La blockchain comme outil probatoire : une analyse au regard de la LCCJTI

Erwan JONCHÈRES et Soleïca MONNIER[1]

Résumé

La blockchain, plus particulièrement celle à caractère public, est une technologie permettant la tenue d'un registre décentralisé, transparent, immuable et infalsifiable. Un bloc de la chaîne — équivalent numérique d'une page d'un registre papier — peut contenir des données informationnelles telle l'empreinte numérique associée à un document. La combinaison de ces deux processus permet ainsi de garantir, à coût modique, l'état d'un document à un moment donné et, incidemment, la preuve du maintien de son intégrité dans le temps. Or, le talon d'Achille du document technologique réside justement dans la difficulté de garantir son intégrité, les falsifications étant aisées tout en étant difficilement détectables. L'utilisation de la blockchain à des fins probatoires constitue donc une avenue à haut potentiel pour le système judiciaire et les institutions qui réfléchissent à des solutions de gestion documentaire innovantes. C'est pourquoi de nombreuses initiatives émergent déjà à l'international, notamment en droit d'auteur ou dans l'identification de contenu vidéo falsifié (par exemple, les *deepfakes*).

Bien qu'alléchante en théorie, l'idée de fixer la preuve documentaire sur une blockchain publique souffre toutefois de lacunes importants en lien avec l'environnement « technologique » qui soutient l'activité des tribunaux au Québec. En effet, l'analyse juridique effectuée nous porte à croire que le cadre juridique actuel saurait appréhender la technologie blockchain à des fins probatoires, mais la disponibilité du matériel judiciaire, ainsi que l'expertise requise à sa compréhension, seraient à l'origine d'un certain désenchantement.

1 Les auteurs Me Erwan Jonchères (erwan@joncheres.ca) et Me Soleïca Monnier (Ministère de la Justice du Québec) tiennent à remercier Me Vincent Gautrais (Université de Montréal), Me Nareg Froundjian (Deloitte Legal) pour leurs commentaires lors de la rédaction de l'article. Les opinions exprimées dans le présent article n'engagent que les auteurs et ne représentent pas nécessairement celles de leurs employeurs respectifs.

Ultimement, ce constat est révélateur du paradoxe technologique dans lequel la Belle Province vit : tout en étant un *hub* de l'intelligence artificielle, son système judiciaire pourrait bénéficier d'une utilisation accrue de la technologie. Le cadre juridique québécois étant prêt à amorcer le virage technologique, il nous tarde que les investissements récents permettent aux institutions judiciaires de prendre ce virage au Québec.

Avertissement

Cet article ne constitue pas une critique de la blockchain comme technologie, par exemple, au regard de son impact fluctuant sur l'écologie, de la volatilité des cryptomonnaies, des possibilités de piratages, de ses usages frauduleux ou encore de l'immuabilité des renseignements qui y sont inscrits. Il constitue une perspective des potentialités de la blockchain pour le droit probatoire.

INTRODUCTION

Il y a des natures purement contemplatives et tout à fait impropres à l'action, qui cependant, sous une impulsion mystérieuse et inconnue, agissent quelquefois avec une rapidité dont elles se seraient crues elles-mêmes incapables.

- Charles Baudelaire[2]

Ces dernières années, une technologie garantissant un des plus hauts degrés de sécurité informatique a monopolisé le débat au sein des gouvernements, des administrations, des entreprises et, plus généralement, de la société civile. Cette technologie, appelée « blockchain », est actuellement utilisée pour effectuer des transactions, échanger des titres, déposer des documents ou encore exécuter des contrats dits « intelligents » (*smart contracts*).

Par exemple, en France, le 12 mai 2019, EDF, Engie, La Poste et la Caisse des Dépôts révélaient une méthode pour authentifier certains justificatifs

2 Le mauvais vitrier, 1869.

émis sous leur signature.[3] Technologie phare du projet, la blockchain permettrait à ces quatre organisations d'éliminer une fraude évaluée à plus de 8 milliards d'euros en 2017. Cette initiative privée française est dans la lignée d'une proposition (toutefois demeurée lettre morte) qui voulait ajouter un alinéa à l'article L330-1 du *Code monétaire et financier*, afin de conférer le statut d'actes authentiques aux opérations effectuées sur un registre décentralisé permanent et infalsifiable utilisant la blockchain.[4] Au Royaume-Uni, le ministère de la Justice enquête sur la possibilité d'utiliser la blockchain comme outil de sécurisation des formes numériques de preuve.[5] Bref, l'actualité internationale récente abonde en utilisations novatrices de la blockchain pour permettre une plus grande sécurité documentaire. Ce constat met la puce à l'oreille quant au potentiel probatoire de cette technologie au Québec.

Sur le territoire de la Belle Province, le droit de la preuve est régi par le Code civil du Québec et par une loi adoptée en 2001 intitulée la *Loi concernant le cadre juridique des technologies de l'information*[6] [ci-après « LCCJTI »]. Lors de son adoption, la LCCJTI avait fait l'objet de critiques. Les transcriptions des débats parlementaires[7] et les déclarations rapportées dans le rapport du Barreau du Québec[8] en témoignent. Parmi les critiques formulées, le vocable influencé par la bibliothéconomie et d'autres sciences est notamment pointé du doigt.

En dépit de cette ambiguïté législative,[9] le domaine des nouvelles technologies demeure en pleine expansion ; pensons intelligence artificielle, réalité virtuelle ou encore blockchain, défraient fréquemment la chronique. Tous font appel à une combinaison de technologies sur des

3 Anne Drif, « Blockchain : EDF, Engie, La Poste et la CDC s'allient contre la fraude », *Les échos*, 12 mai 2019, en ligne : <https://www.lesechos.fr/finance-marches/banque-assurances/blockchain-grande-alliance-publique-contre-la-fraude-aux-documents-1018046>.

4 *Amendement n° 277* relatif à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (France), 1er juin 2016, en ligne : <http://www.assemblee–nationale.fr/14/amendements/3785/AN/227.asp>.

5 David Hundeyin, « UK Government Pilots Storage of Digital Evidence on a Blockchain », *ccn.com*, 26 août 2018, en ligne : <https://www.ccn.com/uk-government-pilots-storage-of-digital-evidence-on-a-blockchain>.

6 RLRQ, c. C-1.1.

7 Québec, Assemblée nationale, *Journal des débats, Commissions parlementaires*, Commission de l'économie et du travail, 2e sess., 36e légis., 22 mai 2001, « Étude détaillée du projet de loi n° 161 - Loi concernant le cadre juridique des technologies de l'information ».

8 Barreau du Québec, *Mémoire sur la Loi sur la normalisation juridique des nouvelles technologies de l'information,* 2000, en ligne : <https://www.lccjti.ca/files/sites/105/2013/08/MEMOIREBARREAU2000.pdf>.

9 À titre illustratif, voir Léo Ducharme, « De l'incohérence et de l'impossibilité d'application du régime dérogatoire en matière de preuve des documents technologiques », (2016) 75 *R. du B.* 319, 319 : « La présente étude vise à démontrer, dans une première partie, que ce régime dérogatoire est incohérent et, dans une deuxième partie, qu'il est inapplicable. »

supports eux-mêmes technologiques.[10] Dans leurs formes les plus primaires également, les technologies de l'information sont omniprésentes. Au travail, nous numérisons, imprimons ou réalisons des photocopies de documents. Côté divertissement, nous passons la journée rivés sur les écrans de nos portables, nos ordinateurs ou encore nos téléviseurs. Et afin de communiquer, nous utilisons des téléphones toujours plus intelligents. Le nombre d'objets technologiques est devenu inestimable. Et pour cause : l'heure est à la transition numérique d'objets traditionnellement appréhendés sur un support papier.[11]

Or cette transition numérique devrait être régie par la LCCJTI, mais très peu la connaissent, la comprennent et la mettent en œuvre. Cette réflexion se veut donc une contribution à cet effort de réconciliation du cadre juridique québécois avec les utilisateurs et concepteurs du monde numérique contemporain. Plus particulièrement, l'objectif est de renseigner le lectorat sur, d'une part, le potentiel inédit qu'offre la blockchain en matière de preuve technologique et, d'autre part, sur la manière dont ce potentiel peut être capturé par les lois en vigueur au Québec.

142

1. LA BLOCKCHAIN : ÉTAT DES LIEUX

Note au lecteur non initié : au besoin, l'Office québécois de la langue française a élaboré, avec la collaboration de l'Autorité des marchés financiers, de l'École de technologie supérieure ainsi que de l'Académie Bitcoin, un vocabulaire portant sur près d'une centaine de concepts, consacré à la terminologie des chaînes de blocs et de la cryptomonnaie.[12]

1.1. HISTORIQUE ET PRÉCISIONS TERMINOLOGIQUES

Comme mentionné, plusieurs gouvernements se penchent sur la possibilité d'utiliser la blockchain à des fins probatoires ou de gestion documentaire. Avant de découvrir différents cas d'usage de la technologie, il est primordial de comprendre pourquoi celle-ci plutôt qu'une autre.

10 LCCJTI, art. 1, par. 2, qui réfère aux « technologies de l'information, qu'elles soient électronique, magnétique, optique, sans fil ou autres ou faisant appel à une combinaison de technologies ».

11 Par exemple, certains documents dont la loi a jusqu'alors exigé la signature manuscrite sont présentement réinventés (actes de procédure dans le cadre de la transformation organisationnelle de la justice, actes notariés).

12 Office québécois de la langue française, « Vocabulaire de la cryptomonnaie », 18 octobre 2019, en ligne : <https://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/vocabulaire-cryptomonnaie.aspx >.

Voilà plus de 10 ans que le mystérieux Satoshi Nakamoto[13] a dévoilé une technologie disruptive en code ouvert : la blockchain, d'abord utilisée pour sécuriser le Bitcoin[14], première cryptomonnaie. L'objectif alors était de permettre les échanges de monnaie numérique sans tiers de confiance, c'est-à-dire à l'aide de méthodes de chiffrement et de protocoles de transmission impliquant de multiples vérificateurs.[15] Ainsi, deux individus qui ne se connaissaient pas pouvaient désormais transiger en ligne sans avoir à bâtir de lien de confiance.

La technologie blockchain s'est développée sous la forme d'un registre décentralisé, distribué[16] et gouverné par consensus,[17] lequel permet de transmettre de l'information et d'effectuer des transactions de manière sécurisée. À l'instar des véhicules motorisés, la blockchain combine donc plusieurs technologies qui ont déjà fait leurs preuves. Par exemple, la blockchain utilise la mise en réseau pair-à-pair (« P2P ») aussi utilisé par les torrents, tandis que l'horodatage sécurisé est utilisé par les banques et les compagnies d'assurances pour les documents contractuels. Dans le même ordre d'idées, la fonction de hachage est utilisée par des logiciels de vérification comme Tripwire et la signature numérique avec infrastructure à clés publiques[18] par de nombreuses autorités de certification (courriels, protocoles SSL/TLS, etc).

13 Satoshi Nakamoto est le pseudonyme du ou des créateurs de la première blockchain (Bitcoin). Malgré de nombreuses tentatives d'usurpation, son identité n'a toujours pas été révélée à ce jour.

14 La blockchain a permis de résoudre le problème de la double dépense, qui était l'obstacle principal à la création de monnaies numériques. Le problème arrive lorsqu'un même utilisateur envoie deux fois la même unité monétaire à deux personnes différentes. En effet, les cryptomonnaies étant, par essence, numériques, il était impossible de s'assurer qu'une pièce de monnaie était originale. Le mode de consensus permis par la blockchain, à travers les preuves de travail (*proof of work*) et d'enjeu (*proof of stake*), a permis de consacrer un caractère d'originalité à l'unité monétaire.

15 Dans les blockchains fonctionnant grâce à un mécanisme de *proof of work*, ces vérificateurs sont appelés mineurs. Ils consomment de l'électricité afin de disposer d'une puissance de calcul suffisante pour résoudre diverses équations mathématiques et trouver le prochain bloc de la chaîne. En parallèle, ils vérifient que la transaction émise par un utilisateur du réseau ne constitue pas une forme de double dépense. Plus la puissance de calcul utilisée est importante, plus le mineur a de chances de découvrir un nouveau bloc et de recevoir la récompense qu'il contient. De la même façon, les blockchains fonctionnant grâce à la *proof of stake* sont gouvernés par des vérificateurs. Toutefois, ces derniers doivent posséder une quantité élevée de cryptomonnaies, puis les « miser » sur la durée en les mettant « en dépôt ». L'un des vérificateurs est ensuite sélectionné aléatoirement afin de valider les blocs ; plus la mise est importante, plus les chances d'être sélectionné sont grandes. Une fois le bloc validé, il est ajouté à la chaîne et les transactions et données qu'il contient sont rendues officielles aux participants du réseau. Vitalik BUTTERIN, « *A Proof of Stake Design Philosophy* », *Medium* (30 décembre 2016) en ligne : <https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51>

16 Tous les nœuds du réseau détiennent une copie de l'intégralité de la blockchain.

17 Dans les systèmes de preuve de travail (*proof of work)*, tant les mises à jour du réseau (*soft* et *hardfork*), l'historique de la chaîne et le contenu des blocs sont déterminés par la majorité de la puissance de calcul, au contraire des systèmes de preuve de participation ou preuve d'enjeu (*proof of stake*), dans lesquels la majorité de mises en jeu détermine ces mêmes éléments. Vitalik BUTTERIN, « *A Proof of Stake Design Philosophy* », *Medium* (30 décembre 2016) en ligne : <https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51>

18 Garrick Hileman et Michel Rauchs, « 2017 Global Blockchain Benchmarking Study », *SSRN.com,* 21 septembre 2017, en ligne : <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3040224>.

Par ailleurs, l'idéologie derrière la première blockchain est libertarienne. En effet, elle a été inventée juste après la crise des *subprimes*,[19] crise pendant laquelle les banques ont vendu à leurs épargnants des produits risqués, pourtant affichés sans risque. Dans le cadre de plans de sauvetage étatiques, l'argent des citoyens avait servi à renflouer les caisses des institutions financières qui les avaient pourtant trompés quelques mois auparavant. Face à ce qui a été perçu comme une injustice, des voix se sont élevées pour redonner aux individus le contrôle sur leur propriété, et plus particulièrement sur leur argent. Les premières cryptomonnaies sont ainsi nées afin d'assurer un niveau de sécurité élevé pour les transactions, et la blockchain en est la technologie sous-jacente. Notons que la blockchain implique un chiffrement des données de compte et des transactions qui assure une sécurité informatique des plus élevées.

144

Les applications bénéfiques de la blockchain se sont multipliées dans de nombreux secteurs et industries où l'enjeu principal est d'établir un lien confiance entre des parties qui ne se connaissent pas : systèmes de vote, de gestion des droits, de mise en place de contrats intelligents ou encore de preuve. Cette vague d'accaparement de la blockchain par les entreprises a contribué à normaliser la technologie dans l'esprit du public et à rassurer les États qui voyaient d'un mauvais œil cette entrave à leur souveraineté monétaire.

À l'occasion de cette « deuxième vague », différents types de blockchains sont apparus : celles *publiques* et celles *privées*. Les deux catégories de blockchains disposent de modes de gouvernance diamétralement opposés.[20] Les blockchains publiques sont sensiblement similaires à la blockchain derrière le Bitcoin, c'est-à-dire qu'elles permettent à tous de participer au transfert d'actifs.[21] Les secondes ont été créées pour répondre aux besoins des entités qui ne pouvaient se satisfaire du caractère public des informations contenues sur le registre. En somme, les secondes s'apparentent davantage à une combinaison de grandes

19 Le premier bloc de la première blockchain au monde, celle du Bitcoin, contenait le texte suivant : « *The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.* »

20 France Stratégie, *Les enjeux des blockchains*, par Joëlle Toledano, juin 2018, en ligne : <https://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/fs-rapport-blockchain-21-juin-2018.pdf>.

21 Les transactions sont validées et traitées par consensus entre les nœuds du réseau. Le consensus, habituellement déterminé par un vote, n'exige pas qu'un nœud du réseau ait une expérience du réseau ou une identité quelconque. Autrement dit, aucune confiance préexistante n'est nécessaire entre les nœuds participants, donc toute personne peut rejoindre le réseau et y participer.

bases de données et de réseaux privés de transactions qui empruntent aux mécanismes de fonctionnement des blockchains publiques.

Parmi les **blockchains publiques,** deux grandes catégories existent :

- Les blockchains publiques *sans permission* : elles sont ouvertes à tous. Quiconque peut lire le registre, réaliser une transaction ou participer à la vérification des blocs et transactions qu'ils contiennent.
- Les blockchains publiques *permissionnées* : leur registre est ouvert à tous. Toutefois, seuls les participants autorisés peuvent réaliser des transactions. La vérification est soit ouverte à tous, soit aux seuls participants autorisés à faire des transactions ou soit à certains d'entre eux.

Parmi les **blockchains privées**, deux grandes catégories existent également :

- Les blockchains *de consortium*, qui sont restreintes aux participants autorisés en ce qui concerne la lecture du registre et la possibilité d'effectuer une transaction. La vérification des blocs et transactions peut être faite par une partie ou par tous les participants autorisés.
- Les blockchains *d'entreprise ou personnelles*, dont la lecture est entièrement privée ou bien limitée à un petit nombre de participants autorisés. La réalisation des transactions peut être ouverte à certaines personnes autorisées,[22] tandis que leur vérification est autorisée à l'opérateur du réseau seulement.

Les blockchains publiques semblent donc offrir les meilleures garanties probatoires et sécuritaires, car elles sont immuables et peuvent être auditées en tout temps et par tous. Comme mentionné, la blockchain (publique) est apparue en réponse à une crise de confiance envers les acteurs centralisés telles l'administration publique ou les banques après la crise de 2009. Au contraire, les blockchains privées sont contrôlées par une personne unique ou un petit nombre de personnes, ce qui s'apparente au tiers de confiance traditionnel à opérateur unique, lequel peut être faillible, malicieux ou pourrait tout simplement disparaître.[23]

22 Ex. : membres de l'entreprise, sous-traitants, fournisseurs, etc.

23 oir l'affaire QuadrigaCX's, « Un marché de cryptomonnaies perd 250 M$ après la mort subite de son fondateur », *Radio–Canada*, 4 février 2019, en ligne : <https://ici.radio–canada.ca/nouvelle/1150906/cryptomonnaies-quadriga-cotten-mort-250-millions-chiffre-chiffrement-portefeuille-wallet-quadrigacx>.

1.2. ATOUTS PROBATOIRES INHÉRENTS À LA BLOCKCHAIN PUBLIQUE

Les blockchains publiques se distinguent des bases de données centralisées par le mode de gouvernance distribué et collectif des nœuds du réseau.[24] L'historique des transactions effectuées est détenu en totalité par chaque « nœud »,[25] qui participe à la validation et à la vérification des transactions en constituant une copie fidèle de la base de données (la blockchain). La protection collective de l'information est donc une propriété essentielle de la fonction « **distribuée** » de la blockchain. Pour que l'information contenue dans la blockchain disparaisse, il faudrait donc que tous les nœuds du réseau n'existent plus ou soient corrompus, ce qui est pratiquement impossible.[26] En somme, dès qu'une transaction est enregistrée sur cette base de données, la sécurité est telle que l'information ne peut plus être effacée ou modifiée.[27] Cela contribue au paramètre « **immuable** » de la blockchain.

146

Un autre atout probatoire de la blockchain provient de la résolution mécanique du *problème des généraux byzantins*,[28] qui suppose d'identifier une méthode pour faire transiter de l'information entre divers interlocuteurs, bien qu'aucun d'eux ne connaisse le degré de fiabilité des autres interlocuteurs et de l'information transmise. La résolution de ce problème est importante, car elle permet de garantir le consensus au sein des réseaux qui nécessitent une certaine synchronisation entre les membres pour parvenir à fonctionner. En pratique, au sein d'une

24 Il est important de distinguer les nœuds du réseau, qui participent activement au bon fonctionnement de la blockchain, et l'utilisation du réseau par des personnes qui ne contribuent pas à son maintien. À toute fin pratique, ces derniers participants seront appelés des « utilisateurs ».

25 « Nœud » est le nom donné à la machine et au logiciel dans les réseaux pair-à-pair. Contrairement à un réseau client-serveur, l'architecture réseau composée de nœuds est symétrique. Chaque nœud a la même capacité d'émettre, de recevoir et de calculer que les autres nœuds de son réseau.

26 Si un nœud arrête de participer aux vérifications de la blockchain temporairement, il lui faudra synchroniser l'information contenue par le logiciel avec la version la plus récente de la blockchain. Toutefois, l'information détaillant les transactions effectuées sur le réseau jusqu'à la dernière participation dudit nœud reste enregistrée sur son disque dur.

27 L'ensemble des transactions effectuées sur une blockchain est stocké dans les nœuds complets qui font partie du réseau. Il faudrait donc un moyen de supprimer au moins 51 % de ces nœuds pour que la majorité de ceux restants pense qu'un bloc n'ait pas existé. Par ailleurs, plus un bloc est ancien, plus il est complexe de modifier l'information qu'il contient sans une puissance de calcul digne d'un État ou d'un géant du numérique (Facebook, Apple, Google, etc.). En effet, chaque transaction fait partie de l'arbre de Merkle, désignant une structure permettant de vérifier l'intégrité d'un ensemble de données sans les avoir nécessairement consultées. Comme tous les blocs sont liés par un mécanisme de hachage, afin de modifier l'information de l'un d'eux, il faudrait supprimer 51 % des nœuds complets et ensuite recalculer la racine de Merkle de chaque bloc déjà extrait après le bloc dans lequel vous voulez que votre transaction soit supprimée. Autrement dit, pour effacer ou modifier l'information contenue dans la chaîne de blocs, il faudrait contrôler 51 % du réseau. Satoshi Nakamoto, « *Bitcoin : A Peer to Peer Elctronic Cash System* », 2008, en ligne : <https://bitcoin.org/bitcoin.pdf>

28 Le problème des généraux byzantins peut se résumer comme suit : des généraux de l'armée byzantine campent autour d'une ville assiégée. Ils ne peuvent communiquer qu'à l'aide d'intermédiaires (messagers) et doivent établir un plan de bataille commun, faute de quoi l'assaut se soldera par un échec cuisant. Cependant, dans le camp byzantin, un certain nombre de ces intermédiaires peuvent être des traîtres, qui essaient de semer la zizanie entre les généraux par la rétention de l'information ou la transmission de fausse information. Il faut donc trouver une méthode pour s'assurer que les généraux loyaux arrivent tout de même à se mettre d'accord. Le problème peut être résolu, quel que soit le nombre de messagers malhonnêtes, si les messages sont écrits et non falsifiables.

blockchain publique, afin qu'une transaction soit enregistrée dans le registre commun, elle doit d'abord être validée par le réseau de nœuds. Après cette validation, un bloc sécurisé est créé et contient les détails de la transaction. Le bloc est finalement joint à la chaîne des blocs existante.

Avant le Bitcoin, le problème des généraux était résolu par des algorithmes traditionnels soumis à des contraintes, notamment quant au nombre de nœuds pouvant interagir sur le réseau. Dorénavant, pour les blockchains publiques, la réponse au problème émane de l'utilisation d'algorithmes de consensus utilisant la preuve de travail (*proof of work*) ou la preuve d'enjeu (*proof of stake*), et qui bénéficient d'un accès au registre commun en temps réel.

Par ailleurs, la sécurisation des comptes et des transactions se fait grâce à un mécanisme d'infrastructure à clés publiques (aussi appelée cryptographie asymétrique). Dans ce dernier système, chaque utilisateur détient une clé privée et une clé publique, la dernière étant accessible à tous. Ces clés complémentaires sont appelées « biclés ». Pour qu'un utilisateur X effectue une transaction avec un utilisateur Y, il doit chiffrer la transaction avec la clé publique de Y, lequel est le seul à pouvoir la déchiffrer avec l'aide de la clé privée rattachée à sa clé publique. Ainsi, X est certain que Y est le seul destinataire de la transaction qu'il a chiffrée puisqu'il est (en principe) le seul à détenir la clé privée rattachée à la clé publique de Y. L'inverse est tout aussi vrai. Si X veut prouver de manière vérifiable qu'il est bien la personne dont émane l'information, il lui suffit de chiffrer la transaction avec sa clé privée (forme de signature numérique). L'information ne pourra alors être déchiffrée qu'avec l'aide de la clé publique de X.

En résumé, les blockchains publiques proposent les caractéristiques suivantes :

- **Décentralisées**, ce qui prévient l'existence d'un point de défaillance unique du réseau et protège contre la perte de données.
- **Distribuées**, ce qui permet à chaque membre du réseau d'avoir une version complète du registre en temps réel.
- **Sécurisées**, grâce aux processus de hachage et d'horodatage, ainsi qu'aux différents procédés cryptographiques.
- **Transparentes,** car accessibles et auditables par tous, en tout lieu et en tout temps.

- **Immuables**, car les transactions et l'information échangées entre les utilisateurs du réseau sont regroupées par blocs horodatés et irréversiblement liés les uns aux autres, formant une « chaîne de blocs » (d'où le terme *blockchain*). Les données enregistrées sur le nouveau bloc et sur tous les précédents qui lui sont liés sont donc inaltérables et infalsifiables.[29]
- **En code ouvert**, ce qui permet la consultation de l'architecture du logiciel par les pairs et, conséquemment, la découverte plus rapide des *bogues*. Également, le code ouvert suppose l'amélioration constante du code puisque toute personne disposant de connaissances pertinentes est libre d'y contribuer.
- **Mode de gouvernance qui habituellement protège les utilisateurs** des développeurs, lesquels peuvent se voir interdire certaines actions lors de leur contribution au code. Par exemple, des vérificateurs votent afin d'accepter (ou non) les modifications de l'architecture réseau suggérées par les développeurs. En somme, ce pouvoir de contrôle des vérificateurs permet d'assurer une confiance accrue dans les développeurs.

148

Toutefois, les blockchains publiques ont « les avantages de leurs inconvénients ». Brièvement, ces inconvénients sont les suivants :

- La difficulté, voire la quasi-impossibilité, de modifier ou mettre à jour les informations qu'elles contiennent. En effet, la blockchain publique est immuable. Il est donc primordial de s'assurer que l'information qu'elle contient n'est pas erronée lors de son insertion dans un bloc.
- La limite de stockage des blocs, nécessaire pour éviter que les registres des blockchains deviennent trop volumineux pour les différents nœuds du réseau.
- La consommation élevée d'électricité des blockchains fonctionnant par preuve de travail (*proof of work*), entrainant un coût financier et écologique.
- L'absence d'interopérabilité entre les différentes blockchains, les empêchant (pour le moment) de communiquer ou de partager librement de l'information à travers divers réseaux de blockchains. Toutefois cet inconvénient tend à être résolu par le biais de diverses

29 Au contraire, la principale critique adressée aux blockchains privées en matière de preuve tient au retour à une centralisation qui empêche la garantie d'immuabilité, car un ou plusieurs opérateurs contrôlent la blockchain et peuvent donc modifier l'information qu'elle contient à loisir. À l'inverse, l'immuabilité des blockchains publiques peut poser problème si les informations qui y sont inscrites sont erronées ou lorsque la loi oblige la suppression de certaines informations (ex. registre des droits personnels et réels mobiliers, registre foncier, etc.).

innovations comme l'*atomic swap* ou des réseaux comme Polkadot, qui n'en sont qu'à leurs débuts.

2. COMMENT SÉCURISER DES DONNÉES DANS UNE BLOCKCHAIN ?

Les avantages inhérents aux blockchains publiques exposés, arrêtons-nous sur l'une des nouvelles applications de la blockchain inspirée de ses paramètres d'immuabilité et de transparence.

Dans ses grandes lignes, la méthode pour sécuriser des données sur une blockchain publique consiste à attacher des données informationnelles compressées à une transaction, et ce, en payant simplement les frais de transaction afférents.[30] En utilisant ce type de programme, il est par exemple possible de certifier la propriété d'actifs, l'intégrité de documents et l'existence d'œuvres.[31] En effet, les données informationnelles compressées sont associées à un fichier que l'on souhaite protéger. Elles sont obtenues à l'aide d'un algorithme de hachage cryptographique[32] et représentent l'« empreinte numérique » de ce dernier. Le hachage permet donc de transformer une grande quantité de données en une empreinte numérique de quelques caractères, et ce, tout en préservant l'intégrité du contenu ainsi haché.

Sur Bitcoin, par exemple, la plupart de ces méthodes utilisent des instructions de type « OP_RETURN », lesquelles permettent d'attacher des données en « brulant » des bitcoins au lieu d'en dépenser — ce qui exige moins d'effort computationnel des vérificateurs. Dans une étude menée en 2017, les chercheurs Pompianu et Barttoleti ont ainsi compté plus de 25 000 transactions de ce type par semaine. Au total, les chercheurs estiment que ces transactions représentent environ 1 % des transactions Bitcoin totales effectuées, et occupent environ 0,3 % de sa taille totale. Il faut comprendre que la fonctionnalité n'avait pas été envisagée par les développeurs de la première blockchain ; elle est aujourd'hui permise, voire facilitée, par d'autres blockchains plus récentes (ex. Ethereum).

30 Cette valeur était équivalente à 0.003 $ le 29 juillet 2019 sur Bitcoin.

31 Massimo Bartoletti et Livio Pompianu, « An Analysis of the Bitcoin OP_RETURN Metadata », *ArXiv.org*, 3 février 2017, en ligne : <https://arxiv.org/abs/1702.01024>.

32 « Opération qui consiste à appliquer un algorithme de chiffrement à un groupe de données de taille variable afin de générer un code unique de taille fixe, utilisé pour l'authentification et le stockage d'information », Office québécois de la langue française, préc., note 12.

2.1. UNE EMPREINTE NUMÉRIQUE + UNE TRANSACTION

Nous verrons désormais deux méthodes d'insertion de données, soit celles des deux blockchains publiques les plus communes : Bitcoin et Ethereum.

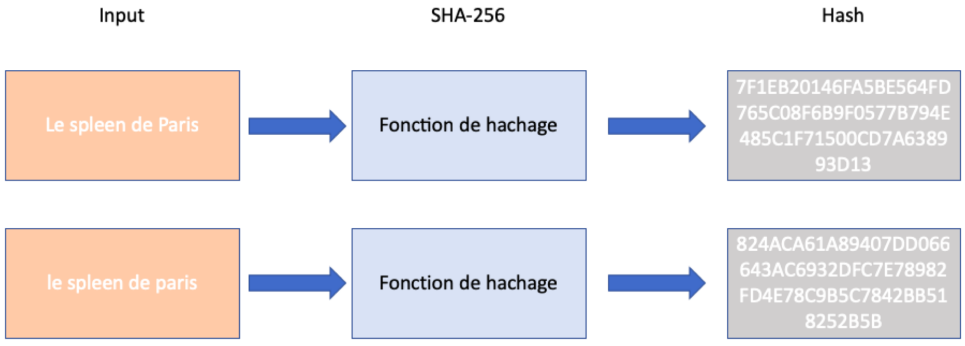
BITCOIN

En suivant la procédure OP_RETURN, il est possible d'insérer des données informationnelles dans une transaction sans « polluer » la blockchain, au contraire d'autres méthodes controversées utilisées sur Bitcoin.[33] En termes généraux, la fonction OP_RETURN est donc comparable au mémo sur les chèques, espace limité dans lequel on peut inscrire de l'information non essentielle au bon fonctionnement de la transaction.

150

La manière de procéder est la suivante[34] :

1. Choix d'un document contenant des données brutes à protéger.
2. Sélection d'un logiciel de hachage cryptographique (ex. : MD5, SHA-1, SHA-2, etc.). Attention, toutes les fonctions de hachage ne bénéficient pas des mêmes propriétés, il faut donc en sélectionner une qui a déjà fait ses preuves.[35]
3. Hachage du document par le logiciel, lequel crée une empreinte numérique unique (voir la figure ci-dessous).



33 Andrew sward, Ivy vecna, Forrest stonedahl, « Data Insertion in Bitcoin's Blockchain», *Ledger* Journal, 2018, en ligne : <https://ledgerjournal.org/ojs/index.php/ledger/article/view/101/93>

34 Massimo Bartoletti et Livio Pompianu, préc., note 31.

35 « Fonction de hachage cryptographique », *Wikipédia*, en ligne : <https://fr.wikipedia.org/wiki/Fonction_de_hachage_cryptographique> : « Une fonction de hachage cryptographique idéale possède les quatre propriétés suivantes : (1) la valeur de hachage d'un message se calcule « très rapidement » ; (2) il est, par définition, impossible, pour une valeur de hachage donnée, de construire un message ayant cette valeur de hachage ; (3) il est, par définition, impossible de modifier un message sans changer sa valeur de hachage ; (4) il est, par définition, impossible de trouver deux messages différents ayant la même valeur de hachage. »

4. Création d'une transaction sur Bitcoin.
5. Sélection du protocole d'insertion OP_RETURN, suivie de l'empreinte numérique obtenue à l'étape 3, dans le *out-script* d'une transaction, c'est-à-dire dans le court programme informatique qui définit les conditions auxquelles une transaction peut être effectuée. Par exemple, si Bob envoie des fonds à Alice, le programme pourrait être « cette somme n'est transférable qu'à la clé publique attachée à Alice ». Attention, les données informationnelles insérées dans le out-script ne peuvent peser plus de 80 bytes. À des fins comparatives, la présente phrase en pèse 60.
6. Résultante : insertion de l'empreinte numérique du document choisi dans une transaction contenue dans un bloc, lui-même diffusé sur le réseau Bitcoin.

Il faut ensuite conserver certaines informations qui permettent de retrouver l'empreinte numérique à travers l'ensemble des blocs contenus de la blockchain.[36] Également, il est important de conserver le document source duquel émane l'empreinte numérique, car l'empreinte seule n'équivaut pas au document et ne permet pas non plus de le reconstituer.

En somme, la blockchain Bitcoin n'est donc pas faite pour le stockage de données brutes. Toutefois, une fois les données insérées dans un bloc, ces dernières bénéficient des propriétés du plus grand réseau blockchain existant. Bitcoin présente ainsi parmi les meilleures garanties probatoires.

ETHEREUM

Une autre blockchain majeure, **Ethereum**, a été construite spécifiquement pour permettre de transiger de l'information ou d'autres objets étrangers à la cryptomonnaie, à l'inverse du Bitcoin. En effet, sur Ethereum, un champ optionnel d'insertion de données informationnelles existe lors de la création d'une transaction. Par exemple, Ethereum permet par défaut aux utilisateurs d'inscrire des données au sein de

36 À savoir : le *hash* de la transaction, le *hash* du bloc qui contient la transaction, l'horodatage, la métadonnée attachée à la fonction OP_RETURN (selon notre protocole, le *hash* du document).

contrats intelligents.[37] Cette fonctionnalité, d'ailleurs prévue dans le livre blanc du réseau, a une place majeure dans l'intérêt que la communauté porte au réseau Ethereum.

Sur le réseau Ethereum, il existe les comptes *détenteurs externes* et les comptes de *contrat*. Les comptes de contrat servent à la création puis à l'exécution de contrats intelligents grâce à l'insertion de segments de code gérant les interactions contractuelles avec le compte, tandis que les comptes détenteurs externes sont des comptes « normaux » contrôlés par un système d'infrastructure à clés publiques. Les deux types de comptes contiennent trois champs[38] :

- Le **nonce**, soit un compteur utilisé pour s'assurer que les transactions ne soient traitées par le réseau qu'une seule fois ;
- Le **solde en éther** (unité de cryptomonnaie sur le réseau Ethereum) du compte ;
- Le **stockage** ou la mémoire de stockage du compte, soit l'endroit où l'utilisateur peut insérer de l'information.

Au sein d'Ethereum, le terme « transaction » réfère donc à un paquet de données signé par un compte détenteur externe et dans lequel on peut stocker un message.[39]

En somme, l'insertion d'information au sein de la blockchain Ethereum — après avoir haché le document avec une fonction de hachage (voir les étapes 1 à 3 du procédé utilisé dans Bitcoin) — fait partie de la procédure régulière d'émission d'une transaction. En effet, il suffit d'insérer, dans le champ optionnel prévu à cet effet, le *hash* du document ou de toute autre donnée plus volumineuse que l'on souhaite admettre en preuve. Dans ce dernier cas, les coûts seront toutefois beaucoup plus importants. En effet, le champ optionnel d'Ethereum ne contient aucune limite de taille (bytes). Toutefois, le stockage de données a un coût et, plus celles-ci sont volumineuses, plus le coût de transaction est élevé, d'où l'intérêt d'utiliser un algorithme de hachage.

37 Un contrat intelligent est une enveloppe logicielle, un code informatique, qui permet d'exécuter automatiquement les obligations et termes définis préalablement par les parties.

38 Le compte contrat contient un quatrième champ, nommé « code du contrat », afin que les comptes externes puissent activer le compte contrat par le biais de messages. Ces messages permettent au compte contrat de lire et d'écrire dans la mémoire interne et d'envoyer d'autres messages ou de créer des contrats à son tour.

39 Vitalik Buterin, « Ethereum White Paper », *blockchainlab*, 2013, en ligne : <http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf>.

2.2. EXEMPLES D'APPLICATION

La technique explicitée, il nous semble pertinent d'illustrer comment ces techniques peuvent donner lieu à des systèmes innovants et performants dans certains pans du droit. Notons que l'utilisation de la méthode s'inscrit ainsi dans un contexte préventif, surtout à des fins de gestion documentaire. Ainsi, les documents qui sont constitutifs d'un droit et dont on anticipe la présentation en preuve pourraient bénéficier des techniques décrites ci-dessus.

Toutefois, le développement d'applications faciles d'utilisation semble un prérequis pour entrevoir une adoption plus généralisée de ces techniques. Par exemple, nous croyons que la constitution d'interfaces utilisateurs simples et esthétiques effectuant les technicités susmentionnées de façon automatisée et ne nécessitant que le téléversement du document à protéger susciterait davantage l'intérêt de l'industrie.

Nous verrons donc l'application des techniques d'insertion de métadonnées dans une blockchain publique en (a) droit d'auteur, puis en (b) authentification de contenu vidéo (*deepfakes*).

DROIT D'AUTEUR ET BLOCKCHAIN : LA POSITION CHINOISE

Brièvement, en droit d'auteur, l'établissement d'un lien fiable entre l'individu et sa création est primordial, car il permet d'en tirer un bénéfice pécuniaire.[40] En effet, l'auteur[41] d'une œuvre bénéficie initialement du droit exclusif de produire ou de reproduire la totalité ou une partie importante de son œuvre, sous une forme matérielle quelconque.[42] Également, il peut céder ou concéder son droit d'auteur, en totalité ou en partie.[43] L'un des enjeux est donc d'établir ce lien avec suffisamment de robustesse afin qu'il ne soit pas remis en question ou bafoué, notamment dans le cadre d'une contrefaçon.[44] Or, en insérant le *hash* d'une création

40 Au Canada, le droit d'auteur est une protection automatique octroyée à l'auteur d'une œuvre, au contraire du brevet qui nécessite un enregistrement auprès de l'Office de la propriété intellectuelle du Canada (OPIC). En sus, il existe aussi un mécanisme de certification (facultatif) de la propriété d'une œuvre, au coût d'environ 50 $, lequel permet de se constituer une preuve advenant un litige. Toutefois, ce certificat est contestable devant les tribunaux.

41 L'auteur est le premier titulaire du droit d'auteur, art. 13(1) *Loi sur le droit d'auteur*, L.R.C. 1985, c. C-42 (ci-après « LDA »).

42 LDA, art. 3.

43 LDA, art. 13(4).

44 Toute reproduction non autorisée d'une partie importante de cette œuvre constitue une contrefaçon au sens de l'article 3 de la LDA, soit une atteinte au droit d'auteur de son titulaire. Elle peut donner lieu à une action en justice.

originale dans une blockchain publique, un auteur se crée une preuve de l'existence de son œuvre à un moment donné.

Dans ce contexte, en 2017, la ville de Hangzhou en Chine s'est dotée d'un cybertribunal spécialisé dans le commerce électronique et les conflits relatifs à Internet.[45] Le tribunal dispose notamment d'une plateforme en ligne pour accepter les dépôts de dossier par voie électronique et juger des affaires par vidéoconférence. Les utilisateurs s'identifient à la plateforme en présentant un document officiel prouvant leur identité ou grâce à leur compte Alipay.[46]

Dans l'une des affaires rendues en juin 2018 par le tribunal, une entreprise de médias avait fait une capture d'écran du code source du site d'un compétiteur et en avait produit une empreinte numérique, laquelle était enregistrée sur les blockchain Factom et Bitcoin afin de garantir l'intégrité et l'horodatage de la preuve quant au site Internet accusé de constituer une contrefaçon.[47] Dans le jugement final, le juge chargé du dossier avait admis la preuve présentée en soutenant sa décision comme suit[48] :

> « The court thinks it should maintain an open and neutral stance on using blockchain to analyze individual cases. We can't exclude it just because it's a complex technology. Nor can we lower the standard just because it is tamper-proof and traceable. [...] In this case, the usage of a third-party blockchain platform that is reliable without conflict of interests provides the legal ground for proving the intellectual infringement. »
>
> [nos soulignements]

45 Surnommée la « capitale du commerce électronique chinois », le choix de cette ville n'est pas anodin. En effet, en procédure civile chinoise, les actions en justice doivent être intentées au lieu du domicile du défendeur. Pour les sociétés, le domicile réfère au siège social ou au lieu d'établissement principal. Or comme Hangzhou abrite de nombreuses entreprises technologiques, lorsque leurs consommateurs ou partenaires d'affaires ont des différends à régler, les poursuites ont principalement lieu à Hangzhou.

46 Ce service en ligne offre aux utilisateurs divers services tels que le paiement de factures, la gestion de comptes bancaires, le transfert P2P, le rechargement prépayé de téléphones mobiles, l'achat de billets d'autobus et de train, la commande de nourriture, la commande de taxi, la souscription à un service d'assurance, le stockage de documents et même un service d'identification numérique.

47 Wolfie Zhao, « Blockchain Can Legally Authenticate Evidence, Chinese Judge Rules », *coindesk*, 28 juin 2018, en ligne : <https://www.coindesk.com/blockchain-can-legally-authenticate-evidence-chinese-judge-rules>.

48 Adrian Zmudzinski, « Chinese Internet Court uses Blockchain to Protect Online Writer's Intellectual Property », *cointelegraph*, 8 décembre 2018, en ligne : <https://cointelegraph.com/news/chinese-internet-court-uses-blockchain-to-protect-online-writers-intellectual-property>.

Ainsi, les auteurs qui publient leurs œuvres en ligne peuvent désormais faire valoir leurs droits grâce à l'utilisation de plateformes vérifiées de stockage de preuve qui utilisent des blockchains publiques « *reliable without conflict of interests* ».

Dans la foulée de cette décision, le vice-président du cybertribunal, Wang Jiangqiao, a rendu officiel l'acceptation de ce type de preuve en matière de droit d'auteur en raison des garanties inhérentes de la blockchain.[49] Ainsi, les empreintes numériques stockées dans un système de blockchain judiciaire y disposent aujourd'hui d'un effet juridique reconnu.

La même année, la plus haute cour du pays a également reconnu la valeur juridique d'une preuve par blockchain en matière de propriété intellectuelle,[50] reconnaissance toutefois conditionnelle à des caractéristiques bien circonscrites de ladite blockchain. Conséquemment, les tribunaux de Chine doivent désormais reconnaître la valeur juridique de la blockchain comme méthode de stockage et d'authentification des preuves numériques :

> « Les tribunaux Internet reconnaîtront les données numériques soumises comme preuve si les parties concernées ont collecté et stocké ces données via une blockchain avec signatures numériques, horodatages fiables, vérification de la valeur de hachage ou via une plateforme de dépôt numérique et qu'elles peuvent prouver l'authenticité de cette technologie ainsi utilisée. »[51]
>
> [nos soulignements]

Par ailleurs, toujours en Chine, si **l'authenticité** d'une donnée numérique générée, collectée, stockée ou transmise est contestée par une partie, il a été déterminé que les six éléments suivants doivent être évalués afin de statuer sur l'admissibilité de la preuve[52] :

49 Ana Alexandre, « Chinese Internet Court Employs AI and Blockchain to render Judgment », *cointelegraph*, 25 avril 2019, en ligne : <https://cointelegraph.com/news/chinese-internet-court-employs-ai-and-blockchain-to-render-judgement>.

50 Cour suprême chinoise, jugement du 6 septembre 2018, en ligne : <http://www.court.gov.cn/zixun-xiangqing-116981.html> (nos traductions).

51 Jérôme Giusti, « La Chine reconnaît la blockchain comme moyen de preuve légale… et nous et nous et nous ? », *Medium*, 11 septembre 2018, en ligne : <https://medium.com/@graldinesalord/la-chine-reconna%C3%ADt-la-blockchain-comme-moyen-de-preuve-l%C3%A9gale-et-nous-et-nous-et-nous-9196ebe04400 >.

52 Cour suprême chinoise, jugement du 6 septembre 2018, en ligne : <http://www.court.gov.cn/zixun-xiangqing-116981.html> (nos traductions).

« (1) L'*environnement matériel et logiciel,* comme les systèmes informatiques sur lesquels les données électroniques sont générées, recueillies, stockées et transmises : est-il sûr et fiable ?

(2) Si le document principal et le moment de la production des données électroniques sont clairs, et si leur contenu est *clair, objectif et précis* ;

(3) Si le *stockage* et les supports de stockage des données électroniques sont clairs et si les méthodes et moyens de stockage sont appropriés ;

(4) Si l'*extraction électronique* des données et les sujets, outils et méthodes fixes sont fiables et si le processus d'extraction peut être reproduit ;

(5) Si le contenu des données électroniques est ajouté, supprimé, modifié ou incomplet, c'est-à-dire si l'*intégrité de l'information est préservée* ;

(6) Si les données électroniques peuvent *être vérifiées* au moyen d'une signature électronique, d'un horodatage fiable, d'un moyen de contrôle de la valeur de hachage, d'une blockchain et d'autres moyens de collecte de preuves, de moyens techniques fixes et inviolables ou d'une certification électronique de la plateforme de preuve judiciaire. »

[nos soulignements]

En précisant l'usage de la blockchain comme élément de validation du dernier critère d'authenticité de données numériques, la Cour suprême chinoise est à la première à reconnaître explicitement les garanties probatoires inhérentes à la preuve par blockchain en matière de document technologique.

Bien qu'elle soit sans doute la nation la plus avancée et proactive en matière d'utilisation de la blockchain pour faire la preuve de droits de propriété intellectuelle, d'autres initiatives émergent ailleurs qu'en

Chine.[53] Par exemple, de nombreux services privés, tels *BlockchainYourIP*, proposent à chacun de protéger leurs créations par le biais de la blockchain.[54] Ces derniers vont de la protection des logiciels aux œuvres littéraires, en passant par l'audiovisuel.

LES DEEPFAKES

Sur un tout autre registre, la blockchain permet, dans une certaine mesure, de lutter contre les « faux profonds » ou *deepfakes*, qui sont des programmes informatiques utilisant une technique de création ou de modification des vidéos à l'aide d'algorithmes d'apprentissage profond (*deep learning*). En d'autres termes, l'intelligence artificielle crée une image à partir de plusieurs sources audiovisuelles. Les *deepfakes* ont surtout fait scandale dans le cadre de fausses vidéos pornographiques mettant en scène des célébrités et des ex-conjoints. Plus généralement, ils peuvent s'appliquer à tout type de contenu vidéo.

L'apparition généralisée de ces programmes commence en 2017, lorsqu'un utilisateur de la plateforme *Reddit* nommé « deepfakes » partage, dans un subreddit éponyme, des vidéos pornographiques modifiées où il insère des visages de célébrités sur des corps d'actrices sans leur consentement. Plus récemment, « des élus américains et des experts ont estimé que les vidéos modifiées avec un logiciel d'intelligence artificielle, mieux connues sous le nom de *deepfakes*, constituaient une menace pour la sécurité nationale et les élections américaines de 2020.[55]

Outre le détournement d'identité d'individus influents et l'atteinte à la vie privée en lien avec la circulation de contenu pornographique non consensuel, on peut aussi penser à la **manipulation d'un contenu original à des fins de constitution de preuve**.

Or, certaines applications de la blockchain permettent de certifier le caractère original d'une vidéo, c'est-à-dire d'établir qu'elle en constitue la

53 Voir la Résolution du Parlement européen du 3 octobre 2018 sur les technologies des registres distribués et les chaînes de blocs: renforcer la confiance par la désintermédiation, 2017/2772 [RSP], laquelle reconnaît, à ses considérants 22 et 23, l'utilité de la blockchain en matière d'« Industries créatives et droits d'auteur ».

54 Notons que créer ce type de service est à la portée de tous, il suffit de mettre en place les processus d'insertion de métadonnée dans un bloc décrits précédemment, tout en proposant une interface utilisateur attrayante.

55 Susannah George, « Les vidéos falsifiées diffusées sur le web préoccupent les élus américains », *La Presse*, 13 juin 2019, en ligne : <https://www.lapresse.ca/affaires/techno/201906/13/01–5230080–les–videos–falsifiees-diffusees-sur-le-web-preoccupent-les-elus-americains.php>.

source première.[56] Par exemple, des services à l'instar de Factom[57] ou Amber Authenticate ont été développés principalement pour lutter contre les *deepfakes*. Le logiciel tourne en arrière-plan des vidéos, c'est-à-dire qu'il travaille dans les métadonnées du fichier lorsqu'il est filmé ou monté.[58] Le logiciel émet alors un *hash*, lequel est envoyé directement sur la blockchain Ethereum. Une fois l'empreinte numérique obtenue d'un l'algorithme de hachage et fixée sur la blockchain, il est alors possible de détecter toute atteinte à l'intégrité du fichier. L'atteinte pourrait se traduire par une modification à l'information qu'il contient ou à une déficience de son environnement matériel ou logiciel, nous y reviendrons.

Ajoutons également qu'en raison de son caractère hautement technologique, il est difficile d'identifier un *deepfake*, rendant sa contestation incertaine advenant son dépôt au tribunal à titre de preuve, par exemple. Dans ce contexte, un logiciel tel *Amber Authenticate*[59] est d'autant plus utile, voire nécessaire.

158

À titre illustratif, dans un contexte où il devient de plus en plus ardu de se fier à nos sens pour déchiffrer le vrai du faux, certifier le caractère original d'enregistrements vidéo dans un contexte préventif pourrait s'avérer un outil pour de nombreux secteurs sensibles. Par exemple, les caméras policières ou de surveillance pourraient être équipées de tels dispositifs afin d'accroître la confiance du public envers le système démocratique. Prenons la situation hypothétique de bavures policières captées sur les réseaux sociaux et modifiées pour propager des *deepfakes* incitant à la haine contre les forces de l'ordre ou, plus généralement, contre tout service public. Dans une telle situation, la preuve de l'absence d'authenticité du contenu en circulation serait automatique et pourrait incidemment éviter, par exemple, des poursuites judiciaires ou la gestion d'une crise médiatique.

3. VERS LA MÉTADONNÉE ABSOLUE ?

Au vu de ce qui précède, les nouvelles utilisations de la blockchain font émerger des potentialités intéressantes en droit probatoire, lesquelles

56 C'est par exemple la terminologie employée dans la LCCJTI, art. 12.

57 Antonio GARCIA MARTINEZ, « The blockchain solution to our deepfakes problems », *The Wired*, 26 mars 2018, en ligne : <https://www.wired.com/story/the-blockchain-solution-to-our-deepfake-problems/>.

58 Arnaud Devillard, « La blockchain comme arme anti-deepfake », *Sciences Avenir*, 17 février 2019, en ligne : <https://www.sciencesetavenir.fr/high-tech/la-blockchain-comme-arme-anti-deepfake_131495>.

59 *Ambervideo*, en ligne : <https://ambervideo.co/>.

ont déjà fait leurs preuves à l'international. Toutefois, ce potentiel peut-il être capturé par le cadre juridique en place au Québec ?

3.1. PRÉCISIONS TERMINOLOGIQUES

Le document et l'intégrité sont sans conteste les notions phares de la loi québécoise concernant les technologies de l'information. Afin de mettre la table pour ce qui suit, nous détaillerons en premier lieu ces notions.

LE DOCUMENT (TECHNOLOGIQUE)

159

Selon la loi québécoise, un document est constitué d'information portée par un support.[60] Par ailleurs, pour que l'information portée par le support soit intelligible, elle nécessite de faire appel à une technologie, aussi appelée format ou logiciel. En somme, la trinité information-support-technologie constitue le document technologique.[61] Revenons sur ces trois composantes.

- **L'information** est délimitée et structurée, de façon logique, et doit être intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles sous l'une de ces formes ou en un autre système de symboles (ex. l'alphabet arabe, le braille, le morse, etc.).[62]

- Le **support** est l'élément matériel ou physique qui sert de base à un document[63]. Par exemple, un support pourrait être un disque dur, une clé USB, un serveur, un ruban magnétique ou encore un vinyle.

- La **technologie** possède un double sens, la technologie « portée par le support » et la technologie « du support ». Dans le premier cas, elle réfère au format ou logiciel qui sert à structurer et à rendre lisible l'information (ex. PDF, DOC, GIF, HTML, etc.). Dans le deuxième, elle réfère plus largement aux technologies de l'information, « qu'elles

60 LCCJTI, art. 3.

61 Vincent Gautrais, *La preuve technologique*, 2e éd., Montréal, LexisNexis, 2018, p. 145 et suiv.

62 LCCJTI, art. 3 al. 1.

63 V. Gautrais, préc., note 62, p. 146 et suiv.

> soient électronique, magnétique, optique, sans fil ou autres ou faisant appel à une combinaison de technologies ».[64]

Par ailleurs, les **métadonnées** sont des données sur les données. En termes plus illustratifs, une métadonnée est « une information qui explique le contexte d'un document, d'un événement ou d'une activité ».[65]Elle peut être interne (heure et date d'envoi d'un courriel, résolution d'une photographie, etc.) ou externe (historique de navigation, journalisation, documentation,[66] etc.) à un document technologique. Lorsqu'elle est interne, elle en fait partie intégrante. Lorsqu'elle est externe, on considère qu'elle appartient à un autre document technologique.[67]

En somme, lorsqu'un document est sur un support faisant appel à une technologie de l'information, on le qualifie de technologique. Ainsi, il a par exemple été déterminé qu'un ruban audio magnétique, c'est-à-dire une cassette, était un document technologique.[68]

Au sujet des documents technologiques, la LCCJTI nous enseigne les principes de l'universalité et de non-discrimination du support ou de la technologie utilisée. En application de ces derniers, des documents sur des supports différents qui comportent la même information possèdent la même valeur juridique[69] si leur intégrité est assurée et s'ils respectent les règles de droit qui les régissent.[70] Autrement dit, au Québec, la valeur juridique d'une preuve documentaire technologique n'est pas minée par sa nature technologique si son **intégrité** est assurée.[71]

L'INTÉGRITÉ, TALON D'ACHILLE DU DOCUMENT TECHNOLOGIQUE

64 LCCJTI, art. 1 par. 3 *in fine*.

65 Patrick Gingras et François Sénécal, « Métadonnées : Plaidoyer pour des mal aimées et des incomprises », (2015) 74 *R. du B.* 249, cités dans *Benisty* c. *Kloda*, 2018 QCCA 608, par. 111.

66 LCCJTI, art. 17 al. 4 : « directement ou par référence ».

67 LCCJTI, art. 3.

68 *Benisty* c. *Kloda*, 2018 QCCA 608.

69 La valeur juridique s'entend notamment de « produire des effets juridiques et [d]être admis en preuve », LCCJTI, art. 5 al. 1.

70 On retrouve notamment cette formulation à l'article 9 de la LCCJTI.

71 Pour approfondir sur la notion d'intégrité en matière de preuve documentaire technologique, voir *Hewlett-Packard France c. Matrox Graphics Inc.*, 2020 QCCS 78, par. 110 et suiv.

En droit de la preuve, celui qui souhaite admettre en preuve un écrit ou un élément matériel de preuve[72] doit en prouver **l'authenticité,** laquelle est composée des deux éléments suivants[73] :

- **L'intégrité** d'un document est assurée lorsqu'il est possible de (a) vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité, et que (b) le support qui porte l'information lui procure la stabilité et la pérennité voulue. L'intégrité du document doit être maintenue tout au long de son cycle de vie, c'est-à-dire de sa création à sa destruction.[74]

- Le **lien entre une personne et le document**, lequel est généralement assuré par la signature,[75] mais pourrait également l'être par tout autre moyen permettant de remplir cette fonction (ex. authentification à un ou plusieurs facteurs, témoignage, documentation, y compris les métadonnées, etc.).[76] En présence d'un document technologique, ces moyens sont circonscrits à l'article 38 LCCJTI.

De ce qui précède, l'intégrité est un sous-ensemble de l'authenticité. Or, dans le monde technologique, la notion d'intégrité est si proéminente qu'elle semble être la condition *sine qua non* de l'admission en preuve.[77] De plus, aucune disposition de la LCCJTI et du chapitre afférent du C.c.Q.[78] n'énonce expressément que l'authenticité est également tributaire de la preuve du lien avec l'auteur.

Selon la doctrine,[79] l'accent marqué sur l'intégrité en matière de document technologique dans la loi s'expliquerait par le caractère fondamentalement moins fiable de ce support.[80] En effet, la modification

72 À l'égard de l'élément matériel de preuve, voir C.c.Q., art. 2855.

73 V. Gautrais, préc., note 62, p. 182-183.

74 LCCJTI, art. 6.

75 LCCJTI, art. 39.

76 V. Gautrais, préc., note 62, p. 184.

77 Voir, par exemple, l'art. 5 al. 1 LCCJTI et l'art. 2838 C.c.Q. Voir aussi *Directeur des poursuites criminelles et pénales c. 3341003 Canada inc. (Restaurant Pizzédélic)*, 2015 QCCQ 8159, par. 13 : « Donc, c'est l'intégrité du document technologique qui détermine son admissibilité et sa force probante. Même si le document est sur plusieurs supports en même temps, l'intégrité de chacun découle du fait que l'information que porte le document est intacte ». Toutefois, autant pour le document papier que technologique, la preuve d'authenticité est requise dans tous les cas afin d'admettre en preuve un écrit ou un élément matériel de preuve, préc., note 75.

78 C.c.Q., art. 2837 à 2842.

79 Gilles de Saint-Exupéry, *Le document technologique original dans le droit de la preuve au Québec*, Montréal, Faculté des études supérieures, Université de Montréal, 2012, p. 80.

80 V. Gautrais, préc., note 62, p. 10.

d'une donnée numérique ne laisse bien souvent aucune trace, au contraire des écrits papier. De plus, l'atteinte à l'intégrité d'un tel document est plus aisée, justement en raison de l'avènement de technologies qui le permettent. Prenons l'exemple des photos de magazines « photoshopées », des *deepfakes* ou encore du code HTML d'une page Internet, dont les falsifications sont bien souvent indétectables, rendant par ailleurs leur quantification difficile. Dans le cas de *Richard c. Gougoux*,[81] la Cour supérieure a d'ailleurs reconnu la faiblesse de la fiabilité d'un courriel vu la facilité avec laquelle il pouvait être modifié, altéré ou falsifié. Notons que l'utilisation du courriel est extrêmement fréquente à titre de preuve judiciaire.

162

En pratique, néanmoins, l'immense majorité des documents technologiques déposés sont admis sans contestation. Ainsi, la preuve d'authenticité a rarement fait l'objet de débats judiciaires depuis l'adoption de la LCCJTI.

Enfin, une fois un écrit jugé admissible par la Cour, sa force probante dépend de la qualification qui lui est donnée en tant que type d'écrit[82] ou, le cas échéant, de sa qualification à titre d'élément matériel de preuve.[83] Par exemple, un acte authentique fait preuve à l'égard de tous,[84] tandis qu'un simple écrit, s'il tient lieu de témoignage, possède une valeur probante qui est laissée à l'appréciation du tribunal.[85]

Dans tous les cas, le fait qu'un support technologique soit en jeu ne change pas la nécessité de qualifier le document en tant que moyen de preuve (écrit, témoignage, élément matériel, aveu ou présomption).[86] C'est ce que le professeur Claude Fabien exprime métaphoriquement en ces termes : « [j]'aime bien dire que le document technologique est un mode de preuve caméléon. Il prend la couleur et la forme du moyen de preuve dont il accomplit la fonction. »[87]

IMPORTANCE GRANDISSANTE DE LA MÉTADONNÉE

81 *Richard c. Gougoux*, 2009 QCCS 2301, par. 75 et 76.

82 Sur la différence entre « admissibilité » et « force probante », voir *Cadieux c. Service de gaz naturel Laval inc.*, 1991 QCCA 3149.

83 C.c.Q., art. 2854 et 2856.

84 C.c.Q., art. 2818.

85 C.c.Q., art. 2832 et 2845.

86 C.c.Q., art. 2811.

87 Claude Fabien, « L'impact des technologies de l'information sur le système de preuve de droit civil québécois », (2004) *106 R. du N.* 493, 499.

Ces dernières années, la notion de métadonnée a pris en importance afin d'évaluer l'admissibilité et la force probante d'un document technologique. À cet égard, la première décision à marquer les esprits de par l'importance qu'elle accorde aux métadonnées est *Sécurité des Deux rives,* en 2013.[88] Dans ce jugement, la Cour du Québec exige des garanties minimales afin d'admettre en preuve un courriel. La cour souligne ainsi la pauvreté de la preuve d'intégrité du courriel en raison de l'absence de métadonnées qui y seraient associées.[89] Plus récemment dans la décision *Benisty* c. *Kloda* (2018), la Cour d'appel du Québec va jusqu'à reconnaître qu'un document qui contiendrait des métadonnées satisfaisantes serait dispensé de la réalisation d'une preuve **d'intégrité**, voire d'authenticité.[90]

Les métadonnées servent ainsi à documenter un large éventail d'événements associés à un fichier numérique :

> Les métadonnées du document, en plus de retranscrire l'information telle qu'on la lirait dans un document papier, permettent de déceler les modifications que le document a subies, les différentes mises à jour dont il a fait l'objet. De sorte qu'il serait aisé pour une partie de prouver que le document présenté par la partie adverse n'est pas intègre, s'il a été modifié en cours de cycle de vie, grâce à l'extraction des métadonnées. Elles jouent un rôle de documentation de la façon dont le document technologique a été géré. Elles révèlent un ensemble de faits, de données, qui peuvent constituer l'assise de la preuve de certains faits matériels, telle l'authenticité (et intégrité), rendant le document mis en preuve plus ou moins probant.[91]

Bien que constituant des indices très importants, les métadonnées ne sont pourtant pas absolues.[92] Selon la situation, elles pourraient être erronées, incomplètes, absentes ou encore falsifiées. Par exemple, des

88 Sécurité des Deux-Rives ltée c. Groupe Meridian construction restauration inc., 2013 QCCQ 1301.

89 *Id.*, par. 51 : « La preuve de l'intégrité du "document" se fera donc par la divulgation des métadonnées qui doivent être révélées sur le document, et ce, indépendamment du type de support employé. »

90 *Benisty*, par. 103 et 105 : « [a]insi, lorsqu'un enregistrement audio est accompagné de métadonnées et que cette documentation satisfait, selon le tribunal, à l'exigence d'authenticité du document, la partie qui produit cet enregistrement sera dispensée de faire une preuve d'authenticité ». Certains auteurs relativisent toutefois ce propos, voir P. Gingras et F. Sénécal, préc., note 66.

91 Christopher Dicceca, *La preuve par métadonnées*, mémoire de maîtrise, Montréal, Faculté de droit, Université de Montréal, 2014, p. 92, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/12536/dicecca_christopher_2015_memoire.pdf?sequence=2&isAllowed=y>.

92 P. Gingras et F. Sénécal, préc., note 66, 291.

logiciels tels *Exifer* ou *Metadata* ++ se vantent justement d'extraire les métadonnées d'un document dans le but de les altérer. C'est pourquoi les métadonnées doivent préalablement « faire l'objet d'une preuve d'authenticité avant qu'il y soit prêté foi, et qu'une fois cela fait, qu'il soit évalué si cette documentation permet de conclure que le document auquel il réfère est fiable ».[93]

En somme, les métadonnées ne suffisent pas toujours. Ce constat constitue une limite intrinsèque de fiabilité du support technologique, lequel comporte son lot de facilitateurs que le support papier ne permet pas, mais dont la fiabilité est fondamentalement moins élevée. Conséquemment, la preuve technologique nécessite des garanties supplémentaires que la blockchain pourrait offrir.

3.2. QUAND LA BLOCKCHAIN VIENT AU SECOURS DU DOCUMENT TECHNOLOGIQUE

> The law is to be a reflection of reality, but it is always playing « catch-up,» i.e., lags behind what reality needs by way of legal infrastructure for its adequate regulation.[94]

Les principes généraux de la preuve technologique présentés, érigeons un pont entre ces derniers et les considérations techniques de la blockchain exposées en première partie. Ainsi, nous traduirons, en termes juridiques, ce qu'offrent les fonctions d'insertion de métadonnées dans une blockchain publique. Également, nous déterminerons dans quelle mesure la technologie blockchain peut être appréhendée par les lois en vigueur au Québec.

L'EMPREINTE NUMÉRIQUE D'UN DOCUMENT EST UNE MÉTADONNÉE

Comme mentionné, la fonction OP_RETURN (ou le champ prévu à cet effet lors de la création d'une transaction dans Ethereum) permet d'inscrire l'empreinte numérique d'un document dans un bloc (ou dans un contrat intelligent). Or, l'empreinte numérique d'un document correspond à une « donnée sur une donnée », c'est-à-dire à une métadonnée. Juridiquement

93 *Id.*

94 Ken Chasse, « Challenging Electronic Systems' and Devices' Ability to Produce Reliable Evidence », *SSRN.com*, 25 avril 2019, p. 3, en ligne : <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3378077>.

parlant, il s'agirait donc de sécuriser la métadonnée associée à un document technologique dans un autre document technologique [95]préalablement à tout litige. Cette métadonnée est alors externe au document qu'elle renseigne,[96] constituant une forme de journalisation sophistiquée.

Rappelons que pour être admissible en preuve, un écrit (ou un élément matériel de preuve) doit faire l'objet d'une preuve d'authenticité, laquelle comprend une preuve d'intégrité et du lien avec son auteur. En matière technologique spécifiquement, **l'intégrité** est pourtant le talon d'Achille du document et de ses métadonnées, les falsifications étant aisées, leur détection complexe.

Or, qu'en serait-il si l'empreinte numérique d'un document était préalablement insérée dans un registre infalsifiable, immuable, décentralisé, sécurisé et parfaitement transparent ?

INTÉGRITÉ

L'utilisation d'une fonction de hachage permet justement de garantir la préservation de l'intégrité de l'information d'un document, c'est-à-dire que celle-ci n'a pas été altérée et qu'elle est maintenue dans son intégralité.[97] En effet, l'exercice de comparaison des valeurs de hachage d'une fonction implique qu'une légère modification de l'information contenue dans le premier document « haché » génère une valeur différente pour le second issu de la modification (*supra*, p. 24).[98] Il faut donc comprendre que le hachage ne permet pas d'empêcher une atteinte effective à l'intégrité d'un document, mais bien de la détecter.

En ce sens, la cristallisation de la valeur de hachage du document dans une blockchain publique est garante de son existence et de l'horodatage de cette existence. Ainsi, la comparaison des valeurs de hachage susmentionnée peut être faite à partir d'un moment vérifiable. La

95 La blockchain pourrait être assimilée à une base de données au sens de l'article 3 al. 2 LCCJTI : « [p]our l'application de la présente loi, est assimilée au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite ».

96 P. Gingras et F. Sénécal, préc., note 66, 272.

97 LCCJTI, art. 6 al. 1.

98 Tous les algorithmes de hachage ne disposent pas des mêmes garanties. Par exemple, l'algorithme *Message Digest 5* (MD5) est reconnu comme étant peu fiable, tandis que les algorithmes de type *Secure Hash Algorithm* (SHA) disposent d'une fiabilité établie. SHA-256 est notamment utilisé dans la blockchain *Bitcoin*. Voir la figure sur le fonctionnement de l'algorithme de hachage, *supra* p. 11.

blockchain étant immuable, il est par ailleurs impossible de falsifier cette information dès lors qu'elle est insérée dans un bloc de la chaîne, bien qu'elle soit accessible à quiconque dispose d'un réseau Internet, à tout moment.

LIEN AVEC L'AUTEUR

Rappelons que le document qui doit être lié à son auteur afin d'être admis en preuve n'est pas la copie du bloc contenant l'empreinte numérique, mais le document d'origine dont est issue cette empreinte. En effet, c'est le contenu de ce document dont on tente d'établir l'authenticité à l'aide de la blockchain et d'un algorithme de hachage. Ainsi, à l'égard de ce document, le lien avec l'auteur peut être établi par les moyens conventionnels susmentionnés (*supra*, p. 21). Par exemple, l'auteur d'un contrat pourrait être identifié par sa signature, en l'absence de contestation,[99] tandis que l'auteur d'un simple écrit pourrait venir témoigner pour établir ce lien.[100]

166

SÉCURITÉ JURIDIQUE

Au risque de nous répéter, la fixation de l'empreinte numérique d'un document dans une blockchain publique équivaut à la constitution d'une preuve de l'état d'un document à un moment donné. Pourtant, la méthode implique également une preuve d'intégrité et, au besoin, permet de conserver le caractère confidentiel d'un document, par exemple s'il contient des renseignements personnels.[101] En effet, seule l'empreinte numérique d'un document est insérée dans la blockchain publique choisie, le document lui-même n'étant pas divulgué.

Bien qu'aucune jurisprudence québécoise n'ait expressément admis la validité d'une preuve par blockchain à ce jour, les discours du législateur et des tribunaux québécois semblent d'ores et déjà s'orienter vers une approche souple et libérale à l'égard de l'intégration des technologies de l'information en droit (par exemple, l'adoption du nouveau code de

99 C.c.Q., art. 2828.

100 C.c.Q., art. 2831 à 2836.

101 *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1, art. 53 : « les renseignements personnels sont confidentiels sauf dans les cas suivants : [...] ».

procédure civile en 2016,[102] l'utilisation de signatures électroniques,[103] etc.).

Sur le plan législatif, l'adoption de la LCCJTI en 2001 s'inscrivait déjà dans cet élan, notamment avec l'introduction des principes de neutralité technologique et d'équivalence fonctionnelle.[104] Selon ces derniers, il ne faut pas favoriser un support ou une technologie plutôt qu'un ou une autre. Ainsi, tant qu'un document est apte à réaliser les mêmes fonctions qu'un autre sur un support ou une technologie différente, les deux documents détiennent la même valeur juridique et un juge ne peut refuser d'en reconnaître la validité du seul fait que l'un d'eux soit sur un support qui utilise les technologies de l'information. Sur le plan jurisprudentiel, l'une des fonctions des tribunaux est d'appliquer et d'adapter le droit à la mouvance des sociétés, y compris dans son volet technologique.

Ainsi, **nous ne doutons pas que le cadre juridique soit assez souple pour être interprété comme admettant une preuve par blockchain**, si une telle blockchain présente les garanties requises par la loi (ex. intégrité).

D'ailleurs, le texte de la LCCJTI a prévu l'édiction de normes ou standards techniques, notamment pour :

> [...] garantir l'intégrité d'un document technologique par des mesures de sécurité physiques, logiques ou opérationnelles ainsi que par des mesures de gestion documentaire adéquates pour en assurer l'intégrité au cours de tout son cycle de vie ;[105]

Pourtant, près de 20 ans après son adoption, les dispositions afférentes aux normes et standards techniques[106] ne sont toujours pas mises en œuvre. Dans l'éventualité où ils le seraient, nous pensons qu'il faudrait s'intéresser aux solutions qu'offre la blockchain, car dans la panoplie de services proposés sur le marché afin de garantir l'intégrité d'un document,

102 Ex. : C.p.C., art. 26.

103 *R.* c. *McIvor*, 2008 CSC 11, par. 30.

104 Pour approfondir sur ces principes, voir : Pierre Trudel, Introduction à la Loi concernant le cadre juridique des technologies de l'information, Cowansville, Éditions Yvon Blais, 2012.

105 LCCJTI, art. 64 par. 4.

106 LCCJTI, art. 63 à 69.

les solutions blockchain sont sans doute parmi les moins coûteuses,[107] tout en étant des plus fiables.[108]

3.3. L'ENVIRONNEMENT « TECHNOLOGIQUE » QUI SOUTIENT L'ACTIVITÉ DES TRIBUNAUX

Sur le plan technologique, les tribunaux de droit commun s'appuient sur des infrastructures qui datent. En effet, les procédures sont jugées lentes, complexes et coûteuses, si bien que l'État canadien perdrait près de 746 millions de dollars par an en raison de l'inefficacité du système judiciaire.[109] Les projets de transformation de la justice lancés en réponse à l'arrêt Jordan[110] ayant amorcé un changement de cap politique, une modernisation institutionnelle ne saurait tarder.

168

Toutefois, dans le contexte actuel, comment anticiper la présentation d'une preuve par blockchain devant un tribunal encore attaché au papier ?

D'une part, comme mentionné, la blockchain étant un registre informatisé, la présentation d'une preuve qui y serait contenue devrait être imprimée afin d'être présentée devant nos tribunaux. Au sens de la loi québécoise, l'impression constitue pourtant un transfert de l'information[111] et implique généralement des garanties de fiabilité appelées « documentation »,[112] lesquelles sont lourdes de formalités. En sus, ce passage vers le support papier nous apparaît antagoniste avec l'essence même de la blockchain, soit un registre numérique transparent, ouvert et disponible à tous en temps réel sur la toile. En effet, l'authenticité des données contenues dans une blockchain est garantie par le réseau informatisé connecté. Une fois imprimé, le document ne devient donc qu'une simple capture d'écran de la blockchain, soit un

107 Seuls les frais de la transaction devraient être payés, lesquels varient selon les blockchains. Par exemple, sur la blockchain Ethereum, les frais de transactions s'élèvent à 0.1 $ US.

108 À titre indicatif, voir la récente norme ISO/TC 307 intitulée « Technologies des chaînes de blocs et technologies de registre distribué », en ligne : < https://www.iso.org/fr/committee/6266604/x/catalogue/p/1/u/0/w/0/d/0>.

109 Forum canadien de la justice civile, *Everyday Legal Problems and the cost of Justice in Canada*, 2015, en ligne : <http://www.cfcj-fcjc.org/sites/default/files//CostofJustice_overivewfactsheet%20.pdf>.

110 *R.* c. *Jordan*, 2016 CSC 27.

111 C.c.Q., art. 2841.

112 LCCJTI, art. 17 et C.c.Q., art. 2841. Nuançons toutefois le propos, car en pratique, les juges ne réclament généralement pas la documentation et ne sanctionnent pas les parties lorsqu'elle n'accompagne pas le document qui émane d'un transfert, voir *Droit de la famille — 1612062016*, QCCS 2378, dans lequel le juge refuse une objection qui semble bien fondée sur la documentation.

élément matériel qui nécessite lui-même une preuve d'authenticité.[113] C'est ce qui est exprimé dans le récent jugement *Fraternité des policiers et policières de Sherbrooke c. Sherbrooke (Ville de)* :[114]

> Il faut prendre en compte que le format papier n'est pas la meilleure preuve d'un fichier électronique. Les risques de fabrication et d'altération augmentent avec l'évolution de la technologie, d'où l'importance des moyens pour vérifier l'authenticité de ces preuves matérielles.

D'autre part, la preuve technologique est fondamentalement complexe et nécessite bien souvent une spécialisation afin d'en saisir les rouages,[115] voir une preuve experte. Dans *Capitale en fête inc.* c.

Ouellet,[116] par exemple, la lecture de simples métadonnées sur des photographies avait nécessité une telle preuve. Or, la blockchain pourrait être encore plus complexe d'utilisation que les métadonnées renseignant un document technologique.[117] L'utilisation des technologies, et de la blockchain plus particulièrement, impliquerait-il alors un système de justice à deux vitesses dans lequel seuls les plus fortunés ont les moyens d'y recourir en se payant les services d'un expert ?[118] Une chose est certaine, tant que les magistrats ne seront pas formés en ces matières, le fardeau de la preuve continuera de reposer sur les justiciables — et plus particulièrement sur les demandeurs — en vertu de l'une des plus vieilles règles de notre droit :

> « Celui qui veut faire valoir un droit doit prouver les faits qui soutiennent sa prétention.

113 C.c.Q., art. 2855.

114 *Fraternité des policiers et policières de Sherbrooke c. Sherbrooke (Ville),* 2019 CanLII 82465 (QC SAT), par. 57.

115 À titre illustratif, voir *Benisty* c. *Kloda*, 2018 QCCA 608, par. 117 : « [e]n pratique, puisque l'atteinte à l'intégrité d'un support technologique se démontre généralement avec un expert [...]. »

116 2019 QCCQ 2607.

117 Dans l'affaire de meurtre de *Dennis James Oland v. R.*, 2015 NBQB 243, l'un des liens établis afin de condamner l'accusé était la preuve de localisation du téléphone de la victime par sa société de téléphonie (voir par. 81 *in fine* de la décision). Toutefois, la décision est présentement en appel notamment puisque ladite preuve aurait été mal interprétée. On y saisit les enjeux de la justesse d'interprétation de la preuve électronique.

118 K. Chasse, préc., note 95, p. 7 : « [o]nly rich and institutional clients can pay for the experts who will educate their lawyers as to the technology that produces the evidence, and be expert witnesses if required. »

> Celui qui prétend qu'un droit est nul, a été modifié ou est éteint doit prouver les faits sur lesquels sa prétention est fondée. »[119]

En définitive, bien que nous pensions la loi québécoise assez souple pour appréhender la blockchain comme outil technologique probatoire, nous croyons qu'il faille attendre le résultat des projets de transformation de la justice au Québec avant de réellement bénéficier du développement des technologies dans le contexte judiciaire, et notamment de la blockchain.

170

119 C.c.Q., art. 2803.