchain. Vers un nouveau paradigme de la confiance numérique* », op. cit., p. 45. ; L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p. 140.

Nous voyons un élément important du rôle de notaire qui est de conseiller les parties au mieux pour qu'elles soient sûres de leurs engagements, ce qui ne peut être le cas si les parties concluent un acte en quelques heures.

### **b. Diminution des coûts**

Un autre élément souvent cité en défaveur du notaire est de dire que passer par un notaire coûte cher. Ainsi, si la *Blockchain* élimine le notaire du processus, cela entraînerait une suppression des frais de notaire également. Il n'en est rien. En réalité, l'immense majorité de ces frais constitue des taxes qui ne sont pas dues au notaire mais à l'État, comme c'est le cas pour les droits d'enregistrement ou la TVA que le notaire collecte pour les rendre ensuite à l'État belge<sup>329</sup>.

De plus, une grosse partie des frais que l'on dépense chez le notaire est due aux recherches et aux formalités administratives<sup>330</sup>. Cela vise tant les demandes d'informations au fisc, au cadastre, mais aussi les demandes d'attestation, comme les attestations hypothécaires ou d'assainissement du sol. Cela vise également les frais nécessaires à l'inscription et à la transcription des actes et aux frais de copie<sup>331</sup>. Ainsi, l'idée d'un registre pour l'administration permettrait de diminuer ces coûts.

Nous voyons donc bien qu'il ne reste à partir de là qu'une petite partie dédiée aux honoraires du notaire. Par exemple, les honoraires du notaire en ce qui concerne un acte immobilier se limiteront à environ un pour cent du bien<sup>332</sup>. Ces honoraires étant justifiés par l'importance de la tâche du notaire mais aussi par l'apparition des outils électroniques chez les notaires. En effet, bien que l'informatisation permette une certaine diminution des coûts, elle a également entraîné une augmentation des obligations imposées par le législateur afin de s'assurer de la sécurité des données à travers ce système informatisé<sup>333</sup>. Nous pouvons citer, par exemple, l'augmentation des obligations à respecter afin de veiller au respect de la vie privée de leurs clients<sup>334</sup>.

### **c. Facilité administrative**

Un autre avantage retenu par Christian Luyten à propos de la *Blockchain* est de pouvoir faciliter certaines opérations de la vie de tous les jours. Nous illustrerons notre propos à l'aide d'un exemple assez simple. Il arrive souvent qu'une personne perde sa carte d'identité. La carte d'identité étant un document indispensable, il y a un certain formalisme à accomplir pour déclarer cette perte et ainsi pouvoir en faire refaire une nouvelle. Il faut tout d'abord se rendre à la police pour déclarer cette perte. Le policier rédigera une attestation de perte qu'il nous donnera, et c'est seulement avec ce papier que nous pourrions nous rendre à la commune afin

---

<sup>329</sup> NOTAIRE.BE, « 7 malentendus sur les "frais de notaire" », 14 juin 2017, disponible sur <https://www.notaire.be/> (28 avril 2017).

<sup>330</sup> NOTAIRE.BE, « Frais d'actes notariés », disponible sur <https://www.notaire.be/> (7 avril 2018).

<sup>331</sup> NOTAIRE.BE, « 7 malentendus sur les "frais de notaire" », 14 juin 2017, disponible sur <https://www.notaire.be/> (28 avril 2017).

<sup>332</sup> *Ibid.*

<sup>333</sup> *Ibid.*

<sup>334</sup> NOTAIRE.BE, « Le rôle du notaire », disponible sur <https://www.notaire.be/> (7 avril 2018)

de faire refaire notre carte d'identité. Il faudra ensuite revenir quelques jours plus tard à la commune afin de récupérer notre nouvelle carte.

A ce stade, nous voyons bien que la police n'opère aucun contrôle, elle ne fait que dresser une attestation sur ce qu'on lui dit. Nous pouvons dès lors nous demander si toutes ces étapes sont réellement nécessaires.

Là où la *Blockchain* intervient, c'est qu'elle permettrait de regrouper ces différentes étapes en simplifiant la procédure. Ainsi, nous pourrions imaginer nous rendre simplement à la police, laquelle remplirait un formulaire sur la perte de carte d'identité sur la *Blockchain* ce qui enclencherait directement le processus pour faire une nouvelle carte d'identité.

Il faut cependant rester conscient que ce genre de solution n'est pour le moment envisageable que pour des actions assez simples.

## **2. Inconvénients**

### **a. Vraisemblance des informations**

Nous pourrions donc imaginer faire des opérations simples sur la *Blockchain*. Cependant, s'il y a un élément très important à prendre en compte lorsque l'on enregistre une action sur la *Blockchain*, c'est qu'il faut pouvoir s'assurer que les informations émises sur celle-ci sont correctes. L'intervention du notaire à ce stade reste indispensable. En effet, le domaine du droit est très complexe et le nombre de lois en vigueur ne cesse d'augmenter, ce qui ne permet pas toujours aux citoyens d'en maîtriser tous les aspects. Le notaire, lui, possède une connaissance approfondie dans tous les domaines du droit puisqu'un même dossier peut en faire intervenir plusieurs branches<sup>335</sup>. Les individus auront donc besoin du notaire pour les éclairer dans les moments importants de leur vie et pour les aider à accomplir les actes qu'ils ne pourraient pas accomplir seuls à cause de leur complexité.

### **b. La responsabilité du notaire**

En outre, le rôle de conseiller du notaire veut que, si ce dernier constate des iniquités dans le contrat, il doit en informer les parties afin qu'elles soient pleinement conscientes de la portée de leurs actes<sup>336</sup>. Enfin, le notaire doit refuser de passer des actes contraires à la bonne foi ou qui ne reflètent pas la réalité<sup>337</sup>. Si tel n'est pas le cas, le notaire engage sa responsabilité à l'égard de ses clients pour tous les dommages relatifs à une faute commise dans l'exercice de ses fonctions<sup>338</sup>. Cet élément est essentiel puisqu'il permet d'assurer que le notaire fera son travail et conseillera ses clients du mieux qu'il le pourra. La *Blockchain* étant accessible à tout le monde, elle permet aussi d'y inscrire des éléments erronés en toute impunité<sup>339</sup>. Il est donc

---

<sup>335</sup> NOTAIRE.BE, « Un notaire, pour quoi faire ? », disponible sur <https://www.notaire.be/> (7 avril 2018).

<sup>336</sup> *Ibid.*

<sup>337</sup> *Ibid.*

<sup>338</sup> *Ibid.*

<sup>339</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p. 13.

selon nous essentiel que quelqu'un de compétent et pouvant engager sa responsabilité serve d'interface à ce que les individus souhaitent inscrire sur la *Blockchain*.

### c. Confidentialité

La *Blockchain* est réputée être « un grand livre de compte ouvert et accessible à tous en écriture et en lecture et qui est partagé sur un grand nombre d'ordinateurs à travers le monde »<sup>340</sup>. Ce caractère public de la *Blockchain* peut poser problème dans un contexte tel que le notariat. En effet, le respect de la vie privée est un enjeu essentiel de notre société. Il est d'ailleurs encadré dans une loi datant de 1992 et toujours en vigueur actuellement bien qu'elle ait reçu quelques modifications<sup>341</sup>.

Aussi, les personnes qui vont chez le notaire demander un conseil par exemple sont en droit de s'attendre à une certaine confidentialité. Le notaire s'est depuis quelques années déjà adapté à l'expansion de la technologie et un certain nombre d'opérations administratives sont exécutées par voie électronique<sup>342</sup>. Certes, cela se traduit par un gain de temps mais cela oblige également le notaire à être attentif au respect de la vie privée<sup>343</sup>. Pour ce faire le législateur a encadré les opérations accomplies par voie électronique<sup>344</sup>. À titre d'exemple, pour pouvoir accéder à certaines données personnelles de ses clients, le notaire doit demander une autorisation à la Commission de la protection de la vie privée<sup>345</sup>.

Pour pouvoir pallier ce problème, une solution serait d'utiliser pour les registres des notaires et des diverses administrations une *Blockchain* privée<sup>346</sup>. Pour rappel, dans les *Blockchains* privées, seules quelques personnes participent au processus de validation des informations et les autres utilisateurs doivent donc demander une autorisation pour consulter les données qu'elles contiennent<sup>347</sup>. Cela permettrait d'avoir une *Blockchain* à laquelle seules les administrations ayant souvent besoin de se communiquer des documents et informations pourraient accéder. Ainsi, les notaires entre autres pourraient directement aller chercher dans cette base de données les informations dont ils ont besoin et qui ont été préalablement postées par les différentes administrations. Ces *Blockchains* permettraient donc d'atteindre le niveau de confidentialité requis par ces administrations<sup>348</sup>.

### 3. Suppression du notaire tiers de confiance ?

Nous avons vu que la *Blockchain* est un grand registre, ce qui représente avant tout un grand intérêt pour les administrations qui sont encore pour la plupart noyées sous les archives papier. C'est moins vrai pour les notaires, pour lesquels une grande partie des tâches est déjà

---

<sup>340</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p. 13.

<sup>341</sup> Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, M.B., 18 mars 1993, p. 5801.

<sup>342</sup> NOTAIRE.BE, « Le rôle du notaire », disponible sur <https://www.notaire.be/> (7 avril 2018).

<sup>343</sup> *Ibid.*

<sup>344</sup> *Ibid.*

<sup>345</sup> *Ibid.*

<sup>346</sup> A. TORDEURS, « Une approche pédagogique de la Blockchain », op. cit., p. 18.

<sup>347</sup> *Ibid.*, p. 18.

<sup>348</sup> *Ibid.*, p. 18.

informatisée. Cependant, d'après nous, le postulat de départ de la *Blockchain*, qui consiste à dire que nous pouvons nous passer des intermédiaires de confiance comme le notaire, est faux. Toute la valeur ajoutée du notaire se retrouve dans sa tâche de garant des actes authentiques, ce qui permet d'assurer aux parties la force probante et l'exécution des actes les plus importants de leur vie. Mais c'est également son rôle de conseiller qui fait de lui un interlocuteur essentiel. Les individus auront toujours besoin d'une personne pour les rassurer et les conseiller. Enfin, il a également un grand rôle à jouer pour vérifier par exemple que les parties consentent bien à un contrat ou encore qu'elles en comprennent bien les termes<sup>349</sup>.

Tous ces éléments permettent de conclure cette partie par le fait que nous ne pouvons pas nous passer du notaire. La vision de la *Blockchain* comme étant la solution miracle qui va tout remplacer est une vision un peu naïve de certaines personnes ayant peu d'expérience dans des domaines tels que celui du droit. Dans ce domaine, les citoyens ont un important besoin de conseils et de pouvoir être sûrs que les actes qu'ils passent sont valables. Il ne s'agit dès lors pas pour nous d'un système qui permettra de se passer du notaire mais d'un outil mis à sa disposition afin de faciliter son travail quotidien.

## **B.- LE SECTEUR BANCAIRE**

### ***1) Introduction***

Un autre secteur pourrait se voir transformé si l'utilisation de la *Blockchain* venait à s'étendre en Belgique. Il s'agit du secteur bancaire. La *Blockchain* et, plus précisément, le *Bitcoin* ont d'ailleurs été créés à la suite de la crise financière de 2008 qui ébranla fortement la confiance que les gens avaient dans les institutions financières<sup>350</sup>. Il fallait dès lors trouver un moyen pour fonctionner sans elles. Cette solution fut trouvée avec la *Blockchain*. La *Blockchain* part du postulat que les tiers de confiance que constituent, par exemple, les institutions financières ne sont plus nécessaires et seraient alors remplacées par un consensus distribué<sup>351</sup>. En effet, cette idée de suppression des intermédiaires traditionnellement nécessaires lors d'opérations financières, comme les paiements, amène certains à penser que les banques telles que nous les connaissons aujourd'hui sont vouées à disparaître<sup>352</sup>. Nous essayerons alors de déterminer les dangers et les opportunités que peut représenter la *Blockchain* pour ce secteur afin de voir si nous pouvons réellement nous passer de ces intermédiaires.

---

<sup>349</sup> A.-L. JOUBAIRE, « Les notaires doivent-ils craindre la Blockchain ? », 11 juillet 2017, disponible sur <https://www.eliott-markus.com/> (7 avril 2018).

<sup>350</sup> P. HERLIN, *La fin des banques ?*, *op. cit.*, p. 56.

<sup>351</sup> A. TORDEURS, « Une approche pédagogique de la Blockchain », *op. cit.* p. 14.

<sup>352</sup> BLOCKCHAIN FRANCE, « Quels impacts de la blockchain sur les banques ? », 17 août 2016, disponible sur <https://blockchainfrance.net> (9 avril 2018).

## 2) *Rôle du banquier*

Les banquiers font partie de ce que nous appelons plus largement les établissements de crédit. Ces établissements de crédit sont définis comme étant « des organismes qui ont pour mission de recevoir des fonds du public et d'octroyer des crédits à leurs clients »<sup>353</sup>. Les missions principales des banques sont donc des missions de dépôt, d'octroi de crédit mais elles réalisent également des opérations financières et interviennent dans les opérations de paiement<sup>354</sup>. Nous avons vu que les autorités européennes considèrent le *Bitcoin* comme un moyen de paiement<sup>355</sup>. C'est ce qui nous amène à réfléchir sur la place qu'il laisse aux institutions financières dans leur rôle de garant des différentes opérations financières.

## 3) *Conditions d'établissement*

Les banques doivent, pour pouvoir exercer leur activité, obtenir un agrément auprès de la Banque centrale européenne<sup>356</sup>. Pour ce faire, elles doivent également remplir un certain nombre de conditions. Par exemple, il faut qu'elles possèdent un capital d'au moins 6 200 000 euros ou encore qu'elles soient constituées sous la forme d'une société commerciale<sup>357</sup>. Ces conditions nous permettent dès à présent de nous renseigner sur l'importance et la place donnée aux institutions financières dans notre société. En effet, n'importe qui ne peut pas s'improviser banquier, il y a des conditions à respecter.

### a) *Avantages*

Nous établirons tout d'abord un état des lieux des avantages que peut apporter une technologie comme la *Blockchain* dans le secteur financier. En effet, ce sont d'abord ses caractéristiques à première vue parfaitement implantables dans le secteur bancaire qui ont poussé les individus à s'intéresser à la *Blockchain*.

#### 1. *Diminution des coûts*

Le premier élément à prendre en compte est le coût des transactions bancaires, surtout en ce qui concerne les transferts d'argent internationaux. À titre d'illustration, dans certains pays en dehors de l'Union européenne, les commissions prélevées lors des différents transferts

---

<sup>353</sup> C. ALTER, *Droit bancaire général*, Bruxelles, *op. cit.*, p. 79.

<sup>354</sup> Banque centrale européenne, « Guide relatif à la surveillance bancaire », septembre 2014, disponible sur <https://www.ecb.europa.eu/pub/pdf/other/ssmguidebankingsupervision201409fr.pdf> (28 avril 2018).

<sup>355</sup> Cf. *supra* section 2) *Le Bitcoin*, p. 16 du travail.

<sup>356</sup> Loi du 22 mars 1993 relative au statut et au contrôle des établissements de crédit, *M.B.*, 19 avril 1993, p. 8650, art. 7.

<sup>357</sup> Loi du 22 mars 1993, art 15 et 16.

vont jusqu'à dix pour cent des montants des transactions, ce qui est une somme considérable<sup>358</sup>. Ce coût est principalement dû aux divers intermédiaires qui interviennent lors d'une opération et à l'infrastructure nécessaire pour les transactions actuelles.

La *Blockchain* pourrait alors constituer une solution à ce problème. En effet, le coût d'une transaction sur la *Blockchain* s'élève seulement à quelques centimes<sup>359</sup>. Ainsi, selon un rapport de la banque de Santander de 2015, la technologie *Blockchain* pourrait entraîner une réduction des coûts d'infrastructure pour les banques de 15 à 20 milliards de dollars par an, ce qui représente une somme d'environ 17,9 milliards d'euros<sup>360</sup>.

## 2. Diminution des risques de défaut de paiement et sécurité des transactions financières

Nous voyons également à travers la *Blockchain* un moyen de sécuriser les transactions bancaires et de diminuer le risque de défaut de paiement<sup>361</sup>. Grâce à la traçabilité et la transparence qu'instaure la *Blockchain*, nous pourrions suivre les transferts d'argent de leur origine jusqu'à leur destination, en quelque main qu'ils passent et ce n'importe où dans le monde<sup>362</sup>. Cela permettrait tout d'abord de pouvoir s'assurer de la solvabilité d'un client mais également de lutter contre la corruption, le blanchiment de capitaux et le financement du terrorisme<sup>363</sup>.

Il s'agit en effet d'une obligation imposée aux banques par la loi mais qui n'est pas toujours facilement réalisable. Elle fut consacrée notamment dans la récente 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 d'espèces, qui vient remplacer la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins de blanchiment de capitaux et du financement du terrorisme<sup>364</sup>.

Il faut cependant noter que certains individus peuvent, au contraire, se servir de l'anonymat dont ils bénéficient sur ces plateformes pour leurs transactions frauduleuses<sup>365</sup>. La Commission européenne est d'ailleurs intervenue dès le 2 février 2016, date à laquelle elle a publié une communication relative à « un plan d'action destiné à renforcer la lutte contre le

---

<sup>358</sup> BLOCKCHAIN FRANCE, « Quels impacts de la blockchain sur les banques ? », 17 août 2016, disponible sur <https://blockchainfrance.net> (9 avril 2018).

<sup>359</sup> *Ibid.*

<sup>360</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, *op. cit.*, p. 22.

<sup>361</sup> T. CAMBRAI, *Tout comprendre sur la Blockchain. Une technologie révolutionnaire au cœur du système économique de demain*, *op. cit.*, p. 57.

<sup>362</sup> *Ibid.*, p. 57.

<sup>363</sup> M. GUERINEAU, « Blockchain : l'ère de la transparence ? », *op. cit.*, p. 78.

<sup>364</sup> ECONOMIE, « Lutte contre le blanchiment de capitaux et le financement du terrorisme », 27 février 2018, disponible sur <https://economie.fgov.be/fr> (10 avril 2018).

<sup>365</sup> D. GEIBEN, O. JEAN-MARIE, T. VERBIEST et J-F. VILOTTE, *Bitcoin et Blockchain. Vers un nouveau paradigme de la confiance numérique ?*, *op. cit.*, p. 87.



financement du terrorisme »<sup>366</sup>. Cette communication avait pour idée principale de contraindre ces plateformes à appliquer les mesures de vigilance lors des échanges de crypto-monnaies<sup>367</sup>. Elle craignait que les organisations terroristes, entre autres, utilisent ces plateformes de transfert de monnaie virtuelle afin de cacher l'origine réelle de leurs mouvements financiers, étant donné, que ces transactions sont enregistrées sans faire l'objet de mécanisme de déclaration comme c'est le cas pour les systèmes bancaires actuels<sup>368</sup>. Nous voyons dès lors apparaître un embryon de cadre juridique. Celui-ci étant cependant davantage lié à la régulation du *Bitcoin* qu'à celle de la *Blockchain* en elle-même.

Il faut donc pouvoir assurer un équilibre entre l'efficacité des registres de la *Blockchain* en matière de traçabilité et les obligations légales de vigilance afin d'avoir un système à la fois efficace et sécurisé.

### 3. Diminution des délais

Le problème avec les paiements en ligne actuels, c'est qu'ils sont lents, car les banques doivent attendre des messages de confirmation avant de pouvoir effectuer une transaction. Par exemple, les transferts internationaux peuvent prendre plusieurs jours<sup>369</sup>.

La technologie *Blockchain* quant à elle permet de certifier une opération de façon quasi instantanée. Pour le moment, le temps nécessaire sur la *Blockchain* afin de valider une transaction en *Bitcoin* est de dix minutes, mais par exemple la *Blockchain* Ethereum n'a besoin que de quinze secondes pour effectuer une opération<sup>370</sup>. Ceci pourrait laisser présager des possibilités d'amélioration rendant les systèmes encore plus rapides.

Au niveau européen aussi on s'intéresse à cette opportunité de la *Blockchain*. Sept banques européennes se sont alors unies en 2016 afin de mettre en place une plateforme de financement pour le commerce international des PME<sup>371</sup>. L'objectif est de créer un espace sécurisé dans lequel les différents acteurs pourront partager des informations, opérer des transactions plus facilement et utiliser des *Smart contracts*, permettant ainsi une diminution des délais de paiement<sup>372</sup>.

---

<sup>366</sup> Communication de la Commission au Parlement européen et au Conseil relative à un plan d'action destiné à renforcer la lutte contre le financement du terrorisme, COM (2016) 50 final, février 2016.

<sup>367</sup> D. GEIBEN, O. JEAN-MARIE, T. VERBIEST et J-F. VILOTTE, *Bitcoin et Blockchain. Vers un nouveau paradigme de la confiance numérique ?*, op. cit., p. 87.

<sup>368</sup> *Ibid.*, p. 87.

<sup>369</sup> M. GUERINEAU, « Blockchain : l'ère de la transparence ? », op. cit., p. 78.

<sup>370</sup> T. CAMBRAI, *Tout comprendre sur la Blockchain. Une technologie révolutionnaire au cœur du système économique de demain*, op. cit., p. 31.

<sup>371</sup> Il s'agit de Deutsche Bank, HSBC, KBC, Natixis, Rabobank, Société Générale et UniCredit. ; LES ECHOS.FR, « Blockchain : sept banques européennes et IBM s'unissent pour le commerce international des PME », 28 juin 2017, disponible sur <https://www.lesechos.fr> (28 avril 2018).

<sup>372</sup> LES ECHOS.FR, « Blockchain : sept banques européennes et IBM s'unissent pour le commerce international des PME », 28 juin 2017, disponible sur <https://www.lesechos.fr> (28 avril 2018).

#### 4. Double dépense

Enfin, la *Blockchain* pourrait être une solution au problème bien connu de la double dépense. Cela consiste à dépenser plusieurs fois une même somme d'argent<sup>373</sup>. Or, dans la *Blockchain*, la vérification faite par les mineurs empêche un tel problème de survenir. En effet, pour qu'une transaction soit exécutée, ces derniers vont obligatoirement intervenir afin de retracer l'origine de ce montant sur le registre de la *Blockchain* et ainsi vérifier qu'il n'a pas déjà été dépensé<sup>374</sup>. Dans un cadre traditionnel c'est au banquier de prévenir mais aussi de détecter ce genre de fraude<sup>375</sup>. Cependant, beaucoup considèrent que le banquier n'est pas à l'abri d'une erreur, contrairement à la *Blockchain* dont l'efficacité de la vérification est assurée par le système de cryptographie asymétrique dont nous avons déjà parlé<sup>376</sup>.

#### 5. Registre uniformisé

Un apport essentiel de la *Blockchain* pour les institutions financières est le fait de pouvoir tenir un registre décentralisé. Elles pourraient alors utiliser ce registre pour créer une grande base de données reprenant tous leurs clients ainsi que les informations personnelles de ces derniers. Ainsi, les nouvelles informations ou les modifications des données personnelles à propos d'un client par exemple pourraient être communiquées à tous les départements, voire à toutes les banques, pour peu qu'elles acceptent de collaborer entre elles<sup>377</sup>. Mais également qu'elles acceptent de remplacer leurs registres privés par un tel registre distribué<sup>378</sup>. Cela assurerait pourtant une connaissance et une utilisation optimale du système. Il y a en effet actuellement un manque d'interaction entre les différentes institutions, ce qui conduit à un manque d'efficacité dans le secteur bancaire<sup>379</sup>. Il faudra cependant tenir compte des lois sur le respect de la vie privée et de la confidentialité des données de leurs clients.

Comme nous l'avons vu, ces registres pourraient également favoriser la prévention contre le blanchiment de capitaux et le financement du terrorisme<sup>380</sup>. La loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation d'espèces oblige les banques à s'informer très précisément sur leurs clients. Cette obligation est une traduction du principe « Know Your Customer »<sup>381</sup>. Il s'agit de l'obligation de vigilance qui se traduit par une obligation de connaissance de ses clients<sup>382</sup>. Les institutions financières doivent également prendre différentes mesures comme des mesures de

---

<sup>373</sup> A. TORDEURS, « Une approche pédagogique de la Blockchain », *op. cit.*, p. 15.

<sup>374</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, *op. cit.*, p. 17.

<sup>375</sup> A. TORDEURS, « Une approche pédagogique de la Blockchain », *op. cit.*, p. 15.

<sup>376</sup> *Ibid.*, p. 15. ; Cf. *supra* B.-Fonctionnement, p. 8 du travail.

<sup>377</sup> A. COLLOMB, L. LEGER et K. SOK, « Technologie des registres distribués : quel impact sur les infrastructures financières ? » in *réalités industrielles*, août 2017, p. 26.

<sup>378</sup> *Ibid.*, p. 26.

<sup>379</sup> M. GUERINEAU, « Blockchain : l'ère de la transparence ? », *op. cit.*, p. 79.

<sup>380</sup> *Ibid.*, p. 78.

<sup>381</sup> D. LEGEAS, « L'apport de la Blockchain au droit bancaire », *op. cit.*, p. 1 et ECONOMIE, « Lutte contre le blanchiment de capitaux et le financement du terrorisme », 27 février 2018, disponible sur <https://economie.fgov.be/fr> (10 avril 2018).

<sup>382</sup> P. STORRER, « Pour la reconnaissance du KYC digital » in *Digitalisation et droit financier*, 2016, p. 64.

contrôle ou de vérification des motifs de leurs clients afin de déceler les opérations anormales<sup>383</sup>.

Un projet « Know Your Customer » nommé « TrustHive » a d'ailleurs été lancé en 2017 à ce sujet<sup>384</sup>. Il s'agit d'une plateforme de collaboration au sein de l'Union européenne qui relie les start-ups de fintech et diverses organisations financières<sup>385</sup>. L'initiative a été prise par un groupe de travail constitué entre autres de Belfius, BNP, AG insurance, Paribas Fortis, Euroclear et KBC<sup>386</sup>. Le but était de créer une plateforme *Blockchain* permettant de simplifier la gestion des identités pour les entreprises en rendant plus faciles et plus rapides les inscriptions de leurs nouveaux clients<sup>387</sup>.

## b) Inconvénients

Nous allons maintenant essayer de voir quels sont exactement les inconvénients de cette technologie. Il convient bien de faire la part des choses entre avantages et inconvénients, car, bien qu'elle soit considérée comme totalement révolutionnaire, la *Blockchain* comporte encore quelques faiblesses.

### 1. Limite d'ordre technique

Il existe premièrement une limite d'ordre purement technique<sup>388</sup>. Cette limite peut rendre difficile l'utilisation de la *Blockchain* dans le secteur bancaire.

Nous l'avons déjà dit, la taille d'un bloc sur la *Blockchain Bitcoin* a été limitée volontairement à un méga-octet. Le but était d'empêcher des utilisateurs aguerris de construire des blocs de taille très importante, ce qui pourrait entraîner des congestions et paralyser le système de minage<sup>389</sup>. Cela constitue à la fois une sécurité et une limite pouvant ralentir l'adaptation des transactions bancaires d'importance sur la *Blockchain*<sup>390</sup>.

En effet, pour pouvoir être adaptée au secteur bancaire, la *Blockchain* doit être à même de supporter un important nombre de transactions, ce qui n'est pas encore le cas actuellement<sup>391</sup>. La *Blockchain* ne supporte que sept transactions par seconde, alors que le réseau Visa, par

---

<sup>383</sup> ECONOMIE, « Lutte contre le blanchiment de capitaux et le financement du terrorisme », 27 février 2018, disponible sur <https://economie.fgov.be/fr> (10 avril 2018).

<sup>384</sup> B-HIVE, « Isabel Group and norbloc bring blockchain KYC initiative to pilot », 15 mars 2018, disponible sur <https://b-hive.eu> (16 avril 2018).

<sup>385</sup> *Ibid.*

<sup>386</sup> *Ibid.*

<sup>387</sup> FEBELFIN, « B-Hive et les banques belges misent sur la nouvelle technologie blockchain », 6 juillet 2017, disponible sur <https://www.febelfin.be/fr> (16 avril 2018).

<sup>388</sup> I. PAVEL, « La blockchain - Les défis de son implémentation », *op. cit.*, p. 20.

<sup>389</sup> *Ibid.*, p. 20.

<sup>390</sup> *Ibid.*, p. 20.

<sup>391</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, *op. cit.*, p. 26.

exemple, en compte en moyenne 2 000 par seconde et sa capacité lui permet d'aller jusqu'à 56 000 transactions par seconde<sup>392</sup>.

## 2. « Attaque des 51 % »

Malgré cette limite technique qui a pour but de sécuriser le système, nous avons vu que la *Blockchain* n'est pas à l'abri d'une attaque. Dans l'environnement de la *Blockchain*, nous parlons de « l'attaque des 51 % »<sup>393</sup>. Pour rappel, il s'agit de la situation au terme de laquelle un individu ou un groupe d'individus parviendrait à contrôler plus de la moitié du réseau lui permettant d'inscrire ce qu'il voudrait sur la *Blockchain*<sup>394</sup>.

Le secteur bancaire est un secteur qui se veut extrêmement sécurisé, ce qui ne permet pas d'inclure la possibilité d'une telle attaque. Surtout qu'à l'heure actuelle, il y a un risque important que la compétitivité présente dans le cadre du processus de validation de la *Blockchain* amène les constructeurs à développer des ordinateurs de plus en plus puissants<sup>395</sup>. Ces ordinateurs pourraient alors écraser les systèmes de cryptographie actuels, ce qui représenterait un réel danger si nous venions à utiliser la *Blockchain* dans le secteur bancaire<sup>396</sup>.

## 3. Risque de fraude

Les autorités étatiques craignent que la *Blockchain* soit utilisée à des fins frauduleuses. En effet, cela ne serait pas la première fois. Nous nous rappelons l'affaire *Silk Road*, dans laquelle un groupe d'individus utilisaient la plateforme à des fins illégales<sup>397</sup>. L'anonymat qui est permis sur la *Blockchain* ne fait qu'augmenter ces risques<sup>398</sup>.

## 4. Problème d'identification

Nous l'avons déjà dit à plusieurs reprises, « une transaction n'a de valeur juridique que si l'on peut identifier son auteur »<sup>399</sup>. Ce postulat n'est cependant pas réalisable au sein de la *Blockchain*. Effectivement, les adresses des parties sont générées par des clés privées et des clés publiques qui ne permettent pas de connaître l'identité de la personne<sup>400</sup>. Or, nous l'avons vu, les banques ont l'obligation de s'informer et donc évidemment de connaître l'identité de

---

<sup>392</sup> I. PAVEL, « La blockchain - Les défis de son implémentation », *op. cit.*, p. 21.

<sup>393</sup> A. TORDEURS, « Une approche pédagogique de la Blockchain », *op. cit.*, p. 17.

<sup>394</sup> *Ibid.*, p. 17.

<sup>395</sup> *Ibid.*, p. 16.

<sup>396</sup> *Ibid.*, p. 18.

<sup>397</sup> D. GEIBEN, O. JEAN-MARIE, T. VERBIEST, et J-F. VILOTTE, *Bitcoin et Blockchain. Vers un nouveau paradigme de la confiance numérique ?*, *op. cit.*, p. 21.

<sup>398</sup> M. GUERINEAU, « Blockchain : l'ère de la transparence ? », *op. cit.*, p. 79.

<sup>399</sup> I. RENARD, « Fonctionnement de la Blockchain – Compatibilité avec un environnement réglementé : que peut-on et que doit-on réglementer dans une Blockchain ? » in *Revue de Droit bancaire et financier*, n°1, janvier 2017, p.3.

<sup>400</sup> I. PAVEL, « La blockchain - Les défis de son implémentation », *op. cit.*, p. 23.

chacun de leurs clients<sup>401</sup>. Il est donc indispensable de trouver une solution à ce problème majeur de la *Blockchain*.

À l'inverse, la traçabilité de la *Blockchain* peut poser un problème de confidentialité, également incompatible avec le secteur bancaire. Les transactions étant effectuées à l'aide de clés, en connaître l'auteur est impossible. Cependant, à l'inverse, le registre étant public, la traçabilité permet de connaître absolument toutes les transactions liées à ces clés et donc aux propriétaires de ces clés<sup>402</sup>. Ainsi, si l'identité de ces personnes venait à être révélée, nous pourrions tout à fait retracer l'entièreté de leurs opérations. Ceci constituerait une grave atteinte à la protection de la vie privée<sup>403</sup>.

Une solution possible à ce problème d'identification des individus serait de confier la tâche d'octroyer les clés nécessaires à une transaction sur la *Blockchain* aux différentes institutions financières<sup>404</sup>. Elles pourraient dès lors conditionner cet octroi à une identification claire des utilisateurs<sup>405</sup>. Cependant, cette solution doit être modérée. En effet, les banques belges seront à partir du 25 mai 2018, au même titre que toutes les entreprises belges, soumises au règlement général sur la protection des données de l'Union européenne<sup>406</sup>. Dans le cadre de ce règlement, le consommateur peut exiger la suppression de toutes les données bancaires mais aussi de toutes les données personnelles que la banque dispose à son égard<sup>407</sup>. Nous voyons dès lors la contradiction naissante entre le droit à l'oubli conféré par ce règlement et le caractère immuable de la *Blockchain*<sup>408</sup>. Cette contradiction devra être réglée avant de pouvoir prétendre à une application complète de la *Blockchain* dans le secteur bancaire.

Il reste encore un problème, celui de la confidentialité des transactions. Pour pallier ce problème, nous pourrions très bien imaginer, à l'instar du secteur du notariat, que le secteur bancaire travaille à l'aide d'une *Blockchain* privée<sup>409</sup>. Cela lui permettrait tant de garder confidentielles les transactions que de garder le contrôle sur celles-ci<sup>410</sup>.

---

<sup>401</sup> ECONOMIE, « Lutte contre le blanchiment de capitaux et le financement du terrorisme », 27 février 2018, disponible sur <https://economie.fgov.be/fr> (10 avril 2018).

<sup>402</sup> I. PAVEL, « La blockchain - Les défis de son implémentation », *op. cit.*, p. 23.

<sup>403</sup> *Ibid.*, p. 23.

<sup>404</sup> M. GUERINEAU, « Blockchain : l'ère de la transparence ? », *op. cit.*, p. 78.

<sup>405</sup> *Ibid.*, p. 78.

<sup>406</sup> Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.U.E.*, L 119, 4 mai 2016.

<sup>407</sup> INTEGRAL, « Règlement général sur la protection des données (GDPR) », disponible sur <http://www.integral.be/fr> (16 avril 2018).

<sup>408</sup> *Ibid.*

<sup>409</sup> A. TORDEURS, « Une approche pédagogique de la Blockchain », *op. cit.*, p. 18.

<sup>410</sup> *Ibid.*, p. 18.

## 5. *Le consortium R3*

Certaines banques ont compris l'enjeu que pouvait représenter la *Blockchain*. Ainsi, en 2015, une entreprise nommée R3 fut créée<sup>411</sup>. Son objectif est de réfléchir aux opportunités de cette technologie et plus précisément d'arriver à établir une infrastructure bancaire simplifiée<sup>412</sup>. L'entreprise R3 a d'ailleurs créé sa propre *Blockchain* privée nommée Corda. Il s'agit d'une « plateforme de comptabilité distribuée pour l'enregistrement et le traitement des accords financiers »<sup>413</sup>. Sa particularité est que Corda ne fonctionne pas par consensus comme c'est le cas d'une *Blockchain* traditionnelle, mais réinstalle l'idée d'un intermédiaire. Corda fonctionne donc grâce à un tiers qui ne validera une transaction que s'il a pu vérifier tous les éléments nécessaires à la validation de cette transaction<sup>414</sup>.

### c) *La Blockchain, un danger pour les banques ?*

Selon nous, il ne faut pas voir la *Blockchain* comme un danger pour le secteur bancaire mais plutôt comme une opportunité de développement venant en soutien au secteur bancaire, leur permettant de travailler dans de meilleures conditions, avec des gains de temps par rapport au schéma traditionnel et également à moindre coût. Cependant, ce système nécessite des adaptations afin de pouvoir s'adapter au secteur bancaire. La première serait une adaptation technologique afin d'augmenter la capacité de la *Blockchain* et ainsi permettre une augmentation du nombre de transactions possibles<sup>415</sup>. La seconde concerne l'identification des différents intervenants. Il faut trouver une solution immédiate pour favoriser leur identification comme par exemple grâce aux *Blockchains* privées. Celles-ci permettent de garder le contrôle et elles assurent un meilleur niveau de confidentialité puisque tant le droit d'écriture que le droit de regard y sont limités<sup>416</sup>. Nous verrions dès lors un affaiblissement du caractère décentralisé de la *Blockchain* qui en fait sa force mais cela au profit d'une augmentation de sa sécurité<sup>417</sup>.

---

<sup>411</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p. 22.

<sup>412</sup> M. GUERINEAU, « Blockchain : l'ère de la transparence ? », op. cit., p. 78.

<sup>413</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, op. cit., p. 112.

<sup>414</sup> *Ibid.*, p. 113.

<sup>415</sup> *Ibid.*, p. 25.

<sup>416</sup> A. TORDEURS, « Une approche pédagogique de la Blockchain », op. cit, p. 18.

<sup>417</sup> *Ibid.*, p. 18.

## IV.- RÔLE DE L'ÉTAT

Il nous paraît à présent important de réfléchir au rôle qu'il reste à l'État dans un système de plus en plus gouverné par la technologie. Nous avons vu à plusieurs reprises que la *Blockchain* a été créée en grande partie pour combler la perte de confiance envers l'État et plus précisément envers les institutions financières<sup>418</sup>. Au terme de cet exposé, il nous vient alors à l'esprit une question : cette nouvelle technologie remplace-t-elle le rôle de régulateur de l'État ou lui vient-elle en soutien ?

Il s'agit principalement du caractère décentralisé de la *Blockchain* qui est incompatible avec le rôle de l'État. Celui-ci constitue, avec toutes ses institutions, l'organe centralisateur par lequel toutes les transactions doivent passer pour en assurer la sécurité<sup>419</sup>. La décentralisation, quant à elle, traduit la volonté de remplacer cette autorité centrale par un « protocole de confiance »<sup>420</sup>. Le contrôle n'est plus effectué par une entité unique mais par la collectivité<sup>421</sup>. Dès lors, il paraît évident que toute forme de tentative de régulation autour de la *Blockchain* serait en totale contradiction avec « la définition et l'originalité de la *Blockchain* »<sup>422</sup>.

Cependant, bien que l'idée d'un système décentralisé rende la *Blockchain* très attrayante, nous voyons que les utilisateurs se tournent davantage vers l'utilisation de *Blockchains* privées<sup>423</sup>. Ces *Blockchains* sont caractérisées par une institution qui gère et contrôle la chaîne, il y a alors des règles de fonctionnement et des règles d'accès à la chaîne<sup>424</sup>. Ceci nous incite à penser que les organisations ne sont pas tellement prêtes à abandonner leur pouvoir de contrôle au profit d'un outil totalement décentralisé.

A notre avis, si la *Blockchain* permet d'augmenter la confiance entre les utilisateurs, elle ne supprime toutefois pas l'utilité de l'État. Ce dernier doit assurer le bon fonctionnement des transactions, à présent virtuelles, en instaurant un cadre autour de la *Blockchain*. Cela permettra d'éviter d'éventuelles dérives mais surtout de faciliter son implantation et de permettre aux entreprises de profiter en toute sérénité de son potentiel.

---

<sup>418</sup> P. HERLIN, *La fin des banques ?*, *op. cit.*, p. 56.

<sup>419</sup> A. TORDEURS, « Une approche pédagogique de la Blockchain », *op. cit.*, p. 11.

<sup>420</sup> *Ibid.*, p. 10.

<sup>421</sup> *Ibid.*, p. 10.

<sup>422</sup> D. GEIBEN, O. JEAN-MARIE, T. VERBIEST et J-F. VILOTTE, *Bitcoin et Blockchain. Vers un nouveau paradigme de la confiance numérique ?*, *op. cit.*, p. 95.

<sup>423</sup> A. TORDEURS, « Une approche pédagogique de la Blockchain », *op. cit.*, p. 18.

<sup>424</sup> H. DE VAUPLANE, « La Blockchain et la loi » in *Chronique / Digitalisation et droit financier*, RTDF n°1, 2016, p. 80.

## CONCLUSION

Dans la partie introductive de notre exposé, nous avons posé deux questions. La première consistait à se demander quels seraient les enjeux juridiques accompagnant l'implantation de la technologie *Blockchain* en Belgique. La deuxième visait à nous interroger sur les conséquences d'une telle implantation dans le secteur bancaire et dans celui du notariat belge.

A travers la première partie du travail, nous avons établi un état des lieux juridique de ce phénomène. Il faut avant toute chose prendre en compte la spécificité de la *Blockchain* pour pouvoir trouver le cadre juridique le plus adapté possible sans compromettre les opportunités qu'elle a à offrir.

Son originalité réside en premier lieu dans son caractère électronique. Ce caractère électronique n'est pas un problème d'un point de vue juridique. En effet, le droit des contrats est applicable au contrat conclu par voie électronique. Le problème, c'est qu'elle permet d'effectuer des transactions sans fournir les données des parties à cette transaction<sup>425</sup>. Cependant, à défaut d'identification des parties, le contrat pourrait se voir privé de ses effets juridiques<sup>426</sup>.

Cet anonymat sur la *Blockchain* pose également un problème quant à l'application du régime de preuve basé sur la signature électronique. En effet, en matière de signature électronique qualifiée, tout l'intérêt d'imposer la délivrance d'un certificat par un prestataire agréé est d'assurer la fiabilité du système et la connaissance des parties au contrat. En l'absence d'un tel certificat, les utilisateurs de la *Blockchain* devront se heurter à la réalité procédurale<sup>427</sup>.

Ensuite, nous avons essayé d'établir les avantages et les inconvénients de l'utilisation de la *Blockchain* dans le secteur du notariat et dans le secteur bancaire belge et nous nous sommes demandé si les tiers de confiance que constituent les notaires et les banquiers étaient réellement menacés par le caractère décentralisé de la *Blockchain*. Nous avons conclu que la *Blockchain* n'est pas un danger pour les tiers mais plutôt une opportunité d'amélioration pour les secteurs qui décideront de l'utiliser.

Cependant, elle nécessite quelques adaptations technologiques. Ces adaptations doivent viser, par exemple, une augmentation de sa capacité pour pouvoir effectuer un plus grand nombre de transactions, permettre la réversibilité des écritures effectuées sur sa chaîne et également permettre l'identification des différents utilisateurs.

Enfin, nous avons vu que la *Blockchain* n'est pas un contrat au sens juridique du terme. Il s'agit avant tout d'une technologie<sup>428</sup>. Mais cela ne l'empêcherait pas de constituer à l'avenir un instrument juridique qui permettrait la conservation, l'opposabilité et, suivant le respect de certaines conditions, la preuve d'un accord, ce qui faciliterait le travail des juristes sans toutefois

---

<sup>425</sup> I. PAVEL, « La blockchain - Les défis de son implémentation », *op. cit.*, p. 23.

<sup>426</sup> M. DUPONT, *Le b.a.-ba du contrat*, *op. cit.*, p. 44.

<sup>427</sup> C.-E. ARMINGAUD, « La blockchain et l'espace de confiance électronique européen », *op. cit.*, p. 3.

<sup>428</sup> L. LELOUP, *Blockchain : La révolution de la confiance*, *op. cit.*, p. 172.



les remplacer. Il faut donc trouver un équilibre entre la liberté que représente la *Blockchain* et la nécessité de régulation.

En définitive, si la *Blockchain* peut révolutionner la façon de travailler de certains secteurs, le manque de réglementation empêche son utilisation par les entreprises qui voudraient s'emparer de son potentiel. Il est donc nécessaire que le législateur se saisisse du problème afin d'établir un cadre juridique permettant l'implantation de la *Blockchain* et son utilisation en toute sécurité.



## BIBLIOGRAPHIE

### Doctrine

- ADALID, S., « La naissance de la monnaie unique : naissance de consensus » in *La banque centrale européenne et l'Eurosystème*, Bruxelles, Bruylant, 2015, spéc. pp. 5 à 26.
- ALTER, C., *Droit bancaire général*, Bruxelles, Larcier, 2010, 391 p.
- ALTER, C., THUNGEN, R., VAN OMMESLAGHE, P., *Incidence des nouvelles technologies de la communication sur le droit commun des obligations*, Bruxelles, Bruylant, 2012, 160 p.
- ANDRE-DUMONT, A-P., « Les services de paiement à l'épreuve des évolutions technologiques » in *La révolution digitale et les start-ups*, Larcier, 2016, 262 p., spéc. pp. 84 à 102.
- ARMINGAUD, C.-E., « La blockchain et l'espace de confiance électronique européen » in *Revue pratique de la prospective et de l'innovation*, n°1, janvier 2017, 4 p.
- BARREAU, C., « La régulation des smart contracts et les smart contracts des régulateurs » in *réalités industrielles*, août 2017, spéc. pp. 74 à 76.
- BEGUE, G., *Confidentialité et prévention de la criminalité financière - Étude de droit comparé*, Bruylant, 2017, 1018 p., spéc. pp. 680 à 735.
- CAMBRAI, T., *Tout comprendre sur la Blockchain. Une technologie révolutionnaire au cœur du système économique de demain*, 2017, 107 p.
- COLLOMB, A., LEGER, L., SOK, K., « Technologie des registres distribués : quel impact sur les infrastructures financières ? » in *réalités industrielles*, août 2017, spéc. pp. 25 à 28.
- CREMERS, T., « La blockchain et les titres financiers : retour vers le futur » in *Bulletin Joly Bourse*, 1<sup>er</sup> Juin 2016, n°06, p. 271.
- DECHAMPS, F., VANCAELEMONT, L., « Les obligations contractuelles et Internet », in *Les obligations contractuelles en pratique : Questions choisies*, Limal, Anthemis, 2013, 183 p., spéc. pp. 75 à 92.
- DE VAUPLANE, H., « La Blockchain et la loi » in *Chronique / Digitalisation et droit financier*, RTDF n°1, 2016, spéc. pp. 80 à 81.
- DELAHAYE, J.-P., « Les blockchains, clefs d'un nouveau monde » in *Logique et calcul*, mars 2015, spéc. pp. 81 à 85.
- DUPONT, M., *Le b.a.-ba du contrat*, Liège, Edipro, 2013, 149 p.
- GEIBEN, D., JEAN-MARIE, O., VERBIEST, T. et VILOTTE, J-F., *Bitcoin et Blockchain. Vers un nouveau paradigme de la confiance numérique ?*, RB édition, 2016, 126 p.
- GUERINEAU, M., « Blockchain : l'ère de la transparence ? » in *Revue internationale des services financiers / International Journal for Financial Services*, Bruylant, 2016, spéc. pp. 78 et 79.
- HERLIN, *La fin des banques ?*, Paris, Eyrolles, 2015, 180 p.

- HOUSSA, C. et STANDAERT, L., « La « Nouvelle frontière » de la finance » in X., 2016, spéc. pp. 153 à 197.
- JACQUEMIN, H., *L'identification électronique et les services de confiance depuis le règlement eIDAS*, Bruxelles, Larcier, 2016, 426 p.
- LEGEAIS, D., « L'apport de la Blockchain au droit bancaire » in *Revue de Droit bancaire et financier*, Larcier, janvier 2017, 10 p.
- LELOUP, L., *Blockchain : La révolution de la confiance*, Paris, Eyrolles, 2017, 223 p.
- MOURLON BEERNAERT, F., « La preuve en matière civile et commerciale » in *pratique du droit*, 2<sup>e</sup> édition, Wolters Kluwer, 212 p.
- PAVEL, I., « La blockchain - Les défis de son implémentation » in *réalités industrielles*, août 2017, spéc pp. 20 à 24.
- RENARD, I., « Fonctionnement de la Blockchain – Compatibilité avec un environnement réglementé : que peut-on et que doit-on réglementer dans une Blockchain ? » in *Revue de Droit bancaire et financier*, n°1, janvier 2017, spéc. pp. 1 à 3.
- RODRIGUEZ, P., *La révolution Blockchain. Algorithmes ou institutions, à qui donnerez-vous votre confiance ?*, Malakoff, Dunod, 2017, 223 p.
- SEGENDORF, B., « What is Bitcoin ? », in *Sveriges Riksbank Economic Review*, 2014, disponible sur <http://www.riksbank.se/>, pp. 71 à 87.
- STORRER, P., « Pour la reconnaissance du KYC digital » in *Digitalisation et droit financier*, 2016, spéc. pp. 64 à 66.
- STROUCKEN, F., OOSTERMEYER, M., “Gaat blockchain de juridische (notariële) wereld veranderen” in *Vastgoed Fiscaal & Civiel*, 22 juin 2017, spéc. pp. 3 à 6.
- TORDEURS, A., « Une approche pédagogique de la Blockchain » in *Revue internationale des services financiers / International Journal for Financial Services*, Bruylant, 2017.
- VAN OMMESLAGHE, P., *Droits des obligations*, t. III., Bruxelles, Bruylant, 2010, 2665 p.
- WAELEBROECK, P., « les enjeux économiques de la blockchain » in *réalités industrielles*, août 2017, pp 10 à 19.
- WERY, P., « La théorie générale du contrat » in *Droit des obligations*, Bruxelles, Larcier, 2010, 927 p.

## **Jurisprudence**

Cass., 7 janvier 1995, *Pas.*, 1995, I, p. 456.

C.J., arrêt *Skatteverket c. David Hedqvist*, 22 octobre 2015, C-264/14, EU:C:2015:718.

## **Législation**

Code civil.

Code judiciaire.

Code de droit international privé.

Code de droit économique.

Loi du 25 ventôse an XI contenant organisation du notariat du 16 mars 1803, *M.B.*, 16 mars 1803, p. 0.

Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, p. 5801.

Loi du 22 mars 1993 relative au statut et au contrôle des établissements de crédit, *M.B.*, 19 avril 1993, p. 8650.

Arrêté royal du 3 mai 1999 déterminant les conditions générales minimales auxquelles le dossier médical, visé à l'article 15 de la loi sur les hôpitaux, coordonné le 7 août 1987, doit répondre, *M.B.*, 30 juillet 1999, p. 28462.

Directive (UE) 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électronique, *J.O.C.E.*, L 13, 19 janvier 2000.

Loi du 20 octobre 2000 introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire, *M.B.*, 22 décembre 2000, p. 42698.

Loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, prise en exécution de la directive communautaire 1999/93/CE du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, *M.B.*, 29 septembre 2001.

Loi du 16 juillet 2004 portant le Code de droit international privé, *M.B.*, 27 juillet 2004, p. 57344.

Directive 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur modifiant les directives 97/7/CE, 2005/60/CE ainsi que 2006/48/CE et abrogeant la directive 97/5/CE, *J.O.U.E.*, L 319, 5 décembre 2007.

Règlement (CE) 593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles (Rome I), *J.O.U.E.*, L 177, 4 juillet 2008.

Directive 2009/110/CE du Parlement européen et du Conseil du 16 septembre 2009 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, modifiant les directives 2005/60/CE et 2006/48/CE et abrogeant la directive 2000/46/CE, *J.O.C.E.*, L 267/7 du 10 octobre 2009.

Règlement (UE) 1215/2012 du Parlement européen et du Conseil du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, *J.O.C.E.*, L 351, 20 décembre 2012.

Règlement de l'Autorité des services et marchés financiers du 3 avril 2014 concernant l'interdiction de commercialisation de certains produits financiers auprès des clients de détail, *M.B.*, 20 mai 2014, p. 40096.

Règlement (UE) 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, *J.O.U.E*, L 257, 28 août 2014.

Communication de la Commission au Parlement européen et au Conseil relative à un plan d'action destiné à renforcer la lutte contre le financement du terrorisme, COM (2016) 50 final, février 2016.

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.U.E*, L 119, 4 mai 2016.

Loi du 21 juillet 2016 mettant en œuvre et complétant le règlement (UE) 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII " Droit de l'économie électronique " du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique, *M.B.*, 28 septembre 2016, p. 67478.

Avis de la Banque centrale européenne du 12 octobre 2016 sur une proposition de directive du Parlement européen et du Conseil modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme et modifiant la directive 2009/101/CE, *J.O.U.E*, C 459, 9 décembre 2016.

Loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme, *M.B.*, 6 octobre 2017, p. 90839.

### **Sites internet**

ACTUALITE DU DROIT BANCAIRE, « les acteurs du droit bancaire », <http://www.actualitesdroitbelge.be> (9 avril 2018).

Banque centrale européenne, « Guide relatif à la surveillance bancaire », septembre 2014, disponible sur <https://www.ecb.europa.eu/pub/pdf/other/ssmguidebankingsupervision201409fr.pdf> (28 avril 2018).

B-HIVE, « Isabel Group and norbloc bring blockchain KYC initiative to pilot », 15 mars 2018, disponible sur <https://b-hive.eu> (16 avril 2018).

BLOCKCHAIN FRANCE, « Quels impacts de la blockchain sur les banques ? », 17 août 2016, disponible sur <https://blockchainfrance.net> (9 avril 2018).

BLOCKCHAIN FRANCE, « Qu'est-ce que la blockchain ? », disponible sur <https://blockchainfrance.net> (10 avril 2018).

CHARRAS, R., « Notaire vs. Blockchain : conflit d'authenticité », 19 juin 2016, disponible sur <http://jurischain.com> (7 avril 2018).

ECONOMIE, « Signature électronique et autres services de confiance », 5 avril 2018, disponible sur <https://economie.fgov.be/fr> (9 avril 2018).

ECONOMIE, « Aspects juridiques et enjeux de la signature électronique », 9 février 2018, disponible sur <https://economie.fgov.be/fr> (9 avril 2018).

ECONOMIE, « Lutte contre le blanchiment de capitaux et le financement du terrorisme », 27 février 2018, disponible sur <https://economie.fgov.be/fr> (10 avril 2018).

FEBELFIN, « B-Hive et les banques belges misent sur la nouvelle technologie blockchain », 6 juillet 2017, disponible sur <https://www.febelfin.be/fr> (16 avril 2018).

INTEGRAL, « Règlement général sur la protection des données (GDPR) », disponible sur <http://www.integral.be/fr> (16 avril 2018).

JOUBAIRE, A.-L., « Les notaires doivent-ils craindre la Blockchain ? », 11 juillet 2017, disponible sur <https://www.eliott-markus.com/> (7 avril 2018).

KIRALY, B., « Comment la blockchain va bousculer la construction », 3 mai 2016, disponible sur <https://www.lemoniteur.fr> (27 avril 2018).

LES ECHOS.FR « Blockchain : sept banques européennes et IBM s'unissent pour le commerce international des PME », 28 juin 2017, disponible sur <https://www.lesechos.fr> (28 avril 2018).

NBB, « A quoi sert la Banque nationale ? », disponible sur <https://www.nbb.be/fr> (27 avril 2018).

NOTAIRE.BE, « L'acte notarié », disponible sur <https://www.notaire.be/> (7 avril 2018).

NOTAIRE.BE, « Un notaire, pour quoi faire ? », disponible sur <https://www.notaire.be/> (7 avril 2018).

NOTAIRE.BE, « Frais d'actes notariés », disponible sur <https://www.notaire.be/> (7 avril 2018).

NOTAIRE.BE, « 7 malentendus sur les "frais de notaire" », 14 juin 2017, disponible sur <https://www.notaire.be/> (28 avril 2017).

Question et réponse écrite n° 0762 de C. Gennez du 7 février 2014, Ch., 2014, QRVA 53 152 disponible sur <https://www.lachambre.be/kvvcr/index.cfm?language=fr> (Consulté le 27 avril 2018).

Rapport de la BCE, « virtual currency schemes », 2012, disponible sur <https://www.ecb.europa.eu>

Rapport de la BCE, « virtual currency schemes - a further analysis », 2015, disponible sur <https://www.ecb.europa.eu>

