Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

La preuve par la blockchain

HUBIN, JEAN-BENOIT

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

Publication date:
2020

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
HUBIN, JEAN-BENOIT 2020, La preuve par la blockchain. dans *Les blockchains et les smart contracts à l'épreuve du droit.* Collection du CRIDS, numéro 49, Larcier , Bruxelles, pp. 185-208. <http://www.crid.be/pdf/crid5978-/8632.pdf>

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 04. May. 2026

La preuve par la blockchain

Jean-Benoit HUBIN

Juge au tribunal de l'entreprise francophone de Bruxelles

Collaborateur scientifique à l'UNamur (NADI) et à l'ULB (Jurislab)

1. Propos introductifs. Si la blockchain est principalement connue pour son usage dans le domaine des cryptomonnaies, ses applications potentielles dépassent largement le secteur de la finance. La blockchain permet en effet le stockage, la conservation et la transmission d'informations de toute nature[1]. Son caractère infalsifiable et la chronologie des données qu'elle contient lui confèrent un attrait indéniable pour mener des projets assurant la certification de transactions financières, la traçabilité de produits de la chaîne alimentaire, la validation de diplômes, ou encore le cadastre de titres de propriété[2].

Si le recours à la blockchain continue à prendre de l'ampleur, cette technologie pourrait être appelée, à terme, à jouer un rôle dans le cadre de litiges impliquant ses utilisateurs. Compte tenu du volume et de la diversité des informations qu'elle permet de conserver, et au vu des garanties qu'elle offre en termes d'authenticité et de sécurité, la blockchain pourrait en effet constituer une nouvelle technique de preuve, apte à établir la réalité ou le contenu de séquences d'opérations[3]. Encore convient-il de déterminer, à l'aune du cadre juridique en vigueur, quelle importance peut être donnée, sur le plan probatoire, aux informations issues de la blockchain. C'est l'objet principal de cette contribution.

---

[1] X., *Rapport d'information déposé en application de l'article 145 du Règlement par la Mission d'information commune sur les chaînes de blocs (blockchains)*, 12 décembre 2018, pp. 11-12, http://www.assemblee-nationale.fr/15/pdf/rap-info/i1501.pdf.

[2] Voy. à titre d'exemple les hypothèses de développement de la blockchain dans différents secteurs industriels européens présentés dans le rapport du JRC « #Blockchain4EU. Blockchain for Industrial Transformations », 2018, pp. 20-35, https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain4eu-blockchain-industrial-transformations.

[3] H. CROZE, « Aspects juridiques de la blockchain », in F. MARMOZ (dir.), *Blockchain et droit*, Paris, Dalloz, 2018, p. 34.

quentin.houbion@unamur.be
La preuve par la blockchain
Éditions Larcier - © Larcier - 30/10/2020

strada lex

Sans effectuer une présentation exhaustive des règles applicables en matière de preuve dans le contentieux civil[4], la présente contribution rappelle, dans un premier temps, certains principes essentiels du droit de la preuve, en particulier ceux qui régissent les actes posés dans l'univers électronique. Elle confronte ensuite ces principes au fonctionnement de la blockchain, dans sa fonction de stockage d'informations, afin de déterminer si, et à quelles conditions, les informations issues de la blockchain peuvent être réutilisées, à des fins probatoires, dans le contexte d'un litige civil. Elle propose enfin une réflexion sur les liens que la blockchain entretient avec les services de confiance, compte tenu du cadre légal qui leur est applicable.

CHAPITRE 1. Présentation synthétique des règles applicables en matière de preuve civile

SECTION 1. – Objet du droit de la preuve et siège de la matière

2. Objet du droit de la preuve. La preuve vise à établir la réalité d'une prétention[5]. Elle consiste « en la démonstration par une partie à un litige de l'exactitude ou de la fausseté d'une allégation »[6]. La preuve peut porter sur des faits matériels ou juridiques, ainsi que sur des actes juridiques. Elle doit être établie chaque fois que de tels actes ou faits sont allégués par une partie, mais font l'objet d'une contestation par son adversaire[7]. Le droit de la preuve a pour fonction de réglementer la manière dont cette démonstration peut être rapportée[8] : il répartit la charge de la preuve, définit les procédés de preuve dont les parties peuvent faire usage dans le cadre d'une procédure judiciaire, réglemente leur utilisation et opère le cas échéant une hiérarchie entre ceux-ci.

---

[4] La présente contribution ne traite pas des questions de preuve en matière pénale.

[5] H. De Page, *Traité élémentaire de droit civil belge*, t. III, liv. III, Bruxelles, Bruylant, 1936, p. 625.

[6] P. Van Ommeslaghe, *Traité de droit civil belge*, t. II, *Les obligations*, coll. De Page, Bruxelles, Bruylant, 2013, p. 2316.

[7] Projet de loi portant insertion du Livre 8 « La preuve » dans le nouveau Code civil, *Doc. parl.*, Ch. repr., sess. 2018-2019, n° 54-3349/001, pp. 11-12.

[8] P. Van Ommeslaghe, *Traité de droit civil belge*, t. II, *Les obligations*, *op. cit.*, p. 2322.

quentin.houbion@unamur.be
La preuve par la blockchain
Éditions Larcier - © Larcier - 30/10/2020

strada lex

L'existence d'une forme de gradation entre les différents modes de preuve permet de distinguer les systèmes de preuve dite « réglementée » ou « légale », par rapport aux systèmes de preuve dite « libre » ou « morale ». Dans un régime de preuve réglementée, « la loi réglemente l'administration de la preuve, elle indique les moyens de preuve qu'elle admet, elle en détermine la valeur et elle établit entre eux une hiérarchie »[9]. Ceci restreint le pouvoir d'appréciation du juge qui ne peut fonder sa conviction que sur la base des modes de preuve admissibles dans le litige qui lui est soumis[10]. Au contraire, lorsque la preuve est libre, le juge peut apprécier souverainement la valeur probante d'un procédé de preuve invoqué par une partie. Les parties peuvent dans ce cas soumettre au juge tous les éléments de preuve dont elles disposent, à charge pour ce dernier de fonder sa conviction en fonction de la valeur probante qu'il leur reconnaît.

3. Siège de la matière. En matière civile, les règles relatives au droit de la preuve sont inscrites aux articles 1315 et suivants du Code civil. Ces dispositions sont abrogées à compter du 1er novembre 2020 et remplacées par celles figurant dans le Livre 8 du nouveau Code civil, qui est consacré à la réglementation de la preuve civile[11]. En matière de nouvelles technologies, les principes définis par le Code civil sont complétés par le règlement européen eIDAS[12] et par certaines dispositions du livre XII du Code de droit économique. Certains secteurs connaissent également des législations spécifiques qui intéressent le droit de la preuve[13].

4. Caractère supplétif du droit de la preuve. Les règles de droit de la preuve présentent un caractère supplétif[14]. Ceci est désormais rappelé à l'article 8.2 du nouveau Code civil, qui précise que « sauf les définitions prévues dans le présent livre et hormis les cas où la loi en dispose autrement, toutes les règles du présent livre sont supplétives ». Sauf exception,

---

[9] D. Mougenot, « La preuve », *Rép. not.*, t. IV, l. 2, Bruxelles, Larcier, 2012, n° 4.

[10] P. Van Ommeslaghe, *Traité de droit civil belge*, t. II, *Les obligations*, *op. cit.*, p. 2323.

[11] Loi du 13 avril 2019 portant création d'un Code civil et y insérant un livre 8 « La preuve », *M.B.*, 14 mai 2019.

[12] Règl. (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

[13] Voy. à titre d'exemples l'article 64 de la loi du 4 avril 2014 relative aux assurances ; l'article 12 de la loi du 3 juillet 1978 relative aux contrats de travail ; l'article 9 de la Convention du 19 mai 1956 relative au contrat de transport international de marchandises par route (CMR).

[14] Cass., 22 mars 1973, *Pas.*, 1973, I, pp. 695-698 ; Cass., 24 juin 1994, *Pas.*, 1994, I, p. 651.

quentin.houbion@unamur.be
La preuve par la blockchain
Éditions Larcier - © Larcier - 30/10/2020

strada lex

les parties à un acte peuvent donc décider de déroger aux règles civiles en matière de preuve, ou renoncer à s'en prévaloir[15].

5. Formalisme probatoire et formalisme d'opposabilité. Au-delà du régime légal régissant la preuve des actes juridiques, il existe également d'autres types de formalisme régissant la validité ou l'opposabilité de certains actes. C'est ainsi que certaines législations instituent un formalisme « de publicité », qui vise à garantir que les tiers à une opération juridique déterminée aient la possibilité de prendre connaissance de celle-ci. Ce formalisme de publicité impose le plus généralement que l'acte juridique que l'on veut rendre opposable aux tiers soit inscrit dans un registre accessible au public ou à certaines catégories de personnes. C'est le cas par exemple pour la cession ou la concession de certains droits de propriété intellectuelle, pour la constitution ou le transfert de droits réels en matière immobilière, ou encore pour les transferts de titres nominatifs de certaines formes de sociétés. Sans affecter la validité de l'acte juridique, ou la preuve de celui-ci, le non-respect de ce formalisme de publicité a pour effet de rendre l'acte inopposable aux personnes que la règle a pour objectif d'informer, et ce jusqu'à ce qu'il soit satisfait à ladite formalité. Bien que cela ne constitue pas l'objet de la présente contribution, au vu de ses propriétés, la blockchain constitue un instrument approprié pour la tenue de ce type de registre sous une forme dématérialisée.

SECTION 2. – Le droit commun de la preuve en matière civile

6. Prééminence de l'écrit signé. Le droit civil envisage cinq modes de preuve distincts : le serment, l'aveu, l'écrit, les présomptions et les témoignages. Il prévoit un régime de preuve réglementé pour les actes juridiques de nature civile, centré sur la prééminence de la preuve par écrit[16]. En vertu de ce régime, les actes juridiques dont la valeur excède 375 euros – dont la valeur est supérieure ou égale à 3.500 euros à partir du 1er novembre 2020 – doivent être prouvés au moyen d'un écrit signé. Par ailleurs, quel que soit le montant de l'acte dont on cherche à rapporter la preuve, lorsque celle-ci est fondée sur un écrit signé, sa preuve contraire doit être établie au moyen d'un autre écrit signé.

---

[15] D. Mougenot, « La preuve », *op. cit.*, n° 10.

[16] Celui-ci est inscrit à l'article 1341 du Code civil, et repris à l'article 8.9 du Livre 8 du nouveau Code civil.

quentin.houbion@unamur.be
La preuve par la blockchain
Éditions Larcier - © Larcier - 30/10/2020

strada lex

Le concept d'écrit a reçu une définition à l'article 8.1 du nouveau Code civil. Il désigne « un ensemble de signes alphabétiques ou de tous autres signes intelligibles apposé sur un support permettant d'y accéder pendant un laps de temps adapté aux fins auxquelles les informations sont destinées et de préserver leur intégrité, quels que soient le support et les modalités de transmission ». Cette définition insiste sur les fonctions d'intelligibilité, de durabilité et d'intégrité des informations constatées sur l'écrit.

Pour que le document écrit reçoive force probante, il faut qu'il soit signé. La signature confère en effet à l'écrit un caractère original et permet ainsi de garantir son authenticité. La signature est définie à l'article 8.1 du nouveau Code civil comme « un signe ou une suite de signes tracés à la main, par voie électronique ou par un autre procédé, par lesquels une personne s'identifie et manifeste sa volonté ». Cette définition met en évidence les fonctions d'identification et d'adhésion qui sont assignées à la signature.

En raison de l'évolution des techniques de reproduction et de conservation, les documents papiers originaux font souvent l'objet de copies, qui sont archivées sur support papier ou numérique. En dépit de leur qualité, ces copies – même lorsqu'elles reproduisent la signature figurant sur le document original – constituent un écrit non signé.

Lorsqu'un écrit est dépourvu de signature – en ce compris lorsqu'il s'agit de la copie d'un acte original signé – il ne peut faire preuve d'un acte juridique d'une valeur supérieure à 375 euros. Toutefois, il peut valoir en tant que « commencement de preuve par écrit », s'il satisfait aux conditions de l'article 1347 du Code civil (art. 8.1, 7°, du nouveau C. civ.). Ceci implique que l'écrit émane de la partie qui conteste l'acte juridique ou de celui qu'il représente, et qu'il rende celui-ci vraisemblable. Si l'écrit rencontre ces conditions, l'existence et le contenu de l'acte peuvent être établis par tous modes de preuve. À défaut, l'écrit a la valeur d'une simple présomption, ce qui s'avère insuffisant pour rapporter la preuve de l'acte juridique allégué.

Une exception à ce principe est inscrite à l'article 1334, alinéa 2, du Code civil (et reprise à l'article 8.25, alinéa 1er, du nouveau Code civil). Elle vise à favoriser l'usage de l'archivage électronique. Elle prévoit que la copie réalisée au moyen d'un service d'archivage électronique qualifié dispose de la même force probante que l'écrit sous signature privée, dont elle est présumée, sauf preuve contraire, être une copie fidèle et durable. L'archivage électronique est défini à l'article I.18, 17°, du Code de droit économique comme un service de confiance qui consiste en la conservation de données électroniques ou la numérisation de documents papiers.

quentin.houbion@unamur.be
La preuve par la blockchain
Éditions Larcier - © Larcier - 30/10/2020

strada lex

En vertu de l'article I.18, 18°, de ce Code, un service d'archivage électronique qualifié est un service d'archivage électronique fourni par un prestataire de services de confiance qualifié se conformant aux dispositions du titre 2 et de l'annexe I du livre XII ou exploité pour son propre compte par un organisme du secteur public ou une personne physique ou morale et se conformant à ces dispositions[17]. C'est dans le respect de ces conditions qu'une copie numérique peut recevoir la force probante d'un écrit signé.

7. Régime de la preuve libre. Le régime de la prééminence de l'écrit connaît d'importantes limites. Avec l'entrée en vigueur du nouveau Code civil, il est d'ailleurs relégué au second plan[18], l'article 8.8 précisant désormais que « hormis les cas où la loi en dispose autrement, la preuve peut être apportée par tous modes de preuve ».

En premier lieu, le principe de la prééminence de l'écrit ne s'applique qu'aux actes juridiques. Ainsi, la preuve d'un fait juridique ou d'un fait matériel peut être rapportée par tous modes de preuve.

De plus, lorsque la preuve d'un acte juridique doit être rapportée par des tiers, ou à leur égard, on peut avoir recours à tous modes de preuve. Cette règle est désormais consacrée à l'article 8.14 du nouveau Code civil.

La preuve est également libre pour les actes juridiques d'une valeur inférieure ou égale à 375 euros – inférieure à 3.500 euros à partir du 1er novembre 2020 – ainsi que pour les actes juridiques unilatéraux.

Enfin, il résulte de l'article 1348*bis* du Code civil (art. 8.11 du nouveau Code) que la preuve est libre à l'égard des entreprises.

Dans ces différentes hypothèses, les témoignages et les présomptions – qui incluent les écrits non signés – disposent donc d'un statut équivalent à celui des écrits signés. En pratique, et bien que ceci relève de l'appréciation souveraine du juge, la valeur probante des écrits signés reste néanmoins plus grande que celle des témoignages et des présomptions.

SECTION 3. – La preuve dans l'environnement numérique

8. Preuve et nouvelles technologies. L'avènement des nouvelles technologies a confronté le droit de la preuve à l'utilisation des données

[17] Sur la notion de prestataire de service de confiance, voy. ci-dessous n° 9.

[18] Voy. F. George et J.-B. Hubin, « La réforme du droit de la preuve », in X., *Les grandes évolutions du droit de obligations*, Limal, Anthemis, 2019, pp. 189-190.

quentin.houbion@unamur.be
La preuve par la blockchain
Éditions Larcier - © Larcier - 30/10/2020

strada lex

électroniques. Ces données offrent aux parties de nouveaux instruments, souvent aussi – voire plus – fiables que ceux que fournit l'univers papier, pour établir la réalité de leurs allégations.

Les dispositions du Code civil consacrées au droit de la preuve sont longtemps restées inchangées – ou presque[19] – en dépit de l'importance croissante du numérique. Ceci ne s'est toutefois pas traduit par l'émergence d'importantes controverses en termes de contentieux[20]. Les parties en litige ont pris l'habitude de soumettre aux tribunaux des pièces issues de fichiers électroniques, afin de prouver leurs prétentions. Ces pièces sont le plus souvent traitées comme des écrits papier, pourvus ou non d'une signature. Selon les cas, elles sont donc assimilées à des écrits signés, à des commencements de preuve par écrit, ou à des présomptions.

Avec l'adoption du Livre 8 du nouveau Code civil, le législateur a exprimé le vœu de moderniser les concepts utilisés en matière de preuve et de les adapter à la réalité du numérique, afin de « faire entrer le droit de la preuve dans le 21e siècle »[21]. En outre, d'autres instruments normatifs

[19] Seules trois modifications législatives inspirées par l'avènement du numérique ont été apportées au Code civil de 1804 :

- la 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) a ouverture l'article 1322 du Code civil à la signature électronique ;
- la loi du 4 mai 2016 relative à l'internement et à diverses dispositions en matière de Justice (*M.B.*, 13 mai 2016) a posé les bases de la dématérialisation des actes authentiques ;
- la loi du 21 juillet 2016 mettant en œuvre et complétant le règlement (UE) n° 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques 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) a conféré un statut particulier à la copie numérique réalisée au moyen d'un service d'archivage électronique qualifié.

[20] Voy. D. Mougenot, « La preuve et les nouvelles technologies », in X., *La preuve au carrefour de cinq disciplines juridiques*, coll. Recyclage en droit, Limal, Anthemis, 2013, pp. 161-185 ; J.-B. Hubin, « La preuve électronique: développements récents et perspectives futures », in X., *La preuve en droit privé : quelques questions spéciales*, Bruxelles, Larcier, 2017, pp. 89-125 ; E. Vanstechelman, « La preuve électronique: enjeux et perspectives au regard du nouveau livre 8 du Code civil », in D. Mougenot (dir.), *La réforme du droit de la preuve*, coll. CUP, n° 193, Limal, Anthemis, 2019, pp. 185-253.

[21] Projet de loi portant insertion du Livre 8 « La preuve » dans le nouveau Code civil, *Doc. parl.*, Ch. repr., sess. 2018-2019, n° 54-3349/001, p. 4.

quentin.houbion@unamur.be
La preuve par la blockchain
Éditions Larcier - © Larcier - 30/10/2020

strada lex

récents, adoptés en marge du Code civil, ont eu pour effet de clarifier le régime juridique applicable aux données électroniques.

9. Règlement eIDAS. Avant l'apparition de la blockchain, pour sécuriser les opérations en ligne, et inciter le public à avoir recours aux communications électroniques, on a vu se développer les « services de confiance ». Ce concept désigne les procédés électroniques utilisés dans l'environnement virtuel, dont la fonction consiste à renforcer la sécurité et la fiabilité des échanges dématérialisés. Ces services sont pris en charge par des organismes tiers à la relation dématérialisée – qualifiés de « tiers de confiance » – dont le rôle est de créer un contexte dans lequel les transactions peuvent s'opérer en toute confiance et de manière sécurisée[22].

En 2014, le législateur européen a pris l'initiative d'adopter le règlement eIDAS, qui pose le cadre réglementaire applicable, dans l'Union européenne, aux principaux services de confiance[23]. Le règlement eIDAS envisage différents services de confiance, tels que la signature électronique, le cachet électronique, l'horodatage électronique, l'envoi recommandé électronique, ainsi que l'authentification de site internet. Il est guidé par un principe de neutralité technologique, qui veut que les règles adoptées soient neutres et ne désignent pas de technologie déterminée, de sorte qu'elles puissent s'adapter à l'évolution des technologies[24].

Le règlement eIDAS a pour but d'harmoniser, au sein de l'Union européenne, les effets juridiques attachés aux services de confiance qu'il réglemente, ainsi que de fixer des conditions uniformes, dans le marché intérieur, au déploiement des services de confiance « qualifiés ». Pour chaque service de confiance, le règlement propose en effet une distinction selon que leur utilisateur a recours à un service de confiance « qualifié » ou à un service de confiance « non qualifié ». Les services de confiance qualifiés sont offerts par des prestataires de services qui satisfont à un standard d'exigences élevé, consacré par le règlement. Ces exigences visent principalement à garantir la sécurité et la fiabilité du procédé électronique utilisé à titre de service de confiance. Afin de promouvoir l'usage de services de confiance qualifiés, le règlement eIDAS réserve l'application d'un régime juridique plus favorable aux parties utilisatrices de ce type de

[22] D. Gobert, « Commerce électronique : vers un cadre juridique général pour les tiers de confiance », *R.D.T.I.*, 2004, n° 18, p. 34.

[23] Règl. (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

[24] Voy. H. Jacquemin, « Principes applicables à tous les services de confiance et au document électronique », in H. Jacquemin (dir.), *L'identification électronique et les services de confiance depuis le règlement eIDAS*, coll. du CRIDS, vol. 39, Bruxelles, Larcier, 2016, p. 126.

quentin.houbion@unamur.be
La preuve par la blockchain
Éditions Larcier - © Larcier - 30/10/2020

strada lex

procédé[25] : ils bénéficient d'une présomption légale, voire d'une clause d'assimilation, qui confèrent au procédé électronique utilisé des effets similaires à ceux d'un procédé réputé équivalent dans le monde réel. À titre de comparaison, les services de confiance « non qualifiés » se voient attacher un simple principe de non-discrimination, en vertu duquel le procédé électronique ne peut être privé d'effet juridique au seul motif qu'il se présente sous une forme électronique.

De manière concrète, et du point de vue du droit de la preuve, cela signifie que l'usage d'un procédé de signature électronique qualifiée présente des effets équivalents à ceux d'une signature manuscrite (principe d'assimilation). Par contre, l'usage d'un procédé de signature électronique non qualifiée a pour seul effet d'interdire qu'il soit refusé en tant que mode de preuve parce qu'il se présente sous un format électronique (principe de non-discrimination)[26]. En présence d'un procédé de signature électronique non qualifiée, il appartient dès lors à la partie qui entend se prévaloir des données électroniques à titre de signature de démontrer que la technologie utilisée rencontre les fonctions assignées à la signature sur le plan légal.

De même, le recours à un procédé d'horodatage électronique qualifié bénéficie d'une présomption d'exactitude de la date et de l'heure qu'il indique et d'intégrité des données auxquelles se rapportent cette date et cette heure. Pour sa part, l'usage d'un procédé d'horodatage électronique non qualifié a pour seul effet d'interdire que ce procédé soit refusé en tant que mode de preuve au seul motif qu'il se présente dans un format électronique. Dans cette hypothèse, il appartient à la partie qui entend fixer les données dans le temps de convaincre le juge de l'exactitude de la date et de l'heure attachées à celles-ci.

Au final, le recours à des services de confiance qualifiés a pour effet de renverser la charge de la preuve, ainsi que son objet. Ainsi, dans l'hypothèse de l'utilisation d'un service de confiance non qualifié, il appartient à l'utilisateur de ce procédé électronique de démontrer que les fonctions attendues de la formalité qu'il entend accomplir sont rencontrées, alors que le recours à un service de confiance qualifié dispense l'utilisateur d'avoir à faire une telle démonstration et impose à celui qui voudrait contester les fonctions assignées audit procédé électronique d'établir que celui-ci ne satisfait pas aux exigences d'un service de confiance qualifié.

[25] *Ibid.*, p. 128.
[26] Art. 25 règl. eIDAS.

quentin.houbion@unamur.be
La preuve par la blockchain
Éditions Larcier - © Larcier - 30/10/2020

strada lex

10. Code de droit économique. Le dispositif prévu par le règlement eIDAS est complété par plusieurs dispositions du livre XII du Code de droit économique, qui réglemente le droit de l'économie électronique.

L'article XII.15 du code, qui transpose l'article 9 de la directive 2000/31 sur le commerce électronique[27]-[28], lève les obstacles formels à la conclusion des contrats par voie électronique. Fondé sur le principe des équivalents fonctionnels[29], son premier paragraphe prévoit que « 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 ». Le deuxième paragraphe de l'article XII.15 précise ensuite dans quelles conditions les exigences relatives à l'écrit, à la signature et à la mention manuscrite sont satisfaites dans l'environnement numérique.

Suite à l'adoption du Livre 8 du nouveau Code civil, qui confère une définition autonome aux concepts d'écrit et de signature, en droit de la preuve, il n'est plus nécessaire d'effectuer le détour par l'article XII.15 du Code de droit économique lorsqu'il s'agit de faire application de ces concepts à des fins probatoires. Par contre, lorsqu'une exigence de forme contractuelle, échappant au formalisme probatoire, se réfère aux concepts d'écrit ou de signature, il faut avoir recours à l'article XII.15 du Code de droit économique pour déterminer sa portée dans l'environnement numérique.

L'article XII.15 du Code de droit économique s'applique à tout type de contrat. Sa portée peut néanmoins être limitée par l'article XII.16, qui prévoit que, pour quatre catégories de contrats[30], les cours et tribunaux peuvent décider de ne pas appliquer le processus d'analyse fonctionnel

---

[27] Dir. 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur.

[28] L'article 9 de la directive 2000/31/CE imposait aux États membres de veiller « à ce que le régime juridique applicable au processus contractuel ne fasse pas obstacle à l'utilisation des contrats électroniques ni ne conduise à priver d'effet et de validité juridiques de tels contrats pour le motif qu'ils sont passés par voie électronique ».

[29] En vertu de ce principe, une exigence de forme doit être définie à la lumière des fonctions qu'elle permet de remplir, de sorte que des procédés techniques différents doivent être en mesure de satisfaire à cette formalité et, par voie de conséquence, de se voir conférer des effets équivalents (voy. H. JACQUEMIN, « Principes applicables à tous les services de confiance et au document électronique », *op. cit.*, p. 119).

[30] Les catégories de contrat concernées sont :

1° les contrats qui créent ou transfèrent des droits sur des biens immobiliers, à l'exception des droits de location ;

2° les contrats pour lesquels la loi requiert l'intervention des tribunaux, des autorités publiques ou de professions exerçant une autorité publique ;

quentin.houbion@unamur.be
La preuve par la blockchain
Éditions Larcier - © Larcier - 30/10/2020

strada lex

prévu à l'article XII.15, pour autant qu'« ils constatent l'existence d'obstacles pratiques à la réalisation d'une exigence légale ou réglementaire de forme dans le cadre du processus de conclusion d'un contrat par voie électronique ».

Le livre XII du Code de droit économique contient par ailleurs des dispositions spécifiques au droit belge qui mettent en œuvre et complètent le règlement eIDAS. Celles-ci sont principalement inscrites à l'article XII.25 du Code.

CHAPITRE 2. Droit de la preuve et blockchain

SECTION 1. – Éléments caractéristiques de la blockchain

11. Définition et principales caractéristiques de la blockchain. La blockchain est présentée comme une technologie « de stockage et de transmission d'informations, permettant la constitution de registres répliqués et distribués, sans organe central de contrôle, sécurisées grâce à la cryptographie, et structurées par des blocs liés les uns aux autres, à intervalles de temps réguliers »[31]. Cette définition met en lumière les principales caractéristiques communes à toutes les blockchains :

- une base de données distribuée entre tous ses membres ;
- fonctionnant indépendamment de toute forme de contrôle centralisé, sur la base de règles de gouvernance préalablement définies et acceptées par ses utilisateurs ;
- dans laquelle les données enregistrées sont sécurisées au moyen d'une méthode de chiffrement appelée cryptographie asymétrique ;
- et organisée sous forme de blocs qui garantissent la chronologie des données enregistrées.

La blockchain permet la gestion communautarisée de données électroniques, entre des acteurs qui ne se connaissent pas nécessairement. Elle prend la forme d'une base de données décentralisée composée

3° les contrats de sûretés et garanties fournis par des personnes agissant à des fins qui n'entrent pas dans le cadre de leur activité professionnelle ou commerciale ;

4° les contrats relevant du droit de la famille ou du droit des successions.

[31] V. Faure-Muntian, C. de Ganay et R. Le Gleut, *Rapport sur les enjeux technologiques des blockchains (chaînes de blocs)*, 20 juin 2018, p. 11, http://www.senat.fr/rap/r17-584/r17-5841.pdf.

quentin.houbion@unamur.be
La preuve par la blockchain
Éditions Larcier - © Larcier - 30/10/2020

strada lex

d'un nombre indéterminé de *nœuds* structurés en réseau *peer to peer*, qui détiennent chacun une version de la base de données[32]. Cette base de données conserve une trace structurée de chaque opération enregistrée en son sein depuis sa création, de sorte qu'il est toujours possible de retracer son historique.

Leur structure permet aux blockchains de contenir des informations réputées infalsifiables, puisqu'elles font l'objet d'un contrôle et d'une validation par la communauté avant d'être ajoutées à la base de données. En effet, avant de venir se superposer, en fin de chaîne, aux autres blocs de la base de données, chaque nouveau bloc doit être validé par les *nœuds* du réseau, selon des règles de gouvernance qui sont décrites dans la plateforme logicielle[33]. C'est donc la technologie en elle-même qui garantit l'authenticité de l'information et justifie la confiance des membres du réseau dans son usage. Ceci rompt avec le modèle de fonctionnement des réseaux numériques reposant sur l'intervention de tiers de confiance[34].

Il est important de souligner, à ce stade, que les blockchains peuvent contenir des informations de nature très variées, figurant dans des fichiers électroniques, qui sont eux-mêmes repris, sous forme d'empreinte cryptée (« *hash* »), au sein de la base de données. La fonction de *hashage* utilisée pour crypter les données inscrites dans les blocs, qui repose sur la cryptographie asymétrique, est réputée infalsifiable. La blockchain ne contient donc pas le fichier électronique faisant état de l'information dont on cherche à rapporter la preuve, mais seulement une empreinte de ce fichier électronique. Lorsqu'on accède à la blockchain, ce sont ces empreintes (« *hash* ») qui peuvent être consultées. Leur contenu n'est par contre pas visible. L'empreinte cryptée ne révèle en effet rien de la donnée originale[35]. Les modalités d'accès aux données originales dépendent des règles de gouvernance décidées par les acteurs de la blockchain.

12. Blockchains publiques et blockchain privées. Historiquement, les blockchains ont été développées sous forme de bases de données ouvertes, accessibles sans restrictions. Dans ces blockchains publiques, la décentralisation du contrôle est totale. Il s'agit du modèle utilisé dans le cadre des cryptomonnaies, par exemple.

Progressivement, certains opérateurs ont cherché à s'approprier les avantages de la technologie blockchain, en reproduisant tout ou partie

[32] Voy. dans cet ouvrage la contribution de J.-N. COLIN, « Du Bitcoin aux DAO : les fondations techniques de la blockchain », p. 10.

[33] *Idem*, p. 10.

[34] Voy. *infra*, n° 20.

[35] J.-N. COLIN, *op. cit.*, p. 15.

quentin.houbion@unamur.be
La preuve par la blockchain
Éditions Larcier - © Larcier - 30/10/2020

strada lex

de son fonctionnement, tout en restreignant l'accès à la base de données à un nombre déterminé d'utilisateurs préalablement identifiés. Ceux-ci disposent d'un *nœud* connu et authentifié par la blockchain[36]. C'est ainsi qu'ont émergé des blockchains dites « privées », qui reproduisent tout ou partie des caractéristiques des blockchains publiques. Dans ces blockchains privées, il existe généralement « une autorité régulatrice » qui valide l'entrée des membres, sur la base de règles préalablement déterminées et acceptées par eux, et leur donne la possibilité de lire la blockchain et d'y inscrire certaines informations[37]. En raison de son attractivité, le terme « blockchain privée » est employé pour désigner différentes formes de bases de données, sans qu'il soit parfois possible de dégager un socle de caractéristiques communes à celles-ci. Le juriste doit par conséquent être attentif au fonctionnement et aux caractéristiques de la base de données, plutôt qu'à l'appellation « blockchain » qui peut parfois lui être trop rapidement attribuée.

SECTION 2. – La preuve par la blockchain : admissibilité de la blockchain en tant que mode de preuve

13. Régime de preuve libre ou régime de preuve réglementé. Afin d'apprécier si les données enregistrées dans une blockchain sont admissibles en tant que mode de preuve, il faut en premier lieu déterminer si l'allégation qui doit être prouvée est soumise à un régime de preuve libre ou de preuve réglementée[38].

Lorsque la preuve est libre, toutes les informations procurées par la blockchain peuvent être soumises au juge – ne fût-ce qu'à titre de présomption – et c'est au magistrat qu'il appartient de fixer la valeur probante qu'il attache à celles-ci, sur la base des explications qui lui sont fournies par les parties. On peut considérer que l'appréciation du juge sera fonction de la fiabilité qu'il reconnaît au procédé technologique utilisé. En effet, s'il est confronté à une blockchain présentant de fortes garanties relatives à l'authenticité des données qu'elle contient, le juge devrait reconnaître la valeur probante de ces informations. Il est donc primordial, pour la partie qui se prévaut d'une information enregistrée dans une

[36] *Idem*, p. 12.

[37] V. Faure-Muntian, C. de Ganay et R. Le Gleut, *Rapport sur les enjeux technologiques des blockchains (chaînes de blocs)*, *op. cit.*, p. 54.

[38] Voy. *supra*, n° 7.

quentin.houbion@unamur.be
La preuve par la blockchain
Éditions Larcier - © Larcier - 30/10/2020

strada lex

blockchain, de bien documenter le tribunal au sujet des caractéristiques de cette blockchain. Son contradicteur veillera, pour sa part, à mettre en évidence les éventuels points faibles de la blockchain en termes de sécurité et de fiabilité. Le cas échéant, une expertise pourrait être ordonnée afin de vérifier, sur le plan technique, l'authenticité des informations issues de la blockchain.

Lorsque le régime de la preuve réglementée s'applique, et qu'un acte juridique doit être prouvé dans le respect de la règle de prééminence de l'écrit, il faut déterminer si les informations contenues dans la blockchain peuvent être assimilées à des écrits signés[39]. À défaut, elles ont la valeur d'un commencement de preuve par écrit, s'il peut être établi qu'elles émanent de la personne qui conteste l'acte juridique ou de celui qu'il représente, ou d'une présomption. Si les données sont qualifiées de commencement de preuve par écrit, elles permettent à la partie qui s'en prévaut de rapporter la preuve de ce qu'elle cherche à établir par tous moyens de preuve. Si elles sont qualifiées de présomption, elles ne permettent pas de faire la preuve de l'acte que l'on cherche à démontrer, à moins que la valeur de cet acte ne dépasse pas 375 euros (3.500 euros à compter du 1er novembre 2020).

14. Régime d'ordre supplétif. En toute hypothèse, dès lors que le régime de la preuve est d'ordre supplétif, et pour autant qu'une telle disposition ne soit pas abusive, les parties à un acte peuvent convenir de donner force probante aux informations contenues dans une blockchain. À titre d'exemple, les membres d'une blockchain privée pourraient s'engager, dans le règlement des opérations de ladite blockchain, à reconnaître la force probante des données stockées au sein de celle-ci, quelle que soit la nature de l'élément à prouver. Ceci démontrerait le niveau de confiance que les membres de la blockchain lui accordent.

15. Difficultés d'ordre technique. D'un point de vue technique, la blockchain ne contient qu'une empreinte cryptée d'un fichier original. Les données inscrites dans la blockchain sont en effet reprises, sous forme d'empreinte cryptée, dans des blocs horodatés, qui se lient les uns aux autres, à l'image d'une chaîne. L'opération de chiffrement a pour effet de transformer le fichier original en une suite de données *a priori* inintelligibles[40]. L'empreinte doit nécessairement pouvoir être décryptée pour pouvoir accéder au contenu du fichier original.

En raison de cette opération de cryptage inhérente au fonctionnement de la blockchain, des discussions pourraient s'élever, en vue de contester

[39] Voy. *Infra*, nos 16-17.
[40] J.-N. Colin, *op. cit.*, p. 15.

quentin.houbion@unamur.be
La preuve par la blockchain
Éditions Larcier - © Larcier - 30/10/2020

strada lex

que l'empreinte numérique enregistrée dans la blockchain corresponde effectivement à l'information dont une partie veut rapporter la preuve en justice. Face à ce type de contestation, et pour autant que celle-ci apparaisse pertinente, le recours à une expertise paraît être l'issue la plus probable. En effet, « pour faire la preuve du document et le rapprocher de celui ayant fait l'objet de l'ancrage à un instant, il faut donc recommencer l'opération, ce qui suppose que le document d'origine ait été conservé sans la moindre altération (...) Il faut rééditer l'opération de *hashage* du document d'origine et faire constater que le hash obtenu est identique à celui figurant sur le certificat de preuve blockchain fourni par le demandeur »[41]. En principe, seul un expert disposant des compétences informatiques requises est en mesure de mettre en œuvre ce type d'opération en vue d'éclairer un tribunal. Au vu du coût que peut présenter une telle expertise, ce genre de contestation, si elle devait se généraliser, pourrait dissuader les parties d'avoir recours à la blockchain en tant que mode de preuve, en particulier dans le cas de litiges présentant un enjeu de faible valeur.

Afin de contourner cet écueil, on pourrait concevoir que la blockchain soit en mesure de procurer par elle-même une forme de certification de l'information stockée. Ceci pose une nouvelle fois la question du crédit que le tribunal peut accorder à la technologie en elle-même. Une telle fonction revient par ailleurs à faire jouer à la blockchain un rôle proche de celui d'un prestataire de services de confiance. Nous reviendrons sur l'interaction entre la blockchain et les services de confiance ci-dessous[42].

SECTION 3. – La preuve par la blockchain : nature et qualification de l'information fournie par la blockchain

16. Les données de la blockchain pourraient constituer des écrits. Au vu des caractéristiques qu'elle présente, la blockchain peut être comparée à une forme de support dans lequel les données enregistrées seraient assimilées à des écrits. Les fonctions assurées par la blockchain permettent en effet de rencontrer les exigences assignées à l'écrit :

– Intelligibilité : À condition de pouvoir faire usage d'un programme informatique permettant de décrypter le hash enregistré, les données inscrites dans la blockchain sont intelligibles.

[41] S. Legrand, « Enjeux de la blockchain du point de vue du praticien », *Dalloz IP/IT*, février 2019, p. 91.

[42] Voy. *infra*, n° 23.

quentin.houbion@unamur.be
La preuve par la blockchain
Éditions Larcier - © Larcier - 30/10/2020

strada lex

– Durabilité : Les données inscrites dans la blockchain ne peuvent être supprimées, puisqu'elles sont inscrites dans des blocs auxquels se superposent de nouveaux blocs. Les informations stockées dans la blockchain présentent donc un caractère immuable.
– Intégrité : La blockchain est utilisée comme un instrument permettant d'authentifier des données. Sa structure implique que chaque nouvelle donnée soit contrôlée et validée par l'ensemble des ordinateurs du réseau, avant d'être intégrée à la base de données. Pour pouvoir porter atteinte à l'intégrité de la blockchain, il faudrait pouvoir prendre le contrôle d'une majorité de *nœuds* du réseau. Ainsi, plus la blockchain contient de membres, plus elle offre de garanties d'intégrité.

17. Les données inscrites dans la blockchain ne sont en principe pas signées. La signature électronique est définie, à l'article 3, 10°, du règlement eIDAS 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 ». Le règlement eIDAS ne précise toutefois pas ce que désigne le terme « signer ». À défaut d'avoir fait l'objet d'une harmonisation européenne, ce concept doit être défini conformément au droit national. En droit belge, l'article 8, 2°, du nouveau Code civil définit la signature comme « un signe ou une suite de signes tracés à la main, par voie électronique ou par un autre procédé, par lesquels une personne s'identifie et manifeste sa volonté ». Il est important de préciser que la fonction d'identification de la signature, telle qu'elle résulte de l'article 8, 2°, doit permettre d'imputer la signature à une personne déterminée[43].

Dans la blockchain, chaque utilisateur doit s'authentifier pour pouvoir passer une opération. Ceci est réalisé par la voie de la cryptographie asymétrique : chaque utilisateur de la blockchain détient une clé publique, qui est liée à une adresse électronique faisant office d'identifiant sur le réseau, et une clé privée, intrinsèquement liée à sa clé publique, qui lui permet de réaliser des opérations qui lui sont propres[44]. Lorsqu'il enregistre une opération dans la blockchain, l'utilisateur est authentifié par sa clé publique. Dans la plupart des blockchains, l'adresse électronique liée à la clé publique des utilisateurs n'identifie pas une personne déterminée,

[43] Projet de loi portant insertion du Livre 8 « La preuve » dans le nouveau Code civil, *Doc. parl.*, Ch. Repr., sess. 2018-2019, n° 54-3349/001, p. 6.

[44] X., *Rapport d'information déposé en application de l'article 145 du Règlement par la Mission d'information commune sur les chaînes de blocs (blockchains)*, 12 décembre 2018, p. 16, http://www.assemblee-nationale.fr/15/pdf/rap-info/i1501.pdf.

quentin.houbion@unamur.be
La preuve par la blockchain
Éditions Larcier - © Larcier - 30/10/2020

strada lex

mais un point du réseau. Ainsi, les acteurs de la blockchain agissent généralement sous un pseudonyme, et non sous leur identité réelle.

En droit belge, l'utilisation d'un pseudonyme à titre de signature ne prive pas nécessairement celle-ci de ses effets juridiques[45]. C'est ainsi que la signature ne doit pas nécessairement porter le nom patronymique de son auteur, pour autant néanmoins que la marque utilisée soit celle par laquelle le signataire « révèle habituellement sa personnalité aux tiers »[46]. Plusieurs auteurs ont souligné que la signature devait exprimer la volonté de s'identifier de son titulaire. C'est l'*animus signandi* qui est l'élément déterminant. L'existence de cet élément est soumise à l'appréciation souveraine du juge[47].

L'utilisation de pseudonymes est également envisagée par le règlement eIDAS. C'est ainsi qu'il est prévu que le certificat de signature électronique peut renseigner le pseudonyme d'une personne physique, plutôt que son nom patronymique[48]. Toutefois, en droit belge, l'article XII.26 du Code de droit économique prévoit que lorsque le titulaire d'un certificat de signature électronique utilise un pseudonyme, le prestataire de services de confiance ayant délivré le certificat est tenu de communiquer aux autorités compétentes, à leur demande, les informations relatives à l'identité du titulaire dont il dispose. Ainsi, dans le régime actuel, le fait de signer par voie électronique sous un pseudonyme ne garantit pas l'anonymat du signataire. La fonction d'identification du signataire n'est donc pas remise en cause par la signature électronique sous pseudonyme.

Dans le contexte de la blockchain, si le fait d'utiliser la cryptographie asymétrique permet à l'émetteur d'une opération de manifester sa volonté, ce procédé ne permet pas, par contre, de l'identifier. Une caractéristique essentielle des blockchains publiques – en particulier des monnaies virtuelles – est l' « anonymat » qu'elles procurent à leurs utilisateurs : lorsqu'ils inscrivent une opération dans la blockchain, ces derniers ne sont pas tenus de s'identifier. Il a à cet égard été relevé que, dans les blockchains, « on ne peut identifier le propriétaire d'une clé publique, mais si le lien est fait, on peut alors retracer toutes les transactions qu'il a reçues et envoyées »[49]. À défaut d'identification de leur auteur, il faut considérer

---

[45] Voy. D. Mougenot, « La preuve », *op. cit.*, n^os^ 110 et 111.

[46] Cass., 7 janvier 1955, *Pas.*, 1955, I, p. 456.

[47] M. Puelinckx-Coene, « Vorm de vereiste van handtekening de valstrik van het eigenhandig testament », *T. Not.*, 1986, p. 319 ; P. Delnoy, « Les libéralités (1981-1987) », *J.T.*, 1989, p. 343.

[48] Art. 3, 14° du règlement eIDAS.

[49] V. Faure-Muntian, C. de Ganay et R. Le Gleut, *Rapport sur les enjeux technologiques des blockchains (chaînes de blocs)*, *op. cit.*, p. 25.

quentin.houbion@unamur.be
La preuve par la blockchain
Éditions Larcier - © Larcier - 30/10/2020

strada lex

que les informations figurant dans la blockchain ne sont pas signées[50]. Le fait d'authentifier l'opération ne traduit en effet pas un *animus signandi* dans le chef de l'utilisateur de la blockchain.

Par contre, si les utilisateurs sont identifiés au moment où ils inscrivent une opération dans la blockchain – comme c'est notamment le cas dans certaines blockchains privées – on pourrait considérer, en fonction des règles de gouvernance de la blockchain – en vertu desquelles l'identification de l'utilisateur devrait avoir pour effet d'exprimer son consentement – que les informations inscrites portent une signature électronique : dans cette hypothèse, le recours à la cryptographie asymétrique permet en effet d'identifier l'auteur de l'opération, qui pourrait ainsi être réputé avoir manifesté son adhésion à celle-ci.

Puisque la blockchain tend, en principe, à s'affranchir du recours aux prestataires de services de confiance[51], et à moins que le règlement des opérations de la blockchain concernée impose le recours à un procédé de signature électronique qualifiée au sens du règlement eIDAS, le procédé utilisé à titre de signature électronique ne constituera pas une signature électronique qualifiée, en dépit du recours à la cryptographie asymétrique. En fonction des caractéristiques présentées par ce procédé électronique, il pourra être qualifié soit de signature électronique ordinaire, soit – très vraisemblablement – de signature électronique avancée. À condition que l'on se trouve dans le champ d'application du règlement eIDAS[52], cette signature électronique pourra bénéficier du principe de non-discrimination prévu par l'article 25 du règlement. Ceci implique que la partie qui entend s'en prévaloir devra encore démontrer que le procédé utilisé rencontre les fonctions d'identification et d'adhésion de la signature.

18. Les informations contenues dans la blockchain sont horodatées. L'horodatage électronique est défini à l'article 3, 33°, du règlement eIDAS comme un procédé électronique qui associe des données sous forme électronique à d'autres données sous forme électronique à un instant particulier et qui établit la preuve que ces dernières données existaient à cet instant.

Les protocoles des blockchains comportent des fonctions d'horodatage afin que chaque information inscrite dans un bloc et chaque nouveau bloc soient fixés de manière précise dans le temps. Cette fonction

[50] X., *Rapport d'information déposé en application de l'article 145 du Règlement par la Mission d'information commune sur les chaînes de blocs (blockchains)*, 12 décembre 2018, p. 91, http://www.assemblee-nationale.fr/15/pdf/rap-info/i1501.pdf.

[51] Voy. *infra*, n° 21.

[52] Voy. *infra*, n° 23.

quentin.houbion@unamur.be
La preuve par la blockchain
Éditions Larcier - © Larcier - 30/10/2020

strada lex

d'horodatage est un aspect essentiel de la blockchain, parce qu'elle permet de donner une chronologie aux informations enregistrées[53]. Elle est indispensable pour lier les blocs entre eux et ainsi donner son authenticité à la blockchain.

L'horodatage est une des propriétés les plus intéressantes de la blockchain dans le contexte probatoire. Bien que ce procédé ne puisse conférer date certaine à un acte au sens de l'article 1328 du Code civil (article 8.22 du nouveau Code civil), il permet néanmoins de fixer dans le temps, de manière réputée infalsifiable, les informations inscrites dans la blockchain. Il peut être envisagé d'y recourir, par exemple, pour régler une contestation quant à l'antériorité d'un titre, ou pour retracer la chronologie d'une opération complexe.

19. La blockchain et l'archivage électronique. D'un point de vue technique, la blockchain opère une forme d'archivage des données, puisqu'elle garantit la conservation de leur empreinte, sans risque d'altération, pendant une période indéterminée.

En droit belge, le concept d'archivage électronique est défini à l'article I.18, 17° du Code de droit économique comme « un service de confiance supplémentaire à ceux visés par l'article 3, paragraphe 16, du règlement 910/2014, qui consiste en la conservation de données électroniques ou la numérisation de documents papiers ». Le service d'archivage électronique peut être fourni par un prestataire de services de confiance au sens du règlement eIDAS ou être exploité pour son propre compte par un organisme du secteur public ou par une personne physique ou morale.

De notre point de vue, si une entité exploite un service d'archivage électronique pour son propre compte, elle aura recours à un système de conservation des documents en interne. On imagine par conséquent difficilement qu'un organisme du secteur public ou une personne physique ou morale utilise la blockchain en vue de déployer un service d'archivage électronique exclusivement pour son propre compte.

Par ailleurs, dans l'hypothèse de la fourniture d'un service d'archivage électronique, par un prestataire de service, à des tiers, le recours à une forme de blockchain pose la question du statut de ce prestataire de service. Pour que l'archivage blockchain se voie conférer les effets juridiques d'un archivage électronique prévus par le Code de droit économique, il faut qu'il soit fourni par un prestataire de services de confiance au sens du règlement eIDAS. Nous analysons, dans la dernière section de cet article, les liens que la blockchain entretient avec les services de confiance.

[53] V. Faure-Muntian, C. de Ganay et R. Le Gleut, *Rapport sur les enjeux technologiques des blockchains (chaînes de blocs)*, *op. cit.*, p. 26.

quentin.houbion@unamur.be
La preuve par la blockchain
Éditions Larcier - © Larcier - 30/10/2020

strada lex

CHAPITRE 3. Blockchain et services de confiance

20. Notion de service de confiance. Comme cela a été exposé ci-dessus, dans l'environnement numérique, c'est le recours aux services de confiance qui a permis de rencontrer les exigences formelles imposées par le droit de la preuve[54].

Les services de confiance recouvrent un ensemble de procédés électroniques, proposés par des prestataires indépendants, qui sont utilisés en vue de certifier la fiabilité d'une information présentée sous forme de données électroniques. Selon le règlement eIDAS, le concept de « service de confiance » désigne un service électronique normalement fourni contre rémunération qui consiste (i) en la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, de services d'envoi recommandé électronique et de certificats relatifs à ces services; ou (ii) en la création, en la vérification et en la validation de certificats pour l'authentification de site internet; ou (iii) en la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services[55].

L'article 19 du règlement eIDAS impose aux prestataires de services de confiance de prendre les mesures techniques et organisationnelles adéquates pour gérer les risques liés à la sécurité des services qu'ils fournissent. En outre, les prestataires de services de confiance qualifiés font l'objet d'un contrôle qui vise à vérifier qu'ils respectent les exigences du règlement eIDAS. Conformément à l'article 17 du règlement, ce contrôle est effectué par un organe de contrôle désigné par chaque État membre. En Belgique, l'organe de contrôle est créé au sein du SPF Économie[56]. Le contrôle des prestataires de service de confiance qualifiés est donc directement assuré par le pouvoir exécutif.

Ainsi, dans le système actuel, la fiabilité des informations échangées par voie électronique est assurée par une réglementation normative, dont le contrôle est assuré par une autorité dépendant des pouvoirs publics s'agissant des services de confiance qualifiés.

21. Blockchain et services de confiance. La blockchain opère une désintermédiation des échanges électroniques et rompt, de ce fait, avec le système de certification consacré par le règlement eIDAS. En effet, cette

[54] Voy. *supra*, n° 9.
[55] Art. 3, 16°, du règlement eIDAS.
[56] Art. I.18, 16, du Code de droit économique.

quentin.houbion@unamur.be
La preuve par la blockchain
Éditions Larcier - © Larcier - 30/10/2020

strada lex

technologie n'a pas recours à un prestataire externe, soumis au respect d'un cadre réglementaire précis et à l'autorité d'organes de contrôle, pour certifier les services électroniques offerts et susciter la confiance de leurs utilisateurs. Dans la blockchain, c'est la technologie en elle-même qui garantit la fiabilité des informations échangées, en raison de son fonctionnement, centré sur le comportement de ses utilisateurs et résultant d'un consensus entre eux. La blockchain constitue donc en elle-même une forme de mécanisme de confiance, qui s'affranchit de la nécessité d'une certification par des organismes tiers. Son caractère infalsifiable, qui résulte de la confiance mutuelle que s'accordent ses utilisateurs, en raison des caractéristiques du système qu'ils utilisent, rend inutile l'intervention d'un prestataire externe de service de confiance[57].

22. La blockchain peut avoir recours à des services de confiance. Certains procédés électroniques utilisés dans le cadre de la blockchain sont également au cœur du fonctionnement des services de confiance. C'est ainsi que la cryptographie asymétrique, qui permet de sécuriser les opérations inscrites dans la blockchain et lui confère son caractère infalsifiable, est utilisée par les prestataires de services de confiance qualifiés, par exemple pour l'émission de certificats qualifiés de signature électronique.

En principe, les blockchains publiques n'imposent pas à leurs utilisateurs de recourir à des services de confiance déterminés au sens du règlement eIDAS. Rien n'empêcherait cependant qu'une telle exigence soit fixée dans les règles de gouvernance de la blockchain. De même, dans le cadre d'une blockchain privée, les membres de la communauté pourraient s'imposer de recourir à des services de confiance pour garantir le bon fonctionnement de la blockchain.

23. La blockchain en tant que prestataire de services de confiance. De manière paradoxale, au vu des propriétés de désintermédiation qui lui sont reconnues, la technologie blockchain pourrait être assimilée à une forme de service de confiance, pour ses fonctions d'horodatage ou d'archivage par exemple.

Plusieurs obstacles juridiques rendent toutefois la blockchain difficilement compatible, pour l'instant, avec un service de confiance au sens du règlement eIDAS.

S'agissant des blockchains publiques, celles-ci sont constituées d'une communauté d'utilisateurs, qui participent à son fonctionnement et garantissent la fiabilité de la base de données. Comme cela a été exposé,

[57] V. Faure-Muntian, C. de Ganay et R. Le Gleut, *Rapport sur les enjeux technologiques des blockchains (chaînes de blocs)*, *op. cit.*, p. 19.

quentin.houbion@unamur.be
La preuve par la blockchain
Éditions Larcier - © Larcier - 30/10/2020

strada lex

il n'y a pas d'autorité qui supervise et contrôle le fonctionnement de la blockchain. Cette communauté d'utilisateurs peut difficilement être assimilée à un prestataire de service de confiance, défini par l'article 3, 19° du règlement eIDAS comme « une personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de confiance qualifié ou non qualifié », sauf à considérer que « tous les membres de la communauté, en ce qu'ils forment une association de fait sans personnalité juridique, doivent être qualifiés de prestataire de services de confiance »[58]. Comme le relèvent MM. Jacquemin et Poullet, une telle éventualité, qui rompt tant avec l'esprit des blockchains publiques, que du règlement eIDAS, est difficilement concevable en pratique[59].

Dans le cadre des blockchains privées, l'infrastructure technologique est généralement fournie par un prestataire externe qui, à l'instar d'un prestataire de services de confiance, garantit le fonctionnement de la blockchain à ses membres, ainsi que l'authenticité des informations qui y sont inscrites. Toutefois, en vertu de son article 2, le règlement eIDAS « ne s'applique pas à la fourniture de services de confiance utilisés exclusivement dans des systèmes fermés résultant du droit national ou d'accords au sein d'un ensemble défini de participants ». Le considérant n° 21 du règlement précise que celui-ci « ne devrait pas couvrir la fourniture de services utilisés exclusivement dans des systèmes fermés au sein d'un ensemble défini de participants, qui n'ont pas d'effets sur des tiers » et que « seuls les services de confiance fournis au public ayant des effets sur les tiers devraient remplir les exigences du présent règlement ». Il a en effet été souligné que « dans un système fermé où, normalement, les parties se connaissent (et ont encadré leur relation par l'adoption de dispositions contractuelles), il n'est pas requis de recourir à un tiers de confiance »[60]. Or, les blockchains privées apparaissent comme des systèmes fermés rassemblant une communauté de participants s'étant préalablement entendus sur les règles de gouvernance de la blockchain. Les services proposés dans le cadre de blockchains privées peuvent donc difficilement se voir qualifier de services de confiance, parce qu'ils sortent du champ d'application du règlement eIDAS.

En l'état, les effets juridiques attachés par le règlement eIDAS aux différents services de confiance qu'il règlemente paraissent donc ne pas pouvoir s'appliquer à la blockchain. La reconnaissance, sur le plan juridique,

[58] H. Jacquemin et Y. Poullet, « Blockchain : une révolution pour le droit ? », *J.T.*, 2018, p. 812.

[59] *Ibid.*, pp. 812-813.

[60] H. Jacquemin, « Principes applicables à tous les services de confiance et au document électronique », *op. cit.*, p. 108.

quentin.houbion@unamur.be
La preuve par la blockchain
Éditions Larcier - © Larcier - 30/10/2020

strada lex

du mécanisme de confiance que constitue la blockchain doit passer soit par des initiatives nationales[61], soit par une révision du règlement eIDAS. À cet égard, nous relevons que l'article 49 du règlement prévoit que celui-ci doit faire l'objet d'un réexamen visant à évaluer s'il convient de modifier son champ d'application ou ses dispositions spécifiques. Nul doute que la blockchain constituera une question centrale de ce réexamen. On peut d'ailleurs déjà relever que le considérant n° 62 du règlement peut être interprété comme une forme timide d'ouverture en ce sens. Il stipule, en effet, en traitant de l'horodatage électronique : « Il est à prévoir que l'innovation pourrait déboucher sur de nouvelles technologies susceptibles d'assurer un niveau de sécurité équivalent pour les horodatages ».

CHAPITRE 4. Conclusion

24. Si la blockchain rompt en principe, par son mode de fonctionnement décentralisé, affranchi du contrôle d'une autorité, avec le régime des services de confiance, il a été démontré dans la présente contribution qu'il était néanmoins envisageable, dans de nombreuses hypothèses, d'avoir recours aux informations contenues dans les blockchains en vue de faire la preuve d'allégations contestées en justice. Au vu de la neutralité des concepts utilisés dans le Code civil, les données enregistrées dans la blockchain paraissent admissibles en tant qu'éléments de preuve. Selon les cas, elles auront le statut de présomption de fait ou de commencement de preuve par écrit, ou accèderont au statut d'écrit signé.

À nos yeux, une incertitude majeure subsiste néanmoins quant au succès que rencontrera la blockchain, si son usage se généralise, dans le contentieux judiciaire. Elle est liée à l'ampleur des opérations de décryptage à mettre en œuvre pour faire le lien entre l'empreinte (« *hash* ») enregistrée dans les blocs et le fichier électronique contenant l'information invoquée à titre de preuve. Si ces opérations de décryptage devaient s'avérer excessivement complexes, et difficiles à documenter, elles pourraient constituer une entrave à l'emploi de la blockchain comme instrument de preuve. À

[61] C'est ainsi qu'en Italie, l'article 8*ter* de la loi n° 12/19 du 11 janvier 2019 relative au soutien et à la simplification des entreprises et de l'administration publique entend conférer un statut juridique à l'horodatage blockchain, en lui attachant les mêmes effets que l'horodatage électronique tels que prévus à l'article 41 du règlement eIDAS. Voy. à ce sujet A. Barbet-Massin, « Réflexions autour de la reconnaissance juridique de l'horodatage blockchain par le législateur italien », *R.L.D.I.*, n° 157, 2019, pp. 40-43.

quentin.houbion@unamur.be
La preuve par la blockchain
Éditions Larcier - © Larcier - 30/10/2020

strada lex

titre d'alternative, on pourrait songer à mettre en place des procédés techniques qui permettraient à la blockchain de fournir, par elle-même, une forme de certification de l'information stockée. Ceci rapprocherait alors les fonctions de la blockchain de celle d'un service de confiance.

Une évolution du cadre légal devrait par ailleurs être réfléchie, dans une perspective de neutralité technologique, en vue de faire correspondre les effets juridiques de la blockchain à ceux qui sont conférés par le règlement eIDAS aux services de confiance.

quentin.houbion@unamur.be
La preuve par la blockchain
Éditions Larcier - © Larcier - 30/10/2020