

Université de Montréal

**La reconnaissance juridique des contrats intelligents
face à la réglementation globale des technologies**

par Maria Ivone Godoy

Faculté de Droit

Mémoire présenté en vue de l'obtention du grade de Maître en Droit (LLM),
option Droit des technologies de l'information

Avril 2019

© GODOY, 2019

Résumé

La technologie de la chaîne de blocs peut être résumée en un réseau décentralisé et distribué de registre de transactions numériques. Sa mise en œuvre dans le marché des cryptomonnaies a été suivie par d'autres utilisations, comme les Organisations autonomes décentralisées (DAO) et les contrats intelligents. Ce mémoire s'attachera à examiner deux volets de la reconnaissance juridique des contrats intelligents : au regard des normes étatiques déjà existantes ou en cours d'élaboration au sein de différentes juridictions, y compris le Québec, et au regard du potentiel des normes alternatives. Le contexte de la globalisation, du pluralisme juridique et des mutations de la souveraineté étatique est pris en considération à cette fin. La première partie de cette étude se concentre sur les aspects technologiques, afin de présenter les fondements du fonctionnement des contrats intelligents. La seconde partie est consacrée à une analyse du panorama juridique. L'encadrement normatif du droit positif présente d'ores et déjà des normes applicables aux contrats intelligents, certaines générales et d'autres spécifiques. Il est également pris en considération que les normes alternatives peuvent être un moyen d'harmoniser un contexte globalisé. Une harmonisation dans cette direction serait importante visant à renforcer la réglementation des nouvelles relations issues de la démarche technologique. L'ensemble de ces faits rend l'utilisation des normes alternatives opportune, conjointement avec les normes étatiques, dans le cadre de la réglementation des nouvelles technologies afin, notamment, de surmonter l'incertitude juridique encore existante dans ce milieu.

Mots-clés : contrats intelligents, chaîne de blocs, droit des technologies de l'information, droit mou, normes alternatives, globalisation, corégulation, souveraineté, régulation, normalisation.

Abstract

The Blockchain technology is essentially a decentralized and distributed network of digital transactions records. Its implementation on the cryptocurrency market was followed by other applications, such as the Decentralized Autonomous Organization (DAO) and Smart Contracts. This thesis will focus precisely on the legal recognition of smart contracts in the light of the established positive law and the regulations currently being drafted in various jurisdictions, including Quebec, as well as in the light of the soft law. The context of globalization, legal pluralism and state sovereignty changes are taken into consideration. The first part of this study focuses on the technological aspects in order to present the foundations of the Smart Contracts operation. The second part is dedicated to analyzing the current juridical panorama. The normative framework of the positive law already provides applicable regulations to Smart Contracts, some general, others more specific. It is further understood that the soft law could be a way of harmonizing the current context. A harmonization in this direction would be relevant in order to enhance the essential regulatory framework of new relations coming from the technological development. Given all these facts, the soft law along with hard law seem to be appropriate to chart the legal framework for the new technologies, in order to overcome the many legal uncertainties existing in this field.

Keywords : smart contracts, Blockchain, Information Technology Law, soft law, globalization, co-regulation, sovereignty, regulation, standardization.

Table des matières

Résumé.....	i
Abstract.....	ii
Table des matières.....	iii
Liste des figures.....	v
Liste des sigles et abréviations	vi
Remerciements	viii
INTRODUCTION	1
TITRE I – CONTRATS INTELLIGENTS : APPROCHE TECHNOLOGIQUE.....	5
Chapitre 1 – L’histoire et la technologie des contrats intelligents.....	5
1.1. Aperçu des aspects techniques de la chaîne de blocs	11
1.1.1. Les blocs et la formation de la chaîne.....	16
1.1.2. Caractéristiques des chaînes de blocs	18
1.1.2.1. Système distribué et décentralisé	21
1.1.2.2. Sécurité	23
1.1.2.3. Consensus	25
1.2. La Chaîne de blocs 2.0.....	28
1.2.1. D’autres détails à propos de la définition et du fonctionnement des contrats intelligents	31
Chapitre 2 – Les aspects pratiques de la chaîne de blocs et des contrats intelligents.....	35
2.1. Des avantages pratiques de la mise en œuvre des contrats intelligents	36
2.1.1. Désintermédiation, gain de temps et d’argent.....	36
2.1.2. Sécurité	38
2.1.3. Transparence et précision	39
2.1.4. Absence de papier	41
2.1.5. Efficience	41
2.2. Des risques particuliers de la mise en œuvre de contrats intelligents.....	42
2.2.1. Manque de compréhension	43
2.2.2. Erreurs de programmation	44
2.2.3. L’immuabilité	47
2.3. Les aspects pratiques des chaînes de blocs: cas d’usage	50
2.3.1. Services financiers	51
2.3.2. Assurance.....	54
2.3.3. Commerce d’énergie.....	55
2.3.4. L’industrie créative	57
TITRE II – CONTRATS INTELLIGENTS : APPROCHE JURIDIQUE	61
Chapitre 1 – Les mutations du droit face aux innovations technologiques.....	61
1.1. Le droit étatique et les enjeux globaux	62
1.1.1. Les contrats intelligents devant le « <i>hard law</i> » aujourd’hui.....	71
1.1.2. Le cadre juridique québécois	73
1.1.3. Les normes étatiques en vigueur ou en cours d’élaboration.....	83
1.1.4. Est-ce que le code pourrait devenir la loi? (« <i>Code is law?</i> »)	87

Chapitre 2 – La reconnaissance juridique des contrats intelligents sous l’angle des normes alternatives	93
2.1. Le rôle juridique des normes alternatives	93
2.1.1. La perspective de l’autorégulation et de la corégulation	96
2.2. Les contrats intelligents face aux normes alternatives.....	100
2.2.1. Des normes alternatives visant à l’harmonisation du droit commercial international: le CNUDCI et l’UNIDROIT.....	103
2.2.2. Les normes alternatives techniques : ISO/TC 307, ISO/DTR 23455 et ISO/AWI 23259	108
2.3. La reconnaissance juridique des contrats intelligents dans le contexte des normes alternatives	114
Considérations finales	120
Bibliographie	i
ANNEXE I – CERTAINES APPLICATIONS DE LA CHAÎNE DE BLOCS	xxiii

Liste des figures

Figure 1. Formation d'une chaîne de blocs	17
Figure 2. Fonctionnement de machines distributrices	33
Figure 3. Les acteurs au niveau international, mondial et global	64
Figure 4. La formation d'un contrat Ricardian.	78

Liste des sigles et abréviations

Termes informatiques

WWW : *World Wide Web*

ECDSA : *Elliptic Curve Digital Signature Algorithm*

P2P : *peer-to-peer* (pair-à-pair)

TCP/IP : *Transmission Control Protocol/Internet Protocol*

SMTP : *Simple Mail Transfer Protocol*

DAO : *Decentralized Autonomous Organization* (Organisation autonome décentralisée)

DLT : *Distributed Ledger Technology* (Technologie des registres distribués)

TIC : Technologies de l'information et des communications

Termes juridiques

C.c.Q. : Code Civil du Québec

LCCJTI : Loi Concernant le cadre juridique des technologies de l'information

PACTE : Plan d'action pour la croissance et la transformation des entreprises

Loi HB : *House Bill*

Loi SB : *Senate Bill*

ODR : *Online dispute resolution* (Règlement des litiges en ligne)

RGPD : Règlement Général pour La Protection des Données

Autres sigles et abréviations

GPS : *Global Positioning System*

FBI : *Federal Bureau of Investigation*

ETH : Ethereum

ETC : *Ethereum Classic*

CNIL : Commission nationale de l'informatique et des libertés

XRP : Ripple

ISO : *International Standards Organization* (Organisation internationale de normalisation)

ICO : *Initial Coin Offering*

FINMA : *Swiss Financial Market Supervisory Authority*

AQIII : Association québécoise des informaticiennes et informaticiens indépendants

CCI : Chambre de commerce internationale

CNUDCI : Commission des Nations Unies pour le droit commercial international

UNIDROIT : Institut international pour l'unification du droit privé

CENELEC: Comité européen de normalisation électrotechnique

CEN: Comité européen de normalisation

Remerciements

Je tiens à exprimer mes sincères remerciements au Monsieur le Professeur Karim Benyekhlef pour avoir accepté de diriger ce mémoire. Sa judicieuse orientation a enrichi mes réflexions critiques à propos des répercussions de la technologie sur le droit. Je suis fier d'avoir eu l'occasion de le rencontrer et de recevoir leurs fructueux commentaires et remarques.

Je souhaiterais remercier la Faculté de droit de l'Université de Montréal, pour son soutien académique, mais également financier, rendu possible par la générosité de Monsieur Stéphane Dansereau, du cabinet Dentons Canada, ainsi que du Fonds André-Savoie et de la Faculté des études supérieures et postdoctorales.

J'aimerais également adresser mes remerciements les plus chaleureux à mes proches, à commencer par mon conjoint, Allan Martin, qui m'a énormément encouragée tout au long de mon nouveau parcours académique. Je le remercie pour sa foi en mon succès et pour sa patience. Merci d'avoir cru en ma réussite et m'avoir soutenue jour après jour. *Obrigada!*

Un grand merci à mes parents, Evaneide e Edson, qui malgré la distance arrivent toujours à me redonner le sourire, particulièrement quand je dois relever des défis. À mes beaux-parents, Enir et Alvacir, qui eux aussi ont joué un rôle important dans ma réussite universitaire. Je voudrais leur exprimer mes remerciements les plus sincères pour leurs encouragements. Sans leur soutien sans faille ce mémoire n'aurait pas pu prendre vie.

Tout au long de mon parcours à l'Université de Montréal, j'ai eu la joie de rencontrer des personnes exceptionnelles, surtout Madame la Professeure Éloïse Graton, chargée du premier cours que j'ai suivi à l'université et qui m'a permis de découvrir la maîtrise en droit des technologies, ainsi que mes collègues Mélanie Ruiz-Pardo, qui m'a encouragée presque quotidiennement à atteindre mes objectifs, Caroline P. M. Pereira et Paola Alvarez Bautista, dont la présence a égayé mes journées, Clémence Frances, avec qui j'ai partagé des moments importants de la rédaction de cette étude, et Carolina Suarez, dont l'enthousiasme m'a rendue encore plus forte pour relever les défis de la maîtrise.

Je vous en suis très reconnaissante.

INTRODUCTION

“First, we want to establish the idea that a computer language is not just a way of getting a computer to perform operations but rather that it is a novel formal medium for expressing ideas about methodology. Thus, programs must be written for people to read, and only incidentally for machines to execute.”
(Hal Abelson & Gerald Jay Sussman, dans le livre Structure and Interpretation of Computer Programs, 1996)

La création de nouvelles relations et défis est inhérente au concept de révolution. Il en va de même quand il s’agit de la révolution numérique. Alors que la société industrielle connaissait une crise, au début des années 70, les technologies ont commencé à prendre une place de plus en plus centrale dans le monde. Depuis, cette révolution se reproduit à chaque fois qu’une nouvelle technologie est créée et est rendue accessible au public.

Les télécopieurs, les traceurs GPS, l’Internet, les téléphones portables, les photos et vidéos numériques, toutes ces innovations influencent les relations personnelles et commerciales, transcendent les frontières géopolitiques établies, conduisent à l’émergence d’un monde plus « délocalisé ». Des avantages, des inconvénients et des enjeux particuliers apparaissent dans des contextes alors inconnus, atteignant ainsi les domaines les plus divers, comme le domaine juridique.

Au gré des innovations, les tâches ordinaires s’automatisent davantage. Outre notre quotidien, les technologies redéfinissent également les frontières des pays permettant une communication accélérée. Enfin, elles modifient la structure du monopole du pouvoir étatique, lequel devient alors partagé avec d’autres acteurs, comme les entreprises et les organismes interétatiques. À la lumière de ces circonstances, il convient de revisiter les normes régissant l’ensemble des relations sociales et commerciales afin de les réinterpréter ou de les mettre à jour

le cas échéant. Ainsi, l'architecture juridique se redéfinit au regard des mutations apportées par les technologies.

L'essor de la technologie de la chaîne de blocs, en 2008, et du protocole Ethereum, en 2014, ont mis en lumière les contrats intelligents ces derniers temps. L'idée d'automatiser les contrats ne date pas d'aujourd'hui. En effet, en 1996, Nick Szabo a publié un article abordant le sujet : « *Smart Contracts : Building Blocks for Digital Markets* »¹. Selon Szabo, l'exécution de diverses clauses contractuelles pourrait être automatisée au moyen de leur incorporation dans un matériel ou logiciel, rendant ainsi les éventuelles violations plus coûteuses et difficiles pour celui qui enfreint les termes du contrat.

Ces contrats sont l'une des technologies pouvant faire basculer les relations sociales et notamment commerciales dans un monde globalisé. Ainsi, certains évoquent une « révolution blockchain » pour parler du phénomène². Avant d'être en mesure d'analyser les aspects juridiques particuliers des contrats intelligents, il importe de comprendre certains de leurs aspects techniques afin de mieux connaître les limites et les perspectives de leur application (Titre I, chapitre 1).

Cette caractéristique du contrat intelligent est considérée comme l'un des avantages promus par la chaîne de blocs : la désintermédiation. Outre l'avantage susmentionné, la technologie des contrats intelligents permet aux différents acteurs qui l'utilisent de gagner du temps. Elle peut être aussi comprise dans une perspective de sécurité, de transparence, de précision du langage de programmation, d'absence de papier, d'efficience et d'efficacité juridique (Titre I, chapitre 2.1.). Cependant, certains inconvénients sont à signaler, comme le manque de compréhension

¹ SZABO, N., *Smart Contracts: Building Blocks for Digital Markets*, 1996, en ligne: < <https://goo.gl/wQH4PX> > (consulté le 10 avril 2018)

² C'est le cas, par exemple, de l'ouvrage intitulée: « La révolution blockchain », de Philippe Rodriguez.

de ces technologies, les erreurs de programmation et l'immutabilité de la chaîne de blocs, lesquels seront également abordés dans cette étude (Titre I, chapitre 2.2.).

Pour ceux qui arrivent à employer les avantages du contrat intelligent tout en surmontant ses inconvénients, les usages sont multiples et s'opèrent dans divers secteurs, comme dans le domaine des services financiers, de l'assurance, du commerce d'énergie et de l'industrie créative (Titre I, chapitre 2.3.).

Face aux applications concrètes, par conséquent, le droit est appelé à prendre position visant à protéger la sécurité juridique au sein de ces nouvelles relations et de prévoir leurs conséquences. C'est ainsi que la reconnaissance juridique des contrats intelligents devient une question importante.

Lorsque nous traiterons de cette reconnaissance, nous l'aborderons au sens large en englobant le « *hard law* » (Titre II, chapitre 1) et les normes alternatives (Titre II, chapitre 2), sans distinction entre les étapes contractuelles. C'est-à-dire que l'analyse des normes applicables aux contrats intelligents abordera le moment de leur conclusion tout comme celui de l'exécution des engagements en découlant. L'une des problématiques soulevées par l'utilisation des contrats intelligents, et des technologies en général, concerne leur statut juridique dans une perspective globale de réglementation, qu'elle soit étatique ou paraétatique.

En ce qui concerne le droit positif, les États connaissent actuellement des mutations structurelles profondes quant au rôle qu'ils ont à jouer. Des concepts associés à ces mutations seront examinés au long de cette étude, comme le pluralisme juridique et l'internormativité. Toutefois, nous pouvons d'ores et déjà résumer ces changements comme une reconfiguration de la souveraineté étatique, impliquant l'intervention de nouveaux acteurs capables de dire le droit. Ainsi, l'État ne disposerait plus du monopole normatif. Par conséquent, les normes

alternatives pourraient acquérir plus de poids dans la mesure où il conviendrait de « repenser la pyramide des normes à l'ère des réseaux »³. Ainsi, le droit fondé au regard du positivisme serait repensé, par exemple, sous la forme d'un réseau sans la hiérarchisation préconisée jusqu'alors.

En effet, « de la crise du modèle pyramidal, émerge progressivement un paradigme concurrent, celui du droit en réseau, sans que disparaissent pour autant des résidus importants du premier, ce qui ne manque pas de complexifier encore la situation »⁴. Afin d'éviter que les contrats intelligents constituent des « zones de non-droit » ou des « vides juridiques », nous pourrions réfléchir sur la notion de droit conçu comme un réseau qui serait composé d'ensemble du droit positif et des normes alternatives.

La recherche présentée dans ce mémoire est à jour au 1er mars 2019.

³ Boris BARRAUD, *Repenser la pyramide des normes à l'ère des réseaux: Pour une conception pragmatique du droit*, L'Harmattan, Paris, 2012, p. 325, en ligne : < <https://hal-amu.archives-ouvertes.fr/hal-01369314/document> > (consulté le 18 fév. 2019)

⁴ François OST et Michel VAN DE KERCHOVE, *De la pyramide au réseau ? : pour une théorie dialectique du droit*, Publications des Facultés universitaires Saint-Louis, Bruxelles, 2002, p. 14.

TITRE I – CONTRATS INTELLIGENTS : APPROCHE TECHNOLOGIQUE

*“Every once in a while, a new technology,
an old problem, and a big idea
turn into an innovation.”*
(Dean Kamen, au magazine économique Forbes)

Chapitre 1 – L’histoire et la technologie des contrats intelligents

Encore aujourd’hui, il est difficile de discuter la situation juridique des contrats intelligents sans comprendre les aspects techniques qui composent leur conclusion et leur exécution. De la même façon, la perspective historique permet d’identifier le chemin parcouru par le raisonnement juridique afin que le droit, les innovations et les besoins actuels soient bien harmonisés.

C’est en 2008, partant alors du concept de B-Money exposé par Wei Dai en 1999⁵ et de BitGold énoncé par Nick Szabo en 2005⁶, que fut mise en œuvre la première chaîne de blocs (en anglais, *blockchain*). Il s’agit de la chaîne de la cryptomonnaie Bitcoin, conçue par Satoshi

⁵ “The protocol proposed in this article allows untraceable pseudonymous entities to cooperate with each other more efficiently, by providing them with a medium of exchange and a method of enforcing contracts. The protocol can probably be made more efficient and secure, but I hope this is a step toward making crypto-anarchy a practical as well as theoretical possibility.” Wei DAI, *B-Money*, 1999, en ligne : <<http://www.weidai.com/bmoney.txt>> (consulté le 18 sept. 2018)

⁶ “My proposal for bit gold is based on computing a string of bits from a string of challenge bits, using functions called variously ‘client puzzle function’, ‘proof of work function’, or ‘secure benchmark function’. The resulting string of bits is the proof of work. Where a one-way function is prohibitively difficult to compute backwards, a secure benchmark function ideally comes with a specific cost, measured in compute cycles, to compute backwards.” Nick SZABO, *Bit gold*, 08 décembre 2008, en ligne : <<http://unenumerated.blogspot.com/2005/12/bit-gold.html>> (consulté le 10 sept. 2018)

Nakamoto – pseudonyme d’une personne ou d’un groupe encore inconnu⁷. Par conséquent, c’est à partir du projet de déploiement de cette première cryptomonnaie que la technologie de la chaîne de blocs est apparue.

Toutefois, la recherche d’une technologie capable d’établir des relations de façon sécuritaire et sans opérateurs intermédiaires – ce qui est le principal but de la chaîne de blocs – n’est pas nouvelle. En fait, différentes technologies qui furent développées au fil des années sont à la l’origine de ce qui signifie la chaîne de blocs aujourd’hui.

Un des premiers fondements fut élaboré lors des recherches de Paul Baran en 1964, alors qu’il réussit à transmettre des informations entre deux ordinateurs au moyen de la technologie ensuite nommée "communication de paquets". C’est partir de cette découverte que le premier réseau d’ordinateurs fut créé par le Département de Défense des États-Unis sous le nom de ARPA, renommé par la suite ARPAnet et, enfin, DARPAAnet. Le but initial de ce réseau était de promouvoir la communication et les échanges entre les chercheurs et les étudiants universitaires⁸.

Au cours des années suivantes, les technologies sous-tendant les réseaux d’ordinateurs furent développées. Par exemple, en 1978, eut lieu l’implémentation du chiffrement RSA, un

⁷ Satoshi NAKAMOTO, *Bitcoin: A Peer-to-peer Electronic Cash System*, 2008, en ligne : <<https://bitcoin.org/bitcoin.pdf>> (consulté le 12 août 2018)

⁸ Primavera DE FILIPPI et Aaron WRIGHT, *Blockchain and the Law. The Rule of Code*, Cambridge, Harvard University Press, 2018, p. 14.

algorithme de cryptographie asymétrique⁹ favorisant la confidentialité¹⁰, la non-altération et la non-répudiation¹¹ des relations menées avec le protocole.

Toutefois, la création du World Wide Web en 1990 fut possiblement la plus grande révolution dans le domaine. Le créateur du premier site web, Tim Bernes-Lee, fit remarquer que la liaison d'information sur le Web permettait la découverte de faits, la création d'idées, le commerce et les relations à une vitesse et à une échelle inimaginable avant l'ère numérique.¹² Ces connexions pouvaient, selon lui, influencer les élections présidentielles, renverser des régimes autoritaires, donner du pouvoir à de grandes entreprises et nourrir nos réseaux sociaux. Le WWW a, par conséquent, permis le développement de la recherche, des publications, du commerce électronique, du courrier électronique et des réseaux sociaux. C'est pourquoi l'idée d'une monnaie électronique pouvait également prendre forme puisqu'elle était la suite logique de ces innovations.

⁹ « Cryptographie asymétrique. Cryptographie dans laquelle on utilise une paire de clés asymétriques, une clé publique et la clé privée correspondante, pour chiffrer et déchiffrer les données. Note(s): Dans un système cryptographique à clé publique, les utilisateurs possèdent deux clés relatives et complémentaires, l'une pouvant être révélée publiquement, l'autre devant rester secrète. La cryptographie asymétrique permet donc d'assurer que le message envoyé demeure confidentiel, et ce, sans être contraint d'utiliser, auparavant, une voie sûre afin de s'échanger les clés. La première clé demeure privée et secrète et n'est généralement connue que par son détenteur. L'autre est publique et figure habituellement dans un répertoire électronique. Si l'on utilise la clé publique pour chiffrer un message, la clé privée permet alors de le déchiffrer. La cryptographie asymétrique rend aussi possible l'utilisation de la signature numérique qui permet de corroborer l'origine d'un message. » GOUVERNEMENT DU QUÉBEC, OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Bibliothèque virtuelle*, « cryptographie asymétrique », en ligne : <http://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/internet/fiches/8383537.html> > (consulté le 12 août 2018)

¹⁰ « La confidentialité : seul le propriétaire de la clé privée pourra lire le message chiffré avec la clé publique correspondante », Jean-François PILLOU (dir.), *Algorithme de chiffrement RSA*, 17 sept. 2012, en ligne : < <https://www.commentcamarche.com/contents/208-algorithme-de-chiffrement-rsa> > (consulté le 13 août 2018)

¹¹ « La non-altération et la non-répudiation : seul le propriétaire de la clé privée peut signer un message (avec la clé privée). Une signature déchiffrée avec la clé publique prouvera donc l'authenticité du message », *Id.*

¹² Tim BERNERS-LEE. *Tim Berners-Lee on the Web at 25. The past, present and future*, 23 août 2014, en ligne : < <https://www.wired.co.uk/article/tim-berners-lee> > (consulté le 18 nov. 2018)

En 1990, David Chaum créa le DigiCash qui fit toutefois faillite en 1998¹³. En 1992, Scott Vanstone proposa un algorithme plus rapide que le chiffrement RSA, l'ECDSA¹⁴ – ce qui devient le mécanisme de signature utilisé par la chaîne de blocs Bitcoin afin d'assurer que seul le détenteur « x » d'un montant « y » puisse le dépenser.

En 1994, Nick Szabo promeut l'idée des smart contracts, concept qui sera abordé plus tard. Quelques années plus tard, entre 1998 et 2005, il développa aussi la monnaie numérique BitGold qui, tel que mentionné précédemment, influença le Bitcoin, mais qui ne fut pas adoptée puisqu'elle comprenait alors de nombreux paramètres vulnérables¹⁵.

Aux alentours de l'année 1995, l'Internet devenait plus démocratisé et le Web comprenait déjà des multiples fonctions : réseau; plateforme de développement; plateforme de transaction et un marché (quelques années après, elle deviendrait également un milieu communautaire avec l'avènement des réseaux sociaux)¹⁶. Dans ces conditions, la base du fonctionnement des monnaies électroniques commença à s'établir – et par conséquent le

¹³ Cf. Stan HIGGINS, *3 Pre-Bitcoin Virtual Currencies That Bit the Dust*, 30 nov. 2014, en ligne: <<https://www.coindesk.com/3-pre-bitcoin-virtual-currencies-bit-dust>> (consulté le 15 sept. 2018) (à propos de l'échec du DigiCash et d'autres monnaies précédentes au Bitcoin).

¹⁴ "ECDSA in counterpart could be a replacement for RSA system, their comptability to be installed in any system with different memory sizes and CPU description and parameters, ECDSA provide the same level of security as RSA but with shorter keys: The smaller key sizes of ECDSA potentially allow for less computationally able light-weight devices and wireless systems to use cryptography for secure data transmissions, data verification and offers less heat generation and less power consumption, less storage space and offers an optimized memory and bandwidth and faster signature generation." Ali Al IMEM « Comparison and Evaluation of Digital Signature Schemes Employed in NDN Network », *International Journal of Embedded Systems and Applications (IJESA)* vol. 5, n. 2, juin 2015, p. 15, à la page 21 (PDF) en ligne: <<https://arxiv.org/pdf/1508.00184.pdf>> (consulté le 15 sept. 2018)

¹⁵ « [...] le manque de sécurité de l'infrastructure monétaire minimise fortement l'importance des avancées conduites. Ses détracteurs condamnent ainsi la reproduction aisée des codes de création de valeur, permettant à chaque utilisateur de s'inventer des crédits supplémentaires en cas de faillite. » Philippe RODRIGUEZ, *La révolution blockchain. Algorithmes ou institutions, à qui donnerez-vous votre confiance ?*, Malakoff, Dunod, 2017, p. 44.

¹⁶ William MOUGAYAR, *The Business Blockchain. Promise, practice, and application of the next Internet technology*, Hoboken, Wiley, 2016, p. 17.

parcours menant aux contrats intelligents d'aujourd'hui. Il n'est pas superflu de rappeler que les chaînes de blocs, tout comme le Web, ont besoin d'Internet pour fonctionner¹⁷.

Ces technologies se sont poursuivies tout au long des années suivantes. En 1997, Adam Back créa le HashCash¹⁸, un système de preuve de travail initialement utilisé afin de limiter le pourriel et les attaques de déni de service, mais qui, plus récemment, fut mis en œuvre sur la chaîne Bitcoin et d'autres cryptomonnaies aussi.

En 1999, la technologie « pair-à-pair » (ou peer-to-peer, P2P) fut lancée sur la plateforme de partage de fichiers audio Napster, fermée en 2001 par le *Federal Bureau of Investigation* (FBI) en raison de violations des droits de propriété intellectuelle¹⁹. En 2000, le Gnutella, la première plateforme de transfert de fichiers P2P entièrement distribuée²⁰, fut également développé. Le Ripplepay, un système monétaire décentralisé, fut ensuite conçu en 2004²¹. Toutes ces marches furent essentielles au développement des cryptomonnaies, nous emmenant vers la technologie de la chaîne de blocs et, ensuite, aux contrats intelligents.

C'est dans ce contexte qu'en 2008 Satoshi Nakamoto publia le livre blanc « Bitcoin : A Peer-to-Peer Electronic Cash System », dans lequel il surmonta les principaux obstacles à la mise en œuvre des systèmes de monnaies électroniques précédents, parmi lesquels se trouve le

¹⁷ MOUGAYAR., *préc.*, note 16, p. 7.

¹⁸ HASHCASH.ORG, *Hashcash*, en ligne : <<http://www.hashcash.org/>> (consulté le 15 nov. 2018)

¹⁹ « L'industrie de la musique a tenté d'éradiquer la menace de la façon la plus ostensible possible, en attaquant devant les tribunaux Napster, le très populaire service Internet qui branchait ses clients sur les musiques qu'ils désiraient et leur permettait de les télécharger gratuitement sous forme de fichiers numériques. Napster a perdu le procès et a été liquidé, mais des services identiques subsistent. » Douglas CLEMENT, « Du mythe de la nécessité des brevets pour susciter l'innovation », *L'Économie politique*, 2003, n° 19, p. 9-24, en ligne : <<https://www.cairn.info/revue-l-economie-politique-2003-3-page-9.htm>> (consulté le 19 sept. 2018)

²⁰ La notion de la nature « distribuée » sera abordée notamment dans le chapitre 1.1.2.1.

²¹ Cf. Bitmex RESEARCH, *The Ripple story*, 06 fév. 2018, en ligne : <<https://blog.bitmex.com/the-ripple-story/>> (consulté le 19 sept. 2018)

problème classique de l'informatique distribué connu sous le nom de « problème des généraux byzantins » et l'enjeu du double paiement²².

Par ailleurs, le livre blanc de Nakamoto donna les assises de la chaîne de blocs en établissant un rapport entre divers concepts, comme ceux du réseau pair-à-pair, d'exemption de tiers de confiance et de consensus²³. Le système Bitcoin est en place depuis janvier 2009, sans subir d'attaques fructueuses dans ce sens jusqu'aujourd'hui²⁴.

Ainsi, la chaîne de blocs était originellement tournée vers le transfert de valeurs relatives aux cryptomonnaies. Toutefois, comme on l'a déjà mentionné, cette technologie permet de mettre en place d'autres usages, notamment le registre d'informations et les contrats intelligents, sujet de cette étude. En bref, indépendamment de l'application, l'idée derrière la chaîne de blocs est de favoriser la sécurité des relations entre toutes les personnes qui souhaitent effectuer des transactions, même entre celles qui n'ont aucun rapport préalable.

Il est primordial d'assimiler ce parcours historique afin de montrer que la chaîne de blocs et les contrats intelligents font partie d'un processus d'innovation actif depuis des années. Chaque étape permet d'en arriver au panorama actuel. De plus, les aspects techniques liés à ces technologies peuvent engendrer des conséquences sur le monde juridique, considérant les limites de ces innovations prévues dans les éventuelles réglementations.

²² Ces deux problèmes seront traités dans le chapitre 1.1.2.3.

²³ W. MOUGAYAR, préc., note 16, p. 2 et 3.

²⁴ Michael J. CASEY et Paul VIGNA, *The Truth Machine. The Blockchain and the Future of Everything*, New York, St. Martin's Press, 2018, p. 45.

1.1. Aperçu des aspects techniques de la chaîne de blocs

Les outils permettant la mise en œuvre des contrats intelligents d'aujourd'hui reposent sur des études entreprises depuis des décennies. Actuellement, les usages et perspectives relatifs aux contrats intelligents sont tellement étendus grâce au progrès technologique, notamment celui qui nous amène à la technologie chaîne de blocs. L'étude de ces aspects techniques nous permettra de comprendre la portée et le sens des réglementations juridiques possibles, objet du chapitre suivant de cette étude.

Plusieurs définitions de la chaîne de blocs ont été formulées, certaines plus techniques, d'autres plus vulgarisées. Au moyen de la fusion de diverses caractéristiques et fonctionnalités qui seront présentées plus avant, il reste possible de définir la chaîne de blocs comme une base de données transactionnelle décentralisée, parfois distribuée, capable de stocker et de transférer des valeurs ou des données via Internet, autonome, partagée, transparente, sécurisée et virtuellement immuable, au moyen d'un système de confiance répartie entre les membres du réseau, ce qui amène l'idée de « consensus ».

Fondamentalement, le système fonctionne au moyen de l'ajout d'informations transactionnelles sur des « blocs », qui à leur tour seront additionnées de façon successive à la « chaîne ». À ce propos, le nom donné à la technologie – chaîne de blocs – indique de façon littérale son fonctionnement pratique.

« Par essence, la blockchain est 'un registre où les transactions numériques réalisées par les membres d'un réseau sont enregistrées les unes après les autres, dont tous les utilisateurs possèdent chacun un exemplaire au contenu identique, qui fait consensus entre eux et ne peut être changé. Ce mode de fonctionnement leur apporte la confiance

nécessaire à la réalisation de nouvelles transactions, sans qu'une tierce partie ne soit nécessaire pour les superviser'. »²⁵

Ainsi, dans le cas des chaînes de blocs, « la confiance se fonde exclusivement sur la technologie »²⁶. Effectivement, c'est un concept complexe qui unifie divers domaines de recherche. Il faut souligner qu'il n'y a pas seulement une chaîne de blocs. Il existe plusieurs chaînes de blocs, par exemple, le Bitcoin, Ethereum, Lisk, Ripple, IOTA, Hyperledger, Interledger, Tendermint, Monax, Corda, beAchain²⁷, entre autres.

Dans la perspective de ses usages, la chaîne de blocs est définie comme un outil numérique qui sert fondamentalement au transfert de cryptomonnaies, à l'enregistrement de données et à l'exécution d'un contrat intelligent sans intermédiaires. Le premier usage mentionné – les transactions de cryptomonnaies – est celui avec lequel la chaîne de blocs est encore la plus associée. Malgré leur méconnaissance, les autres fonctionnalités ont gagné de l'espace au cours des dernières années.

En effet, l'ensemble de ces trois usages résume plusieurs autres fonctions exercées par les chaînes de blocs, comme les infrastructures informatiques, les plateformes de transactions, les plateformes de développement, les logiciels libres, les marchés de services financiers et les réseaux pair-à-pair²⁸.

Le processus *via* la chaîne de blocs est régi conformément aux caractéristiques du logiciel, de telle sorte que les caractéristiques des transactions équivaldront à celles qui sont

²⁵ Stéphane LOIGNON, *Big Bang Blockchain. La seconde révolution d'internet*, Paris, Tallandier, 2017, p. 46.

²⁶ Eric CAPRIOLI, *La blockchain ou la confiance dans une technologie*, La semaine juridique, édition générale, n. 23, 06 juin 2016, p. 1163.

²⁷ Laurent LELOUP, *Blockchain. La deuxième révolution numérique*, Paris, Edito, 2017, p. 99 et 111.

²⁸ W. MOUGAYAR, préc., note 16, p. 18.

assurées par le réseau. En d'autres termes, le niveau d'autonomie, de partage, de transparence, de sécurité et d'immutabilité des transactions sont le résultat d'existence (et du niveau) de ces caractéristiques dans le réseau des chaînes de blocs sur lesquelles elles sont consignées.

D'un point de vue révolutionnaire, l'ensemble des caractéristiques et des usages composant la notion de la chaîne de blocs, parfois, assimilent cette technologie aux débuts d'Internet. À propos de son existence, il faut garder à l'esprit qu'Internet ne dépend pas de la chaîne de blocs, mais l'inverse n'est pas vrai : cette nouvelle technologie dépend du réseau global pour fonctionner.

Les parallèles entre ces deux innovations sont quand même nombreux. Par exemple, de la même façon que le protocole TCP/IP – qui permet le transfert de données sur Internet – sert de base au développement d'usages pratiques (comme les transactions bancaires, l'échange de messages instantanés et le commerce électronique), la chaîne de blocs est aussi un outil de base.

En ce qui concerne le caractère révolutionnaire de la chaîne de blocs, il est également possible de la reconnaître comme une :

" [...] meta technology because it affects other technologies, and it is made up of several technologies itself. It is as an overlay of computers and networks that are built on top of the Internet. (...) In essence, it is technology that changes other technology"²⁹.

Du point de vue juridique, cette nouvelle technologie de réseau distribuée demanderait un traitement similaire à celui accordé au protocole TCP/IP. Ces protocoles associés au transfert de données sur Internet ne sont pas soumis à des réglementations juridiques. En effet, ce sont leurs applications qui le seront. Ainsi, il semblerait approprié d'accorder une plus grande

²⁹ W. MOUGAYAR, préc., note 16, p. 10.

attention à la réglementation des applications de la chaîne de blocs, et pas purement du développement de la technologie. Les transactions de cryptomonnaies, les registres, les contrats intelligents ou toute autre possibilité d'usage pourraient être objet de réglementation – nationale, internationale ou même globale. Rien ne permet encore de déterminer la portée des futures applications sur les chaînes de blocs puisque ses usages ne sont pas complètement connus. C'est pour cette raison que le droit se heurte à d'incessants défis lorsqu'on parle de technologie – d'Internet à la chaîne de blocs.

La création d'Internet et de la technologie de chaîne de blocs comportent également des similarités dans la mesure où ils visent trois objectifs généraux : (1) la solution de problèmes spécifiques (comme l'émergence du commerce électronique afin de favoriser le commerce international *via* Internet, ainsi que la chaîne de blocs en visant la suppression de tiers afin de réduire les coûts de certaines transactions, par exemple); (2) la création de nouvelles possibilités (comme la révolution des médias d'information grâce à Internet, ainsi que la création du marché des monnaies digitales dans le cas de la chaîne de blocs); et (3) l'application concrète de ses capacités (par exemple, avec la création des réseaux sociaux au sein d'Internet et de la chaîne de blocs³⁰, en impactant les relations humaines)³¹.

Par ailleurs, une dernière comparaison entre la chaîne de blocs et Internet concerne l'explication de ses aspects techniques aux usagers. Aujourd'hui, l'usage ordinaire d'Internet ne requiert pas une expertise technique approfondie relative aux fondements de son fonctionnement. Il suffit de se servir d'un ordinateur pour naviguer sur les sites web ou pour

³⁰ À propos de réseaux sociaux basés sur blockchain, voir : Andreas SANDRE, *7 social media startups powered by blockchain*, 03 avril 2018, en ligne : <<https://hackernoon.com/6-social-media-powered-by-blockchain-fdc41d16cb12>> (consulté le 28 sept. 2018)

³¹ W. MOUGAYAR, préc., note 16, p. 141.

réaliser d'autres opérations disponibles. Il n'est pas nécessaire ou même utile à la population en général de comprendre ce qu'est cette technologie ou comment elle fonctionne au plan technique. La même chose pourrait se produire au sein de la chaîne de blocs à mesure que ses cas d'usage deviennent plus tangibles et accessibles au public.

Au début, l'Internet supposait de créer un environnement où les *“legal concepts of property, expression, identity, movement, and context”*³² ne seraient pas appliquées. Pareillement, *“blockchain-based applications do not depend on these rules to structure their functions; instead they depend on lex cryptographica to organize economic and social activity”*³³. Nous traiterons de la *lex cryptographia* dans le titre II, mais nous pouvons d'ores et déjà souligner qu'elle stimulerait la création d'un ordre juridique pas exclusivement fondé sur le droit étatique³⁴. Certaines dispositions sous-jacentes du code et des contrats intelligents seraient prises en considération – ce qui pourrait impliquer une « régulation par le code »³⁵.

Toutefois, même s'il y a certains points de convergence entre la chaîne de blocs et l'Internet, il convient de noter qu'il existe des différences importantes, comme le caractère de publication d'Internet *versus* le caractère de certification de la chaîne de blocs, ainsi que le système décentralisé sur lequel Internet est basé *versus* le système de consensus distribué de la chaîne de blocs, ce qu'on verra plus loin³⁶.

³² John Perry BARLOW, *A Declaration of the Independence of Cyberspace*, Danvos, 8 fév. 1996, en ligne : <<https://www.eff.org/cyberspace-independence>> (consulté le 10 nov. 2018)

³³ P. DE FILIPPI et A. WRIGHT, préc., note 8, p. 6.

³⁴ Corin FAIFE, *The Authors of “Blockchain and the Law” Want You to Rethink the Internet*, 17 septembre 2018, en ligne : <<https://breakermag.com/the-authors-of-blockchain-and-the-law-want-you-to-rethink-the-internet/>> (consulté le 16 nov. 2018)

³⁵ P. DE FILIPPI et A. WRIGHT, préc., note 8.

³⁶ L. LELOUP, préc., note 26, p. 17.

Finalement, au-delà de la simple utilisation de la chaîne de blocs, afin d'identifier la cause des discussions actuelles et d'exploiter les développements futurs, il est essentiel de bien comprendre son fonctionnement et, comme on le verra, son développement.

1.1.1. Les blocs et la formation de la chaîne

D'une manière générale, tout commence avec un accord relatif à une opération de registre, de transfert ou d'automatisation d'un engagement (les trois fonctionnalités générales de la chaîne de blocs mentionnées dans le sous-chapitre précédent).

Cet accord est vérifié par les autres membres du réseau, où chaque ordinateur est considéré un nœud (terminologie technique) responsable pour attester la transaction, s'il l'estime valide. Une fois validée par le consensus des nœuds à la proportion prédéfini (51%, par exemple), l'opération sera inscrite dans le dernier bloc formé qui, à son tour, sera ajouté à l'extrémité plus récente de la chaîne, inauguré par un « bloc genèse ». Cet aperçu est schématisé dans l'image ci-dessous³⁷ :

³⁷ BLOCKCHAIN FRANCE, *Qu'est-ce que la blockchain ?*, 2016, en ligne : <<https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/>> (consulté le 28 oct. 2018)

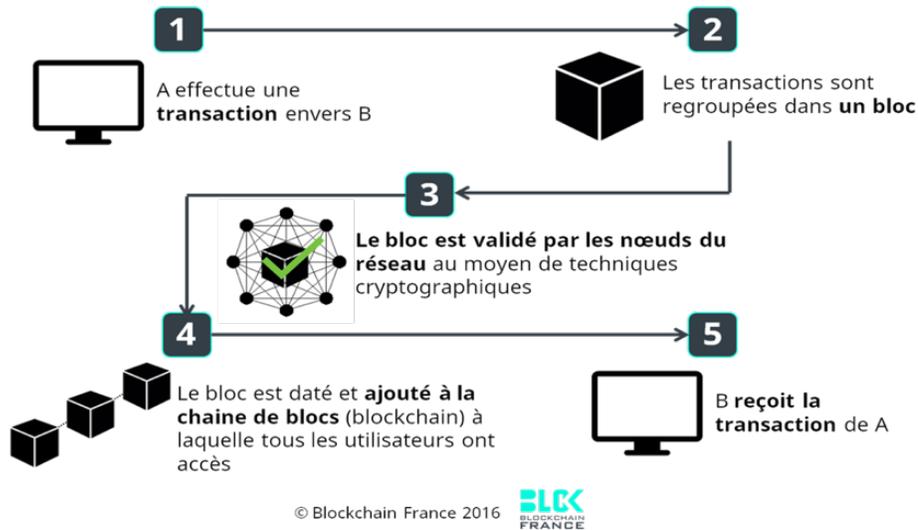


Figure 1. Formation d'une chaîne de blocs

En ce qui concerne l'arrangement effectué entre A et B, il faut garder à l'esprit que la volonté est ce qui déclenche toute la transaction. En premier lieu, les parties décident de faire un échange d'une cryptomonnaie ou de quelque actif entre eux. À partir de la vérification de la concordance de volontés, la transaction sera enregistrée avec d'autres qui, de la même façon, attendent la validation. Cet ensemble de transactions forme un bloc (étape 2). La poursuite du registre se produit grâce aux autres membres du réseau. Chacun constitue un nœud dans le système et possède une « copie » mise à jour de toutes les transactions déjà enregistrées sur la chaîne de blocs. Ils sont aussi les responsables de la validation des transactions (étape 3) et d'ajouter les blocs à la chaîne (étape 4).

Un des concepts plus importants lorsqu'on parle de la chaîne de blocs est le *hash*, ou le processus connu comme hachage³⁸, puisqu'il est l'élément de liaison des blocs. Le *hash* (ou

³⁸ « Hashes are generated using standard cryptographic hashing functions invented by the U.S. National Security Agency (NSA), providing a way to represent the bundle of transactions in a block as a string of characters and

somme de contrôle) se définit comme le code de l'information transcrite sur le bloc. Nous pouvons considérer le *hash* comme une empreinte digitale de la transaction ou comme une synthèse des informations existantes dans un document externe ou dans une transaction. Techniquement, le hachage est une fonction mathématique qui permet de transformer un ensemble de caractères de longueur varié en une chaîne de longueur standard qui cache les informations de la transaction.

En somme, l'importance de ce concept est que le *hash* permet de constater toute altération dans les données enregistrées justement parce que lorsque le *hash* d'un bloc est créé, on utilise la référence du *hash* antérieur. Ainsi, le changement d'un caractère d'une transaction est capable de modifier le *hash* du bloc et, par conséquent, de rendre notable l'identification d'une altération dans ce bloc.

Enfin, après les étapes d'engagement des parties, de validation, de formation du bloc et de son registre sur le réseau, l'exécution de l'arrangement aurait lieu, avec le transfert des actifs concernés, le cas échéant.

1.1.2. Caractéristiques des chaînes de blocs

Reprenant le concept de la chaîne de blocs, certaines caractéristiques méritent d'être ponctuellement appréciées. Ainsi, dans les pages qui suivent, une attention particulière sera

numbers that are uniquely associated with that block's transactions. » P. DE FILIPPI et A. WRIGHT, préc., note 8, p. 22.

Et : « Une fonction de hachage permet de transformer une information ou un message de taille et de nature diverses en une suite de caractères de longueur constante et qui semble être générée de manière aléatoire ». Dr. Billal CHOULI, Frédéric GOUJON et Yves-Michel LEPORCHER, *Les blockchains. De la théorie à la pratique, de l'idée à l'implémentation*, St. Herblain, Éditions ENI, 2017, p. 30.

portée à l'étude du système distribué et décentralisé, du caractère sécuritaire et du consensus. Il faut simplement garder à l'esprit que ces propriétés du réseau peuvent varier d'un type à l'autre.

En outre, lorsqu'il s'agit des caractéristiques des chaînes de blocs, une distinction fondamentale est à faire entre celles qui sont publiques, privées et hybrides, différenciées notamment en ce qui concerne le processus de consensus³⁹.

Dans les premières, tout le monde peut devenir une partie du réseau (un nœud), effectuer et valider les transactions et conserver une copie des registres. Il n'y existe pas de tiers de confiance ni d'entité centrale responsable du réseau de sorte que la corruption d'une plateforme publique serait possible la rendant vulnérable à une importante attaque de la plupart des nœuds⁴⁰. L'idée d'une chaîne de blocs publique est la notion plus innée de cette technologie. Bitcoin et Ethereum sont ses deux principaux exemples aujourd'hui.

Dans le cas des chaînes de blocs privées, les réseaux y sont plus fermés. Elles sont mises en place à l'intérieur d'un milieu particulier, comme une communauté, un groupe d'entreprises ou un secteur du gouvernement. L'accès n'est pas exercé que par une autorité supérieure préétablie, comme la direction d'une entreprise. D'autre part, la lecture peut être publique aux autres nœuds ou non selon les besoins de l'organisme⁴¹. Cette modalité est parfois critiquée par ceux qui ont une vision plus liée à l'idée innée des chaînes de blocs, parce que quelques

³⁹ W. MOUGAYAR, préc., note 16, p. 26.

⁴⁰ « The most plausible way to change a record in the Bitcoin blockchain would be for a group of attackers to engage in a “51% attack” and effectively take over the network so that they can approve transactions at a rate that outpaces the rest of the network. Given the scale of Bitcoin’s distributed network, such an attack is becoming increasingly remote. » P. DE FILIPPI et A. WRIGHT, préc., note 8, p. 25.

⁴¹ “Likely applications include database management, auditing, etc. internal to a single company, and so public readability may not be necessary in many cases at all, though in other cases public auditability is desired.” Vitalik BUTERIN, *On Public and Private Blockchains*, 6 août 2015, en ligne: <<https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>> (consulté le 2 nov. 2018)

caractéristiques originales importantes sont mitigées, comme le caractère décentralisé. Malgré l'absence de décentralisation, il reste le cryptage typique de cette technologie⁴².

Il y a encore une différence en ce qui concerne le but des chaînes de blocs publiques et celles privées:

“One of the primary differences between a public and private blockchain is that public blockchains typically have a generic purpose and are generally cheaper to use, whereas private blockchains have a more specific usage, and they are more expensive to set up because the cost is born by fewer owners. We can also expect special purpose public blockchains to emerge, for example, the Zcash one that promises to deliver total privacy.”⁴³

Enfin, dans le type hybride, connu aussi comme semi-privé ou de consortium, il n'y a pas une centralisation en ce qui concerne le processus de consensus, comme dans le cas des chaînes de blocs privées, ni la possibilité de n'importe quel nœud à participer à la validation des transactions, comme c'est le cas dans celles qui sont publiques.

En effet, les chaînes de blocs hybrides constituent une option à moyen terme où certains nœuds sont sélectionnés à agir dans le processus de consensus⁴⁴. Autrement dit, *"a central authority or consortium selects the parties permitted to engage in a blockchain-based network imposing limits on who can access or record information to the shared database"*⁴⁵. L'exemple

⁴² B. CHOULI, F. GOUJON et Y. LEPORCHER, préc., note 37, p. 144.

⁴³ W. MOUGAYAR, préc., note 16, p. 58.

⁴⁴ « Dans les Blockchains 'de consortium', un certain nombre de nœuds sont en charge du processus d'approbation, c'est-à-dire que le consensus est contrôlé par un ensemble présélectionné de nœuds. Par exemple, une trentaine d'organisations pourraient se mettre d'accord et mettre en place une Blockchain dans laquelle un bloc devrait être approuvé par au moins quinze d'entre elles pour être valide. Nous voyons donc deux différences importantes par rapport au système originel : non seulement les participants au processus d'approbation sont limités et sélectionnés, mais en plus, ce n'est plus la règle de la majorité qui s'impose. Dans ce cas, la Blockchain est partiellement décentralisée. Le droit de lire la Blockchain, c'est-à-dire l'accès au registre, peut alors être public, réservé aux participants, ou bien hybride. » B. CHOULI, F. GOUJON et Y. LEPORCHER, préc., note 37, p. 144.

⁴⁵ P. DE FILIPPI et A. WRIGHT, préc., note 8, p. 31.

plus connu est celui du R3 CEV⁴⁶, un consortium dont plus de 100 banques, régulateurs, associations commerciales et cabinets de services spécialisés font partie afin de développer une plateforme pour le marché financier.

Bien que la chaîne de blocs publique soit la première variante et la plus connue, les modalités hybride et privée comportent certains avantages qui attirent l'attention notamment d'entreprises et d'institutions financières, comme « gouvernance simplifiée, acteurs connus, coûts réduits, rapidité, confidentialité ». ⁴⁷ Néanmoins, en général, les différentes chaînes de blocs partagent diverses caractéristiques. Dans ce contexte, nous analyserons leur nature distribuée et décentralisée, ainsi que la sécurité et le processus de consensus.

1.1.2.1. Système distribué et décentralisé

La chaîne de blocs permet d'envisager une redistribution de rôles dans les domaines les plus divers, notamment en raison de son éventuelle capacité à répondre aux besoins d'un monde globalisé en termes d'automatisation des relations. Dans ce sens, elle pourrait être considérée également comme un moyen de redistribuer le pouvoir de décision entre les différents acteurs du monde globalisé, c'est-à-dire entre les États, les organismes interétatiques, le secteur privé etc. ⁴⁸ La nature distribuée et décentralisée des chaînes de blocs semble être une caractéristique essentielle pour cette redistribution de pouvoir.

⁴⁶ Anna IRRERA, « Bank-backed R3 launches new version of its blockchain », *Reuters*, 3 oct. 2017, en ligne : <<https://www.reuters.com/article/us-r3-blockchain/bank-backed-r3-launches-new-version-of-its-blockchain-idUSKCN1C80MS>> (consulté le 2 nov. 2018)

⁴⁷ B. CHOULI, F. GOUJON et Y. LEPORCHER, préc., note 37, p. 145.

⁴⁸ P. RODRIGUEZ, préc., note 15, p. 199.

Nous pourrions définir le réseau distribué comme « une interconnexion d'une collection d'ordinateurs autonomes, de processus et de processeurs. Les ordinateurs, les processus ou les processeurs sont appelés nœuds »⁴⁹. Ces nœuds sont considérés autonomes puisque chacun possède une copie du réseau mise à jour. Ils sont interconnectés en raison de leur capacité d'échange informationnel et chaque fois qu'un des membres du réseau inscrit une information sur la chaîne de blocs, tous les autres membres y auront accès. L'ensemble de ces caractéristiques donne une vision générale de ce que serait la nature distribuée.

Concernant les transactions sur une chaîne de blocs, on constate qu'elles sont vérifiées et enregistrées automatiquement au moyen de la validation par les membres du réseau (nœuds), sans avoir besoin d'une autorité centrale ou d'un point unique de contrôle. Nous nous trouvons donc devant le caractère décentralisé des chaînes de blocs.

Ainsi, la nature distribuée et décentralisée de ce genre de plateforme est capable de produire des effets importants, comme l'accélération des procédures dans la conclusion et l'exécution d'accords, l'absence de longs délais entre les intermédiaires ainsi qu'une bonne capacité de résistance à des attaques. Cela crée aussi un environnement libre de censure et sans point central de vulnérabilité⁵⁰. Toutes ces caractéristiques sont fortement appréciées quand on traite des contrats, qu'ils soient considérés comme « intelligents » ou traditionnels.

Les deux autres caractéristiques des chaînes de blocs, abordées dans les pages suivantes (sécurité et consensus), sont aussi liées à sa nature distribuée et décentralisée.

⁴⁹ B. CHOULI, F. GOUJON et Y. LEPORCHER, préc., note 37, p. 118.

⁵⁰ W. MOUGAYAR, préc., note 16, p. 152.

1.1.2.2. Sécurité

Tel qu'indiqué, le caractère sécuritaire de la chaîne de blocs découle de la nature distribuée et décentralisée de son système, spécifiquement en raison du renforcement de la fiabilité par réplication⁵¹, c'est-à-dire qu'il n'y aura pas de conséquences négatives au fonctionnement du réseau dans le cas où un des nœuds échoue, car les autres continuent d'exercer leurs fonctions normalement. La cryptographie participe à la nature sécuritaire des chaînes de blocs, basée sur les notions de hachage, de clés privées et publiques et de signatures numériques⁵².

*"A 'hash' is a unique fingerprint that helps to verify that a certain piece of information has not been altered, without the need to actually see it. Keys are used in at least a combination of two: a public and private one. (...) A digital signature is a mathematical computation that is used to prove the authenticity of a digital message or document."*⁵³

L'ensemble de ces mécanismes rendraient les transactions sur la chaîne de blocs plus sûres en protégeant les identités, les valeurs, le processus de transfert d'actifs, etc.

Lorsque nous avons commencé à examiner les caractéristiques des chaînes de blocs, il a été souligné que leurs attributs peuvent varier conformément au type de réseau (privé, public ou hybride). Par exemple, les chaînes privées et hybrides sont considérées sécuritaires grâce aux

⁵¹ « The participants in a blockchain maintain a log of the systems' transactions and reach distributed consensus on their order with a high degree of replication to overcome node failure and attacks. While this approach is responsible for the security and reliability of blockchain protocols, it is also responsible for their greatest weakness: performance is limited by the rate and latency that it takes for nodes to reach consensus. » Joshua LIND, Ittay EYAL, Florian KELBERT, Oded NAOR, Peter PIETZUCH et Emin Gun SIRER, « Teechain: Scalable Blockchain Payments using Trusted Execution Environments », *Cornell University Library*, (PDF) en ligne : <<https://arxiv.org/pdf/1707.05454.pdf>> (consulté le 18 nov. 2018)

⁵² W. MOUGAYAR, préc., note 16, p. 12.

⁵³ *Id.*

« *backups* » créés dans chaque nœud (ce qui arrive également dans le cas des chaînes publiques). Chacun d'eux sauvegarde une copie intégrale des registres, de sorte que le réseau continuera à fonctionner bien qu'il ait une faille ponctuelle. Dans les chaînes de blocs en général, "*the common record of truth resides in multiple locations, underpins this core idea of distributed security, that the risk of failure is backstopped by multiple 'redundancies'*"⁵⁴, ce qui confirme cette idée de partage, de décentralisation et de réplique.

Néanmoins, dans le cas spécifique des réseaux publics, cette notion de sécurité – ou même de *security by-design*⁵⁵ – présente une particularité. Sans aucun contrôle en ce qui concerne les membres autorisés à intégrer le réseau, elle s'occupe d'augmenter le coût des attaques jusqu'à ce qu'elles perdent leur caractère lucratif⁵⁶. L'efficacité de cette mesure peut être observée dans le cas de la chaîne de blocs Bitcoin, qui n'a jamais subi d'attaque fructueuse (il est utile de souligner que ce n'est pas le cas des portefeuilles de cryptomonnaies, mais simplement de la chaîne de blocs jusqu'ici).

En matière de sécurité, il faut aussi traiter de l'attaque à 51%, dont l'appellation est déjà illustrative. Il s'agit du contrôle de plus de la moitié la puissance de calcul dans un réseau, ce qui permettrait à cet individu ou groupe de contrôler les transactions à son gré – les refuser, les valider ou même de réaliser des doubles dépenses (la même valeur X pourrait servir à plus d'un versement – cette définition sera vue dans le prochain sous-chapitre). Dans ce sens, en concordance avec la notion de rendre les attaques coûteuses afin de les décourager le plus possible :

⁵⁴ M. J. CASEY et P. VIGNA, préc., note 24, p. 44.

⁵⁵ *Id.*, p. 45.

⁵⁶ *Id.*, p. 45-46.

« En effet, le coût de la puissance de calcul et de l'énergie nécessaire est prohibitif : en février 2016, la puissance totale du bitcoin était de 1,2 million de Téra Hash. Sachant que le Téra Hash coûte environ 4.000\$, il ne faudrait pas moins de 4,8 milliards de dollars américains pour obtenir une telle puissance. Enfin, si la sécurité du réseau était compromise, une procédure d'urgence existe. »⁵⁷

D'ailleurs, dans une perspective optimiste, les questions de sécurité pourraient dépasser les attaques. Toutefois, des risques sont toujours présents, ce qui sera examiné au chapitre 2.2.

1.1.2.3. Consensus

En plus de favoriser le système distribué par la participation de plusieurs nœuds, le consensus est l'outil qui permet de régler les transactions dans la chaîne de blocs, en validant ou non son inscription sur le réseau.

Habituellement, la preuve de travail (*proof of work*, en anglais) est la première méthode de consensus connue de ceux qui commencent à étudier le thème parce que c'est le mécanisme utilisé par le réseau Bitcoin (l'application qui a inauguré la mise en œuvre des chaînes de blocs). Dans cette méthode de validation des transactions se trouve le rôle des mineurs (*miners*). Ces sont les personnes qui, en validant les transactions, recevront une récompense puisqu'elles auront investi leur temps et la puissance de calcul de leur ordinateur afin de trouver la solution du problème mathématique nécessaire à l'inscription de la transaction sur le bloc et du bloc sur la chaîne. Seul le premier à trouver la solution est récompensé par des cryptomonnaies ou tokens.

⁵⁷ David TERUZZI, *Combien ça coûterait une attaque 51% ?*, 11 février 2016, en ligne : <<http://blogchaincafe.com/combien-ca-couterait-une-attaque-51>> (consulté le 12 nov. 2018)

Toutefois, il existe d'autres méthodes de consensus⁵⁸, comme le Paxos⁵⁹, la délégation de preuve de possession⁶⁰, le Raft⁶¹, le Tangaroa⁶² et la « preuve d'enjeu » ou « preuve de participation » (*proof of stake*, en anglais). Cette dernière est de plus en plus prise en considération. Dans le cas de la preuve de participation, le pouvoir des nœuds afin de valider et d'ajouter des blocs à la chaîne se mesure en raison de la quantité de cryptomonnaies qu'ils possèdent.

Indépendamment des différences entre ces formes de consensus, ce qu'il faut garder à l'esprit c'est qu'ils ont tous la même finalité : ils visent à apporter une solution à une question informatique présentée pour la première fois en 1982, « le problème des généraux byzantins »⁶³.

Ce problème, en somme, pèse sur la coordination de la confiance entre les interlocuteurs dans un réseau. La métaphore fait allusion à l'organisation des généraux en mission d'attaque, qui ont besoin d'échanger de l'information de façon fiable sans l'interférence d'autres généraux considérés comme traîtres. Ainsi, la manière d'éviter l'échec du plan est d'arriver à un consensus en empêchant la réussite d'actions non voulus par les traîtres. Dans ce but, il faut trouver un

⁵⁸ « Nous croyons que les mécanismes de consensus vont évoluer pour atteindre des besoins spécifiques, qu'il s'agisse d'une application particulière, de possibilités techniques ou d'un environnement réglementaire. » Sigrid SEIBOLD et George SAMMAN, *Consensus. Immutable Agreement for the Internet of Value*, juin 2016, p. 9, (PDF) en ligne : <<https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf>> dans S. LOIGNON, préc., note 25, p. 59.

⁵⁹ Cf. MARKCC. *Paxos, a really beautiful protocol for distributed consensus*, 30 janv. 2015, en ligne : <<http://www.goodmath.org/blog/2015/01/30/paxos-a-really-beautiful-protocol-for-distributed-consensus/>> (consulté le 2 nov. 2018)

⁶⁰ Cf. BITSHARES. *Delegated Proof of Stake*, en ligne : <<http://docs.bitshares.org/bitshares/dpos.html>> (consulté le 2 nov. 2018)

⁶¹ Cf. GITHUB, *The Raft Consensus Algorithm*, en ligne : <<https://raft.github.io/>> (consulté le 2 nov. 2018)

⁶² Cf. Christopher COPELAND et Hongxia ZHONG, *Tangaroa: a Byzantine Fault Tolerant Raft*, 2014, (PDF) en ligne : <http://www.scs.stanford.edu/14au-cs244b/labs/projects/copeland_zhong.pdf> (consulté le 03 nov. 2018)

⁶³ S. LOIGNON, préc., note 25, p. 51.

code (algorithme) capable d'assurer que les bons généraux approuvent une décision au moyen des messages partagés entre tous les membres impliqués, formant le consensus entre eux⁶⁴.

Il est simple de transposer ce problème à la situation des chaînes de blocs : il s'agit d'éviter que certains nœuds soient capables de guider la validation des transactions et d'ajouter des blocs à la chaîne de façon malveillante. En réalité, « les désaccords sont réglés par consensus d'une majorité des membres du réseau. »⁶⁵, ce qui pourrait nous amener au cas des attaques à 51% déjà mentionnées.

Au-delà du problème des généraux byzantins, le problème technique connu comme « double dépense »⁶⁶, ce qui était considérée une des principales difficultés à la mise en œuvre des monnaies électroniques décentralisées⁶⁷, est également lié au consensus. Avant la cryptomonnaie Bitcoin, il n'y avait pas de « contrôle » fiable sur les dépenses dans le cas des monnaies décentralisées, c'est-à-dire qu'un même montant pouvait servir à plusieurs transactions sans la mise à jour des valeurs effectivement disponibles.

Ainsi, la même valeur X pourrait servir à plus d'un versement. Les monnaies fiat ou électroniques centralisées ne connaissent pas ces problèmes, car une tierce partie de confiance surveille leurs transactions, et s'assure de la mise à jour des valeurs qui peuvent être dépensées, ce qui évite la duplicité d'utilisation d'un montant. Par conséquent, le consensus s'est imposé comme la manière d'éviter la double dépense des monnaies électroniques décentralisées.

⁶⁴ L. LELOUP, préc., note 26, p. 46-48.

⁶⁵ S. LOIGNON, préc., note 25, p. 45.

⁶⁶ « Double-spending and fraud are not illegal in Bitcoin ; in other words, they are just 'taxed' to such degree that it's prohibitively expensive. » M. J. CASEY et P. VIGNA, préc., note 24, p. 68.

⁶⁷ Grahame JOHNSON et Lukasz POMORSKI, « Exposé sur les monnaies électroniques », *Banque du Canada*, 2 avril 2014, Ottawa, (PDF) en ligne : <https://www.banqueducanada.ca/wp-content/uploads/2014/04/discours_senat.pdf> (consulté le 26 oct. 2018)

Finalement, étant donné qu'une transaction ne pourra pas être modifiée ou effacée, il faut bien reconnaître l'authenticité de l'opération avant de la valider et l'inscrire dans le réseau. Ainsi, l'importance du consensus est évidente puisqu'elle renforce le fondement d'immutabilité des informations mises sur la chaîne de blocs.

1.2. La Chaîne de blocs 2.0

Le parcours historique et de développement technologique exposé dans les chapitres précédents nous conduit au panorama actuel des contrats intelligents. La plateforme Ethereum, lancée le 30 juillet 2015, peut être considérée une des étapes de ce parcours, donnant origine à ce qu'il est convenu d'appeler la « chaîne de blocs 2.0 »⁶⁸.

Les progrès récents des contrats intelligents reposent sur les piliers de la chaîne de blocs. L'intention d'automatiser les accords, ce qui résume la fonctionnalité des contrats intelligents, existe depuis longtemps. Ce qui attire l'attention aujourd'hui est l'élargissement et le raffinement de cette idée en termes de sécurité et de portée ainsi que l'intérêt grandissant de l'industrie et des gouvernements à la mise en œuvre de cette technologie.

Il faut brièvement aborder certains aspects techniques derrière les contrats intelligents afin de situer l'état de l'art aujourd'hui. L'analyse de la structure de la chaîne de blocs est fondamentale pour comprendre l'hypothèse de la reconnaissance juridique de ses applications aujourd'hui, soit par la *hard law*, soit par les normes alternatives.

⁶⁸ Cf. UNIBRIGHT.IO, *Blockchain evolution: from 1.0 to 4.0*, 7 déc. 2017, en ligne : <<https://medium.com/@UnibrightIO/blockchain-evolution-from-1-0-to-4-0-3fbdccfc666>> (consulté le 26 oct. 2018) (à propos de la classification de la technologie blockchain aujourd'hui)

En novembre 2013, Vitalik Buterin, un programmeur russo-canadien, après avoir étudié la technologie chaîne de blocs du Bitcoin, a publié le livre blanc d'Ethereum sous le titre "*A Next Generation Smart Contract & Decentralized Application Platform*"⁶⁹. Aujourd'hui, l'Ethereum est reconnu comme une fondation suisse à but non lucratif⁷⁰ dont la particularité repose sur la création et l'exécution de contrats intelligents et d'applications décentralisées.

À partir de cela, l'établissement de marchés, de relations commerciales, de registres de transactions et de transfert de fonds est désormais possible indépendamment de la confiance préalable entre les parties ou en un intermédiaire⁷¹. En bref, le but de création de la plateforme Ethereum était d'élargir la portée des fonctions des chaînes de blocs qui n'étaient utilisées que pour des transactions monétaires jusqu'alors. Néanmoins, selon les idées diffusées par Buterin, le réseau Bitcoin « a été conçu pour être un protocole SMTP, (...) excellent pour une tâche particulière, le transfert d'argent, mais il n'a pas été pensé en tant que couche fondamentale sur laquelle on pourrait bâtir tout type de protocoles »⁷².

De manière générale, la chaîne Ethereum conserve diverses caractéristiques similaires à celles de la chaîne Bitcoin. Les deux sont publiques⁷³ et utilisent le minage *proof of work* (bien que l'Ethereum envisage de changer au minage *proof of stake*⁷⁴). De la même façon, elles présentent une monnaie cryptographique décentralisée (le bitcoin pour le réseau du même nom, et l'ether pour le réseau Ethereum). Toutefois, une différence significative entre les deux chaînes

⁶⁹ Vitalik BUTERIN, *Ethereum White Paper. A next generation smart contract & decentralized application platform*, nov. 2013, (PDF) en ligne : <http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf> (consulté le 26 oct. 2018)

⁷⁰ B. CHOULI, F. GOUJON et Y. LEPORCHER, préc., note 37, p. 174.

⁷¹ ETHEREUM. *Blockchain App Platform*, en ligne : <<https://www.ethereum.org/>> (consulté le 28 oct. 2018)

⁷² L. LELOUP, préc., note 26, p. 73.

⁷³ Infra, chapitre 1.1.2.

⁷⁴ L. LELOUP, préc., note 26, p. 76.

de blocs plus connues, toujours indiquées par les spécialistes, concerne le délai de traitement des transactions : le réseau Bitcoin prend 10 minutes pour confirmer la validité d'un bloc et l'ajouter sur la chaîne tandis que l'Ethereum peut le faire en 12 seconds.⁷⁵

Sur un regard plus technique, la plateforme Ethereum utilise des langages informatiques Turing-Complet⁷⁶. À ce propos, il faut simplement garder à l'esprit que ce type de langage est essentiel au déploiement des contrats intelligents et des applications décentralisées.⁷⁷

Pour se faire une idée plus précise de ce que signifie l'Ethereum, la plateforme est considérée par certains comme un ordinateur mondial composé de milliers d'ordinateurs partout dans le monde⁷⁸, accessible à tous, et qui fixe les « *smart contracts* » et les DAO (*Decentralized Autonomous Organization* ou l'Organisation Autonome Décentralisée) comme des points centraux de distinction de cette chaîne de blocs par rapport à d'autres comme celle du Bitcoin⁷⁹.

« Le but d'Ethereum est de créer un protocole alternatif pour construire des applications décentralisées, fournissant un ensemble différent de compromis que nous pensons être très *utile pour une vaste classe d'applications décentralisées*, avec un accent particulier sur les situations où le développement rapide, la sécurité des petites applications rarement utilisées et la possibilité pour les différentes applications d'interagir ensemble de manière très efficace sont importants. »⁸⁰

⁷⁵ P. DE FILIPPI et A. WRIGHT, préc., note 8, p. 31.

⁷⁶ « Turing completeness. A machine is Turing complete if it can perform any calculation that any other programmable computer is capable of. All modern computers are Turing-complete in this sense. The Ethereum Virtual Machine (EVM) which runs on the Ethereum blockchain is Turing complete. Thus, it can process any 'computable function'. It is, in short, able to do what you could do with any conventional computer and programming language ». BLOCKCHAIN HUB, *Glossary*, « Turing completeness », en ligne : <<https://blockchainhub.net/blockchain-glossary/>> (consulté le 28 oct. 2018)

⁷⁷ P. DE FILIPPI et A. WRIGHT, préc., note 8, p. 28.

⁷⁸ L. LELOUP, préc., note 26, p 77.

⁷⁹ *Id.*

⁸⁰ Stéphane ROCHE, Jean ZUNDEL, Frédéric JACQUOT, Alexandre KURTH et Etienne JOUIN. *Traduction du Livre Blanc Ethereum. Plateforme de contrats autonomes et d'applications décentralisées de nouvelle génération*, 09 nov. 2016, en ligne : <<http://www.asseth.fr/2016/11/09/traduction-whitepaper-ethereum/>> (consulté le 18 oct. 2018) (nos italiques)

Partant de tous les aspects historiques et techniques mentionnés, on pourrait envisager certains avantages et inconvénients apportés par la chaîne de blocs 2.0 au développement des contrats intelligents, ce qui sera l'objet du chapitre suivant.

1.2.1. D'autres détails à propos de la définition et du fonctionnement des contrats intelligents

Tout d'abord, il faut souligner que l'ensemble des caractéristiques favorables à la mise en œuvre des contrats intelligents n'est pas une raison suffisante pour remplacer les contrats traditionnels. En effet, cette nouvelle technique est incapable de remplir tous les rôles de la vie quotidienne dans les mêmes proportions que les contrats « classiques ».

Cela n'est qu'une réalité lointaine, sinon impossible quand on pense à une subrogation complète. Toutefois, certains cas sont effectivement favorisés par la mise en œuvre des contrats intelligents, comme on le verra dans quelques pages (chapitre 2.3.). La distinction primordiale entre les contrats traditionnels et les contrats intelligents est, en réalité, la méthode d'exécution : les premiers, exigibles et exécutés par la loi; les deuxièmes, par le code.

La compréhension de ce qui définit aujourd'hui un contrat intelligent peut être résumée comme suit :

« [...] des programmes informatiques qui enregistrent et/ou exécutent les termes d'un contrat lorsque les échéances arrivent à terme (un prêt financier, l'émission d'une action, un vote, un contrat de mariage, tout type de contrat...) dont les caractéristiques ont été au préalable clairement définies »⁸¹.

⁸¹ L. LELOUP, préc., note 26, p 78.

Ce concept traduit l'idée derrière ces contrats d'une façon très simple, mais suffisante pour la compréhension de son fonctionnement et, par conséquent, de ses implications au-delà du monde numérique. Dans le cas des contrats intelligents, la transaction peut commencer et suivre son exécution automatiquement, sans l'interférence des parties ou de tiers, jusqu'à la fin.

Depuis 2014, les contrats intelligents gagnent de plus en plus de terrain : économiquement⁸², socialement⁸³, technologiquement, et juridiquement. Toutefois, l'idée derrière les contrats intelligents n'est pas si récente. Depuis longtemps, l'automatisation des formalités intéresse divers secteurs.

Bien souvent, les contrats intelligents sont comparés au système des machines distributrices, comme ceux de vente de boissons chaudes ou fraîches dans lesquelles un arrangement est conclu entre la personne qui veut acheter le produit et la machine directement. Le point important pour cette comparaison c'est que l'exécution des transactions dans les machines distributrices se réalise automatiquement, sans aucune interférence humaine.

Le système est programmé pour entamer une série de procédures à partir d'un événement déclencheur. Dans le cas des machines distributrices, c'est le choix du produit et l'insertion de l'argent qui engendre la remise de l'item sélectionné. La machine possède des mécanismes pour faire avancer la transaction seulement si les exigences sont accomplies (cf. figure 3⁸⁴). Par

⁸² Sur les aspects économiques des contrats intelligents, voir : Lin William CONG et Zhiguo HE, *Blockchain Disruption and Smart Contracts*, September 10, 2018, (PDF) en ligne : <<https://goo.gl/EdDRvo>> (consulté le 19 oct. 2018)

⁸³ Sur l'usage des contrats intelligents dans le domaine social, voir : DEMOCRACY EARTH, *Introducing the Social Smart Contract*, 06 oct. 2017, en ligne : <<https://words.democracy.earth/introducing-the-social-smart-contract-8c7aa1d19682>> (consulté le 19 oct. 2018)

⁸⁴ Andrea M. ROZARIO et Miklos A. VASARHELYI, « Auditing with Smart Contracts », *The International Journal of Digital Accounting Research*, vol. 18, 2018, (pdf) en ligne : <http://rabida.uhu.es/dspace/bitstream/handle/10272/14419/Auditing_with_Smart.pdf?sequence=2> (consulté le 08 sept. 2018)

exemple, il est impossible d’acheter les items avec de fausses pièces ou celles qui ne sont pas acceptées par la machine grâce à un dispositif interne qui identifie les propriétés physiques et chimiques des pièces introduites⁸⁵.

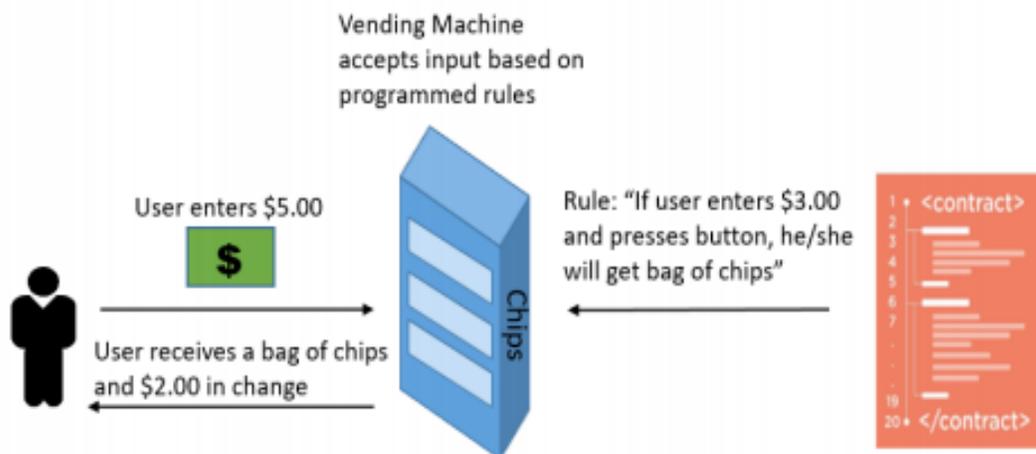


Figure 2. Fonctionnement de machines distributrices

Effectivement, le système des machines distributrices applique des concepts similaires à ceux qui sont utilisés par les contrats intelligents sur la chaîne de blocs aujourd’hui. C’est le cas de l’existence de règles prédéfinies et de la tenue des effets dans le monde réel au moyen d’une exécution automatisée – par la machine, dans le cas des boissons, par la chaîne de blocs, dans les cas des contrats intelligents. C’est essentiellement ainsi que fonctionnent ces contrats dont certains exemples seront présentés plus loin pour éclairer leur application.

En somme, les contrats intelligents sont basés sur une logique “*if this, then that*” (si telle stipulation est réalisée, alors tel effet en découle) en visant différentes finalités, comme le

⁸⁵ Sur le fonctionnement des machines distributrices, voir : GENERAL CULTURE, *Comment un distributeur reconnaît-il les pièces que j’insère ?*, 2012, en ligne : <<https://goo.gl/d9336j>> (consulté le 20 oct. 2018)

transfert d'actifs, la vérification de signatures, l'enregistrement de votes et la mise en œuvre de systèmes de gouvernance basés sur la chaîne de blocs⁸⁶.

En ce qui concerne la définition, nous pouvons soumettre la dénomination de cette technologie – contrats intelligents – à un examen critique. En général, cela n'est pas considéré comme un contrat, ni vraiment intelligent.

Au sujet de la notion de contrat, une grande partie de la doctrine ne considère pas ces programmes informatiques équivalents aux contrats au sens juridique. Aujourd'hui, ce serait traité en général comme un dispositif parajuridique⁸⁷ (cette question sera abordée au titre II).

Quant à la notion d'intelligence, le cœur de la controverse réside dans les capacités de cette technologie qui demande encore une action externe pour qu'elle se déclenche. D'autres points qui sapent l'intelligence des *smart contracts* sont l'impossibilité d'enregistrer des changements ou même d'enrayer leur exécution après le déclenchement.

Reste que, indépendamment de l'adéquation de la dénomination donnée à cet outil, aujourd'hui les contrats intelligents font l'objet de plusieurs recherches. Ces protocoles informatiques semblent être capables de faciliter, de vérifier, d'exécuter et de faire respecter les termes des accords commerciaux⁸⁸, peu importe la confiance préalable entre les parties. C'est en cette qualité que réside une certaine euphorie autour des fonctionnalités des contrats intelligents.

⁸⁶ P. DE FILIPPI et A. WRIGHT, préc., note 8, p. 29.

⁸⁷ Sébastien LAPOINTE, « La technologie des contrats intelligents », *Thomson Reuters Centre de développement professionnel au Canada*, Webinaire en rediffusion, Éditions Yvon Blais, 2018, en ligne : <https://cpdcentre.ca/eyb/blocks/rtecomm_catalog/view.php?id=1797&lang=fr> (consulté le 14 nov. 2018)

⁸⁸ Tim SWANSON, *Consensus-as-a-Service. A Brief Report on the Emergence of Permissioned, Distributed Systems*, 6 avril 2015, en ligne : <<http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf>> (consulté le 08 sept. 2018)

Chapitre 2 – Les aspects pratiques de la chaîne de blocs et des contrats intelligents

La chaîne de blocs a permis la création d'applications soi-disant prometteuses au regard des défis du monde globalisé en transférant des actifs numériques, en sécurisant les registres de plus en plus nombreux et en automatisant l'exécution des contrats. Une fois que les aspects historiques et techniques de la technologie de base des contrats intelligents sont compris, nous pouvons examiner leur perspective pratique. Les aspects techniques et pratiques sont importants pour comprendre dans quelle mesure les normes déjà existantes influencent les contrats intelligents ainsi que les voies à suivre dans les prochaines années.

Dans ce contexte, nous examinerons les avantages de leur mise en place ainsi que certains inconvénients qui leur sont associés. Les avantages de leur usage dans le monde réel sont divers et, d'une manière générale, liés aux caractéristiques de la technologie de la chaîne de blocs. Soulignons la désintermédiation, le gain de temps et d'argent, la sécurité, la transparence et la précision dans les transactions et dans l'exécution, ainsi que l'absence de papier.

D'autre part, il est évident que la mise en œuvre des contrats intelligents présente aussi certains inconvénients, notamment parce que ce système en est encore à ses débuts. Nous examinerons ici le manque de compréhension des technologies concernées, les erreurs de programmation et l'immutabilité qui entrave certains changements parfois vitaux lors de l'enregistrement d'une information dans la chaîne ou de l'exécution d'un contrat intelligent.

Une analyse combinée des aspects techniques et pratiques pourra permettre une meilleure compréhension de la position des contrats intelligents dans le domaine juridique actuellement. Les caractéristiques techniques et d'application pratique semblent être plus uniformes, alors que les ordres juridiques peuvent présenter des variations importantes en fonction des limites géopolitiques et du contexte social, culturel et économique local. Ainsi, ces deux aspects servent de base pour l'analyse juridique des contrats intelligents.

2.1. Des avantages pratiques de la mise en œuvre des contrats intelligents

Les contrats intelligents ont gagné du terrain au cours des dernières années en raison de quelques avantages importants qu'ils offriraient dans les domaines les plus variés. Nonobstant, cette croissance ne signifie pas un remplacement des contrats « fiat » ou traditionnels, auxquels nous sommes habitués.

Bien qu'il subsiste une incertitude à l'égard de ce nouveau dispositif parajuridique et quelques inconvénients non résolus, ces attributs spéciaux qui rendent les contrats intelligents si intéressants méritent d'être mis en exergue. À la fin de ce titre, certains cas d'usages illustreront la mise en œuvre de ces prétendus avantages dans le monde réel.

2.1.1. Désintermédiation, gain de temps et d'argent

L'absence d'un tiers de confiance est une des caractéristiques les plus importantes de la chaîne de blocs, également applicable aux contrats intelligents. Comme on le verra dans la dernière partie de ce titre, qui aborde certains cas d'application de la technologie de la chaîne

de blocs, ces transactions ne demandent pas un tiers, de sorte que les parties intéressées sont capables de mener les engagements directement entre elles, sans interférence. Par exemple, certains types d'opérations bancaires traditionnelles pourraient être conduites au moyen de la chaîne de blocs, sans l'intermédiation des institutions financières.

Dans ces cas, le système de la chaîne de blocs sera chargé de consolider la transaction au moyen des techniques vues dans le chapitre précédent, ce qui pourrait avoir pour conséquence une horizontalisation des activités⁸⁹, c'est-à-dire que les parties ne dépendront pas d'un tiers pour mener leurs affaires. Ils ne seront ainsi plus soumis aux heures ouvrables, au fonctionnement ou à la localisation des intermédiaires⁹⁰.

En effet, malgré qu'il soit plus courant de parler d'une désintermédiation de la confiance, il serait encore plus opportun de le concevoir comme une « ré-intermédiation »⁹¹. Les rôles des tiers existants aujourd'hui seront surmontés ou au moins révisés à la lumière des innovations. Il ne faut pas confondre la désintermédiation (ou la ré-intermédiation) avec l'absence de confiance⁹². La chaîne de blocs représente l'inverse. Elle représente simplement une redistribution de la confiance vers les parties elles-mêmes. En somme, “[T]he Internet was about replacing some intermediaries. Now the blockchain is about replacing other intermediaries once again. But it's also about creating new ones. And so was the Web”⁹³.

Ainsi, ces transformations semblent se diriger vers un gain de temps et d'argent. En ce qui concerne la vitesse des transactions, les contrats intelligents font gagner du temps, puisque certaines étapes de validation par des tiers sont contournées quand les codes de programmation

⁸⁹ L. LELOUP, préc., note 26, p. 120.

⁹⁰ W. MOUGAYAR, préc., note 16, p. 23.

⁹¹ W. MOUGAYAR, préc., note 16, p. 33.

⁹² *Id.*

⁹³ W. MOUGAYAR, préc., note 16, p. xxiii.

sont en tête de la procédure transactionnelle. Par exemple, dans le cas des contrats intelligents, le registre de documents ou les signatures n'exigent plus la présence physique des parties. Sous l'angle financier, il n'y aurait plus de frais de service dus aux tiers de confiance, de dépenses de déplacement ou même d'impression et de stockage de documents sur un support papier.

Dans cet ordre d'idées, l'économie de temps et d'argent par la mise en œuvre d'un contrat intelligent se fait notamment en raison de l'exécution automatique, ce qui décourage les longues renégociations ou même les procédures judiciaires. Voilà deux autres avantages aux contrats intelligents, avec la désintermédiation.

2.1.2. Sécurité

L'orientation essentiellement sécuritaire de la technologie chaîne de blocs donne plus de confiance aux transactions menées sur le système et, par conséquent, aux contrats intelligents. Sa nature « décentralisée et distribuée permet de répliquer l'information et de multiplier les points de contrôle et de validation »⁹⁴ de façon que l'existence de ces multiples points contenant une copie intégrale du réseau et des transactions évite qu'une faille ponctuelle affecte toute la chaîne, c'est-à-dire que le stockage des informations dans différents nœuds rend plus difficile (ou plus coûteuse) une attaque capable de menacer l'intégrité des données ou l'exécution des transactions.

Les mécanismes de la technologie de la chaîne de blocs – comme la cryptographie – sont tournés vers la protection du son fonctionnement continu. Néanmoins, il y a encore des

⁹⁴ B. CHOULI, F. GOUJON et Y. LEPORCHER, préc., note 37, p. 20.

inquiétudes autour de cette question, notamment en ce qui concerne le réseau Ethereum, qui est basé sur un code *Turing complete*, ce qui permet l'exécution des programmes à l'infini⁹⁵. De manière positive, ce langage (*Turing complete*) permet la mise en œuvre d'innombrables opérations. Par ailleurs, « cela crée aussi des opportunités pour des hackers malveillants qui peuvent inscrire un smart contract pour détourner de l'argent jusqu'à la fin des temps »⁹⁶.

De toute façon, nous avons opté de placer la sécurité comme un avantage des chaînes de blocs en raison de l'absence de grandes défaillances du système jusqu'à présent et en vertu du potentiel des recherches d'amélioration dans ce domaine.

2.1.3. Transparence et précision

La transparence et la précision des informations dans les contrats intelligents sont deux avantages habituellement soulignés. À la différence des contrats traditionnels, lorsque nous utilisons un langage de programmation, il n'y a pas de place pour l'interprétation ou l'ambiguïté. Étant donné qu'un code informatique doit être exact pour bien fonctionner, l'exécution du contrat suivra strictement les dispositions initialement prévues, c'est-à-dire que toutes les informations doivent être préalablement et précisément définies.

Cette caractéristique de précision est aussi vérifiée dans les contrats intelligents parce que, considérant l'immutabilité des registres sur la chaîne, les parties sont sûres qu'aucune modification n'a été apportée⁹⁷. La précision est donc un avantage lié principalement à l'écriture

⁹⁵ Supra, note 75.

⁹⁶ S. LOIGNON, préc., note 25, p. 244.

⁹⁷ P. DE FILIPPI et A. WRIGHT, préc., note 8, p. 38.

du contrat, qui dans ce cas est fait par un code de programmation, conçu de façon plus exacte que le langage courant.

“For decades, scholars have recognized that symbolic logic, like software code, can decrease contractual ambiguity by turning promises into objectively verifiable technical rules. Because smart contracts are nothing more than bits of logic executed in a deterministic manner, they can decrease the possibility of misinterpretation in instances where parties can reliably identify objectively verifiable performance obligations.”⁹⁸

Au sujet de la transparence, toutes les conditions de l’engagement sont faciles d’accès aux parties et éventuellement à des tiers⁹⁹ (il faut souligner que c’est l’accès ce qui est facilité, et non la compréhension en raison du langage de programmation, comme sera traité dans le sous-chapitre 2.2.1). Au sein d’une chaîne de blocs, les transactions sont également toujours disponibles pour consultation.

Comme nous l’avons mentionné à l’occasion de l’examen de la désintermédiation, une des révolutions apportées aux contrats intelligents par cette technologie repose sur la confiance. Il faut préciser que la transparence est un des éléments qui composent la confiance, parallèlement à la quête de la vérité¹⁰⁰.

En bref, les contrats intelligents permettent un renforcement de la transparence et de la précision depuis la conclusion jusqu’à l’exécution de ces contrats¹⁰¹. Ces engagements sont considérablement plus objectifs, ce qui est clairement lié aussi à l’avantage de gain de temps et

⁹⁸ P. DE FILIPPI et A. WRIGHT, préc., note 8, p. 82.

⁹⁹ P. DE FILIPPI et A. WRIGHT, préc., note 8, p. 38.

¹⁰⁰ « Transparency and truth seeking are complementary characteristics of trust. Transparency asks the question: can we see it? Truth asks: can we verify it? » W. MOUGAYAR, préc., note 16, p. 34.

¹⁰¹ Mustapha MEKKI, *Blockchain : l’exemple des smart contracts – Entre innovation et precaution*, 2018, p. 5, en ligne : < <https://lesconferences.openum.ca/files/sites/97/2018/05/Smart-contracts.pdf> > (consulté le 01 oct. 2019)

d'argent (par exemple, les violations à l'accord sont plus difficiles et les batailles judiciaires sont, par conséquent, découragées).

2.1.4. Absence de papier

De plus, les contrats intelligents réduisent la dépendance au papier ce qui protège le stockage et l'intégrité du contrat. Les pertes, falsifications ou amendements non autorisés des documents sur la chaîne de blocs sont plus difficiles par rapport à ceux sous format papier.

Dans le cas d'une éventuelle perte de données ou d'une attaque, la récupération des documents serait plus facile et sûre grâce aux caractéristiques de la chaîne de blocs, comme l'absence d'un point unique de contrôle et des copies mises à jour enregistrées dans chaque nœud.

Contrairement aux documents sur un support papier, les contrats intelligents enregistrés sur la chaîne de blocs n'auraient pas besoin de la présence physique des parties ou de leurs représentants dans un lieu particulier. Cette caractéristique démontre un lien direct avec l'idée de transparence dans la mesure où les documents seraient disponibles quel que soit le moment ou le lieu ayant accès à Internet. Cette dématérialisation permettrait également de gagner du temps et de l'argent en évitant des déplacements superflus. Parmi diverses questions qui méritent l'attention, l'utilisation d'autres supports que le papier est constamment encouragé dans la vague d'inquiétude sur l'environnement ces dernières années.

2.1.5. Efficience

Reste à noter que tous ces avantages sont connectés entre eux. Cet ensemble de qualités des contrats intelligents peut se résumer en efficacité. Il est vrai que les dispositions contractuelles revêtent une grande importance pour l'exécution d'un contrat. Toutefois, cette exécution peut être renforcée et favorisée à l'aide d'instruments technologiques capables de l'automatiser. Les gains de temps, de ressources financières, de sécurité et de fiabilité mènent à l'efficacité derrière ces engagements auto exécutables.

En fin de compte, l'efficacité résulte d'abord de la bonne formation d'un contrat, ce qui est essentiel à sa bonne exécution. Cependant, cette bonne exécution en soi est également primordiale à l'efficacité du contrat. Ainsi, bien que les contrats intelligents soient majoritairement connus grâce à leur exécution automatique, ils semblent être capables de renforcer l'efficacité contractuelle lors de ces deux moments d'un engagement – sa formation et son exécution.

2.2. Des risques particuliers de la mise en œuvre de contrats intelligents

Bien que les avantages des contrats intelligents soient notables, il faut faire attention aux risques de leur mise en œuvre. Nous pouvons qualifier ces points comme des risques ou comme des entraves à l'application plus effective des contrats intelligents aujourd'hui.

Parmi ces obstacles, divers points portent à discussion, comme des aspects techniques liés à la structure de communication entre deux chaînes de blocs¹⁰², ainsi que le manque d'une

¹⁰² « On a par exemple la chaîne proposée par la fondation Ethereum et la chaîne déjà longue du protocole Bitcoin. En l'état actuel de la technologie, il n'existe pas de solution pour faire converger deux chaînes. (...) Une telle table de correspondance entre Blockchains n'existe pas à l'heure actuelle et il est très peu probable qu'elle existe avant de nombreuses années tant les difficultés sont grandes. » B. CHOULI, F. GOUJON et Y. LEPORCHER, préc., note 37, p. 396.

méthode de recherche directe d'informations sur une chaîne de blocs¹⁰³. Néanmoins, il faut en aborder certains qui sont présents dans la plupart des discussions actuelles : le manque de compréhension de la technologie encore en développement; les fautes dans la programmation; et l'impossibilité d'effectuer des changements au cours du contrat, le cas échéant.

La reconnaissance de l'existence de faiblesses dans un système est généralement le premier pas vers son amélioration. Ainsi, passons à l'analyse des obstacles mentionnés.

2.2.1. Manque de compréhension

Le manque de compréhension relatif aux contrats intelligents et à sa base, la chaîne de blocs, est encore un obstacle à une éventuelle diffusion de cette technologie. Au cas où ces technologies soient plus connues et leur fonctionnement mieux compris, les gouvernements, entreprises et les personnes physiques pourraient être plus enclines à les utiliser, en prenant en compte leurs nécessités particulières.

Le principal problème créé par le manque de compréhension sur la chaîne de blocs est la méfiance¹⁰⁴. Cette technologie n'est pas la première à faire face à ce défi, qui ne date pas d'aujourd'hui. En effet, le manque de confiance dans les innovations en général a été constaté il y a plusieurs décennies :

“Distrust of new technologies is deeply rooted in Western culture. It could well be, as suggested in an earlier chapter, that some forms of resistance to new technology are endemic to the societal process of innovating technology. The very conceptual

¹⁰³ « Le problème de recherche d'une information se retrouve sur une Blockchain. Chaque bloc est validé avec des informations à l'intérieur. (...) Si on a l'identifiant de transaction, on peut retrouver le hash de la transaction avec les montants et le pseudo de l'émetteur et du destinataire, mais c'est tout. Il n'existe pas de langage pour faire une requête rapide et efficace dans une chaîne. » B. CHOULI, F. GOUJON et Y. LEPORCHER, préc., note 37, p. 398.

¹⁰⁴ « *A lack of comprehensive understanding of the basic capabilities surrounding the blockchain will deter any smart executive from seeing the fullness of its potential value. This challenge will be only solved via a concerted effort to get educated about the blockchain and its potential.* » W. MOUGAYAR, préc., note 16, p. 80.

framework in which we have discussed technology as ideas, as skills, and as behavior, involves a complex of institutional beliefs and practices, sentiments and symbols, to which people acquire an emotional attachment that makes them resistant to change."¹⁰⁵

Ainsi, la compréhension de la chaîne de blocs est encore restreinte considérant la diversité et l'ampleur de tous ces changements entrevus dans les domaines les plus variés. Fréquemment, une grande capacité de changement est attribuée à la technologie de la chaîne de bloc, concernant, par exemple, l'absence ou le changement des intermédiaires traditionnels, l'établissement de la confiance directement entre les parties orientées vers la promotion d'une culture pair-à-pair, et l'automatisation de tâches historiquement lentes et coûteuses. Ces changements indiqueraient d'importantes mutations de paradigme social et commercial dans le domaine privé et public. Néanmoins, les contours de la technologie ne sont pas bien compris, notamment parce qu'ils sont encore en train d'être expérimentés dans la réalité globale qui comprend la rapidité des relations numériques chaque fois plus sans frontières.

2.2.2. Erreurs de programmation

En ce qui concerne le risque découlant des erreurs de programmation, il est déjà possible d'indiquer des cas réels dans lesquels une mauvaise écriture du code a permis des attaques de pirates informatiques.

L'incident le plus connu est celui de l'attaque d'un contrat de mise en œuvre d'une plateforme de financement participatif connu comme « The DAO » qui, jusqu'à l'assaut, avait

¹⁰⁵ Thomas R. DEGREGON, *A Theory of Technology. Continuity and Change in Human Development*, Iowa City, The Iowa State University Press, 1985, p. 67.

collecté environ 150 millions de dollars¹⁰⁶. Le pirate avait été capable de voler plus de 60 millions de dollars. Dans ce cas, il avait exploité les vulnérabilités de *reentrancy*¹⁰⁷ : au moyen d'une transaction unique, le pirate avait réussi à transférer les fonds de la plateforme originelle plusieurs fois vers une copie qu'il avait créé – comme nous l'avons déjà vu (chapitre 2.1.2.), cette fonction est possible grâce au langage *Turing complete*. Dans ce cas,

« La procédure d'attaque est assez simple. La personne, ou le groupe à l'origine de l'attaque, a créé une DAO fille, en tout point identique à TheDAO, a utilisé a priori une boucle récursive pour capter les fonds, comme s'il s'agissait d'un projet voté par les investisseurs, et s'est donc approprié ces fonds. Or, cette captation des fonds suit les règles de TheDAO. Cela implique que ces fonds doivent rester bloqués pendant 28 jours avant de pouvoir les transférer à nouveau dans l'économie réelle. »¹⁰⁸

Généralement, les DAO permettent aux participants de donner des fonds aux contrats de leur choix. Une attaque comme celle qui s'est produite fut essentiellement causée par la programmation initiale qui a permis le transfert du montant avant la mise à jour du crédit qui figure réellement dans le compte. Ainsi, la transaction est effectuée, mais le montant n'est pas réduit de sorte qu'il est « utilisé » plusieurs fois.

Dans ce cas, la solution trouvée devant l'attaque a été la constitution d'un *hard fork* (l'introduction d'importants modifications des règles qui régissent une chaîne de blocs).

¹⁰⁶ Giulio PRISCO, *The DAO raises more than \$117 million in world's largest crowdfunding to date*, 16 mai 2016, en ligne : <<https://bitcoinmagazine.com/articles/the-dao-raises-more-thanmillion-in-world-s-largest-crowdfunding-to-date-1463422191>> (consulté le 12 nov. 2018)

¹⁰⁷ « One of the major dangers of calling external contracts is that they can take over the control flow, and make changes to your data that the calling function wasn't expecting. This class of bug can take many forms, and both of the major bugs that led to the DAO's collapse were bugs of this sort. » Nikhil MOHAN, *Solidity Smart contract Security best practices*, 07 août 2017, en ligne : https://consensys.github.io/smart-contract-best-practices/known_attacks/ (consulté le 12 nov. 2018)

¹⁰⁸ B. CHOULI, F. GOUJON et Y. LEPORCHER, préc., note 37, p. 417.

D'ailleurs, le remboursement a pu par la suite être fait, puis la cryptomonnaie ETH fut créé en substitution à l'ETC de la Ethereum Classic, la chaîne dépassée par l'attaque¹⁰⁹. Ces sont deux des mesures appliqués, mais c'est certain que les conséquences d'un tel attaque ne sont pas facilement réglables.

Quand il s'agit d'erreurs de programmation, il est possible d'établir un parallèle avec la machine distributrice, déjà mentionnée. Il n'est pas difficile d'imaginer une situation où elle garde l'argent, mais ne fournit pas la cannette demandée, par exemple, à cause d'un problème quelconque dans son système de reconnaissance du paiement. Les contrats intelligents dans une chaîne de blocs, de la même façon, peuvent avoir leur exécution compromise par des revers de leur système basé sur le langage de programmation. Il s'agit d'un des principaux risques de leur mise en œuvre.

Un autre exemple de risque qui porte sur les contrats intelligents arrive dans les cas où l'exécution de ces contrats dépend d'un mécanisme d'horodatage (*timestamp*, en anglais). Ce mécanisme permet d'associer l'information de date et d'heure à des données. Néanmoins, il existe la possibilité d'adultération de ce timbre de temps¹¹⁰. Ce qu'il convient de garder à l'esprit est l'existence de manières d'altérer l'heure du registre ou du contrat (même de quelques secondes seulement). Cette modification peut dénaturer indûment la relation en faveur d'une des parties.

Dans tous les cas, les programmeurs et les chercheurs en la matière essaient de discuter des vulnérabilités, notamment sur les forums de discussion en ligne d'Ethereum¹¹¹. Ils procèdent

¹⁰⁹ B. CHOULI, F. GOUJON et Y. LEPORCHER, préc., note 37, p. 419.

¹¹⁰ Cf. Loi LUU, Duc-Hiep CHU, Hrish Olickel, Prateek SAXENA, Aquinas HOBOR, *Making Smart Contracts Smarter*, Vienna, oct. 2016, (PDF) en ligne : <<https://eprint.iacr.org/2016/633.pdf>> (consulté le 14 nov. 2018) (à propos du système d'horodatage)

¹¹¹ Cf. ETHEREUM, *Research*, 2018, en ligne : <<https://ethresear.ch/>> (consulté le 14 nov. 2018)

aussi à des tests afin d'identifier de nouvelles complications et les possibles solutions. Nonobstant l'impossibilité d'une protection intégrale de tous les systèmes, ces initiatives de prévention et de réparation sont importantes pour le perfectionnement des chaînes de blocs et des contrats intelligents.

2.2.3. L'immutabilité

L'impossibilité d'effectuer des changements au cours du contrat, le cas échéant, est un autre risque – ou plutôt un obstacle – à l'acceptation de la mise en œuvre des contrats intelligents à grande échelle. La fonctionnalité de changement serait importante afin de garder la primauté de la volonté des parties pendant toute l'existence de l'engagement ainsi que de corriger les erreurs de programmation ou de bogues, en visant également l'intégrité du pacte.

L'immutabilité est une caractéristique généralement considérée positive lorsqu'on traite des chaînes de blocs et des contrats intelligents puisque cela sécurise les registres. Toutefois, cette autre perspective pourrait être prise en compte si les acteurs intéressés par cette technologie envisagent d'élargir son application dans le contexte du monde réel. Les chaînes de blocs sont connues comme « en ajout seulement » (*append-only*, en anglais), ce qui veut dire qu'il n'est pas possible de retirer les données enregistrées, seulement d'en additionner d'autres¹¹². C'est dans cette dynamique que réside l'obstacle. “*No single party has the power to modify or roll*

¹¹² ACCENTURE, *Editing the uneditable blockchain. Why distributed ledger technology must adapt to an imperfect world*, 2016, (PDF) en ligne : <https://www.accenture.com/t20160927T033514Z_w_/ro-en/acnmedia/PDF-33/Accenture-Editing-Uneditable-Blockchain.pdf> (consulté le 15 nov. 2018)

*back information stored on a blockchain, and no single party can halt the execution of a smart contract once it has been deployed, unless provided for in the code*¹¹³.

Le changement d'un contrat intelligent déjà déployé est parfois envisageable, mais il n'est pas facile. En fait, il ne s'agit pas d'une altération proprement dite sur le contrat original parce que cela impliquerait de modifier les registres sur la chaîne de blocs, ce qui n'est pas faisable. Il faut, par exemple, récupérer toute l'information déjà programmée et la récrire sur un autre contrat, en mettant à jour l'adresse d'accès aux usagers/parties, ou encore au moyen d'une séparation entre les données et la logique du contrat.

Aujourd'hui, des alternatives sont examinées afin de trouver une solution plus uniforme et pratique au changement des contrats intelligents après leur déploiement. Selon une étude publiée en 2016, “[h]aving the ability to edit, rather than append, smart contracts would preserve time and resources”¹¹⁴, notamment en raison de la croissante complexité et de l'envergure des contrats sur la chaîne de blocs.

En visant une innovation dans le caractère d'immutabilité des contrats intelligents, le *US Patent & Trademark Office* (Bureau américain de brevets et de marques de commerce) a analysé la demande de brevet présenté par le conglomérat chinois de commerce électronique Alibaba. La demande proposait l'intervention d'un tiers dans un contrat intelligent dans les cas d'activités illicites sur la plateforme. Il serait ainsi capable d'intervenir sur le réseau ou même d'arrêter ou d'interrompre les comptes d'utilisateur dont les opérations seraient considérées illégales¹¹⁵.

¹¹³ P. DE FILIPPI et A. WRIGHT, préc., note 8, p. 35.

¹¹⁴ ACCENTURE, préc., note 110.

¹¹⁵ Ana ALEXANDRE, *Alibaba Files Patent for Blockchain System That Allows 'Administrative Intervention'*, 05 oct. 2018, en ligne : <<https://cointelegraph.com/news/alibaba-files-patent-for-blockchain-system-that-allows-administrative-intervention>>(consulté le 15 nov. 2018)

L'idée centrale de l'étude mentionnée et de la demande de brevet, en somme, converge vers l'insertion des contrats intelligents dans le contexte du monde réel, où des défaillances ou les abus peuvent survenir et ont besoin d'être corrigés par le droit.

À cet égard, il faut noter que les pirates informatiques cherchent quotidiennement de nouvelles manières d'interférer dans les opérations sur les chaînes de blocs, mais il faut bien considérer que de l'autre côté, il y a aussi de gros efforts en faveur de la sécurité des transactions sur ces réseaux. Certains projets analysent statistiquement les codes des contrats afin de trouver les vulnérabilités possibles, comme Oyente¹¹⁶, qui simule l'exécution d'un contrat intelligent sur l'Ethereum afin de vérifier l'existence de bogues.

Un autre enjeu qui découle de l'immutabilité est lié au droit à l'oubli. Sur Internet, il y a déjà des efforts pour respecter ce droit : « Par exemple, en 2015, Google a été mis en demeure par la CNIL de déréférencer du moteur de recherche les utilisateurs qui le souhaitent (CNIL, 2015). Cela implique que certaines pages ne soient plus accessibles via le moteur »¹¹⁷.

Dans le cas des chaînes de blocs, nous avons déjà mentionné la difficulté de retrouver un registre sans avoir le numéro d'identification correspondant à la transaction. Parallèlement, l'immutabilité ne permet pas d'effacer ou de changer ces registres, c'est-à-dire que l'information sera toujours, en quelque sorte, disponible aux tiers. Une situation fictive serait le casier judiciaire d'un condamné qui aurait vu son registre nettoyé après l'exécution de la peine et le respect de la loi. Si cela était enregistré sur une chaîne de blocs, le droit à l'oubli ne serait pas respecté¹¹⁸.

¹¹⁶ Cf. OYENTE, *An Analysis Tool for Smart Contracts*, en ligne : <<https://www.comp.nus.edu.sg/~loiluu/oyente.html>> (consulté le 15 nov. 2018)

¹¹⁷ B. CHOULI, F. GOUJON et Y. LEPORCHER, préc., note 37, p. 405.

¹¹⁸ *Id.*

Ce sont des exemples des enjeux entraînés par l'immutabilité. Il faut apprécier leur incidence sur le développement de cette technologie dans le monde réel, ce qui nous amène à l'examen de certains cas d'usage dans le sous-chapitre suivant.

2.3. Les aspects pratiques des chaînes de blocs: cas d'usage

Les aspects techniques évoqués dans le chapitre précédent servent de base aux applications générales des chaînes de blocs. Il s'avère que, malgré cette base commune, les cas d'usage possibles sont des plus variés, par exemple : authentification des œuvres d'art; microcontrats; cartes prépayées; chaîne d'approvisionnement; numérisation de contrats; lutte contre la contrefaçon; gestion de diamants; authentification de diplômes; authentification de documents, preuve d'existence, preuve de propriété de contenus numériques; bases de données publiques; énergie renouvelable et économie de partage; cartes de fidélité; identités digitales; Internet alternatif; Internet des objets; jeux; gestion de dossiers médicaux; musique; gestion de noms de domaines; paiement en ligne simple et sécurisé; prêts entre particuliers; propriété intellectuelle; bâtiments intelligents; stockage décentralisé; signature électronique; traçabilité; transport de personnes; vote¹¹⁹.

Bien évidemment, cet inventaire n'est pas exhaustif. Plusieurs autres usages sont menés (voir l'annexe I, « Certaines applications de la chaîne de blocs »), dont quatre seront examinées

¹¹⁹ L. LELOUP, préc., note 26, p. 125-128.

dans les pages suivantes : les services financiers, les assurances, le commerce d'énergie et l'industrie créative.

2.3.1. Services financiers

Le domaine des cryptomonnaies fut la première expérience d'emploi de la chaîne de blocs, avec le Bitcoin. Nous avons vu le parcours historique de la technologie de la chaîne de blocs jusqu'aux contrats intelligents. Toutefois, il faut souligner d'emblée la pertinence de la chaîne de blocs pour les transactions financières en général par le biais des paiements électroniques, qu'ils soient par des cryptomonnaies ou non.

Dans le marché financier, la flambée des *fintechs* révèle le grand potentiel de changement apporté par les technologies dans l'univers financier. Le terme *fintech* découle de l'expression *Financial Technology* (ou « technologie financière ») et, en bref, vise l'amélioration des pratiques dans le secteur aussi bien par les organisations traditionnelles que par les startups.

À cet égard, l'apprentissage machine, l'intelligence artificielle, l'analyse de mégadonnées, la biométrie et aussi la chaîne de blocs figurent parmi les moyens par lesquels les *fintechs* transforment la prestation de services financiers en créant de nouveaux services, produits ou en remodelant ceux déjà existants, toujours à l'aide de la technologie¹²⁰.

Lorsque nous parlons de la chaîne de blocs dans le domaine financier, le projet Ripple mérite d'être souligné notamment en raison de son envergure. À l'origine, comme nous l'avons

¹²⁰ Gustavo CLEMENTONI, *The Difference Between Blockchain and Fintech*, 17 juill. 2018, en ligne : <<https://www.e-zigurat.com/digital/the-difference-between-blockchain-and-fintech> > (consulté le 04 nov 2018)

vu lors de l'examen de ses caractéristiques, l'idée de la chaîne de blocs se fonde spécialement sur l'absence d'un tiers de confiance ou d'une autorité centrale.

En effet, l'industrie financière semble croire aux prétendus avantages des chaînes de blocs. Par exemple, le Santander a émis un rapport en analysant de données de la Banque mondiale, de la World Federation of Exchanges, de l'Oxera, du Financial Times et d'Oliver Wyman Analysis, où il a suggéré que « *distributed ledger technology could reduce banks' infrastructure costs attributable to cross-border payments, securities trading and regulatory compliance by between \$15-20 billion per annum by 2022* »¹²¹.

Dans ce contexte d'optimisme, certains considèrent qu'« il aurait été difficile pour les banques et les établissements financiers de passer à côté du sujet. »¹²² Un des slogans du projet Ripple est: “*In a world where three billion people are connected online, cars drive themselves and appliances can communicate, global payments are still stuck in the disco era.*”¹²³

Ainsi, les banques et les institutions financières ont reconnu le besoin de changements dans le secteur. Tel est le but de la RippleNet, une plateforme qui connecte les fournisseurs de services financiers et de paiement afin de faciliter les échanges transfrontaliers de façon simple, rapide et moins coûteuse. Un des aspects principaux de son fonctionnement, selon eux, est la possibilité d'encadrer des transactions avec la cryptomonnaie de la plateforme (« XRP »), des monnaies fiduciaires ou même d'autres actifs. Aujourd'hui, ce projet est encore en expansion¹²⁴.

¹²¹ OLIVER WYMAN, ANTHEMIS GROUP AND SANTANDER INNOVENTURES, *The Fintech 2.0 Paper. Rebooting financial services*, 2015, (PDF) en ligne : <<http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf>> (consulté le 04 nov. 2018)

¹²² L. LELOUP, préc., note 26, p. 22.

¹²³ RIPPLE, *Today's Payment Rails Don't Cut It*, en ligne : <<https://ripple.com/>> (consulté le 04 nov. 2018)

¹²⁴ Voir : Laurent BIJON, *SBI veut adopter la technologie Ripple à une plus grande échelle via le consortium R3*, oct. 2018, en ligne : <<https://www.placecrypto.fr/cryptos/sbi-veut-adopter-la-technologie-ripple-a-une-plus-grande-echelle-via-le-consortium-r3.html>> (consulté le 4 nov. 2018); Anna IRRERA, *Blockchain startup Ripple*

Les gouvernements établissent également leurs propres projets, comme ceux promus par la Banque du Canada et par l'autorité monétaire de Singapour, décrits ci-dessous.

Le Projet Jasper¹²⁵, par exemple, annonce la coopération entre la Banque du Canada, représentant le secteur public, et d'autres institutions privées, comme Payments Canada, TMX Group et Accenture, et R3, afin de mener des recherches sur la technologie des registres distribués (DLT). Subdivisé en trois phases, le projet vise à analyser la compensation et le règlement des paiements interbancaires en utilisant la DLT, ainsi que les avantages potentiels de l'incorporer à d'autres actifs, comme les valeurs mobilières.

Le projet Ubin, coordonné par l'autorité monétaire de Singapour en partenariat avec des entreprises du secteur¹²⁶, a été conçu dans le but d'exploiter la DLT pour rendre les paiements transfrontaliers plus rapides et moins chers¹²⁷.

Ainsi, nous constatons que l'application pratique de la chaîne de blocs attire l'attention des acteurs de l'industrie financière, privés et publiques, engendrant de nombreux projets fondés sur cette technologie.

signs up PNC as a customer for its payment tech, 19 sept. 2018, en ligne : <<https://goo.gl/4tW9Me>> (consulté le 04 nov. 2018)

¹²⁵ Voir : James CHAPMAN, Rodney GARRATT, Scott HENDRY, Andrew MCCORMACK et Wade MCMAHON, « Projet Jasper. Les systèmes de paiement de gros décentralisés sont-ils aujourd'hui chose faisable ? », *Banque du Canada*, juin 2017, en ligne : <<https://www.banqueducanada.ca/wp-content/uploads/2017/05/rsf-juin-2017-chapman.pdf>> (consulté le 04 nov. 2018)

¹²⁶ Les entreprises membres du projet sont les suivantes: Bank of America Merrill Lynch, BCS Information Systems, Credit Suisse, DBS Bank, HSBC, J.P. Morgan, Mitsubishi UFJ Financial Group, OCBC Bank, R3, Singapore Exchange et UOB Bank. Cf. DELLOITTE. *The future is here. Project Ubin. SGD on Distributed Ledger*, 2017, en ligne : <<http://www.mas.gov.sg/~media/ProjectUbin/Project%20Ubin%20%20SGD%20on%20Distributed%20Ledger.pdf>> (consulté le 04 nov. 2018)

¹²⁷ MONETARY AUTHORITY OF SINGAPORE, *Project Ubin: Central Bank Digital Money using Distributed Ledger Technology*, 11 nov. 2018, en ligne : <<http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/Project-Ubin.aspx>> (consulté le 15 nov. 2018)

2.3.2. Assurance

Le domaine des contrats d'assurance constitue une autre sphère considérablement touchée par le développement de la technologie de la chaîne de blocs et pour les contrats intelligents. Plusieurs entreprises du milieu sont déjà intéressées par leur déploiement¹²⁸.

L'exemple le plus saillant de l'usage de cette technologie dans le secteur est la mise en œuvre de contrats intelligents d'assurance contre des vols retardés. Il s'agit du registre d'un engagement sur le réseau de façon à déclencher automatiquement le remboursement aux consommateurs dès que le retard du vol est constaté selon les conditions définies au préalable¹²⁹.

La constatation de ces conditions introduit un autre concept important dans le contexte des chaînes de blocs : les oracles. *“You can think of them as off-chain data sources that a smart contract can use to modify its behavior”*¹³⁰. Comment est-ce que la plateforme, de façon sécuritaire et impartiale, peut être au courant de la survenance des conditions afin de déclencher le contrat ? C'est précisément la fonction des oracles, qui attestent la réunion des conditions exigées pour le déclenchement de la convention.

Par ailleurs, il y a encore la possibilité de créer une base de données cryptée et partagée entre les acteurs avec le même centre d'intérêt, comme celle lancée par un consortium entre diverses entreprises européennes¹³¹. Connue comme projet B3i, l'objectif serait de mettre en pratique certaines mesures capables d'automatiser les versements d'indemnisation et de partage

¹²⁸ C'est le cas des Britanniques Lloyds et EY, ainsi que de la géante Allianz.

¹²⁹ Michiel BERENDE, *The potential of blockchain. From flight-delay to agriculture insurance*, 23 mai 2018, en ligne : <<https://medium.com/impact-insurance/the-potential-of-blockchain-from-flight-delay-to-agriculture-insurance-eb774e8f8508>> (consulté le 16 nov. 2018)

¹³⁰ W. MOUGAYAR, préc., note 16, p. 44.

¹³¹ B3i, *The Blockchain Insurance Industry Initiative*, en ligne : <<https://b3i.tech/home.html>> (consulté le 16 nov. 2018)

de données, ce qui, par conséquent, met des solutions de la chaîne de blocs à la disposition du marché d'assurances.

Les assurances récolte/indicielles¹³² peuvent également tirer parti de cette technologie. Au moyen des oracles, des informations sur les cultures seraient également présentées à la chaîne de blocs. Les versements pertinents seraient déclenchés selon les stipulations accordées dans le contrat intelligent au préalable. Prenez l'exemple d'un cas de sécheresse dans une période supérieure à 180 jours, considérant que les parties ont stipulé cette période comme étant la limite sans pluie. Le contrat intelligent recevrait l'information d'un centre de météorologie prédéfini (l'oracle) entraînant le paiement de la prime de l'assurance conventionnée directement à l'agriculteur.

Parmi les principaux avantages de la mise en œuvre des contrats intelligents, deux d'entre eux sont plus évidents dans les cas d'assurances : la réduction du temps nécessaire au traitement des demandes et des coûts afférents.

2.3.3. Commerce d'énergie

Depuis des décennies, la consommation énergétique cause des inquiétudes partout dans le monde. Dans ce contexte, des sources d'énergie renouvelables sont devenues essentielles, ce qui englobe l'énergie solaire, éolienne, géothermique, hydroélectrique et océanique, entre autres.

¹³² FRAZ FINANCE CENTRE DE FORMATION FINANCIÈRE, *Blockchain. L'assurance indicielle. Nouvelle assurance agricole pour l'Afrique*, 30 nov. 2017, en ligne : <<http://centre-de-formation-financiere.over-blog.com/2017/11/blockchain-l-assurance-indicielle-nouvelle-assurance-agricole-pour-l-afrique.html>> (consulté le 16 nov. 2018)

L'utilisation de ces moyens alternatifs s'est développée conjointement aux technologies, comme dans la construction des parcs éoliens et des centrales solaires thermodynamiques.

La chaîne de blocs émerge comme une nouvelle possibilité dans le contexte des énergies renouvelables. La commercialisation d'énergie pair-à-pair serait facilitée par le biais de cette technologie en évitant le gaspillage et en créant un marché dans lequel les consommateurs deviennent « consomm'acteurs »¹³³.

En 2016, dans le quartier de Brooklyn à New York, évoquons l'exemple des mini-réseaux (*microgrids*¹³⁴) reliant les habitants intéressés à échanger de l'énergie entre eux. Il s'agissait d'une manifestation de l'économie de partage, pour laquelle la chaîne de blocs peut servir de catalyseur. Ce marché fonctionne de la manière suivante : certains membres du réseau produisent un excédent énergétique à partir de sources renouvelables qui leur appartiennent; cet excédent est mis à la disposition des autres membres, voisins du quartier, qui souhaitent l'acheter ou l'échanger. Toute la relation est sécurisée et monétisée *via* le réseau créé dans la chaîne de blocs.

En plus de l'initiative nord-américaine, d'autres actions ont eu lieu partout dans le monde. En juillet 2016, la plateforme Enerchain¹³⁵, créée par la start-up allemande Ponton, a

¹³³ Myriam-Deborah AMICHIA, *UtilityWise. La blockchain, une technologie au service du secteur de l'énergie*, 24 avril 2018, en ligne : <<https://www.utilitywise.fr/2018/04/24/la-blockchain-une-technologie-au-service-du-secteur-de-lenergie/>> (consulté le 29 oct. 2018)

¹³⁴ « *A microgrid is a small-scale power production and delivery system comprising distributed generation facilities co-located with the loads they serve. Microgrids encompass multiple types of energy generation resources, storage systems, and efficiency programs, allowing for optimal utilization of renewable energy resources and facilitating advanced energy management, demand response, and load reduction solutions. Microgrids are able to be connected to the utility grid to purchase power from the grid or sell power back to the grid as conditions dictate. Microgrids can be designed to operate 'islanded' when the utility grid is not available.* » GREEN ENERGY CORP, *Microgrid Overview*, en ligne : <<http://www.greenenergycorp.com/about-us/about-us/technology/>> (consulté le 2 nov. 2018)

¹³⁵ Cf. ENERCHAIN, *The Enerchain Project*, en ligne : <<https://enerchain.ponton.de/>> (consulte le 5 nov. 2018)

inauguré le marché d'énergie sur la chaîne de blocs en Europe. Nous trouvons aussi la plateforme ElectricChain¹³⁶, visant à suivre les échanges d'énergie solaire mondialement et en temps réel.

Fondée en 2016 en Australie, la startup Power Ledger¹³⁷ emploie la chaîne de blocs pour l'échange pair-à-pair de l'énergie solaire produit en excès par les participants. En Allemagne, le projet Conjoule¹³⁸ développe la technologie dans le domaine. Il existe plusieurs autres initiatives dans le monde, comme le Drift (aux États-Unis), Greeneum (en Europe, à Chypre, en Israël, en Afrique et aux États-Unis), Grid Singularity (en Autriche), Electron (au Royaume-Uni), LO3 Energy (aux États-Unis), Electrify (à Singapour), EIBlox (en Suisse) et Sunchain (en France)¹³⁹.

Considérant que la plupart de ces projets sont encore en cours, il sera peut-être possible, dans quelques années, de vérifier l'efficacité et l'utilité de ces mécanismes adoptés aujourd'hui au moyen de la chaîne de blocs au regard de l'implémentation de sources renouvelables à plus grande échelle.

2.3.4. L'industrie créative

Finalement, une dernière illustration des usages pratiques de la chaîne de blocs serait liée au milieu artistique. Dans ce domaine, plusieurs enjeux courants peuvent être surmontés grâce à la chaîne de blocs, notamment les défis relatifs à la rémunération et à la protection des droits d'auteur.

¹³⁶ Cf. ELECTRICCHAIN, en ligne : <<https://www.electricchain.org/>> (consulté le 5 nov. 2018)

¹³⁷ Cf. POWERLEDGER, en ligne : <<https://www.powerledger.io/>> (consulté le 5 nov. 2018)

¹³⁸ Cf. CONJOULE, en ligne : <<http://conjoule.de/de>> (consulté le 5 nov. 2018)

¹³⁹ Karim BEDDIAR et Fabien IMBAULT, *Blockchain pour l'énergie*, Malakoff, Dunod, 2018, p. 58-61

Certains enjeux sont atténués grâce à l'enregistrement des données au sujet des œuvres (livres, musiques, peintures, photographies, etc.) sur une chaîne de blocs. Le marché de la musique a déjà ses représentants, parmi lesquels il convient de mettre en évidence la plateforme Ujo¹⁴⁰, basée sur la chaîne de blocs Ethereum. Les artistes y sont ainsi capables de publier et d'exploiter leurs travaux sans intermédiaires ni frontières.

C'est ce que la chanteuse et musicienne britannique Imogen Heap a fait lorsqu'elle a enregistré une de ses chansons sur la plateforme. Les usagers furent en mesure de télécharger la musique *Tiny Human* ainsi que d'utiliser un bout de l'œuvre dans leurs propres projets non commerciaux – la voix ou le son des instruments de musique¹⁴¹. Ce régime de commercialisation d'œuvres artistiques apporte plus de transparence et de contrôle en faveur des créateurs, puisqu'il garantirait que chaque partie concernée recevrait les sommes qui lui sont dues plus rapidement.

Dans les arts visuels, nous retrouvons la plateforme Monegraph, qui permet l'enregistrement des travaux d'artistes-plasticiciens, de photographes, des graphistes, d'illustrateurs etc. sur la chaîne de blocs¹⁴², et permettant également leur commercialisation¹⁴³.

Les spectacles artistiques en tireront également bénéfice, par exemple, par l'entremise des billets vendus et achetés à l'aide de la chaîne de blocs. De la sorte, les limites d'achat par personne seraient garanties et les initiatives des revendeurs non autorisés seraient entravées. Tout comme pour les cas précédents, la rémunération serait plus transparente et versée plus rapidement aux parties concernées.

¹⁴⁰ Voir : UJO, *Empowering music*, en ligne : <<https://ujomusic.com/>> (consulté le 6 nov. 2018)

¹⁴¹ M. J. CASEY et P. VIGNA, préc., note 24, p. 233.

¹⁴² Voir : MONEGRAPH, *How it works*, en ligne : <<https://monegraph.com/>> (consulté le 5 nov. 2018)

¹⁴³ B. CHOULI, F. GOUJON et Y. LEPORCHER, préc., note 37, p. 332.

La chaîne de blocs émerge également comme un moyen de lutte contre la piraterie dans le domaine audiovisuel, ce qui est l'objet de startups comme la Veredictum¹⁴⁴. Le fonctionnement de cette plateforme se présente en quatre étapes : elle propose que les créateurs (i) téléversent leurs contenus (ii) en certifiant leur propriété, (iii) en définissant les termes de leur utilisation par des tiers et finalement, (iv) en favorisant sa distribution. La technologie adoptée par cette plateforme et les procédés de sténographie permettent de créer des filigranes dans le contenu numérique aussi bien qu'un lien immuable avec une identité précédemment reconnue. À partir de là, il serait possible de mener des recherches en ligne afin de découvrir d'éventuels fichiers pirates¹⁴⁵.

Dans tous ces exemples, la technologie de la chaîne de blocs facilite la gestion des droits sur les œuvres artistiques, des règles de commercialisation, ainsi que la répartition de la rémunération correspondante entre toutes les personnes impliquées. Enfin, le système qui s'applique dans ces plateformes de l'industrie créative, quelle que soit la forme d'art, est le suivant :

“In these decentralized marketplaces, sellers can offer a product for sale by recording information to a blockchain, like a description of the good and its price. Interested buyers can send money to a virtual escrow account implemented via a smart contract (often referred to as a multisignature account), which autonomously controls and manages any posted funds. If everything goes as planned and the buyer receives the good in question, the buyer sends a digitally signed blockchain-based oracle steps in to analyze the facts of the case and determine who should receive the escrowed funds.”¹⁴⁶

¹⁴⁴ Voir : VEREDICTUM. Decentralised anti-piracy & content distribution platform, 2015, en ligne : <<https://www.veredictum.io/>> (consulté le 6 nov. 2018)

¹⁴⁵ Samuel BROOKS, *Incentivised Distributed Computation for Registered Digital Content Search*, juill. 2017, (PDF) en ligne : <<https://goo.gl/fE1xHK>> (consulté le 06 nov. 2018)

¹⁴⁶ P. DE FILIPPI et A. WRIGHT, préc., note 8, p. 76.

À cet égard, ces « marchés décentralisés » menés sur la chaîne de blocs seraient capables d'ébranler le monopole des tiers gestionnaires de droits des artistes, ce qui pourrait offrir un avantage aux créateurs en termes financiers. Les artistes deviendraient également capables d'accéder directement à plusieurs données qui peuvent servir à des initiatives de promotion et de ciblage concernant leur carrière¹⁴⁷.

En conséquence, les caractéristiques fondamentales de la chaîne de blocs sont transposées à chaque cas d'usage dans lequel elle est appliquée. Ainsi que tout domaine, le marché artistique utilise la chaîne de blocs visant à reproduire ses caractéristiques avantageuses aux relations dans le secteur respectif. Et les inconvénients de la technologie seraient également transposés à ses applications. Ainsi, il conviendrait de procéder à un examen cas par cas, s'il comporte plus d'avantages que d'inconvénients.

¹⁴⁷ M. J. CASEY et P. VIGNA, préc., note 24, p. 234

TITRE II – CONTRATS INTELLIGENTS : APPROCHE JURIDIQUE

« La mondialisation est au XXI^e siècle ce que la guerre froide était aux années 1950 : la structure narrative qui assemble toutes les pièces du puzzle. Si vous ne comprenez rien à la mondialisation, vous ne comprenez rien au monde. »
(Thomas L. Friedman, à Radio-Canada Information)

Chapitre 1 – Les mutations du droit face aux innovations technologiques

L'encadrement juridique des diverses affaires sur Internet est discuté depuis des nombreuses années. Différentes questions se posent dans un contexte de frontières mondiales atténuées. La liberté individuelle est-elle protégée dans le monde virtuel de la même manière qu'elle l'est dans le monde réel ? Comment protéger la vie privée et l'autodétermination informationnelle¹⁴⁸ (la faculté de l'individu de décider lui-même le destin des informations concernant sa vie privée) ? En cas de conflits, comment définir la compétence juridictionnelle ? Aujourd'hui encore, les réponses ne sont pas toujours unanimes.

Lorsque nous parlons du droit devant les innovations technologiques, la mise en œuvre d'une réglementation qui n'entrave pas le développement des technologies¹⁴⁹ et qui, parallèlement, soit capable de répondre aux nouvelles questions juridiques et d'assurer la protection collective et individuelle est un grand défi. C'est dans ce contexte qu'interviennent les contrats intelligents et que se pose la question de leur reconnaissance juridique.

¹⁴⁸ Voir : Yves POULLET et Jean-Marc DINANT, *L'autodétermination informationnelle à l'ère de l'Internet*, Conseil de l'Europe, Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 18 nov. 2004, en ligne : < <https://rm.coe.int/16806ae51f> > (consulté le 20 fév. 2019).

¹⁴⁹ S. LOIGNON, préc., note 25, p. 259.

L'idée de traduire les contrats traditionnels en langage informatique ou même de les programmer directement sur une chaîne de blocs représente un petit aperçu d'une vaste branche du droit qui essaye de concilier l'architecture juridique et le progrès technologique. Depuis longtemps, nous parlons d'une rencontre entre le droit et les technologies. Les mutations technologiques exercent, d'ores et déjà, une influence directe sur le droit et réciproquement.

Ainsi que dans les autres domaines du droit, le contrôle juridique complet et parfait des technologies n'est pas envisageable. Cela ne semble pas possible et ce pour diverses raisons, notamment à cause de la différence du rythme de développement entre le droit et les technologies, mais également à cause de la part d'erreur pouvant survenir dans ces deux domaines, du droit et des technologies. En effet, l'erreur est dans la nature humaine et ces deux domaines sont résultats de l'esprit humain. Toutefois, « *just because perfect control is not possible does not mean that effective control is not possible* »¹⁵⁰, c'est-à-dire qu'une régulation imparfaite n'empêche pas qu'elle puisse être effective.

Ainsi, afin de surmonter l'absence d'un contrôle parfait et afin d'avoir un contrôle effectif, deux voies juridiques peuvent être empruntées : le droit étatique et les normes alternatives.

1.1. Le droit étatique et les enjeux globaux

Sans prétendre à l'exhaustivité, lorsque nous examinons les enjeux juridiques d'aujourd'hui, y compris la réglementation des technologies de l'information, certains concepts

¹⁵⁰ Lawrence LESSIG, *Code: And Other Laws of Cyberspace*, Version 2.0, Basic Books, New York, 2006, p. 73, en ligne : < <http://codev2.cc/download+remix/Lessig-Codev2.pdf> > (consulté le 10 janv. 2019)

non juridiques ont de l'importance, comme la mondialisation, la globalisation, les mutations de la souveraineté, l'émergence du droit global, le pluralisme juridique et l'internormativité. Pour éviter les confusions conceptuelles, il convient de les examiner tout d'abord.

Les définitions de mondialisation et de globalisation sont parfois floues¹⁵¹. Bien que la mondialisation reflète dans une certaine mesure les aspects du mot anglais *globalization*, en français elle n'est pas toutefois synonyme de globalisation. Divers pans de la société sont touchés par la mondialisation ou par la globalisation. Toutefois, le domaine économique est le premier à influencer et à être influencé par ces phénomènes.

*“Sometimes it [globalization] obscures, sometimes it illuminates: global by definition, it does not just deal with the economic, nor the sociological in isolation; neither demography separately, nor traditional historicity taken as criteria of direction. It implies the criticism of separations, especially if they have had their moment and their need. Here we try to grasp it through a process of becoming worldwide, of the State, which supposes the world market, world technicality, etc. but which goes beyond these determinations.”*¹⁵²

La globalisation, quant à elle, s'étend au-delà des espaces. Elle serait un fait social¹⁵³ fondé sur des « rapports délocalisés qui surplombent, voire défient, les souverainetés étatiques et qui portent, en germe, une juridicité propre »¹⁵⁴. Ces deux phénomènes (la mondialisation et

¹⁵¹ Mireille DELMAS-MARTY, « Le flou du droit », dans Louis ASSIER-ANDRIEU (dir.), *Droit et société*, n°5, 1987, p. 140, en ligne : < https://www.persee.fr/doc/dreso_0769-3362_1987_num_5_1_1567_t1_0140_0000_1 > (consulté le 20 déc. 2018)

¹⁵² Stuart ELDEN, “Mondialisation before Globalization”, p. 80-93, p. 87, dans Kanishka GOONEWARDENA (ed.), Stefan KIPFER (ed.), Richard MILGROM (ed.), Christian SCHMID (ed.), *Space, Difference, Everyday Life: Reading Henri Lefebvre*, Abingdon, Routledge, 2008, 344 p.

¹⁵³ Guy ROCHER, « La mondialisation: un phénomène pluriel », dans Daniel MERCURE, *Une société-monde? Les dynamiques sociales de la mondialisation*, Québec, 2001, p. 19, en ligne : < <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/89/0046.pdf?sequence=1&isAllowed=y> > (consulté le 20 déc. 2018)

¹⁵⁴ Karim BENYEKHLEF., *Une possible histoire de la norme, Les normativités émergentes de la mondialisation*, 2^e Édition, Montréal, Les Éditions Thémis, 2015, p. 64.

la globalisation) sont également à distinguer d'une approche purement internationale, qui toucherait les relations entre les nations – ou plutôt entre les États – dans une sorte de « coordination des souverainetés »¹⁵⁵. On pourrait essayer de les représenter graphiquement pour rendre cette différence plus claire:

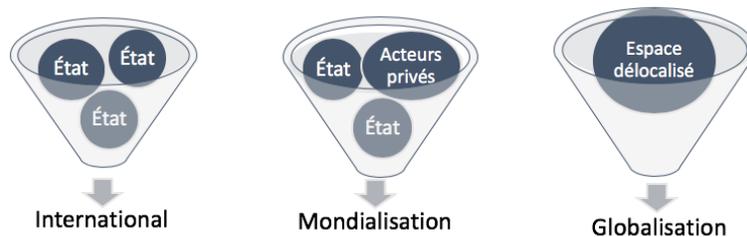


Figure 3. *Lex niveaux international, mondial et global*

Le terme mondialisation pourrait être appliqué dans le contexte de cette étude, toutefois l'expression « globalisation » semble encore plus adéquate, particulièrement en raison du caractère délocalisé des nouveaux enjeux engendrés par le développement technologique (comme dans le contexte du cyberspace). C'est grâce à cette absence de définition géographique que l'on pourrait prendre en considération une plus grande variété d'acteurs (les États et les acteurs privés, tels que les individus, les entreprises, les organisations non gouvernementales et les organisations internationales) dans le contexte de toutes leurs relations.

Ensuite, la reconfiguration de la notion de souveraineté attire l'attention. La souveraineté des États a connu certaines mutations qui exercent une influence sur le rôle du droit étatique, notamment face aux défis posés par la globalisation. Depuis quelques décennies, le modèle de monopole du droit par les États, basé sur leur souveraineté, a créé une fragmentation des ordres

¹⁵⁵ Pierre-Marie DUPUY et Yann KERBRAT, *Droit international public*, 11^e éd., Dalloz, Paris, 2012, p. 29.

juridiques qui réclame une solution – pas parfaite, mais au moins efficace. Ce modèle de monopole a progressivement été transformé. Dans un espace délocalisé comme celui d’aujourd’hui, la souveraineté des États résulte de la coexistence entre le pouvoir étatique et le pouvoir des acteurs privés, ce qui engendre un contexte fragmenté¹⁵⁶. Il est paradoxal d’observer une telle fragmentation juridique dans un monde de plus en plus connecté.

Par conséquent, nous sommes face à une reconsidération des dispositions traditionnelles de la souveraineté étatique. Néanmoins, cela ne signifie pas que l’État est ou sera remplacé. Cependant « il cédera en partie les rênes de son monopole normatif – ce qui a déjà commencé depuis la Seconde guerre mondiale – au profit d’agents (le marché, la société civile transnationale, les organisations internationales, etc.) [...]»¹⁵⁷

Au regard du monopole du droit comme une caractéristique importante de la souveraineté, il semblerait que les mutations du pouvoir étatique influencent également sa capacité de dire le droit. Ceci nous amène à considérer les autres concepts mentionnés au début de ce chapitre : le droit global, le pluralisme juridique et l’internormativité.

Au fil des siècles, le droit national et international – produits de la souveraineté de chaque État – sont devenus les fondements de la régulation des rapports sociaux. Toutefois, les mouvements actuels (mondialisation, globalisation, multitude de souverainetés et de sources normatives) ont créé des enjeux qui exigent plus de flexibilité et de rapidité du droit. Ainsi, le droit étatique ne semble pas être suffisant, pris isolément, pour régler ces nouvelles situations de façon effective.

¹⁵⁶ Karim BENYEKHLEF, « Vers une gouvernance globale: l’émergence d’un droit postnational », p. 123, dans Louise LALONDE et Stéphane BERNATCHEZ (dir.), *La place du droit dans la nouvelle gouvernance étatique*, Sherbrooke, Les Éditions Revue de Droit, 2011, 220 p.

¹⁵⁷ *Id.*

Une des raisons qui motive l'émergence d'un droit global serait le processus d'élaboration des normes étatiques : on est souvent confronté aux mécanismes lents qui exigent plusieurs étapes jusqu'à la réglementation. Et, aujourd'hui, dans le contexte globalisé et connecté, où les frontières territoriales et temporelles ne sont plus bien définies, la lenteur dans l'élaboration d'une norme peut la rendre obsolète et inefficace au plan pratique.

Pour sortir de l'impasse entre le temps d'élaboration d'une norme et l'efficacité de son application, l'idéal serait d'avoir des règles susceptibles d'être posées plus rapidement en suivant le rythme des changements sociaux, économiques, culturels etc. En raison de la lenteur d'implémentation, il semble logique que le contexte d'application de la norme puisse être sensiblement différent de celui pour lequel elle a été initialement conçue. Ainsi, son efficacité serait menacée. C'est l'une des principales raisons de l'inefficacité du droit étatique, qu'il soit national ou international, face aux besoins d'un monde globalisé.

Il convient de souligner que le droit international, en particulier, n'est pas capable à lui seul de faire face aux besoins de rapidité et de flexibilité de réglementation déjà mentionnés, puisqu'il est encore une représentation de la souveraineté des États.

De plus, il faut prendre en considération la « coexistence des souverainetés »¹⁵⁸ : les États doivent concilier leurs intérêts et leurs pouvoirs. La création de barrières tarifaires¹⁵⁹, ou même de barrières non tarifaires¹⁶⁰, engendrent des exigences qui peuvent empêcher un pays de faire la commercialisation internationale d'une marchandise déterminée, par exemple, en raison des normes liées aux « matériaux, produits, processus, services, systèmes ou personnes », comme les normes de l'Organisation internationale de normalisation (ISO).

La difficulté rencontrée avec le droit international, c'est qu'il ne régit que les relations entre les États. Ainsi, dans un monde globalisé au sein duquel participent d'autres acteurs, qui tout comme l'État ont une influence sur le droit, envisager une méthode de réglementation qui n'est pas capable de les englober ne semble pas être la réponse la plus efficace face aux défis globaux.

À la lumière des éléments exposés, le droit global semble être une alternative plus opportune pour répondre à des enjeux globalisés. Il accompagne la reconfiguration de la souveraineté étatique et, par conséquent, il s'avère capable de créer un ordre plus adapté aux phénomènes actuels comme la délocalisation, le pluralisme et l'internormativité juridique.

¹⁵⁸ « Le juge Anthony Kennedy, dans son opinion concurrente au soutien de l'arrêt rendu en 1995 par la Cour suprême des États-Unis dans l'affaire *U.S. Term Limits, Inc. v. Thornton*, décrit le fédéralisme comme « une tentative pour briser l'atome de la souveraineté » (« federalism as an attempt to split the atom of sovereignty »). La formule est devenue classique car elle illustre de manière plastique comment le fédéralisme – en tant que construction politique – conduit à reconsidérer une notion fondamentale comme l'est la souveraineté, notion sur laquelle se sont édifiés, depuis la Renaissance, les États actuels et sur laquelle repose, aujourd'hui, la coexistence des souverainetés étatiques, appelée – non sans exagération – 'société internationale', et reposant sur l'égalité souveraine des États. » Vlad CONSTANTINESCO, « La souveraineté est-elle soluble dans l'Union européenne ? », p. 119-135, dans *L'Europe en formation : Revue d'études sur la construction européenne et le fédéralisme*, Centre international de formation européenne, n° 368, 2013.

¹⁵⁹ Voir : ORGANISATION MONDIALE DU COMMERCE, *Données sur le commerce international et l'accès aux marchés*, 2017, en ligne : < <https://bit.ly/2Bfdao4> > (consulté le 12 déc. 2018)

¹⁶⁰ Voir : Gaulier GUILLAUME et Zignago SOLEDAD, « La discrimination commerciale révélée comme mesure désagrégée de l'accès aux marchés », dans *l'Economie internationale*, 2002, n° 89-90, p. 261-280, en ligne : < <https://www.cairn.info/revue-economie-internationale-2002-1-page-261.htm> > (consulté le 12 déc. 2018)

« Le droit global se crée et se déploie dans les interstices laissés vacants tant par le droit national que par le droit international, désormais incapables de répondre aux défis des interdépendances, de la globalisation et de la mondialisation des risques, pour reprendre une expression de Ulrich Beck. Force est de constater que le droit moderne, tant au plan national qu'international, est en crise. Sans perdre toute leur pertinence, ces deux ordres juridiques se laissent compléter par une autre catégorie juridique. »¹⁶¹

Convient-il d'ajouter que d'autres concepts pertinents pourraient faire objet de cette étude¹⁶² ? Toutefois, tel qu'indiqué au début du chapitre, ce document ne prétend pas être exhaustif. Par conséquent l'important est de comprendre l'existence d'une relation entre différentes notions juridiques et sociologiques qui caractérisent les particularités et mutations du rôle du droit étatique aujourd'hui.

Cette acception actuelle de la souveraineté, qui n'est plus absolue comme dans les monarchies mais dans les faits très atténuée, est étroitement liée aux vicissitudes du monde actuel. Un des facteurs qui façonne la mondialisation, par exemple, est l'émergence du néolibéralisme. Cette orientation étatique a gagné du terrain dès la fin des années 1970 en mettant en évidence la liberté et la compétition dans le marché, « des privatisations, de la propriété privée, des dérégulations, de la concurrence, de l'individualisme exacerbé, de la baisse des impôts »¹⁶³. Ces exemples sont quelques-unes des mesures capables de définir le néolibéralisme, basées fondamentalement sur la liberté des individus d'entreprendre une activité économique.

¹⁶¹ K. BENYEKHLEF, *préc.*, note 154, p.102-103.

¹⁶² Par exemple, le droit polycentrique. Selon ce concept, en général, une compétition entre les gouvernements partout le monde aurait lieu concernant les systèmes juridiques applicables. Le monopole d'un État en particulier dans la réglementation juridique de la vie de ses citoyens ne serait plus souhaitable.

¹⁶³ Serge AUDIER, *Penser le néolibéralisme. Le moment néolibéral, Foucault et la crise du socialisme*, Paris, Le Bord de l'Eau, 2015, p.8.

D'autres facteurs participent à l'émergence du néolibéralisme, notamment la multiplication des acteurs ayant une influence internationale reliant les différentes sociétés. Dans ces conditions, la conception d'autorité souveraine des États fait l'objet d'un réexamen, de manière à ce qu'aujourd'hui plusieurs acteurs, outre l'État, soient responsables pour encadrer le déroulement des relations internationales et influencer les sociétés. À cet égard, l'économie et le marché deviennent plus importants tandis que le rôle étatique – tel qu'il était connu – est en train d'être reconfiguré.

Bien que la souveraineté de l'État reste la clé de son pouvoir, aujourd'hui son hégémonie est partagée dans une certaine mesure avec d'autres acteurs. Les organisations non gouvernementales, les entreprises, les corporations et les personnes physiques, entre autres, jouent un rôle plus significatif dans la société globalisée.

Au lieu d'un antagonisme entre les normes étatiques des différents ordres juridiques d'un monde globalisé, il serait plus opportun d'envisager une convergence entre eux. Le droit global permettrait de combler les lacunes du droit étatique. Ainsi, lorsqu'il s'agit de la création de normes dans le contexte du monde globalisé, il convient de considérer les notions du pluralisme et de l'internormativité.

D'une manière générale, le pluralisme fait référence à la pluralité des ordres juridiques qui peuvent coexister, y compris les ordres étatiques et non étatiques, dans la mesure où « dans un monde pluriel, le droit est un processus continu d'articulation, d'adaptation, de réarticulation, d'absorption, de résistance, de déploiement, etc. »¹⁶⁴. On constate que le droit ainsi que la

¹⁶⁴ Paul Schiff BERMAN, *Le nouveau pluralisme juridique*, Revue internationale de droit économique, 2013, en ligne : < <https://www.cairn.info/revue-internationale-de-droit-economique-2013-1-page-229.htm> > (consulté le 20 déc. 2018)

société sont toujours en mutation; et l'internormativité¹⁶⁵, liée au pluralisme, émerge comme un des moyens de l'actualiser.

Cela implique aussi l'importance de la corégulation entre le pouvoir étatique et la sphère privée/communautaire¹⁶⁶. À cet égard, le droit global – basé sur le pluralisme juridique et l'internormativité – émerge comme un mécanisme possiblement plus efficace que le droit étatique selon le modèle actuel. Cela ne signifie pas qu'il faille écarter l'application du droit étatique mais seulement lui apporter un nouveau regard en harmonie avec les concepts énoncés dans ce chapitre. Ainsi l'exclure ne serait pas la réponse. La sécurité juridique et la légitimité reconnue des manifestations étatiques peuvent apporter encore une valeur considérable à ces normes.

Finalement, il faut reconnaître que le droit étatique dispose de certains instruments qui illustrent son utilité dans le contexte de changements majeurs et rapides. C'est le cas, par exemple, des règlements. Subordonnés à la loi, ils sont formulés afin de développer et de rendre une loi concrète. Cela permet que la loi soit plus adaptée au contexte dans lequel elle s'insère¹⁶⁷.

¹⁶⁵ « L'internormativité est donc bien, comme Jean Carbonnier l'avait montré, un concept-clé dès l'instant où l'on adopte un point de vue sociologique sur le droit : partant du constat que l'ordre social est construit autour d'une pluralité de systèmes normatifs, elle montre que, non seulement ceux-ci entretiennent des rapports d'interaction et d'échange, mais encore qu'ils soient imbriqués et entrelacés, en constituant un tissu normatif de texture plus ou moins serrée. L'internormativité met ainsi l'accent sur la relation fondamentale qui unit la normativité juridique aux autres sources de normativité qui corsètent le corps social : conférant une portée nouvelle aux normes sociales préexistantes qu'il formalise et officialise, le droit est, dans le même temps, producteur de normalité sociale, en imposant certains modèles de comportement. » Jacques CHEVALLIER, « L'internormativité », p. 13-14 (PDF), dans COLLECTIF, *Les sources du droit revisitées*, v. 4, Anthémis, Théorie des sources du droit, Wavre, 2013, en ligne : < <https://hal.archives-ouvertes.fr/hal-01723912/document> > (consulté le 16 déc. 2018)

¹⁶⁶ B. BARRAUD, *préc.*, note 3.

¹⁶⁷ « Les règlements servent à concrétiser les objectifs des lois générales ou à les développer et ils ont force de loi. Par exemple, il existe des règlements qui assurent la salubrité de nos aliments ou qui définissent quelle sorte de réservoir peut servir à entreposer des produits pétroliers ». MINISTÈRE DE LA JUSTICE DU CANADA. *L'origine de notre système juridique*, 10 mars 2018, en ligne : < <https://www.justice.gc.ca/fra/pr-rp/pm-cp/just/03.html> > (consulté le 10 janv. 2019)

Ainsi, le droit étatique, national ou international, demeure un outil de réponse aux enjeux globaux, bien qu'il fasse face aux défis précédemment mentionnés.

1.1.1. Les contrats intelligents devant le « *hard law* » aujourd'hui

Les obstacles que le droit étatique rencontre en raison des phénomènes évoqués jusqu'ici n'empêchent pas que les États essaient de créer des normes applicables aux nouvelles technologies. En tout cas, il serait possible d'argumenter que le droit étatique en vigueur est déjà capable de réguler les relations basées sur la technologie des contrats intelligents dans les chaînes de blocs. Ce pourrait être le cas si nous considérons que les « *smart contracts are valid under existing law and do not require additional authorization to be enforceable* »¹⁶⁸. Par contre, il y a aussi ceux qui défendent le besoin de normes plus spécifiques.

L'application du droit étatique aux contrats intelligents reste un point qui mérite notre attention essentiellement en raison de la variété des ordres juridiques mondiaux en constante relation. Cela renforcerait la sécurité juridique dans l'emploi des contrats intelligents impliquant plus d'une juridiction. Tout comme nous avons des règles étatiques régissant les relations dans des domaines variés, les relations au sein de la chaîne de blocs peuvent et doivent faire l'objet d'une certaine réglementation. Au fur et à mesure que les contrats intelligents prennent part aux

¹⁶⁸ CHAMBER OF DIGITAL COMMERCE, “*Smart Contracts*” *Legal Primer*, 2018, p. 1, Washington DC, (PDF) en ligne : < <https://digitalchamber.org/wp-content/uploads/2018/02/Smart-Contracts-Legal-Primer-02.01.2018.pdf> > (consulté le 13 déc. 2018)

relations de la société il est nécessaire que l'État exerce son pouvoir dans l'établissement des normes au regard du rôle du droit d'intégration sociale dans un contexte complexe ¹⁶⁹.

Ce faisant, plusieurs questions peuvent émerger concernant la reconnaissance juridique des relations menées via les contrats intelligents face aux règles de droit au sein de chaque État. Les contrats intelligents sont-ils un simple moyen d'exécution contractuelle ou sont-ils effectivement des contrats au sens juridique avec des effets légaux pertinents ? Est-ce que le langage de programmation équivaudrait au langage naturel dans la formation d'un contrat, notamment en ce qui concerne la notion de consentement libre et éclairé ? Comment les contrats intelligents seraient-ils révisés, modifiés ou arrêtés dans le cas où un vice juridique serait constaté ? Quels sont les éléments de preuve relatifs aux contrats intelligents ? Considérant la cryptographie appliquée aux contrats intelligents, comment les tribunaux seraient-ils capables d'y accéder et d'identifier toutes les parties impliquées ?

Cette étude n'a pas l'audace de répondre à toutes ces questions. Néanmoins, l'application du principe de l'équivalence fonctionnelle – exposé plus longuement dans le prochain sous-chapitre dans la cadre du droit québécois – semble constituer un début de réponse pratique à certaines de celles-ci. Partant de ce principe, dans le cas où toutes les conditions de fond et de forme d'un contrat, prévues par le droit étatique, serait remplies, aucune raison ne pourrait être opposée à ce qu'ils soient considérés comme des contrats au sens juridique.

Certaines conditions exigées par le droit dans des situations particulières, comme l'écriture et l'authenticité, ne seraient pas des obstacles absolus à la reconnaissance des contrats

¹⁶⁹ « [...] ou si le droit fonctionne encore comme un médium de l'intégration sociale, (...) le droit apporte encore quelques moyens de maintenir ensemble des sociétés complexes et centrifuges qui sans cela se désagrègeraient. » Jürgen HABERMAS, *Sur le droit et la démocratie*, Note pour un débat, *Le Débat*, 1997, n° 97, p. 42, (PDF) en ligne : < <http://www.sietmanagement.fr/wp-content/uploads/2016/04/Habermas1997.pdf> > (consulté le 13 déc. 2018)

intelligents au sens juridique, que ce soit dans le contexte du droit étatique ou des normes alternatives, comme on le verra plus tard. Si les chaînes de blocs deviennent effectivement mises en œuvre à grande échelle, avec le temps, cela affectera les procédures d'engagement dans plusieurs domaines. Par exemple, les contrats de mariage conclus devant un « célébrant compétent »¹⁷⁰ seraient valides même si enregistrés dans la chaîne de blocs dans la mesure où l'exigence légale serait remplie – dans le cas où le « célébrant compétent » utilise cette technologie pour enregistrer ses célébrations.

Ainsi, nous verrons que le droit étatique est capable d'embrasser les nouvelles technologies. Il est nécessaire d'envisager les innovations dans le contexte du droit puisqu'elles sont à chaque fois plus enracinées dans les sociétés d'aujourd'hui. Concernant la chaîne de blocs, certaines applications sont plus présentes dans la réalité que d'autres, comme par exemple les cryptomonnaies. Ainsi, le droit s'est occupé de ces sujets en priorité en créant des normes adaptées qui seront présentées plus loin dans cette étude.

1.1.2. Le cadre juridique québécois

Le Canada est organisé en forme de fédération, composé d'un gouvernement central et de gouvernements provinciaux. Le droit canadien est basé sur le régime de la *Common law* anglaise, qui s'applique partout dans le pays, avec une particularité pour le Québec qui dispose

¹⁷⁰ Article 365 et 366 C.c.Q.

d'un système mixte qui prend également racine dans le système civiliste français, de sorte qu'on parle alors du bijuridisme¹⁷¹.

La différence entre les deux systèmes – anglais et français – est fondée essentiellement sur l'existence ou non d'une codification des normes. Dans leurs jugements, au Québec, les tribunaux priorisent la loi avant d'analyser la teneur de la jurisprudence, qui sert comme source d'uniformisation mise au second plan. D'une part, le droit civil trouve son fondement dans des textes codifiés, qui énoncent usuellement les principes généraux qui s'appliquent à des cas très divers. D'autre part, au sein de la *Common Law*, certaines décisions sont prises au regard de cas similaires antérieurs. Cependant, ces décisions conservent un caractère souple dans la mesure où les juges ont la possibilité de les adapter aux particularités de chaque cas, ainsi qu'aux changements opérés au cours du temps.

Nonobstant les différences, il convient de mentionner que les deux traditions juridiques semblent capables de régler les affaires relatives aux contrats intelligents. Au Canada, les principes fondamentaux de la formation valide d'un contrat demeurent l'offre et l'acceptation, la considération, l'intention de créer une relation légale, ainsi que la certitude concernant les termes du contrat. De la même manière, il n'existe pas une exigence générale d'écriture. C'est pourquoi, par exemple, le contrat peut être considéré juridiquement contraignant même si verbal. Il en va ainsi, également, pour les contrats au Québec, mais avec la particularité de l'application des droits de tradition civiliste, c'est-à-dire basé sur la codification des normes.

¹⁷¹ « On peut aborder le bijuridisme de plusieurs manières : simple coexistence de fait de deux traditions juridiques, interaction entre deux traditions, intégration formelle de deux traditions dans un cadre donné [...] ou, encore, sur un plan plus général, reconnaissance et respect de cultures et d'identités appartenant à deux traditions juridiques. » France ALLARD, *La Cour suprême du Canada et son impact sur l'articulation du bijuridisme*, Ministère de la Justice du Canada, 2001, en ligne : < <https://www.justice.gc.ca/fra/pr-rp/sjc-csj/harmonization/hlf-hfl/f3-b3/bf3a.html#introduction> > (consulté le 10 janv. 2019).

Au regard de ces faits, cette étude tient compte de certaines dispositions de la législation de la province orientées vers les relations contractuelles ou vers les aspects technologiques, ou les deux ensembles, pouvant avoir des répercussions sur les contrats intelligents. C'est le cas du *Code Civil du Québec* (ci-après C.c.Q.) et de la *Loi Concernant le cadre juridique des technologies de l'information* (ci-après LCCJTI).

Le C.c.Q., dans sa disposition préliminaire, énonce que l'ensemble de ses règles régissent « les personnes, les rapports entre les personnes, ainsi que les biens ». Son cinquième livre (« des obligations ») est spécifiquement rédigé pour les contrats, avec plus de 70 articles (de l'article 1377 au 1456). Tout d'abord, il convient de souligner la définition de contrat selon le C.c.Q., qui en grande partie ressemble aux définitions civilistes traditionnelles :

« **1378.** Le contrat est un accord de volonté, par lequel une ou plusieurs personnes s'obligent envers une ou plusieurs autres à exécuter une prestation. Il peut être d'adhésion ou de gré à gré, synallagmatique ou unilatéral, à titre onéreux ou gratuit, commutatif ou aléatoire et à exécution instantanée ou successive; il peut aussi être de consommation. »

Un peu plus loin, le C.c.Q prend soin d'énumérer les conditions de formation du contrat.

En vertu de la disposition générale :

« **1385.** Le contrat se forme par le seul échange de consentement entre des personnes capables de contracter, à moins que la loi n'exige, en outre, le respect d'une forme particulière comme condition nécessaire à sa formation, ou que les parties n'assujettissent la formation du contrat à une forme solennelle. Il est aussi de son essence qu'il ait une cause et un objet. »

Au regard de cette disposition et en l'appliquant à l'idée de contrat intelligent, nous pourrions dire qu'ils sont des programmes informatiques capables d'enregistrer et d'exécuter

automatiquement les dispositions convenues entre les parties, mais à la particularité de ne pas avoir besoin d'une relation préalable de confiance mutuelle. Dans ce sens, c'est la volonté qui déclenche la relation de prestation-contreprestation menée par le biais de la chaîne de blocs, au moyen d'un contrat intelligent. Imaginons que le terme « programmes informatiques » soit remplacé par « papiers » dans le début de ce paragraphe. Toutes proportions gardées, le concept ne serait donc pas si différent de ce qui est déjà connu et présent dans la loi. Il est évident que les diverses problématiques mentionnées au cours de cette étude rendent la question plus complexe. Cependant, nous pouvons constater que le caractère fondamental de l'accord semble être le même.

À cet égard, une question épineuse est soulevée à l'occasion de la formation des contrats en général, celle de la présence du consentement libre et éclairé. Cette question pèse également sur les contrats intelligents, notamment au regard du langage de programmation. Comment les parties, sans connaître ce langage, pourraient être sûres de consentir exactement à ce qu'elles ont souhaitées dans le monde physique ?

Il s'avère que le consentement est l'un des prérequis les plus complexes à satisfaire lorsque l'on traite des contrats intelligents. En effet car le langage de programmation peut voir des conséquences indésirables pour les parties sans qu'il leur soit possible de connaître le contenu de cet accord et par conséquent, de donner son consentement libre et éclairé.

Bien qu'après le déclenchement d'un contrat intelligent son exécution ne puisse pas être empêchée, il serait possible d'invoquer des outils juridiques capables de résilier l'accord,

ultérieurement, comme l'allégation *non est factum*¹⁷², approprié dans certaines situations comme l'illettrisme. En effet, l'ignorance du langage de programmation pourrait être assimilée à ces cas. Néanmoins, la simple ignorance n'invalide pas le contrat de facto dans la mesure où l'intervention d'un conseiller ou d'un professionnel qualifié pourrait éclairer son contenu et éviter cette possibilité de résiliation. Il faut prendre toutes les précautions possibles (« *take reasonable care* »¹⁷³).

« *A person who cannot read English will be unable to understand an English language contract by attempting to read it. However, if she signs the contract regardless, without taking any steps to obtain assistance in ascertaining its contents, she should be bound to its terms.* »¹⁷⁴

Ce raisonnement pourrait être également énoncé au regard de la formation et exécution des contrats écrits en langage informatique.

Un autre moyen de favoriser la reconnaissance du consentement dans le cadre des contrats intelligents serait de les associer à ce qu'il est convenu d'appeler le contrat Ricardian. Ces contrats ont été créés dans le cadre du système de paiement Ricardo en 1995 par Ian Grigg¹⁷⁵. Ce dernier les a conçus dans l'optique de créer des documents lisibles par le langage

¹⁷² “*Non est factum is a defence which may be available to someone who has been misled into signing a document which is fundamentally different from what he or she intended to execute or sign.*” Charles Y C CHEW, *The Application of the Defence of Non Est Factum: an Exploration of its Limits and Boundaries*, University of Western Sydney Law Review, Editor Francine Feld, v. 13, 2009, (PDF), en ligne : < https://www.westernsydney.edu.au/_data/assets/pdf_file/0009/435573/UWS_2009LR09Vol13.pdf > (consulté le 12 janv. 2019)

¹⁷³ “*There are three main features of the doctrine of non est factum: it is restricted to certain persons and documents; it requires a fundamentally incorrect explanation; and the signer must not have been careless.*” Simon CONNELL, *Not my doctrine? Finding a Contract law explanation for Non est factum*, Victoria University of Wellington Law Review, 47, p. 245-265, 2016, p. 248, (PDF), en ligne : < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3195011 > (consulté le 12 janv. 2019)

¹⁷⁴ Paul MICHELL, *Illiteracy, Sophistication and Contract Law*, Queen's Law Journal, 31, 2005-2006, p. 327 en ligne : < https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/queen31&id=323&men_tab=srchresults > (consulté le 12 janv. 2019)

¹⁷⁵ Usman W. CHOHAN, *What Is a Ricardian Contract?*, UNSW Business School, 2017, en ligne : < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3085682 > (consulté le 12 janv. 2019)

naturel et des machines, en utilisant des termes et dispositions légalement contraignants. Leur fonctionnement est illustré dans le schéma ci-dessous, mais en résumé le contrat Ricardian est un document écrit dans le langage naturel, ayant les termes juridiques nécessaires, dont le contenu est transformé en langage informatique permettant sa lecture par un ordinateur.

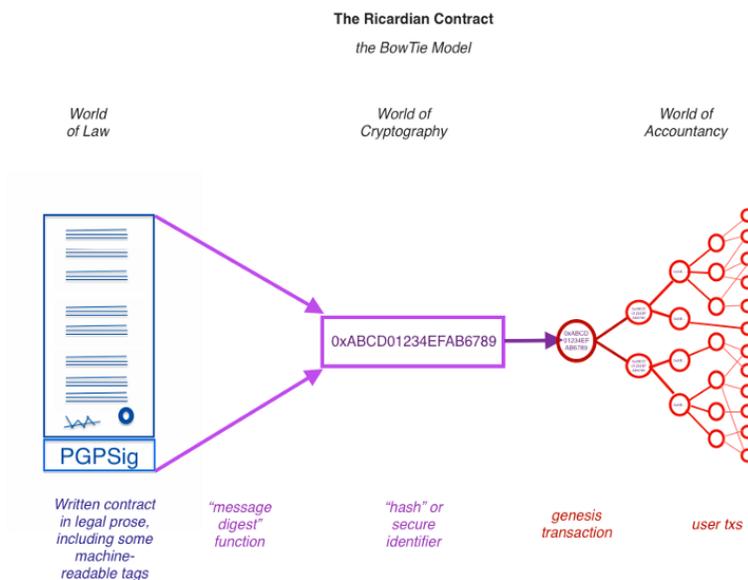


Figure 4. La formation d'un contrat Ricardian

Ainsi, avec l'emploi hybride des concepts de contrats intelligents et de contrat Ricardian, les doutes sur le consentement pourraient être atténués, puisqu'un contrat en langage humain serait également conclu.

La capacité des parties, c'est-à-dire « l'aptitude décrétée par la loi à s'obliger par un acte juridique »¹⁷⁶, est l'un des autres éléments exigés par le droit québécois pour la formation valide

¹⁷⁶ Jean-Louis BAUDOIN, *Les obligations*, Yvon Blais, Cowansville, 1989, p. 173.

des contrats. Comment serait-il possible d'assurer la capacité des contractants lors d'un accord exécuté dans la chaîne de blocs ? Possiblement, de la même façon que pour les contrats dans le commerce électronique : par la déclaration personnelle ou au moyen de systèmes de certification. Il est envisageable que dans le futur, il y ait des registres de l'état civil sur la chaîne de blocs ou dans les systèmes capables de communiquer directement avec les contrats intelligents (comme les oracles) de façon à assurer l'identification personnelle des parties contractantes.

Enfin, la norme québécoise exige également une cause et un objet dans la formation des contrats. La cause est la motivation de chaque partie à s'engager dans le pacte, sans l'exigence qu'elle soit exprimée (art. 1410 C.c.Q.), en respectant toujours la loi et l'ordre public (art. 1411 C.c.Q.). L'objet, quant à lui, « est l'opération juridique envisagée par les parties au moment de sa conclusion » (art. 1412 C.c.Q.). Ces deux prérequis sont, eux aussi, indispensables à l'éventuelle reconnaissance du caractère juridiquement contraignant des contrats intelligents. L'inobservation de ces prérequis rend le contrat invalide, qu'il soit un contrat traditionnel ou un contrat intelligent dans la chaîne de blocs.

En outre, dans le contexte légal du Québec, il est nécessaire de mentionner ce qui est prévu par la LCCJTI, en vigueur depuis le 1^{er} novembre 2001, et qui a des effets sur d'autres lois, y compris le C.c.Q. Cette loi vise à garantir :

« 1° la sécurité juridique des communications effectuées par les personnes, les associations, les sociétés ou l'État au moyen de documents quels qu'en soient les supports ;

2° la cohérence des règles de droit et leur application aux communications effectuées au moyen de documents qui sont sur des supports faisant appel aux technologies de l'information, qu'elles soient électroniques, magnétique, optique, sans fil ou autres ou faisant appel à une combinaison de technologies ;

3° l'équivalence fonctionnelle des documents et leur valeur juridique, quels que soient les supports des documents, ainsi que l'interchangeabilité des supports et des technologies qui les portent ;

4° le lien entre une personne, une association, une société ou l'État et un document technologique, par tout moyen qui permet de les relier, dont la signature, ou qui permet de les identifier et, au besoin, de les localiser, dont la certification ;

5° la concertation en vue de l'harmonisation des systèmes, des normes et des standards techniques permettant la communication au moyen de documents technologiques et l'interopérabilité des supports et des technologies de l'information. »¹⁷⁷

Au regard des dispositions précédemment citées, on constate que la LCCJTI pourrait être applicable dans le contexte des contrats intelligents si on le considère comme un document numérique. En effet, cette loi précise que l'ensemble des informations inscrites sur un support, c'est-à-dire un document, quand bien même ce document soit sur un support numérique, bénéficie du même traitement que ceux qui sont rédigés sur le format papier, tant que ces documents respectent certaines conditions¹⁷⁸. En conséquence, ces documents sur support numérique pourraient être utilisés comme éléments de preuve et comme source de création d'obligations et d'éventuelles responsabilités au regard du droit.

À cet égard, nous sommes face à la notion d'équivalence fonctionnelle, mentionnée dans l'article précité ainsi que dans la section III (articles 9 à 16) de la LCCJTI, intitulée « équivalence de documents servant aux mêmes fonctions ». La loi présente une définition de ce principe, comme suit :

¹⁷⁷ *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, art. 1. (nos soulignés)

¹⁷⁸ « Par conséquent, un document technologique remplira les fonctions d'un écrit traditionnel original dès lors que son intégrité sera assurée et que sa fonction sera d'être la source première d'une reproduction, de présenter un caractère unique ou d'être la forme première d'un document relié à une personne (article 12). De plus, pour qu'un document soit considéré comme valable, il faudra qu'il respecte les critères d'authenticité, d'intégrité, de confidentialité, de non-répudiation et d'accès contrôlé. » Raymond PICARD, *Cadre juridique des technologies de l'information au Québec*, Réseau juridique du Québec, 2013, en ligne : < <https://www.avocat.qc.ca/affaires/iicadre-ti-quebec.htm> > (consulté le 18 déc. 2019)

« 9. Des documents sur des supports différents ont la même valeur juridique s'ils comportent la même information, si l'intégrité de chacun d'eux est assurée et s'ils respectent tous deux les règles de droit qui les régissent. L'un peut remplacer l'autre et ils peuvent être utilisés simultanément ou en alternance. De plus, ces documents peuvent être utilisés aux mêmes fins.
En cas de perte, un document peut servir à reconstituer l'autre. »

Ainsi, la valeur juridique des documents n'est pas attachée à son support¹⁷⁹, mais à sa finalité, en autant qu'il respecte les autres exigences légales. Ainsi, peu importe si l'accord est conclu à l'aide d'un programme informatique ou de manière traditionnelle sur un support papier. C'est l'accomplissement de la fonction qui mériterait l'attention du droit tout d'abord.

Il est nécessaire de souligner que cette idée ne date pas d'aujourd'hui. La Loi-type de la CNUDCI sur le commerce électronique¹⁸⁰, en 1996, a déjà signalé l'importance du concept d'équivalence fonctionnelle. Au fil des années, d'autres normes ont émergé en faisant référence à ce principe, y compris au Canada¹⁸¹ et au Québec avec la LCCJTI.

Tout en respectant la satisfaction des exigences juridiques, l'idée de se concentrer sur l'intention de la création du document, et non sur son support, semble extrêmement pertinente quand il s'agit des technologies de l'information, qui sont en constante mutation. Il est important

¹⁷⁹ Vincent GAUTRAIS et Patrick GINGRAS, « La preuve des documents technologiques », *Les Cahiers de propriété intellectuelle*, vol. 22, n. 2, en ligne (PDF) : < <https://cpi.openum.ca/files/sites/66/La-preuve-des-documents-technologiques.pdf> > (consulté le 19 déc. 2018)

¹⁸⁰ NATIONS UNIES, *Loi type de la CNUDCI sur le commerce électronique et Guide pour son incorporation*, New York, 1999, en ligne (PDF) : < https://www.uncitral.org/pdf/french/texts/electcom/05-89451_Ebook.pdf > (consulté le 19 déc. 2019)

¹⁸¹ DIRECTIVE 1999/93/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 13 DÉCEMBRE 1999 SUR UN CADRE COMMUNAUTAIRE POUR LES SIGNATURES ÉLECTRONIQUES, *Journal officiel des Communautés européennes*, en ligne : < <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:013:0012:0020:FR:PDF> > (consulté le 19 déc. 2018)

DIRECTIVE 2000/31/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 8 JUIN 2000 RELATIVE À CERTAINS ASPECTS JURIDIQUES DES SERVICES DE LA SOCIÉTÉ DE L'INFORMATION, ET NOTAMMENT DU COMMERCE ÉLECTRONIQUE, DANS LE MARCHÉ INTÉRIEUR («DIRECTIVE SUR LE COMMERCE ÉLECTRONIQUE»), *Journal officiel* n° L 178 du 17/07/2000, en ligne : < <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:FR:HTML> > (consulté le 19 déc. 2018)

Loi de 2000 sur le commerce électronique, LO 2000, c 17, en ligne : < <http://canlii.ca/t/69jzp> > (consulté le 19 déc. 2018)

de rappeler que dans ce chapitre nous étudions les dispositions du droit étatique. Ce principe de l'équivalence fonctionnelle a une relation avec le droit établi par les États dans la mesure où il peut être employé comme une méthode de rédaction de lois ou de son interprétation¹⁸².

Par ailleurs, l'étude de l'équivalence fonctionnelle nous amène généralement à analyser trois concepts juridiques présents souvent dans les normes des États et qui établissent un lien étroit avec le droit contractuel : l'écrit, la signature et l'original.

En ce qui concerne le premier concept, l'écrit, la loi exige l'intégrité et l'identification de l'auteur du document : « l'intégrité peut être répartie en deux qualités qui sont l'authenticité du contenu et l'authenticité de l'origine »¹⁸³. Ainsi, il est nécessaire d'appliquer les exigences du droit quel que soit le support utilisé. Le deuxième concept, la signature, se résume à l'identité de l'auteur et sa manifestation de volonté¹⁸⁴. Enfin, le concept d'originalité d'un document peut être traduite par l'intégrité du document qui peut être la source première d'une reproduction, ou présenter un caractère unique ou, encore, peut être « la forme première d'un document reliée à une personne », selon l'article 12 de la LCCJTI. On assiste à des discussions sur la notion d'originalité, parmi lesquelles il émerge la possible exigence d'un support-papier¹⁸⁵. Cet aspect pèse aussi sur les contrats intelligents dans la mesure où le contrat peut être dans un premier temps conclu sur un format papier puis inséré dans la chaîne de blocs pour son exécution automatique.

¹⁸² Voir : *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, Équivalence fonctionnelle, en ligne : < <https://www.lccjti.ca/definitions/equivalence-fonctionnelle/#ancr1> > consulté le 19 déc. 2018.

¹⁸³ Joël HUBIN et Yves POULLET, *La sécurité informatique, entre technique et droit*, Namur, Centre de recherches informatique et droit, 1998, p. 7.

¹⁸⁴ *Loi concernant le cadre juridique des technologies de l'information*, préc., note 180.

¹⁸⁵ *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, Original, en ligne : < <https://www.lccjti.ca/definitions/original/> > (consulté le 19 déc. 2018)

En appliquant tous ces points de la LCCJTI aux contrats intelligents, il serait possible de reconnaître sa validité dans le cadre juridique québécois tant qu'il remplit les exigences des contrats traditionnellement reconnus par le droit. Cette considération est rendue possible notamment à la lumière du principe d'équivalence fonctionnelle, comme nous l'avons vu.

1.1.3. Les normes étatiques en vigueur ou en cours d'élaboration

En dépit de la possibilité d'adapter et d'appliquer au contexte technologique les normes étatiques générales déjà existantes, certaines juridictions votent des règles spécifiquement tournées vers la chaîne de blocs et ses applications, comme les contrats intelligents.

Tout d'abord, il convient de préciser que, encore une fois, cette étude n'a pas la prétention d'être exhaustive, dans la mesure où le rythme des propositions des nouveaux projets de loi sur ces sujets « à la mode » est effréné et que de nombreuses juridictions entrent en jeu rendant cette tâche encore plus difficile.

Malgré la possible diversité d'applications de la technologie de la chaîne de blocs, dans la plupart des cas l'attention législative actuelle porte sur les cryptomonnaies. Au Canada, celles-ci ont été incluses dans la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*¹⁸⁶, en plus d'être soumises aux exigences législatives applicables en matière de valeurs mobilières¹⁸⁷. En France, le Plan d'action pour la croissance

¹⁸⁶ *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*, L.C. 2000, c. 17, en ligne : <<https://laws-lois.justice.gc.ca/fra/lois/P-24.501/>> (consulté le 08 janv. 2019)

¹⁸⁷ AUTORITÉS CANADIENNES EN VALEURS MOBILIÈRES, *Canadian Securities Regulators Outline Securities Law Requirements That May Apply to Cryptocurrency Offerings*, Toronto, 24 août 2017, en ligne : <<https://www.securities-administrators.ca/aboutcsa.aspx?id=1606>> (consulté le 08 janv. 2019)

et la transformation des entreprises (PACTE) vise, entre autres propositions, à faciliter l'accès à des financement par ICO¹⁸⁸. En Suisse, l'Autorité fédérale de surveillance des marchés financiers FINMA précise que « le droit régissant les marchés financiers n'est pas applicable à tous les ICO et l'obligation d'assujettissement n'est pas systématique, car la définition des ICO est extrêmement variable »¹⁸⁹.

Néanmoins, nous trouvons également des propositions spécifiquement tournées vers les contrats intelligents, bien qu'elles soient moins fréquentes. Un bon exemple d'activité des autorités publiques dans ce sens est constaté dans le projet de la Commission du droit du Royaume-Uni, un « organe statutaire indépendant créé par la loi de 1965 sur les commissions juridiques pour surveiller le droit anglais et le pays de Galles et pour recommander une réforme, le cas échéant »¹⁹⁰.

Bien qu'il ne s'agisse pas d'un projet de loi, cela démontre l'intérêt des institutions étatiques pour le sujet. Diverses questions sont proposées dans le cadre de cette étude, principalement au regard de l'interaction entre le droit contractuel, déjà existant, et les contrats intelligents. En conséquence, des concepts comme la nullité contractuelle et les conditions implicites, ainsi que les notions d'interprétation, de responsabilité et de résolution de litiges seront étudiés dans le contexte de cette recherche de la Commission du droit du Royaume-Uni.

¹⁸⁸ RÉPUBLIQUE FRANÇAISE, *Plan d'Action pour la Croissance et la Transformation des Entreprises*, en ligne : < <https://www.gouvernement.fr/en/pacte-the-action-plan-for-business-growth-and-transformation> > (consulté le 08 janv. 2019)

¹⁸⁹ AUTORITÉ FÉDÉRALE DE SURVEILLANCE DES MARCHÉS FINANCIERS (FINMA), *La FINMA publie un guide pratique sur les ICO*, 16 fév. 2018, en ligne : < <https://www.finma.ch/fr/news/2018/02/20180216-mm-ico-wegleitung/> > (consulté le 08 janv. 2019)

¹⁹⁰ LAW COMMISSION, en ligne : < <https://www.lawcom.gov.uk/> > (consulté le 08 janv. 2019) (traduction libre)

Une grande partie des normes élaborées en matière de chaîne de blocs provient des États-Unis¹⁹¹. Nous pouvons mentionner des exemples de « *hard law* » concernant précisément les contrats intelligents : la loi HB 2417 de l'état américain de l'Arizona¹⁹², la loi HB1507 du Tennessee¹⁹³ et le projet de loi SB 300 d'Ohio¹⁹⁴.

La première loi citée, celle de l'Arizona, prévoit que les contrats intelligents sur la chaîne de blocs ne peuvent pas avoir leur statut juridique, leur validité ou leur force exécutoire niés simplement en raison de leur forme. L'autre aspect important de cette loi est la définition de contrat intelligent comme suit : an “*event-driven program, with state, that runs on a distributed, decentralized, shared and replicated ledger that can take custody over and instruct transfer of assets on that ledger.*”¹⁹⁵ Dans le contexte des technologies, afin de garder la compréhension des normes, la clarification des concepts est une démarche pertinente.

La deuxième loi mentionnée, celle du Tennessee, « *recognizes the legal authority to use distributed ledger technology and smart contracts in conducting electronic transactions; protects ownership rights of certain information secured by distributed ledger technology.* »¹⁹⁶ Ainsi, de la même façon, les relations menées au moyen d'une chaîne de blocs et par des contrats intelligents pourront produire des effets juridiques.

¹⁹¹ LAW COMMISSION, *Smart Contracts*, en ligne : < <https://www.lawcom.gov.uk/project/smart-contracts/> > (consulté le 08 janv. 2019)

¹⁹² ÉTATS-UNIS, *House of Representatives Bill 2417*, State of Arizona, en ligne : < <https://www.azleg.gov/legtext/53leg/1r/bills/hb2417p.pdf> > (consulté le 08 janv. 2019)

¹⁹³ ÉTATS-UNIS, *House of Representatives Bill 1507*, State of Tennessee, en ligne : < <https://legiscan.com/TN/bill/HB1507/2017> > (consulté le 10 janv. 2019)

¹⁹⁴ ÉTATS-UNIS, *Senate Bill 300*, State of Ohio, en ligne : < <https://legiscan.com/OH/text/SB300/id/1795258> > consulté le 10 janv. 2019)

¹⁹⁵ ÉTATS-UNIS, *préc.*, note 190.

¹⁹⁶ ÉTATS-UNIS, *préc.*, note 191.

Dans le même sens, le projet de loi SB 300 d’Ohio définit « *records and contracts secured by blockchain technology as electronic records* »¹⁹⁷ en autorisant l’utilisation des termes des contrats intelligents. Tout comme pour les deux normes précédemment mentionnées, en Ohio, les contrats intelligents sont reconnus comme des contrats juridiquement contraignants comme le sont les contrats traditionnels¹⁹⁸.

Récemment, l’Italie a reconnu le caractère juridique de la chaîne de blocs et des contrats intelligents par la Loi n° 12 de 11 février 2019, qui a converti le Décret-loi n° 135 de 14 décembre 2018 en loi.¹⁹⁹ Parallèlement à la définition de ces deux technologies, la nouvelle réglementation prévoit que les registres dans une chaîne de blocs détenant un mécanisme de validation de l’heure seront valides.

En ce qui concerne les contrats intelligents, la loi italienne reconnaît leur validité juridique et leur caractère contraignant. En résumé, les contrats intelligents sont équivalents aux contrats traditionnels au regard des notions de consentement et valeur probante, dans la mesure où l’authentification des parties respecte les normes établies par l’Agence pour l’Italie numérique (*Agenzia per l’Italia digitale*), qui n’ont pas encore été publiées.

Par conséquent, nous constatons qu’actuellement les gouvernements à travers le monde se penchent sur les questions liées à la chaîne de blocs et ses applications. Chaque État le fait dans le cadre de sa propre procédure, préservant ses particularités à l’instar des sujets de la

¹⁹⁷ ÉTATS-UNIS, *préc.*, note 192.

¹⁹⁸ Molly Ryan KOWALESKI, *Ohio to consider information stored in a blockchain valid and legal in SB 300*, 21 juin 2018, en ligne : < <https://www.ohiocpa.com/search/utilities/displaynewsitem/2018/06/21/ohio-to-consider-information-stored-in-a-blockchain-valid-and-legal-in-sb-300> > (consulté le 10 janv. 2019)

¹⁹⁹ ITALIE, *Loi 11 février 2019, n. 12*, en ligne : < <http://www.gazzettaufficiale.it/eli/id/2019/02/12/19G00017/sg> > (consulté le 13 fév. 2019)

réglementation. Ainsi, nous constatons que les contrats intelligents et la chaîne de blocs de manière générale font déjà l'objet de régulation par le *hard law*.

1.1.4. Est-ce que le code pourrait devenir la loi? (« Code is law? »)

En sus de toutes ces nouvelles propositions étatiques de réglementation de la technologie, nous pouvons aussi accorder une attention particulière à l'idée contraire : la possibilité d'utiliser ces mêmes technologies à des fins de réglementation – c'est-à-dire qu'elles sortent de la position d'objet de réglementation et deviennent un moyen de règlementer. La chaîne de blocs et les contrats intelligents pourraient être employés comme des outils de réglementation, devenant ainsi du droit étatique, toutes proportions gardées bien sûr. L'idée serait celle-ci : « *With blockchain technology and associated smart contracts, a growing range of legal and contractual provisions can be translated into simple and deterministic code-based rules that are automatically executed by the underlying blockchain network.* »²⁰⁰ Ainsi, on parlerait donc d'une transposition de la loi en langage numérique²⁰¹. Cette transposition codée serait alors la loi et en même temps le responsable de sa mise en œuvre.

C'est dans ce sens que l'expression, formulée par Lawrence Lessig, a été consacrée : « *code is law* »²⁰². Une autre citation, « *life in cyberspace is regulated primarily through the code of cyberspace* »²⁰³, nous permet de réfléchir à la régulation des contrats intelligents. L'idée de Lessig ne signifie pas que le code va remplacer le droit dans sa fonction réglementaire, mais

²⁰⁰ P. DE FILIPPI et A. WRIGHT, préc., note 8, p. 193.

²⁰¹ *Id.*, p. 195-196.

²⁰² Lawrence LESSIG, *Code Is Law: On Liberty in Cyberspace*, Harvard Magazine, janv.-févr., 2000, 5 p., en ligne : < <https://harvardmagazine.com/2000/01/code-is-law-html> > (consulté le 18 janv. 2019)

²⁰³ P. DE FILIPPI et A. WRIGHT, préc., note 8, p. 194.

que le domaine du cyberspace serait indéniablement régulé par le langage informatique – les protocoles et logiciels. Dans le cas des contrats intelligents, et des autres applications de la chaîne de blocs, la régulation par le langage semble être une réalité : “ (...) *bitcoin is a classic example of a Code is Law regulated space. (...) it is most certainly a **heavily regulated** financial system. It’s just that the regulation of bitcoin happens through Code.*”²⁰⁴

Rappelons que les normes et règles revêtent un caractère positif lorsqu’elles ont pour objectif de stimuler un comportement, ou négatives lorsqu’elles visent réprimer d’autres attitudes. Il en est de même pour la technologie. Sa mise en œuvre a un impact significatif sur certaines de nos habitudes. Cette influence s’opère, par exemple, au moyen des applications mobiles, lesquelles ont des finalités diverses telles que : faire la connaissance de nouvelles personnes, garder une alimentation saine ou même se déplacer et conduire.

Nous savons que le fonctionnement de la technologie repose sur des règles strictes et objectives. Cela ne donne pas lieu à des divergences d’interprétation. Ses règles sont plus techniques et moins discrétionnaires, c’est-à-dire que « *Unlike laws written in natural language, code-based rules leave less room for interpretation and can therefore be implemented more consistently and predictably* »²⁰⁵. Ainsi, les normes qui exigent certains niveaux d’interprétation ou de subjectivisme pour leur application ne sont pas adaptées à la codification en langage informatique. Toutefois, celles qui sont plus objectives s’intégrerait plus aisément dans un contexte d’une loi rédigée sous la forme de code informatique. Comme nous avons pu le constater, les contrats intelligents sont déployés à partir d’un modèle « *if-then* ».

²⁰⁴ Patrick MURCK, *Code as law?*, 5 juill. 2014, en ligne : < <http://virtuallylaw.com/code-as-law> > (consulté le 20 déc. 2018) (gras dans le texte originel)

²⁰⁵ P DE FILIPPI et A. WRIGHT, préc., note 8, p. 195.

Ce faisant, les normes qui s'inscrivent dans ce sillon ont tendance à mieux réussir leur intégration dans un système dématérialisé. Regardons cet exemple, sans nous pencher cependant sur ses exceptions : le gouvernement québécois concède une rente d'invalidité dès qu'il y a une « invalidité grave et permanente reconnue par l'équipe médicale de Retraite Québec » et la cotisation suffisante Régime de rentes du Québec²⁰⁶. La présence de ces deux prérequis est un élément objectif. L'éligibilité de ce droit n'existe pas sans la reconnaissance d'une invalidité grave et permanente, si une telle reconnaissance n'est pas effectuée par l'équipe médicale de Retraite Québec, mais par un tiers. En outre, le droit ne pourra être octroyé si la personne n'a pas préalablement cotisé dans les conditions fixées par le gouvernement²⁰⁷. Plutôt, si ces critères sont remplis, le demandeur bénéficiera de la rente d'invalidité. Au regard du caractère objectif de ces critères, cette norme pourrait être transposée en langage informatique et être exécuté dans ce contexte.

L'exemple suivant nous montre un autre cas possible dans lequel le code informatique est utilisé à la place du droit :

« As an illustration, governments around the globe implement anti-money laundering (AML) regulations, which require that financial institutions track flows of value (including virtual currencies) and report suspicious activity to stamp out money laundering, tax evasion, and terrorism financing. By relying on a blockchain, laws could require that regulated intermediaries – such as virtual currency exchanges – implement or interact with specific smart contracts that control the flow of transactions to occur only if they satisfy the strict logic of the underlying code. A blockchain could be used, for instance, to verify whether an individual is permitted to transfer virtual currency and – according to the information retrieved from the

²⁰⁶ RETRAITE QUÉBEC, *Admissibilité à la rente d'invalidité*, en ligne : < https://www.rrq.gouv.qc.ca/fr/retraite/rrq/autres_rentes/Pages/admissibilite_ri.aspx > (consulté le 21 déc. 2018)

²⁰⁷ Ce cotisation est objective aussi: “Vous avez suffisamment cotisé au Régime de rentes du Québec si vous répondez à l'un des critères suivants : Vous avez cotisé pour au moins 2 des 3 dernières années de votre période de cotisation. Vous avez cotisé pour au moins 5 des 10 dernières années de votre période de cotisation. Vous avez cotisé pour la moitié des années de votre période de cotisation, et pour au moins 2 années.” *Id.*

blockchain – a smart contract could limit the amount of virtual currency a person is legitimately entitled to transfer at any given time. »²⁰⁸

Ainsi, les avantages et inconvénients déjà présentés de l'usage des contrats intelligents et de la chaîne de blocs sont transposés au sein des régulations. Leur exécution reste plus rapide et sécuritaire dans la mesure où ces contrats seront enregistrés dans un environnement moins susceptible de subir les vulnérabilités usuelles. La simple mise en œuvre de la loi sur un logiciel commun, et non dans la chaîne de blocs, n'apporte pas ces caractéristiques particulières des réseaux distribués et décentralisés, comme l'autonomie et la résilience. Il ne faut cependant pas oublier que la chaîne de blocs ne se révèle pas pertinente dans tous les cas. L'immutabilité et les erreurs de programmations, deux inconvénients de cette technologie, peuvent parfois causer des problèmes majeurs.

Nous pourrions envisager au-delà de cette idée de « *code is law* », la notion du « *code as law* ». Cette autre notion est proposée par Primavera de Filippi et Samer Hassan qui affirment que la technologie des chaînes de blocs, et notamment des contrats intelligents, encouragent le développement de la loi d'une façon plus technique s'apparentant davantage à la caractéristique essentielle du langage informatique.

Une autre problématique pourrait être l'automatisation des règles au sein de la chaîne de blocs. Cela pourrait être bénéfique si elle est bien appliquée, mais pourrait avoir des conséquences néfastes en cas de bogue informatique, par exemple, lors de la « traduction » de la norme du langage humain au langage de programmation. Ainsi, considérant le caractère automatique de la chaîne de blocs, certains dommages ne pourraient être évités ou corrigés.

²⁰⁸ P. DE FILIPPI et A. WRIGHT, préc., note 8, p. 197.

Cependant, dans certains cas, ces erreurs pourraient être traitées à un moment ultérieur, grâce à une intervention humaine²⁰⁹.

Toutes ces remarques concernant la capacité du code de programmation d'être efficient au titre de loi, nous amène à considérer la notion de *lex cryptographica*. Cette version d'un système juridique, basé sur la technologie, possède les caractéristiques propres à l'usage de la chaîne de blocs. L'idée serait d'opérer un changement dans le fonctionnement du système d'application des lois. Avec la *lex cryptographica*, les comportements seraient réalisés conformément aux prescriptions du code informatique.

Ainsi, les affaires portées devant les tribunaux ne traiteraient que d'une mauvaise application des lois par le code informatique, dans le cadre, bien entendu, de lois pouvant être transposées en langage informatique, comme nous l'avons vu précédemment. Le risque majeur de cette transformation serait le passage d'un État de droit (*rule of law*) à un État de code (*rule of code*) où l'intervention étatique serait réduite à la révision des décisions prises selon/par le code informatique²¹⁰.

Ainsi, nous constatons que, plus qu'envisager les technologies comme collaborant avec le droit étatique, il convient de les considérer comme partie intégrante de ce dernier. Si l'on regarde ce phénomène sous un angle positif, “[s]uch approaches could enable blockchain technology to achieve specific regulatory objectives in ways that are more efficient and less costly than those of existing laws and regulations”²¹¹. Dans le contexte actuel, le code informatique jouerait un rôle complémentaire et supplémentaire au droit étatique dans la mesure

²⁰⁹ P. DE FILIPPI et A. WRIGHT, préc., note 8, p. 201-202.

²¹⁰ *Id.*, p. 204.

²¹¹ *Id.*, p. 198.

où il semble capable de le rendre plus efficace et efficient²¹². Ces deux notions se joindraient à tous les autres avantages au regard d'un meilleur fonctionnement de la justice et d'application du droit dans un monde globalisé. Les chaînes de blocs, quant à elles, serviraient cette cause.

²¹² « [...] l'efficacité du droit (droit efficace), qui permet d'évaluer les résultats et les effets sociaux du droit, et celle de l'efficience du droit (droit efficient) qui consiste à vérifier que les objectifs assignés à la règle de droit ont été atteints au meilleur coût. » CANADA, *Juridictionnaire*, Travaux publics et services gouvernementaux Canada, Centre de traduction et de terminologie juridiques (CTTJ), Faculté de droit, Université de Moncton, en ligne : < https://www.btb.termiumplus.gc.ca/tpv2guides/guides/juridi/index-eng.html?lang=eng&lettr=indx_catlog_e&page=9BDkX3TldFmE.html > (consulté le 21 avril 2019)

Chapitre 2 – La reconnaissance juridique des contrats intelligents sous l’angle des normes alternatives

2.1. Le rôle juridique des normes alternatives

Au regard des défis du droit étatique dans un contexte actuel globalisé, les normes alternatives y jouent un rôle particulier. Quand les rapports sociaux, commerciaux ou économiques, par exemple, se trouvent fragmentés, cela implique de changements naturels dans l’ordre juridique. À son tour, le droit global apparaît comme l’une des solutions proposées afin de satisfaire le besoin de normes adaptées aux situations émanant de la globalisation. Outre le droit global, les normes alternatives seraient une solution envisageable permettant l’harmonisation du droit et de faire face aux innovations dans ce contexte globalisé.

Si nous mettons de côté la théorie selon laquelle les normes de droit positif sont suffisantes pour satisfaire les besoins actuels de réglementation, les normes alternatives pourraient être un instrument capable de combler les lacunes du droit étatique et de ses normes déjà en vigueur.

Il est incontestable que dans certaines situations le marché a besoin de l’État, notamment pour que l’État puisse le protéger, assurant la sécurité de la société, comme les règles canadiennes prévues dans la loi C-59 (*Loi modifiant la loi sur l’Investissement au Canada*), visant de « permettre au gouvernement d’examiner des investissements pour raison de sécurité nationale, quelle que soit l’importance de l’opération »²¹³. Ainsi, l’État demeure encore

²¹³ CANADA, *Résumé législatif. Projet de Loi C-59 : Loi modifiant la loi sur l’Investissement au Canada*, Bibliothèque du Parlement, Service d’information et de recherche parlementaires, 14 oct. 2005, p. 1, (PDF), en ligne : <

aujourd'hui un acteur central et majeur dans la réglementation des rapports sociaux, commerciaux et économiques.

Néanmoins, comme nous avons pu le constater, la configuration actuelle des systèmes juridiques nécessite une restructuration afin de répondre aux nouveaux enjeux sociétaux. Dans ce sens, il faut garder à l'esprit qu'il n'est pas nécessaire de choisir entre, d'un côté, le droit global et les normes alternatives, et, de l'autre, le droit en vigueur. En fait, la combinaison de ces sources semble être la voie idéale afin de combler leurs lacunes réciproques et ainsi les rendre plus efficaces.

Le droit est intimement lié aux transformations sociales. Ainsi, deux thèses s'opposent. La première, celle du « droit-miroir » (*the mirror thesis*²¹⁴), soutient que les changements survenus dans l'ordre juridique sont le produit des modifications dans la société dans les domaines les plus variés (culturel, politique, économique etc.). La seconde, quant à elle, explique que les changements sociaux sont le résultat des mutations du droit²¹⁵.

Quelle que soit la théorie adoptée, il faut noter qu'il y a effectivement un rapport de « cause et effet » entre le droit et la société. Il y a un jeu d'influence mutuelle entre les deux. Le droit n'est pas une science indifférente aux changements sociaux et les transformations dans la société ne sont pas détachées des mouvements du droit. Ce flux à double sens implique plusieurs acteurs et nous amène à considérer la notion de pluralisme juridique.²¹⁶ De nombreux exemples

https://lop.parl.ca/sites/PublicWebsite/default/fr_CA/ResearchPublications/LegislativeSummaries/381LS515E > (consulté le 28 déc. 2018)

²¹⁴ Cf. : Mark A. EDWARDS, *The Alignment of Law and Norms: Of Mirrors, Bulwarks, and Pressure Valves*, FIU Law Review, FIU Law Library, vol. 10, n° 1, 2014, en ligne : < <https://bit.ly/2TwM6de> > (consulté le 28 déc. 2018)

²¹⁵ Julie RINGELHEIM, « Droit, contexte et changement social », *Revue interdisciplinaire d'études juridiques*, 2013, en ligne : < <https://www.cairn.info/revue-interdisciplinaire-d-etudes-juridiques-2013-1-page-157.htm> > (consulté le 26 déc. 2018)

²¹⁶ « Les anthropologues du droit qui ont étudié les sociétés coloniales et postcoloniales y ont fréquemment observé que le droit édicté par l'État demeurait, dans une large mesure, en décalage par rapport aux normes réellement

récents témoignent de la pertinence des normes alternatives comme réponse aux multiples défis rencontrés par les organes juridictionnels. « Les États ne sont donc pas forcément rébarbatifs au développement d'un droit global. Ces moyens de régulation les arrangent, puisqu'ils ne peuvent vraisemblablement pas répondre à toutes les demandes de droit qui sont formulées. »²¹⁷

Qu'il prenne forme dans le périmètre analysé, national, international ou même global, rappelons que l'État conserve un rôle qui mérite d'être préservé. Les codes de conduite volontaires ou le *soft law* ne sont pas capables de remplacer complètement le droit originaire du pouvoir étatique, bien qu'ils aient toujours eu une place importante dans le contexte de la réglementation.

Dans ce sens, la *Lex mercatoria* sert d'exemple. Comme les normes alternatives en général, elle a été fondée sur les bases du pluralisme juridique. En vertu de l'importance du commerce au Moyen Âge et des défis de sa réalisation pratique, les coutumes des marchands sont devenues le système juridique appliqué, à l'époque, à de nombreux secteurs, en respectant les particularités de chacun.

Sur les mêmes bases, la *lex electronica* est apparu comme faisant partie de l'ordre juridique actuel. Elle a été créée dans un contexte similaire à celui des normes alternatives en général, « décentralisé, centrifuge, fragmenté, non territorial et pluraliste, dont le paradigme du réseau peut s'accommoder »²¹⁸. La *lex electronica* est encore en développement, de sorte que certaines questions – comme celles présentées au début de ce titre – demeurent souvent sans une réponse précise.

suivies par la population, qui continuait de se référer aux systèmes normatifs traditionnels. C'est ce constat qui a d'ailleurs donné naissance à la théorie du pluralisme juridique.» *Id.*

²¹⁷ K. BENYEKHLEF, *préc.*, note 154, p. 115-116.

²¹⁸ K. BENYEKHLEF, *préc.*, note 154, p.112.

Le niveau de participation étatique dans la formation des normes alternatives varie en fonction de la technique de production adoptée. Dans le cas de la *lex electronica*, suivant le chemin tracé par la *lex mercatoria*, la technique employée est celle de l'autorégulation – le marché formule ses règles.

Nous pouvons également mentionner ce que l'on appelle la corégulation. Dans ce cas, de la corégulation, l'État conserve son rôle normatif, mais il n'est pas le seul à intervenir. Le pouvoir étatique s'associe au pouvoir des autres acteurs qui ont de l'influence dans les divers domaines de la société. Ensemble, ils créent des normes alternatives basées sur la technique de la corégulation.

Des différences existent entre ces deux méthodes de création de normes alternatives, car l'autorégulation serait la régulation *par* le marché tandis que la corégulation serait une régulation *avec* le marché²¹⁹. Cependant, elles ne sont pas diamétralement opposées. Les marchés et d'autres acteurs importants, autres que les États, jouent un rôle dans l'élaboration de ces normes indépendamment de la méthode appliquée, comme nous le verrons ci-après.

2.1.1. La perspective de l'autorégulation et de la corégulation

Compte tenu de l'ampleur des discussions concernant les normes alternatives, nous nous limiterons ici à dresser les grandes lignes de l'autorégulation et de la corégulation afin de démontrer comment ces deux techniques de production normative pourraient être applicables aux contrats intelligents, de manière alternative (mais toujours complémentaire) au droit

²¹⁹ K. BENYEKHLEF, *préc.*, note 152, p. 740-743.

étatique. Rappelons à ce titre qu'il n'y a pas de consensus au sujet des formes de création des normes alternatives, ni même au sujet des méthodes de classifications afférentes, comme celle basée sur leur contenu²²⁰.

Nous pouvons dire que l'autorégulation couvre les mesures de régulation découlant exclusivement des acteurs privés. Il s'agit, alors, d'une régulation *par* le marché : les règles créées au sein des entreprises, des organismes non étatiques et des sociétés. Il est évident que les normes imposées par l'État doivent être respectées lors de la formation de ces autres dispositions. Pourtant, le droit étatique n'interfère pas dans les règles créées en accord avec lui et que régleront les relations des acteurs privés.

Il est important de noter que le fonctionnement des chaînes de blocs s'accorde bien avec cette idée de régulation par le marché, en intégrant la participation de l'État et des acteurs privés concernés :

« Le concept, signifie, par essence, que les règles encadrant le comportement dans un marché sont développées, administrées et appliquées par les personnes (ou leurs représentants) dont le comportement doit justement être encadré. Les acteurs privés édictent alors, de manière autonome, des normes qui sont reconnues et appliquées par d'autres acteurs privés. »²²¹

Au regard des aspects techniques que nous avons abordés dans le premier titre de cette étude, les normes au sein d'une chaîne de blocs régissent les relations entre les nœuds, c'est-à-dire que les affaires reliant les membres sur la chaîne de blocs doivent suivre les normes

²²⁰ K. BENYekhlef, *préc.*, note 152, p. 745-746.

²²¹ K. BENYekhlef, *préc.*, note 152, p. 741.

préétablies dans ce réseau, à l'instar de l'idée de consensus et de forks²²², tout en respectant les normes de droit étatiques en vigueur.

L'importance de cette méthode de production de normes dans le contexte actuel est fondée sur une série de raisons comme la flexibilité, l'autonomie des normes alternatives et particulièrement l'attention portée sur les intervenants contribuant à leur propre régulation²²³.

Comme nous l'avons déjà évoqué au cours de cette étude, l'État a encore un rôle important à jouer dans le contexte de la production normative. L'inquiétude qui entoure l'exercice de ses activités viendrait d'une éventuelle incapacité de répondre de la façon la plus efficiente aux défis juridiques posés dans le contexte globalisé. Ainsi l'attention sur les normes alternatives a été intensifiée de même que sur le droit global. De ce fait, la proposition d'une corégulation entre ces acteurs semble pertinente. La corégulation ouvrirait la voie d'une harmonisation entre les protagonistes majeurs que sont les acteurs étatiques et non-étatiques.

À cet égard, le mot d'ordre est coopération. « Il s'agit donc, non pas de définir une nouvelle forme de régulation, mais de trouver une méthode adaptée aux temps nouveaux »²²⁴.

²²² "Because the blockchain is a decentralized data structure, different copies of it are not always consistent. Blocks might arrive at different nodes at different times, causing the nodes to have different perspectives of the blockchain. To resolve this, each node always select and attempts to extend the chain of blocks that represents the most Proof-of-Work, also know as the longest chain or greatest cumulative work chain. By summing the work recorded in each block in a chain, a node can calculate the total amount of work that has been expended to create that chain. As long as all nodes select the greatest-cumulative-work chain, the global bitcoin network eventually converges to a consistent state. Fork occurs as temporary inconsistencies between versions of blockchain, which are resolved by eventual reconvergence as more blocks are added to one of the forks." Andreas M. ANTONOPOULOS, *Mastering Bitcoin: Programming the Open Blockchain*, 2^e ed., Sebastopol, O'Reilly Media, 2017, p. 257.

²²³ Maria Eduarda GONÇALVES et Maria Inês GAMEIRO. *Project : the Landscape and Isobars of European Values in Relation to Science and New Technology. A Critical Discussion of Soft Law in a Governance Perspective*, Community Research and Development Information Service (CORDIS), European Commission, septembre 2011, en ligne : https://www.researchgate.net/publication/319065378_A_critical_discussion_of_soft_law_in_a_governance_perspective_Work_package_4_Authors_Maria_Ines_Gameiro_Maria_Eduarda_Goncalves > (consulté le 06 janv. 2019)

²²⁴ Christian PAUL, *Du droit et des libertés sur l'Internet*, Rapport au premier ministre, Paris, La Documentation française, 2000, p. 75, dans K. BENEKHELF, *préc.*, note 152, p. 744.

Certaines mesures caractéristiques de l'autorégulation sont mises en place conjointement avec d'autres mesures propres à la réglementation étatique.

La séparation et la balance des pouvoirs traditionnels (le législatif, l'exécutif et le judiciaire)²²⁵ pourraient être révisées pour y inclure les nouveaux acteurs de la globalisation. Cela permettrait de créer des systèmes de réglementation plus efficaces car plus adaptés aux particularités de chaque domaine, territoire et temps. Cependant ces derniers revêtiraient un caractère strict afin de ne pas favoriser indûment un pouvoir au détriment des autres.

L'Internet matérialise un contexte plus traditionnel pour expliquer l'influence de la méthode de corégulation. L'expérience du Forum des droits sur l'Internet est un exemple de mise en œuvre de la corégulation. Au cours de ses dix années de fonctionnement, depuis 2001, cet organisme s'est penché sur les enjeux juridiques soulevés par l'Internet. Grâce à des conseils et des groupes de travail, plusieurs questions ont été traitées, comme la protection du consommateur, la protection des mineurs et la publicité sur l'Internet, conduisant à la publication de rapports sur ses activités de recherche²²⁶. Les études étaient menées par de nombreux acteurs, allant des représentants du pouvoir public à ceux du secteur privé et de la société civile.

Force est de constater que parfois la corégulation peut être confondue avec le transgouvernementalisme. En effet, ces deux concepts possèdent la même caractéristique qui est de reconnaître d'autres acteurs au-delà des États. Pourtant, la corégulation va plus loin : elle réserve une place à la table de discussion sur les réglementations à la société civile, tandis que

²²⁵ Voir : MONTESQUIEU, *De l'esprit des lois*, Paris, Garnier-Flammarion, 1979.

²²⁶ Par exemple, voir : LE FORUM DES DROITS SUR L'INTERNET, *Rapport d'activité année 2009*, La documentation française, 2009, en ligne : < <https://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/104000464.pdf> > (consulté le 22 déc. 2018)

le transgouvernementalisme se limite aux États et aux « experts des administrations et des agences de régulation »²²⁷.

Ainsi, nous pouvons constater que ce genre d'initiative multi parties visant à regrouper différents acteurs et également diverses juridictions est ce qui permet de comprendre et de cultiver le développement des cadres législatif dans le contexte des technologies émergentes et des systèmes globaux. La corégulation associe le pouvoir d'autorégulation des parties directement intéressées à la sécurité et légitimité de la participation étatique dans le processus de réglementation.

Ces deux formes alternatives de réglementation présentent une approche du pluralisme juridique dans le contexte globalisé et technologique, prenant en compte également l'émergence de la chaîne de blocs et des contrats intelligents.

2.2. Les contrats intelligents face aux normes alternatives

Lorsque nous avons examiné la réglementation étatique concernant les contrats intelligents, nous avons pu constater l'existence de deux théories. La première énonce que les normes déjà existantes sont capables de bien régir cette technologie d'une manière générale. La seconde, quant à elle, met en avant le fait que certaines situations exigent une réponse juridique plus spécifique ou plus rapide. Réponse que le droit positif peut avoir des difficultés à offrir. Ainsi, les normes alternatives émergent comme une possible réponse de réglementation des technologies, soit au moyen de l'autorégulation, soit par la corégulation.

²²⁷ K. BENYEKHFLEF, *préc.*, note 152, p. 713.

Outre cette classification relative aux techniques d'élaboration, les normes alternatives peuvent aussi être groupées en raison de leur teneur : les normes comportementales et informatives, ainsi que les normes techniques et contractuelles.

Les deux premières normes sont orientées vers la mise en œuvre d'une conscience éthique dans le contexte commercial. Dans le cas des contrats intelligents, nous pourrions imaginer l'influence des « codes de bonne conduite » sur les plateformes d'hébergement des données ou un code de déontologie des programmeurs, à l'instar de l'initiative de l'Association québécoise des informaticiennes et informaticiens indépendants (AQIII).

L'AQII est une association à but non lucratif créée en novembre 1993 et qui regroupe nombreux travailleurs autonomes du milieu des TIC de la province canadienne. Elle a mis en place un « code d'éthique » pour ses membres qui prévoit des comportements à adopter comme le respect de la confidentialité et des « standards techniques et professionnels généralement acceptés dans l'industrie des TIC »²²⁸.

Ces deux aspects mentionnés – la confidentialité et le respect des standards techniques du milieu – sont deux enjeux comportementaux centraux qui demandent l'attention dans le cas de programmation en général et, par conséquent, des contrats intelligents. Ainsi, les normes comportementales et informatives jouent un rôle important dans l'efficacité des contrats intelligents, de sa création jusqu'à son exécution, dans la mesure où les informaticiens possèdent un pouvoir important dans le contexte de la société actuelle, globalisée et technologique.

²²⁸ ASSOCIATION QUÉBÉCOISE DES INFORMATIENNES ET INFORMATIENS INDÉPENDANTS, Code d'éthique pour les membres de l'AQIII, en ligne : < <https://www.aqiii.org/fr/membres/code-dethique/> > (consulté le 06 janv. 2019)

Les deux autres genres de normes mentionnées, les techniques²²⁹ et les contractuelles, quant à elles, ont pour objectif « la standardisation des comportements des acteurs économiques dictée par l'interdépendance des différents marchés et l'impérieuse nécessité de faciliter les échanges »²³⁰. En d'autres termes, chacune d'elles vise à créer un milieu plus stable au développement des activités commerciales, avec ses propres mécanismes et au moyen d'une normalisation des relations et procédures appliquées dans un domaine spécifique (par exemple, alimentaire, de combustibles, de la santé) ou relatif à une action particulière (par exemple, un contrat commercial d'achat et de vente de produits ou de prestation d'un service de logistique).

Par conséquent, les contrats intelligents, dans le cadre des normes alternatives, peuvent faire l'objet de différentes configurations de réglementation. Il est possible qu'ils soient régis par des normes créées exclusivement par les acteurs privés (autorégulation), mais aussi avec une participation étatique (corégulation). De la même façon, les normes découlant de l'autorégulation ou de la corégulation des contrats intelligents peuvent porter sur les pratiques éthiques, sur les démarches mieux acceptées par le marché (comportementales et informatives) ainsi que sur les aspects de standardisation (techniques et contractuelles).

En ce qui concerne les contrats intelligents, leur reconnaissance dans le monde juridique peut provenir des normes alternatives. Certaines d'entre elles sont déjà en vigueur et peuvent être appliquées aux contrats intelligents, comme notamment les publications de la Commission des Nations Unies pour le droit commercial international (CNUDCI) et les principes de l'Institut International pour l'unification du droit privé (UNIDROIT). Il existe également d'autres normes

²²⁹ Voir Michaël ROULAND, « La normalisation technique (instrument de concurrence à la loi) », dans Emmanuel CLAUDEL et Béatrice THULLIER (dir.), *Le droit mou : une concurrence faite à la loi*, Paris, Centre de Droit civil des Affaires et du Contentieux Économique de l'Université de Paris X-Nanterre, 2004, (PDF) en ligne : < <http://www.glose.org/CEDCACE7.pdf> > (consulté le 06 janv. 2019)

²³⁰ K. BENYEKHEF, *préc.*, note 152, p. 745.

en cours d'élaboration tournées particulièrement vers cette technologie, comme les projets ISO/TC 307, ISO/DTR 23455 et ISO/AWI 23259.

2.2.1. Des normes alternatives visant à l'harmonisation du droit commercial international: le CNUDCI et l'UNIDROIT

Lorsqu'on traite des contrats intelligents, le domaine plus souvent impliqué, ou à plus grande échelle, est généralement le commerce international. Au regard de la complexité de l'harmonisation des normes dans ce domaine, certaines organisations intergouvernementales travaillent à cette fin.

Dans ce contexte, bien qu'il existe d'autres organismes comme par exemple la Conférence de La Haye de droit international privé et la Chambre de commerce internationale (CCI), cette étude se concentrera sur les lois-type et conventions de la CNUDCI et les principes d'UNIDROIT. Il y a lieu d'examiner dans quelles mesures les lignes directrices de ces organisations peuvent être appliquées dans le contexte de mise en œuvre des contrats intelligents aujourd'hui, quand bien même elles ont été formulées plusieurs années avant le lancement de cette technologie.

En 1996, l'Assemblée générale de l'Organisation des Nations Unies a créé la CNUDCI dont le rôle vise à « encourager l'harmonisation et la modernisation progressives du droit commercial international en élaborant des instruments, législatifs ou non, dont elle encourage l'utilisation et l'adoption dans un certain nombre de domaines clefs du droit commercial »²³¹.

²³¹ COMMISSION DES NATIONS UNIES POUR LE DROIT COMMERCIAL INTERNATIONAL (CNUDCI), *Accueil*, en ligne : < <https://uncitral.un.org/fr> > (consulté le 20 janv. 2019)

Dans la mesure où les normes de la CNUDCI visent à un rapprochement des différents cadres juridiques, elles jouent un rôle important dans le contexte des discussions concernant la possible reconnaissance des contrats intelligents comme des accords juridiquement contraignants dans différentes juridictions.

Parmi les documents publiés par la commission, il faut mentionner la *Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux*²³². Cet ensemble de normes s'appliquerait aux contrats intelligents dans la mesure où ils peuvent être assimilés à l'objet de la convention, comme étant des communications électroniques connectées, formant ou réalisant un contrat entre des parties dont les lieux d'affaires se trouvent dans des États différents (article 1). L'incidence de la convention sur les contrats intelligents est renforcée car selon l'article 12, elle n'exclut pas les systèmes totalement automatisés de son application. Les dispositions de cette convention sont souvent appliquées aux contrats internationaux et habituellement fonctionnent comme des normes alternatives contractuelles.

En outre, les textes de la *Loi type de la CNUDCI sur l'arbitrage commercial international*²³³ et de la *Loi type de la CNUDCI sur les signatures électroniques*²³⁴ peuvent être appliqués aux contrats intelligents. Ils peuvent également trouver leur fondement dans

²³² COMMISSION DES NATIONS UNIES POUR LE DROIT COMMERCIAL INTERNATIONAL (CNUDCI), *Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux*, Vienne, Commission des Nations Unies pour le droit commercial international, 2007, en ligne : < http://www.uncitral.org/pdf/french/texts/electcom/06-57453_Ebook.pdf > (consulté le 20 janv. 2019)

²³³ COMMISSION DES NATIONS UNIES POUR LE DROIT COMMERCIAL INTERNATIONAL, *Loi type de la CNUDCI sur l'arbitrage commercial international*, 1985 avec les amendements adoptés en 2006, < https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/fr/07-86999_ebook.pdf > (consulté le 25 janv. 2019)

²³⁴ COMMISSION DES NATIONS UNIES POUR LE DROIT COMMERCIAL INTERNATIONAL, *Loi type de la CNUDCI sur les signatures électroniques*, en ligne : < <https://www.uncitral.org/pdf/french/texts/electcom/ml-elecsign-f.pdf> > (consulté le 25 janv. 2019)

dispositions de la CNUDCI « *Technical Notes on Online Dispute Resolution* »²³⁵, permettant ainsi d'établir dans le contrat intelligent une clause de règlement des litiges en ligne (« ODR »), dans les cas des conflits dépassant son exécution automatique.

La *Loi type de la CNUDCI sur le commerce électronique*²³⁶ pourrait être, de la même façon, applicable aux contrats intelligents, notamment car elle énonce des principes primordiaux pour le commerce électronique : la non-discrimination, la neutralité technologique et l'équivalence fonctionnelle. Analysons de plus près ces principes :

Le principe de non-discrimination garantit qu'un document ne se verra pas privé d'effet juridique, de validité ou de force obligatoire au seul motif qu'il est sous forme électronique. Le principe de neutralité technologique oblige à adopter des dispositions neutres s'agissant de la technologie utilisée. Eu égard à la rapidité des progrès technologiques, des règles neutres ont pour but de tenir compte des évolutions futures sans nécessiter de travail législatif supplémentaire. Le principe d'équivalence fonctionnelle énonce les critères selon lesquels les communications électroniques peuvent être considérées comme équivalentes aux communications sur support papier. Il définit notamment les exigences particulières auxquelles doivent satisfaire les communications électroniques afin de remplir les mêmes objectifs et fonctions que certaines notions du système traditionnel papier, par exemple "écrit", "original", "signature" et "enregistrement".²³⁷

Par conséquent, si nous considérons les contrats intelligents à la lumière de ces trois principes, il est plus facile de les assimiler à des contrats au sens juridique du terme. Il faut

²³⁵ COMMISSION DES NATIONS UNIES POUR LE DROIT COMMERCIAL INTERNATIONAL, *Technical Notes on Online Dispute Resolution*, en ligne : < http://www.uncitral.org/pdf/english/texts/odr/V1700382_English_Technical_Notes_on_ODR.pdf > (consulté le 25 janv. 2019)

²³⁶ COMMISSION DES NATIONS UNIES POUR LE DROIT COMMERCIAL INTERNATIONAL, *Loi type de la CNUDCI sur le commerce électronique et Guide pour son incorporation 1996 avec le nouvel article 5 bis tel qu'adopté en 1998*, en ligne : < http://www.uncitral.org/pdf/french/texts/electcom/05-89451_Ebook.pdf > (consulté le 25 janv. 2019)

²³⁷ COMMISSION DES NATIONS UNIES POUR LE DROIT COMMERCIAL INTERNATIONAL, *Commerce électronique: loi type de la CNUDCI sur le commerce électronique (1996)*, en ligne : < https://uncitral.un.org/fr/texts/ecommerce/modellaw/electronic_commerce > (consulté le 25 janv. 2019)

préciser que ces principes sont reconnus comme « les éléments fondateurs du droit du commerce électronique moderne »²³⁸. Ainsi, il est inévitable que l'analyse juridique des nouvelles technologies employées dans ce domaine les aborde.

Il en va de même pour les principes d'UNIDROIT relatifs aux contrats du commerce international qui figurent dans sa quatrième édition depuis 1994, la plus récente datant de 2016²³⁹. Cet ensemble de principes a « été élaboré comme un droit uniforme destiné à régir les rapports des opérateurs du commerce international », mais sans « aucune sanction officielle par des États ou des organismes internationaux »²⁴⁰. Il s'agit d'une norme alternative contractuelle, respectant la division et le concept traité dans le chapitre précédent.

Ainsi, les textes de la CNUDCI et les principes d'UNIDROIT consacrent un outil important au commerce international dans le contexte d'un monde globalisé. Cet outil permet une harmonisation entre les normes les plus diverses afin de répondre de manière adéquate aux besoins des acteurs internationaux.

“The UNIDROIT Principles provide a balanced set of rules covering virtually all the most important topics of general contract law, such as formation, interpretation, validity including illegality, performance, non-performance and remedies, assignment, set-off, plurality of obligors and of obligees, as well as the authority of agents and limitation periods.”²⁴¹

²³⁸ *Id.*

²³⁹ UNIDROIT, *Principes d'Unidroit relatifs aux contrats du commerce international*, 2016, en ligne : < <https://www.unidroit.org/instruments/commercial-contracts/unidroit-principles-2016> > (consulté le 25 janv. 2019)

²⁴⁰ Élise CHARPENTIER, « Les Principes d'Unidroit: une codification de la lex mercatoria? », *Les Cahiers de Droit*, vol. 46, n. 1-2, mars-juin 2005, p. 194, en ligne : < <https://bit.ly/2F86OYe> > (consulté le 26 janv. 2019)

²⁴¹ UNIDROIT, *Model Clauses for the Use of the UNIDROIT. Principles of International Commercial Contracts*, Uniform Law Review, Oxford University Press, 18 oct. 2013, en ligne : < <https://academic.oup.com/ulr/article/18/3-4/630/1636799> > (consulté le 18 déc. 2019)

Considérant l'espoir d'employer les contrats intelligents dans le commerce international, ces principes s'avéreraient un bon instrument de normalisation de ces relations, dans la mesure où le droit possède un caractère flou face au pluralisme juridique et la globalisation. Depuis sa première édition, les principes d'UNIDROIT sont considérés comme des « principes généraux du droit des contrats »²⁴². À partir de la deuxième édition, publiée en 2004, ces principes ont été étendus de manière à englober les besoins du commerce électronique²⁴³.

En général, nous pouvons dire que « son mandat est d'harmoniser et de coordonner la *lex mercatoria* »²⁴⁴. De manière analogue, ce rôle influence également la *lex electronica* dans le domaine des contrats. Ainsi, l'application des principes d'UNIDROIT porte sur les contrats internationaux, qu'ils soient écrits dans le langage humain ou de programmation, en version papier ou électronique. L'enjeu est de savoir comment appliquer le droit aux innovations comme les contrats intelligents²⁴⁵.

En outre, l'UNIDROIT a déjà clairement exprimé la possibilité d'application de ses principes aux contrats intelligents :

UNIDROIT has not produced any instruments that focus solely on e-commerce or smart contracts. However, throughout its four editions, the operation of the UNIDROIT Principles have been routinely audited to reflect emerging technologies and innovative e-commerce practices. As such, the UNIDROIT Principles remain a

²⁴² UNIDROIT, *Principes d'Unidroit relatifs aux contrats du commerce international*, 2010, en ligne : < <http://www.gdr-elsj.eu/wp-content/uploads/2012/10/principes-unidroit-integralversionprinciples2010-f.pdf> > (consulté le 26 janv. 2019)

²⁴³ Nika WITTEBORG, *Les Principes d'UNIDROIT relatifs aux contrats du commerce international comme source de connaissance du droit*, Séminaire L'harmonisation du droit du contrat en Europe – 38^e séminaire commun des Facultés de Droit des Universités de Montpellier et Heidelberg, p. 6, (PDF), en ligne : < <https://www.ipr.uni-heidelberg.de/md/jura/ipr/montpellier/vortraege/38witteborg.pdf> > (consulté le 25 janv. 2019)

²⁴⁴ Amélia SALEHABADI, *Une position unique en droit commercial international*, *Journal du Barreau*, Québec, v. 36, n° 16, 1^{er} oct. 2004, en ligne : < <https://www.barreau.qc.ca/pdf/journal/vol36/no16/position.html> > (consulté le 26 janv. 2019)

²⁴⁵ Michael FURMSTON et Gregory TOLHURST, *Contract formation: law and practice*, Oxford, Oxford University Press, 2016, p. 159-161.

*highly relevant and important source of law in considering the regulation and use of modern technology for contract management.*²⁴⁶

Il est évident que ces organismes sont capables de formuler des normes spécifiques au sujet des contrats intelligents, contribuant ainsi un peu plus à l'harmonisation du traitement juridique au sein des différentes juridictions. Ainsi, les normes alternatives déjà existantes constituent un point de départ intéressant pour la réglementation des technologies.

2.2.2. Les normes alternatives techniques : ISO/TC 307, ISO/DTR 23455 et ISO/AWI 23259

Les contrats intelligents font bouger les contours juridiques et le rôle des États dans le monde entier. Rappelons que les normes alternatives sont parties du résultat de ces mutations de la souveraineté des États et de la présence du pluralisme juridique. Face à ces changements, la présence d'autres acteurs dans la création des normes contemporaines se fait de plus en plus pertinente. Au-delà du pouvoir étatique, les normes alternatives peuvent être reconnues par les systèmes juridiques²⁴⁷. Cela pourrait entraîner la reconnaissance des contrats intelligents par le droit.

²⁴⁶ UNIDROIT. William Brydie-Watson. *Workshop on the Use of Modern Technology for Dispute Resolution and Electronic Agreement Management Particularly Online Dispute Resolution*, Port Moresby, Papua New Guinea, 3-4 March 2018, International Institute for the Unification of Private Law Instruments that Facilitate the Use of Modern Technology for Contract Management, en ligne : http://mddb.apec.org/Documents/2018/EC/WKSP2/18_ec_wksp2_008.pdf > (consulté le 27 janv. 2019).

²⁴⁷ À propos de la reconnaissance du caractère contraignant des normes alternatives : « La mise en évidence des effets produits par le *soft law* à l'aune des émotions suscitées montre que des actes non juridiquement obligatoires peuvent être contraignants. L'absence d'effets juridiques au sens classique ne saurait donc leur permettre de se soustraire à l'adoption d'un régime de légitimation et de contrôle adapté que les règles de *hard law* connaissent depuis longtemps dans les États de droit. » Alexandre FLÜCKIGER, *Pourquoi respectons-nous la soft law ?*, Revue européenne des sciences sociales, 2009, p. 73-103, en ligne : < <https://journals.openedition.org/ress/68#toc> > (consulté le 07 janv. 2019)

Les normes techniques et celles produites par la méthode d'autorégulation jouent un rôle indispensable sur la scène du commerce international. Eu égard aux besoins pratiques et de standardisation, ces normes – en raison de leur méthode de formation et/ou de leur teneur – sont capables de bien répondre aux enjeux de la globalisation.

En effet, ces normes sont parfois plus appropriées que le droit positif lorsque le processus de réglementation traditionnel ne semble pas capable de répondre au besoin de flexibilité et de rapidité caractéristique du marché global contemporain. Ces normes permettent ainsi l'adaptation des pratiques aux progrès technologiques.

Dans cette perspective, les normes techniques et d'autorégulation présentent un potentiel indéniable dans l'emploi de la chaîne de blocs et de la reconnaissance juridique des contrats intelligents. C'est le cas des normes ISO/TC 307, ISO/DTR 23455 et ISO/AWI 23259, orientées spécifiquement vers ce sujet.

En 2016, le Comité technique 307 a été créé au sein de l'Organisation internationale de normalisation (ISO), dont la première rencontre a eu lieu en Australie en 2017. Le but du comité est d'élaborer les lignes directrices sur la technologie de la chaîne de blocs et les technologies de registre distribué. Aujourd'hui, le comité compte 39 membres participants²⁴⁸, 13 membres observateurs²⁴⁹ et 11 projets divisés initialement entre six groupes de travail spécialisés : « (1)

²⁴⁸ Les pays membres sont : Afrique du Sud (SABS); Allemagne (DIN); Australie (SA); Autriche (ASI); Belgique (NBN); Brésil (ABNT); Cambodge (ISC); Canada (SCC); Chine (SAC); Chypre (CYS); Corée, République de (KATS); Croatie (HZN); Danemark (DS); Émirats arabes unis (ESMA); Espagne (UNE); États-Unis (ANSI); Finlande (SFS); France (AFNOR); Hongrie (MSZT); Inde (BIS); Irlande (NSAI); Italie (UNI); Jamaïque (BSJ); Japon (JISC); Kazakhstan (KAZMEMST); Luxembourg (ILNAS); Malaisie (DSM); Norvège (SN); Nouvelle-Zélande (NZSO); Pays-Bas (NEN); Pologne (PKN); Portugal (IPQ); Royaume-Uni (BSI); Russie, Fédération de (GOST R); Singapour (ESG); Suède (SIS); Suisse (SNV); Thaïlande (TISI); Ukraine (DSTU).

²⁴⁹ Ces pays sont: Argentine (IRAM); Bélarus (BELST); Hong Kong (ITCHKSAR); Indonésie (BSN); Iran, République islamique d' (ISIRI); Israël (SII); Kenya (KEBS); Maroc (IMANOR); Mexique (DGN); Philippines (BPS); Slovaquie (UNMS SR); Tchèque, République (UNMZ); Uruguay (UNIT).

foundations; (2) security, privacy and identity; (3) smart contracts and their applications; (4) use cases; (5) governance; (6) interoperability »²⁵⁰.

Le Guide pour les standards de la chaîne de blocs²⁵¹, publié en 2017 en préparation à la première rencontre du comité, prend en considération le rôle de la normalisation « *in supporting potential future regulation on blockchain and the relationship between the law and standards* ». L'objectif de la norme technique n'est pas de se substituer immédiatement au contenu des normes juridiques relatives à la vie privée, à la sécurité, à l'identité et aux contrats intelligents.

Elle vise, dans les faits, à constituer un point d'ancrage basé sur les aspects techniques sous la forme d'orientation aux *stakeholders* et « *potentially be referenced by regulators in policy and regulation* ». Le rapport souligne également l'importance du rôle de la normalisation, particulièrement dans le contexte des contrats intelligents, dans la mesure où elle permet de concilier le développement de la technologie de la chaîne de blocs et du droit.²⁵²

Les normes juridiques existantes sont suffisantes dans un certain nombre de cas, mais peuvent présenter des lacunes dans d'autres. Cela signifie que la normalisation de l'ISO concernant les chaînes de blocs et les technologies connexes émerge avec le potentiel de remplir ces lacunes.

Les projets portent sur les enjeux les plus importants de la chaîne de blocs : *terminology (ISO/CD 22739); privacy and personally identifiable information protection considerations*

²⁵⁰ ORGANISATION INTERNATIONALE DE NORMALISATION, *Strategic Business Plan ISO/TC 307, Blockchain and distributed ledger technologies*, 30 août 2018, en ligne : < https://isotc.iso.org/livelink/livelink/fetch/-17853836/17853838/17855344/ISO-TC307_N0326_ISO_TC_307_Strategic_Business_Plan.pdf?nodeid=19912672&vernum=-2 > (consulté le 07 janv. 2019)

²⁵¹ STANDARDS AUSTRALIA, *Roadmap for Blockchain Standards*, Report, mars 2017, en ligne : < <https://bit.ly/2TCWaBx> > (consulté le 07 janv. 2019)

²⁵² STANDARDS AUSTRALIA, *préc.*, note 249.

(ISO/NP TR 23244); security risks, threats and vulnerabilities (ISO/NP TR 23245); overview of identity management using blockchain and distributed ledger technologies (ISO/NP TR 23246); reference architecture (ISO/AWI 23257); taxonomy and ontology (ISO/AWI TS 23258); overview of and interactions between smart contracts in blockchain and distributed ledger technology systems (ISO/DTR 23455); security management of digital asset custodians (ISO/NP TR 23576); discovery issues related to interoperability (ISO/NP TR 23578); guidelines for governance (ISO/NP TS 23635); et enfin, et surtout, legally binding smart contracts (ISO/AWI TS 23259)²⁵³.

Parmi les onze projets, deux sont dédiés spécifiquement à la normalisation des contrats intelligents : l'ISO/DTR 23455 et l'ISO/AWI TS 23259. Notons que ce dernier, appelé « *legally binding smart contracts* », ne s'occupe pas simplement de la mise en œuvre des contrats intelligents mais il permet de les créer de façon contraignante. C'est un point important relatif aux normes proposées qui révèle leur potentiel dans la création d'un socle de concepts, de fonctionnement et de procédures qui viendra appuyer les dispositions du droit.

En ce qui concerne le statut juridique des contrats intelligents, par exemple, il faut mentionner le rapport élaboré comme support des travaux de formulation de l'ISO/TC 307 par le Comité européen de normalisation (CEN) et le Comité européen de normalisation électrotechnique (CENELEC). Ils mentionnent un projet, le DECODE²⁵⁴, lancée en 2017, qui a pour intention principale de concéder à tous les acteurs un pouvoir sur leurs données personnelles. Soulignons également que ce projet analyse le statut juridique des contrats

²⁵³ ORGANISATION INTERNATIONALE DE NORMALISATION, *Standards catalogue ISO/TC 307, Blockchain and distributed ledger technologies*, en ligne : < <https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0> > (consulté le 08 janv. 2019)

²⁵⁴ Cf. : PROJET DECODE, en ligne : < www.decodeproject.eu/ > (consulté le 09 janv. 2019)

intelligents en examinant, par exemple, son adéquation au *Règlement général sur la protection des données* (RGPD) et les hypothèses où ils seraient juridiquement contraignants²⁵⁵.

L'opposition entre la caractéristique d'automatisation des contrats intelligents et la protection contre l'automatisation du traitement des données personnelles prévue dans le RGPD²⁵⁶ est un des enjeux invoqués par le rapport du CEN et CENELEC. Ainsi, nous revenons à la question générale au sujet de l'adéquation de la chaîne de blocs et des contrats intelligents dans le contexte juridique actuel.

Il convient également de mentionner l'existence d'un livre blanc publié en juillet 2018 par les chercheurs européens contenant 26 recommandations concernant, par exemple, le développement durable, l'identité numérique, la vie privée et la protection de données, la transformation numérique de l'État et la gouvernance de la mise en œuvre de la chaîne de blocs²⁵⁷.

Le document présente quelques cas d'usage de la technologie en Europe. Ceci est important pour comprendre les lacunes encore existantes entre ce que le monde juridique

²⁵⁵ EUROPEAN PARLIAMENT, *General Data Protection Regulation*, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, en ligne : < <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679> > (consulté le 09 janv. 2019)

²⁵⁶ "Automated processing. A final point that is not often discussed is the right that GDPR gives data subjects to be protected from automated processing of personal data. One of blockchain's great innovations, at the heart of many of its most important applications, is the ability to automatically process many transactions via smart contracts. Can these be reconciled with GDPR?" EUROPEAN COMMITTEE FOR STANDARDIZATION (CEN) et EUROPEAN COMMITTEE FOR ELECTROTECHNICAL STANDARDIZATION (CENELEC), *Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies*, Torino, 2018, p. 35, (PDF), en ligne : < https://www.gleif.org/content/1-about/7-consultation-responses/fg-bdlt-white_paper.pdf > (consulté le 09 janv. 2019)

²⁵⁷ EUROPEAN COMMITTEE FOR STANDARDIZATION (CEN) et EUROPEAN COMMITTEE FOR ELECTROTECHNICAL STANDARDIZATION (CENELEC), *préc.*, note 254, p. 4.

propose et ce que la société réclame. Parmi les exemples mentionnés nous trouvons les contrats intelligents incluant un outil de consentement.

Il s'agit du projet KONFIDO qui entend déployer un contrat intelligent enregistrant le consentement spécifique lorsqu'un membre du réseau (médecin, pharmacien, infirmier) demande l'accès aux données d'un patient. L'idée fondamentale est d'assurer la vérifiabilité et la traçabilité, qui plus est dans les cas où le patient n'est pas capable de s'exprimer²⁵⁸. Considérant le cas susmentionné, le consentement enregistré *via* un contrat intelligent serait-il reconnu valide par les règles juridiques en vigueur ? Tel est le défi, quasi « insurmontable » de la norme ISO²⁵⁹.

Malgré les difficultés, ce groupe de normes alternatives tente d'harmoniser les aspects techniques et les exigences du droit visant à mettre en œuvre des résultats concrets dans les termes exacts souhaités par la libre volonté des parties. Cette idée est semblable à la notion juridique de contrat.

La rencontre plus récente du comité au sein de l'ISO/TC 307 a eu lieu en octobre 2018 à Moscou²⁶⁰. À cette occasion, les groupes de travail 2 (« *security, privacy and identity* ») et 3 (« *smart contracts and their application* ») se sont réunis afin de préparer l'étude présentée lors de la réunion plénière du 27 au 31 mai 2019, en Irlande.

L'entrée en vigueur de ces normes ISO relatives à la chaîne de blocs et ses usages est prévue pour l'année 2021. D'autres questions technologiques ont été déjà soumises à normalisation de l'ISO, et sont aujourd'hui réglementées par des normes appliquées

²⁵⁸ Id., p. 18-19.

²⁵⁹ ORGANISATION INTERNATIONALE DE NORMALISATION, *préc.*, note 248. (consulté le 10 janv. 2019)

²⁶⁰ ROSSTANDART FEDERAL AGENCY ON TECHNICAL REGULATING AND METROLOGY. *ISO/TC 307 "Blockchain and distributed ledger technologies" session took place in Moscow*, 30 oct. 2018, Moscow, en ligne : < <https://bit.ly/2J9nx1o> > (consulté le 08 janv. 2019)

internationalement, comme par exemple l'ISO/IEC 27001 et 27002 relatives à la sécurité de l'information et la norme ISO 20000 relative au système de gestion de services informatiques. L'objectif de ces standards est d'aider la mise en œuvre globale, fiable et effective des aspects technologiques en général.

Fondées sur la reconnaissance de l'ISO comme une organisation de renommée globale, les normes présentées soutiendront peut-être la promotion de solutions réelles face aux enjeux de la technologie de la chaîne de blocs et des contrats intelligents au niveau mondial. Aujourd'hui, l'absence d'une standardisation est encore source d'insécurité juridique.

2.3. La reconnaissance juridique des contrats intelligents dans le contexte des normes alternatives

L'ensemble de l'étude qui a été effectuée au cours de ce mémoire nous amène à nous poser des questions plus factuelles au sujet des contrats intelligents. Seraient-ils juridiquement reconnus sur le même plan que les contrats traditionnels et ainsi seraient le fondement des relations de droit entre les parties ? Les contrats intelligents seraient-ils juridiquement contraignants ?

Nous avons pu découvrir que dans le cadre de la loi québécoise il n'y a aucun obstacle juridique à leur reconnaissance à condition que les prérequis légaux traditionnels soient respectés. Tout au long de cette étude, nous avons également constaté que certaines questions qui ont fait l'objet de discussions lors de l'émergence du commerce électronique réapparaissent aujourd'hui pour les contrats intelligents. En effet, théoriquement les défis sont semblables.

À l'image des problématiques invoquées à propos des contrats électroniques, la doctrine s'interroge sur les questions liées au consentement valide, à la compréhension des clauses rédigées, à ce qui peut être compris comme une offre et une acceptation dans le contexte électronique etc.

Dans l'ordre juridique canadien et québécois, il n'existe pas encore une législation spécifique traitant des contrats intelligents ou même de décisions des tribunaux à ce sujet. Ainsi, il est raisonnable de supposer que les règles du commerce électronique et d'autres normes connexes pourraient être également appliquées aussi aux contrats intelligents. Dans ce sens :

“In many ways, smart contracts are no different than today's written agreements. To execute a smart contract, parties must first negotiate the terms of their agreement until they reach a “meeting of the minds”. Once agreed upon, parties memorialize all or part of their understanding in smart contract code, which is triggered by digitally signed blockchain-based transactions. In the case of a dispute, parties can either renegotiate the underlying arrangement or seek redress from a court or arbitration panel to reverse the effects of the smart contract.”²⁶¹

En raison de cette nature « d'accord », il est envisageable que les contrats intelligents soient contestés devant les tribunaux tôt ou tard, notamment lors d'un conflit de volontés ou d'intérêts. C'est à ce moment-là que d'autres conclusions plus concrètes pourront voir le jour. Les manifestations des législateurs locaux pourraient contribuer également à la discussion dans une échelle plus spécifique. Toutefois, à l'heure actuelle, les instruments mentionnés dans cette étude permettent aux contrats intelligents d'être assimilés aux contrats traditionnels déjà reconnus par le droit.

Lorsque nous avons traité de la norme ISO, nous avons mentionné qu'elle comporte, dans le contexte actuel, un potentiel juridique. De la même façon, les normes alternatives déjà

²⁶¹ P. DE FILIPPI et A. WRIGHT, préc., note 8, p. 74.

existantes provenant d'organismes d'harmonisation du droit international possèdent également ce potentiel.

Les normes alternatives s'avèrent être des instruments importants dans la mesure où elles permettent l'actualisation continue des normes, conservant ainsi l'harmonie avec les innovations technologiques et les besoins sociaux. Cette harmonie concerne également la diversité des juridictions. Au-delà de la notion de droit étatique, les règles appliquées dans une transaction commerciale internationale échappent à un système juridique positif et fermé.

Ainsi, dans la mesure où les contrats intelligents deviennent de nouvelles figures dans le commerce international, ils peuvent et doivent bénéficier d'un instrument permettant leur réglementation et la réussite des affaires, quand bien même le droit positif n'a pas toujours une réponse adaptée à ce milieu du commerce international. À ses débuts, l'Internet a affronté le même défi. Il était considéré par beaucoup comme une zone de non-droit, tout comme l'est le *darknet* aujourd'hui.

Les conflits et les difficultés d'application des normes du droit étatique (*common law* ou *civil law*), en raison par exemple de leur nature décentralisée, rendent les normes alternatives plus adéquates pour accepter les contrats intelligents. Des solutions pour les contrats intelligents sont généralement basées sur celles appliquées aux contrats traditionnels. Ce n'est toutefois pas toujours possible, en vertu des particularités des contrats intelligents.

La discussion ne concerne pas exclusivement la capacité des contrats intelligents d'obtenir une reconnaissance juridique dans les cas où ils remplissent les critères légaux régissant le droit des contrats pour chaque juridiction concernée. L'idée d'un monde (et d'un système juridique) avec ses frontières chaque fois plus souples nous amène également à examiner la façon la plus efficace de rendre les contrats intelligents juridiquement contraignants,

notamment au regard des caractéristiques de cette technologie : décentralisée, distribuée et automatisée.

L'idée de reconnaissance juridique des contrats intelligents par le « *hard law* » semble être possible, comme nous avons pu le constater grâce aux récentes normes établies à ce sujet. Les normes étatiques déjà existantes, quant à elles, restent applicables, c'est-à-dire qu'un contrat intelligent ne pourra jamais être reconnu valide lors d'une transaction qualifiée d'illégale par le droit, de la même manière que les contrats traditionnels. Par exemple, la négociation de drogues illicites et la violation des restrictions à l'importation ne seront pas admises simplement parce qu'elles sont régies via contrats intelligents²⁶². *“If a particular type of exchange is prohibited or if a contractual provision is illegal or unenforceable under the rules of a specific jurisdiction - it remains prohibited, illegal or unenforceable if embodied in a smart contract.”*²⁶³

Encore une fois, il s'agit de reconnaître que les chaînes de blocs et ses applications ne sont pas une zone de non-droit. Ainsi, la discussion dépasse la simple analyse de la reconnaissance juridique des contrats intelligents et met en avant la façon plus convenable de le faire. C'est alors qu'interviennent les normes alternatives.

La normalisation de l'ISO concernant la chaîne de blocs et les technologies connexes, analysée dans le chapitre précédent, ainsi que les normes émanant d'autres organismes interétatiques, émergent avec le potentiel juridique de combler les lacunes du droit positif en réponse aux défis qui se dressent face aux différentes juridictions.

²⁶² Eliza MIK, *Smart contracts: Terminology, technical limitations and real world complexity*, Law, Innovation and Technology, Research Collection of School of Law, Singapore, 2017, p. 15, en ligne : < https://ink.library.smu.edu.sg/sol_research/2341 > (consulté le 15 févr. 2019)

²⁶³ Id., p. 15.

Certains considèrent que les “*standards can provide guidance to developers and users of blockchain technologies, but that these standards are not able to take priority over the law or act as a substitute*”²⁶⁴. Dans les faits, il ne s’agit pas d’un remplacement des lois par des standards, mais d’une adaptation selon les besoins réels.

Par exemple, si un contrat intelligent est déployé entre deux parties soumises à la même compétence juridictionnelle, c’est-à-dire sans dépasser les limites d’une juridiction donnée, le droit étatique qui les régit suffira, théoriquement, pour régler le cas. Dès lors, il doit être évident que :

*“To deny the possibility of ‘delegating’ the formation and performance of contracts to computers is to deny the legal viability of automated securities trading, vending machines and practically all e-commerce websites. In each of these examples, the computer executes a prior human decision to engage in a transaction within pre-set parameters with whoever complies with these parameters. The intention to be legally bound is manifested by means of a computer. In this sense, smart contracts represent the intentions of the transacting parties, who chose to express their obligations in code and automate certain aspects of contractual performance.”*²⁶⁵

La reconnaissance juridique des contrats intelligents peut être basée sur les règles de droit habituellement appliquées aux contrats traditionnels, mais aussi sur les autres sources du droit selon les besoins du contexte des relations globalisées. À ce titre, dans le panorama actuel, les normes alternatives se posent comme une méthode plausible de reconnaissance juridique des contrats intelligents.

De plus, assimiler les contrats intelligents à des contrats juridiquement contraignants est une tâche complexe qui exige la combinaison du droit positif et des normes alternatives. Toutefois, celles-ci se détachent dans le contexte globalisé et numérique dans la mesure où la complexité du panorama actuel exige des mesures rapides et flexibles plutôt que des dispositions

²⁶⁴ STANDARDS AUSTRALIA, *préc.*, note 249. (consulté le 15 févr. 2019)

²⁶⁵ E MIK, *préc.*, note 260, p. 15.

rigides et lentes caractéristiques du droit étatique, qui, quant à lui, est notamment capable d'offrir une sécurité juridique et une légitimité au droit des technologies.

Considérations finales

*Just because something doesn't do what you planned it to do
doesn't mean it's useless.
(Thomas Edison)*

À propos de la reconnaissance juridique des contrats intelligents, ce mémoire n'a pas eu l'ambition de parvenir à une conclusion dans le sens strict du terme. Ainsi que d'autres technologies en vogue, ces derniers pourraient subir des changements rapides et peut-être même intégraux. Par conséquent, les conclusions éventuellement formulées au sein de cette étude pourraient être rapidement et entièrement contredites dans ce contexte de mutation constante, en rendant ce mémoire obsolète. Pour cette raison, nous choisissons de formuler certaines considérations finales, afin de fonder et d'inciter les réflexions à ce sujet, mais sans pour autant avoir l'intention d'y mettre fin.

Le premier titre de ce mémoire nous a permis de formuler quelques remarques sur les aspects technologiques des contrats intelligents. Il n'était alors pas question d'envisager ces contrats sous l'angle purement juridique mais de les étudier avec un regard technique et pratique. Ainsi, nous avons constaté que la portée des applications de cette technologie n'est pas encore totalement connue.

Au regard de ce que nous avons appris, la chaîne de blocs et les contrats intelligents pourraient avoir un important potentiel de transformer la manière de s'engager partout le monde. Néanmoins, nous devons veiller à ce que cela ne devienne pas un simple engouement collectif démesuré. Il est recommandé que l'examen de ce potentiel de changement soit réalisé au cas par

cas. Il oscillerait en fonction, par exemple, des industries touchées et de la portée des activités menées dans chaque situation ²⁶⁶.

Outre le potentiel transformateur de cette technologie, l'évaluation du rapport avantages-inconvénients pourrait également varier entre les différents cas en raison, par exemple, des risques auxquels le projet basé sur la chaîne de blocs est disposé à s'exposer. Dans son ensemble, les avantages et les inconvénients établis à propos de l'utilisation des contrats intelligents sont liés aux caractéristiques de cette technologie.

Toutefois, il s'avère que ces caractéristiques ne sont pas totalement rigides, par conséquent les avantages et inconvénients ne le sont pas non plus. Ainsi, tout comme dans le cas des applications pratiques, les caractéristiques de la chaîne de blocs et des contrats intelligents ne sont pas totalement connues. Par exemple, l'immutabilité des contrats intelligents fait l'objet de nombreuses recherches et de nombreux débats afin de dégager la meilleure façon de rendre ces engagements automatisés modifiables lors de leur exécution sans pour autant risquer, le cas échéant, de mettre en péril leurs avantages tels que la transparence et la sécurité.

Le deuxième titre, quant à lui, se concentre sur la perspective juridique de ces contrats. La réflexion proposée dans ce mémoire vise principalement à examiner les nuances de la reconnaissance juridique des contrats intelligents dans un contexte global présent et à venir. Le cadre juridique de certains États et certaines normes alternatives ont été exposés dans l'étude afin d'illustrer le scénario actuel de réglementation. Ce qu'il convient d'en retenir, c'est qu'il est parfaitement possible d'envisager la coexistence des normes étatiques et paraétatiques,

²⁶⁶ « The blockchain is not for everything. And not everything fits the blockchain paradigm. The blockchain is a 'state machine', which is another concept that needs to be understood. [...] A state machine is a computer or device that remembers the status of something at a given instant in time. » W. MOUGAYAR, *préc.*, note 16, p. 24.

comme on l'a vu. En effet, cette articulation est souhaitable notamment dans un contexte globalisé où se l'on parle d'une possible émergence de la technocratie²⁶⁷.

De manière générale, le droit étatique ne semble pas être capable de – tout seul – faire face aux défis dématérialisés et transnationaux apportés par les technologies au sein d'un monde globalisé. L'idée de « *hard law* » traduit ce caractère rigide du droit étatique. Selon cette logique, la concurrence des nombreux droits nationaux et la limitation des acteurs présents dans le contexte du droit international empêcheraient les droits étatiques de formuler une réponse aux besoins d'un monde globalisé.

Ainsi, les normes alternatives se présentent comme un outil indispensable pour une réglementation effective. En effet, le caractère souple de ces normes contraignantes leur permet de se rapprocher du rythme soutenu et sans frontières des changements technologiques. Par conséquent, la combinaison du droit mou, proposant la sécurité juridique, et la légitimité des normes du « *hard law* » serait une manière de créer un ordre juridique plus effectif²⁶⁸ en ce qui concerne le droit des technologies.

Dans ce sens, « la compréhension de la révolution juridique actuelle est exigeante. Elle oblige à confronter le droit à des disciplines qui lui étaient jusqu'à présent étrangères comme l'informatique, à quoi les juristes ne sont pas habitués »²⁶⁹.

²⁶⁷ À propos de la notion de technocratie : « Dans le cadre de la société postmoderne, la technicité des enjeux en présence oblige les gouvernants à se délester de certaines de leurs prérogatives au profit de spécialistes davantage au fait desdits enjeux et donc plus aptes à produire des normes pertinentes et efficaces. Bien qu'elle permette de « sauver le droit », cette prééminence de la technique ne manque pas d'interroger gravement à différents points de vue et en particulier socialement ». B. BARRAUD, *préc.*, note 3, p. 325.

²⁶⁸ « La crise du droit moderne est en premier lieu le fruit du peu d'efficacité du droit produit par l'État. En effet, sur l'Internet, les activités échappent le plus souvent au contrôle juridico-étatique, les internautes ne craignant pas d'être atteints par une quelconque sanction légale. Cela oblige – pour ne pas qu'il s'agisse d'une zone de non droit – à trouver de nouvelles formes de normativité plus pertinentes et plus aptes à contraindre les individus évoluant sur le réseau. » *Id.*

²⁶⁹ GARAPON, A., LASSÈGUE, J., *Justice digitale*, Paris : Presses Universitaires France, 2018 (édition Kindle).

Nous réalisons donc que cette reconfiguration de l'architecture du droit demande aux juristes bien plus que la simple connaissance des règles positives applicables ou non aux contrats intelligents ou aux technologies en général. Le contexte globalisé actuel suppose une analyse critique du rôle du droit comme instrument de régulation sociale et, également, du besoin de partage de la souveraineté étatique pour la création des normes.

Nous constatons ainsi l'insuffisance du droit mou et des normes étatiques s'ils sont pris individuellement. Ensemble, ces deux techniques pourraient créer un système de réglementation plus effectif pour les contrats intelligents, pour aujourd'hui et pour l'avenir. Loin de l'idée de la pyramide, les normes dans ce contexte semblent s'organiser, dans ce contexte, de façon horizontale tel un réseau où elles sont juxtaposées « en synergie »²⁷⁰.

La seule conclusion qu'il soit possible d'apporter à ce mémoire est que beaucoup de chemin reste à parcourir en matière de droit des technologies et d'intégration effective des contrats intelligents dans la sphère juridique.

²⁷⁰ A FLÜCKIGER, *préc.*, note 246, p. 73-103.

Bibliographie

Législation et réglementation

Au Canada

CANADA, *Résumé législatif. Projet de Loi C-59 : Loi modifiant la loi sur l'Investissement au Canada*, Bibliothèque du Parlement, Service d'information et de recherche parlementaires, 14 oct. 2005, (PDF), en ligne : <

https://lop.parl.ca/sites/PublicWebsite/default/fr_CA/ResearchPublications/LegislativeSummaries/381LS515E > (consulté le 28 déc. 2018)

Loi de 2000 sur le commerce électronique, LO 2000, c 17, en ligne : <

<http://canlii.ca/t/69jzp> > (consulté le 19 déc. 2018)

Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes,

L.C. 2000, c. 17, en ligne : < <https://laws-lois.justice.gc.ca/fra/lois/P-24.501/> > (consulté le 08 janv. 2019)

Au provincial

Loi concernant le cadre juridique des technologies de l'information, L.R.Q., c. C-1.1,

Original, en ligne : < <https://www.lccjti.ca/definitions/original/> > (consulté le 19 déc. 2018)

À l'international

DIRECTIVE 1999/93/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 13 DÉCEMBRE 1999 SUR UN CADRE COMMUNAUTAIRE POUR LES SIGNATURES ÉLECTRONIQUES, *Journal officiel des Communautés européennes*, en ligne : < <https://eur->

lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:013:0012:0020:FR:PDF > (consulté le 19 déc. 2018)

ÉTATS-UNIS, *House of Representatives Bill 1507*, State of Tennessee, en ligne < <https://legiscan.com/TN/bill/HB1507/2017> > (consulté le 10 janv. 2019)

_____, *House of Representatives Bill 2417*, State of Arizona, en ligne : < <https://www.azleg.gov/legtext/53leg/1r/bills/hb2417p.pdf> > (consulté le 08 janv. 2019)

_____, *Senate Bill 300*, State of Ohio, en ligne : < <https://legiscan.com/OH/text/SB300/id/1795258> > (consulté le 10 janv. 2019)

ITALIE, *Loi 11 février 2019*, n. 12, en ligne : < <http://www.gazzettaufficiale.it/eli/id/2019/02/12/19G00017/sg> > (consulté le 13 fév. 2019)

NATIONS UNIES, *Loi type de la CNUDCI sur le commerce électronique et Guide pour son incorporation*, New York, 1999, en ligne (PDF) : < https://www.uncitral.org/pdf/french/texts/electcom/05-89451_Ebook.pdf > (consulté le 19 déc. 2019)

PARLEMENT EUROPÉEN, *Directive sur le commerce électronique*, journal officiel n° L 178 du 17/07/2000, en ligne: < <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:FR:HTML> > (consulté le 19 déc. 2018)

_____, *General Data Protection Regulation*, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, en ligne : < <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679> > (consulté le 09 janv. 2019)

RÉPUBLIQUE FRANÇAISE, *Plan d'Action pour la Croissance et la Transformation des Entreprises*, en ligne : < <https://www.gouvernement.fr/en/pacte-the-action-plan-for-business-growth-and-transformation> > (consulté le 08 janv. 2019)

Doctrine

Monographies et ouvrages collectifs

ANTONOPOULOS, A.M., *Mastering Bitcoin: Programming the Open Blockchain*, 2^e ed., Sebastopol, O'Reilly Media, 2017.

AUDIER, S., *Penser le néolibéralisme. Le moment néolibéral, Foucault et la crise du socialisme*, Paris, Le Bord de l'Eau, 2015.

BARRAUD, B., *Repenser la pyramide des normes à l'ère des réseaux: Pour une conception pragmatique du droit*, L'Harmattan, Paris, 2012, en ligne : < <https://hal-amu.archives-ouvertes.fr/hal-01369314/document> > (consulté le 18 fév. 2019)

BAUDOUIN, J-L., *Les obligations*, Yvon Blais, Cowansville, 1989.

BEDDIAR, K., IMBAULT, F., *Blockchain pour l'énergie*, Malakoff, Dunod, 2018.

BENYEKHELF, K., « Vers une gouvernance globale: l'émergence d'un droit postnational », dans Louise LALONDE et Stéphane BERNATCHEZ (dir.), *La place du droit dans la nouvelle gouvernance étatique*, Sherbrooke, Les Éditions Revue de Droit, 2011, 220 p.

_____, K., *Une possible histoire de la norme, Les normativités émergentes de la mondialisation*, 2^e Édition, Montréal, Les Éditions Thémis, 2015.

CAMPAGNOLO, Y., DEBRUCHE, A., GRAMMOND, S., *Quebec Contract Law*, Montréal : Wilson & Lafleur, 2016.

CAPRIOLI, E., *La blockchain ou la confiance dans une technologie*, La semaine juridique, édition générale, n. 23, 06 juin 2016.

CASEY, M. J., VIGNA, P., *The Truth Machine. The Blockchain and the Future of Everything*, New York : St. Martin's Press, 2018.

CHEVALLIER, J., « L'internormativité », p. 13-14 (PDF), dans COLLECTIF, *Les sources du droit revisitées*, v. 4, Anthémis, Théorie des sources du droit, Wavre, 2013, en ligne : < <https://hal.archives-ouvertes.fr/hal-01723912/document> > (consulté le 16 déc. 2018)

CHOULI, B., GOUJON, F., LEPORCHER, Y. M., *Les Blockchains. De la théorie à la pratique, de l'idée à l'implémentation*, Saint-Herblain : Éditions Eni, 2017.

DE BELLEFONDS, X.L., *Le droit du commerce électronique*, Presses Universitaires de France, 2005, en ligne : < https://www.cairn.info/feuilleter.php?ID_ARTICLE=PUF_LINAN_2005_01_0036 > (consulté le 15 janv. 2019)

DE FILIPPI, P., WRIGHT, A., *Blockchain and the Law. The Rule of Code*, Cambridge, Harvard University Press, 2018.

DEGREGON, T.R., *A Theory of Technology. Continuity and Change in Human Development*, Iowa City, The Iowa State University Press, 1985.

DELMAS-MARTY, M., « *Le flou du droit* », dans Louis ASSIER-ANDRIEU (dir.), *Droit et société*, n°5, 1987, en ligne : < https://www.persee.fr/doc/dreso_0769-3362_1987_num_5_1_1567_t1_0140_0000_1 > (consulté le 20 déc. 2018)

DUPUY, P.-M., KERBRAT, Y., *Droit international public*, 11^e éd., Dalloz, Paris, 2012.

ELDEN, S., “*Mondialisation before Globalization*”, p. 80-93, dans Kanishka GOONEWARDENA (ed.), Stefan KIPFER (ed.), Richard MILGROM (ed.), Christian SCHMID (ed.), *Space, Difference, Everyday Life: Reading Henri Lefebvre*, Abingdon, Routledge, 2008, 344 p.

FURMSTON, M., TOLHURST, G., *Contract formation: law and practice*, Oxford, Oxford University Press, 2016.

GARAPON, A., LASSÈGUE, J., *Justice digitale*, Paris : Presses Universitaires France, 2018 (édition Kindle).

GAUTRAIS, V., *Réécrire l'écrit*, Mélanges en l'honneur du professeur Prujiner, Montréal : Éditions Yvon Blais, 2011.

HUBIN, J., POULLET, Y., *La sécurité informatique, entre technique et droit*, Namur, Centre de recherches informatique et droit, 1998.

KARIM, V., *Les obligations*, Montréal : Wilson & Lafleur, 2015.

LANGEVIN, L., VÉZINA, N., *Obligations et contrats*, Cowansville : Éditions Yvon Blais, 2017.

LELOUP, L., *Blockchain. La deuxième révolution numérique*, Montréal : Éditions Edito, 2017.

LESSIG, L., *Code: And Other Laws of Cyberspace*, Version 2.0, Basic Books, New York, 2006, en ligne : < <http://codev2.cc/download+remix/Lessig-Codev2.pdf> > (consulté le 10 janv. 2019)

LOIGNON, S., *Big Bang Blockchain. La seconde révolution d'internet*, Paris, Tallandier, 2017,

MONTESQUIEU, *De l'esprit des lois*, Paris, Garnier-Flammarion, 1979.

MOUGAYAR, W., *The Business Blockchain. Promise, practice, and application of the next Internet technology*, Hoboken, Wiley, 2016.

ROCHER, G., « La mondialisation: un phénomène pluriel », dans Daniel MERCURE, *Une société-monde? Les dynamiques sociales de la mondialisation*, Québec, 2001, en ligne : < <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/89/0046.pdf?sequence=1&isAllowed=y> > (consulté le 20 déc. 2018)

RODRIGUEZ, P., *La Révolution Blockchain : Algorithmes ou institutions, à qui donnerez-vous votre confiance ?* Paris : Dunod, 2017.

TANCELIN, M., *Des obligations en droit mixte du Québec*, Montréal : Wilson & Lafleur, 2009.

Articles de revue, de journaux et rapports

BARRAUD, B., *Répondre à la plurinormativité par l'internormativité : la corégulation de l'internet*, Les Cahiers de droit, Faculté de droit de l'Université Laval, 2018, en ligne : < <https://hal.archives-ouvertes.fr/hal-01527784> > (consulté le 19 déc. 2018)

BERMAN, P.S., *Le nouveau pluralisme juridique*, Revue internationale de droit économique, 2013, en ligne : < <https://www.cairn.info/revue-internationale-de-droit-economique-2013-1-page-229.htm> > (consulté le 20 déc. 2018)

CHEW, C.Y.C., *The Application of the Defence of Non Est Factum: an Exploration of its Limits and Boundaries*, University of Western Sydney Law Review, Editor Francine Feld, v. 13, 2009, (PDF), en ligne : < https://www.westernsydney.edu.au/_data/assets/pdf_file/0009/435573/UWS_2009LR09Vol13.pdf > (consulté le 12 janv. 2019)

CLEMENT, D., « Du mythe de la nécessité des brevets pour susciter l'innovation », Revue l'Économie politique, 2003, no 19, p. 9-24, en ligne: <<https://www.cairn.info/revue-l-economie-politique-2003-3-page-9.htm>> (consulté le 19 sept. 2018)

CONNELL, S., *Not my doctrine? Finding a Contract law explanation for Non est factum*, Victoria University of Wellington Law Review, 47, p. 245-265, 2016, (PDF), en ligne : < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3195011 > (consulté le 12 janv. 2019)

CONSTANTINESCO, V., « La souveraineté est-elle soluble dans l'Union européenne ? », p. 119-135, dans *L'Europe en formation : Revue d'études sur la construction européenne et le fédéralisme*, Centre international de formation européenne, n° 368, 2013.

EDWARDS, M.A., *The Alignment of Law and Norms: Of Mirrors, Bulwarks, and Pressure Valves*, FIU Law Review, FIU Law Library, vol. 10, n° 1, 2014, en ligne : < <https://bit.ly/2TwM6de> > (consulté le 28 déc. 2018)

FLÜCKIGER, A., *Pourquoi respectons-nous la soft law ?*, Revue européenne des sciences sociales, 2009, p. 73-103, en ligne : < <https://journals.openedition.org/ress/68#toc> > (consulté le 07 janv. 2019 et 18 fév. 2019)

GAUTRAIS, V., GINGRAS, P., « La preuve des documents technologiques », *Les Cahiers de propriété intellectuelle*, vol. 22, n. 2, en ligne (PDF) : < <https://cpi.openum.ca/files/sites/66/La-preuve-des-documents-technologiques.pdf> > (consulté le 19 déc. 2018)

GUILLAUME, G., SOLEDAD, Z., « La discrimination commerciale révélée comme mesure désagrégée de l'accès aux marchés », dans *l'Economie internationale*, 2002, n° 89-90, p. 261-280, en ligne : < <https://www.cairn.info/revue-economie-internationale-2002-1-page-261.htm> > (consulté le 12 déc. 2018)

HABERMAS, J., *Sur le droit et la démocratie*, Note pour un débat, Le Débat, 1997, n° 97, (PDF) en ligne : < <http://www.sietmanagement.fr/wp-content/uploads/2016/04/Habermas1997.pdf> > (consulté le 13 déc. 2018)

IMEM, A.A., « Comparison and Evaluation of Digital Signature Schemes Employed in NDN Network », *International Journal of Embedded Systems and Applications (IJESA)* vol. 5, n. 2, juin 2015, (PDF) en ligne : <<https://arxiv.org/pdf/1508.00184.pdf>> (consulté le 15 sept. 2018)

LE FORUM DES DROITS SUR L'INTERNET, *Rapport d'activité année 2009*, La documentation française, 2009, en ligne : <<https://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/104000464.pdf>> (consulté le 22 déc. 2018)

LESSIG, L., *Code Is Law: On Liberty in Cyberspace*, Harvard Magazine, janv-févr., 2000, en ligne : <<https://harvardmagazine.com/2000/01/code-is-law-html>> (consulté le 18 janv. 2019)

LIND, J., EYAL, I., KELBERT, F., NAOR, O., PIETZUCH, P., SIRER, E.G., « Teechain: Scalable Blockchain Payments using Trusted Execution Environments », *Cornell University Library*, (PDF) en ligne : <<https://arxiv.org/pdf/1707.05454.pdf>> (consulté le 18 nov. 2018)

MICHELL, P., *Illiteracy, Sophistication and Contract Law*, Queen's Law Journal, 31, 2005-2006, p. 327 en ligne : <https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/queen31&id=323&men_tab=srchresults> (consulté le 12 janv. 2019)

MIK, E., *Smart contracts: Terminology, technical limitations and real world complexity*, Law, Innovation and Technology, Research Collection of School of Law, Singapore, 2017, en ligne : <https://ink.library.smu.edu.sg/sol_research/2341> (consulté le 15 févr. 2019)

OST, F., VAN DE KERCHOVE, M., *De la pyramide au réseau ? : pour une théorie dialectique du droit*, Publications des Facultés universitaires Saint-Louis, Bruxelles, 2002, p. 14.

ROZARIO, R.M., VASARHELYI, M.A., « Auditing with Smart Contracts », *The International Journal of Digital Accounting Research*, vol. 18, 2018, (pdf) en ligne : <http://rabida.uhu.es/dspace/bitstream/handle/10272/14419/Auditing_with_Smart.pdf?sequence=2> (consulté le 08 sept. 2018)

SALEHABADI, A., *Une position unique en droit commercial international*, Journal du Barreau, Québec, v. 36, n° 16, 1^{er} oct. 2004, en ligne : < <https://www.barreau.qc.ca/pdf/journal/vol36/no16/position.html> > (consulté le 26 janv. 2019)

STANDARDS AUSTRALIA, *Roadmap for Blockchain Standards*, Report, mars 2017, en ligne : < <https://bit.ly/2TCWaBx> > (consulté le 15 févr. 2019)

Documents gouvernementaux

ALLARD, F., *La Cour suprême du Canada et son impact sur l'articulation du bijuridisme*, Ministère de la Justice du Canada, 2001, en ligne : < <https://www.justice.gc.ca/fra/pr-rp/sjc-csj/harmonization/hlf-hfl/f3-b3/bf3a.html#introduction> > (consulté le 10 janv. 2019).

AUTORITÉ FÉDÉRALE DE SURVEILLANCE DES MARCHÉS FINANCIERS (FINMA), *La FINMA publie un guide pratique sur les ICO*, 16 fév. 2018, en ligne : < <https://www.finma.ch/fr/news/2018/02/20180216-mm-ico-wegleitung/> > (consulté le 08 janv. 2019)

JOHNSON, G., POMORSKI, L., « Exposé sur les monnaies électroniques », *Banque du Canada*, 2 avril 2014, Ottawa, (PDF) en ligne : < https://www.banqueducanada.ca/wp-content/uploads/2014/04/discours_senat.pdf > (consulté le 26 oct. 2018)

LAW COMMISSION, *Smart Contracts*, en ligne: < <https://www.lawcom.gov.uk/project/smart-contracts/> > (consulté le 08 janv. 2019)

MINISTÈRE DE LA JUSTICE DU CANADA. *L'origine de notre système juridique*, 10 mars 2018, en ligne : < <https://www.justice.gc.ca/fra/pr-rp/pm-cp/just/03.html> > (consulté le 10 janv. 2019)

RETRAITE QUÉBEC, *Admissibilité à la rente d'invalidité*, en ligne : < https://www.rrq.gouv.qc.ca/fr/retraite/rrq/autres_rentes/Pages/admissibilite_ri.aspx > (consulté le 21 déc. 2018)

Documents internationaux

COMMISSION DES NATIONS UNIES POUR LE DROIT COMMERCIAL INTERNATIONAL, *Loi type de la CNUDCI sur l'arbitrage commercial international, 1985 avec les amendements adoptés en 2006*, < https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/fr/07-86999_ebook.pdf > (consulté le 25 janv. 2019)

_____, *Technical Notes on Online Dispute Resolution*, en ligne : < http://www.uncitral.org/pdf/english/texts/odr/V1700382_English_Technical_Notes_on_ODR.pdf > (consulté le 25 janv. 2019)

_____, *Loi type de la CNUDCI sur le commerce électronique et Guide pour son incorporation 1996 avec le nouvel article 5 bis tel qu'adopté en 1998*, en ligne : < http://www.uncitral.org/pdf/french/texts/electcom/05-89451_Ebook.pdf > (consulté le 25 janv. 2019)

_____, *Commerce électronique: loi type de la CNUDCI sur le commerce électronique (1996)*, en ligne : < https://uncitral.un.org/fr/texts/ecommerce/modellaw/electronic_commerce > (consulté le 25 janv. 2019)

ORGANISATION MONDIALE DU COMMERCE, *Données sur le commerce international et l'accès aux marchés*, 2017, en ligne : < <https://bit.ly/2Bfdao4> > (consulté le 12 déc. 2018)

UNIDROIT, *Model Clauses for the Use of the UNIDROIT. Principles of International Commercial Contracts*, Uniform Law Review, Oxford University Press, 18 oct. 2013, en ligne : < <https://academic.oup.com/ulr/article/18/3-4/630/1636799> > (consulté le 18 déc. 2019)

_____, *Principes d'Unidroit relatifs aux contrats du commerce international*, 2010, en ligne : < <http://www.gdr-elsj.eu/wp-content/uploads/2012/10/principes-unidroit-integralversionprinciples2010-f.pdf> > (consulté le 26 janv. 2019)

_____, *Principes d'Unidroit relatifs aux contrats du commerce international*, 2016, en ligne : < <https://www.unidroit.org/instruments/commercial-contracts/unidroit-principles-2016> > (consulté le 25 janv. 2019)

_____, *Workshop on the Use of Modern Technology for Dispute Resolution and Electronic Agreement Management Particularly Online Dispute Resolution*, William Brydie-Watson, Port Moresby, Papua New Guinea, 3-4 March 2018, International Institute for the Unification of Private Law Instruments that Facilitate the Use of Modern Technology for Contract Management, en ligne : < http://mddb.apec.org/Documents/2018/EC/WKSP2/18_ec_wksp2_008.pdf > (consulté le 27 janv. 2019).

EUROPEAN COMMITTEE FOR STANDARDIZATION (CEN) et EUROPEAN COMMITTEE FOR ELECTROTECHNICAL STANDARDIZATION (CENELEC), *Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies*, Torino, 2018, (PDF), en ligne : < https://www.gleif.org/content/1-about/7-consultation-responses/fg-bdlt-white_paper.pdf > (consulté le 08 janv. 2019)

ORGANISATION INTERNATIONALE DE NORMALISATION, *Strategic Business Plan ISO/TC 307, Blockchain and distributed ledger technologies*, 30 août 2018, en ligne : < https://isotc.iso.org/livelink/livelink/fetch/-17853836/17853838/17855344/ISO-TC307_N0326_ISO_TC_307_Strategic_Business_Plan.pdf?nodeid=19912672&vernum=-2 > (consulté le 07 janv. 2019)

_____, *Standards catalogue ISO/TC 307*, Blockchain and distributed ledger technologies, en ligne : < <https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0> > (consulté le 08 janv. 2019)

Glossaire

BLOCKCHAIN HUB, *Glossary*, « Turing completeness », en ligne : < <https://blockchainhub.net/blockchain-glossary/> > (consulté le 28 oct. 2018)

CANADA, *Juridictionnaire*, Travaux publics et services gouvernementaux Canada, Centre de traduction et de terminologie juridiques (CTTJ), Faculté de droit, Université de Moncton, en ligne : < https://www.btb.termiumplus.gc.ca/tpv2guides/guides/juridi/index-eng.html?lang=eng&lettr=indx_catlog_e&page=9BDkX3TldFmE.html > (consulté le 21 avril 2019)

GOUVERNEMENT DU QUÉBEC, OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Bibliothèque virtuelle*, « cryptographie asymétrique », en ligne : < <http://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/internet/fiches/8383537.html> > (consulté le 12 août 2018)

MONETARY AUTHORITY OF SINGAPORE, *Project Ubin: Central Bank Digital Money using Distributed Ledger Technology*, 11 nov. 2018, en ligne : < <http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/Project-Ubin.aspx> > (consulté le 15 nov. 2018)

Exposés

LAPOINTE, S., « La technologie des contrats intelligents », *Thomson Reuters Centre de développement professionnel au Canada*, Webinaire en rediffusion, Éditions Yvon Blais, 2018, en ligne :

<https://cpdcentre.ca/eyb/blocks/rtecomm_catalog/view.php?id=1797&lang=fr> (consulté le 14 nov. 2018)

Autres documents

ACCENTURE, *Editing the uneditable blockchain. Why distributed ledger technology must adapt to an imperfect world*, 2016, (PDF) en ligne :

<https://www.accenture.com/t20160927T033514Z_w_/ro-en/acnmedia/PDF-33/Accenture-Editing-Uneditable-Blockchain.pdf> (consulté le 15 nov. 2018)

ALEXANDRE, A., *Alibaba Files Patent for Blockchain System That Allows 'Administrative Intervention'*, 05 oct. 2018, en ligne : <<https://cointelegraph.com/news/alibaba-files-patent-for-blockchain-system-that-allows-administrative-intervention>>(consulté le 15 nov. 2018)

AMICHIA, M-D., *UtilityWise. La blockchain, une technologie au service du secteur de l'énergie*, 24 avril 2018, en ligne : <<https://www.utilitywise.fr/2018/04/24/la-blockchain-une-technologie-au-service-du-secteur-de-lenergie/>> (consulté le 29 oct. 2018)

ASSOCIATION QUÉBÉCOISE DES INFORMATIENNES ET INFORMATIENS INDÉPENDANTS, *Code d'éthique pour les membres de l'AQIII*, en ligne : < <https://www.aqiii.org/fr/membres/code-dethique/> > (consulté le 06 janv. 2019)

AUTORITÉS CANADIENNES EN VALEURS MOBILIÈRES, *Canadian Securities Regulators Outline Securities Law Requirements That May Apply to Cryptocurrency Offerings*, Toronto, 24 août

2017, en ligne : < <https://www.securities-administrators.ca/aboutcsa.aspx?id=1606> > (consulté le 08 janv. 2019)

BARLOW, J.P., *A Declaration of the Independence of Cyberspace*, Danvos, 8 fév. 1996, en ligne : <<https://www.eff.org/cyberspace-independence>> (consulté le 10 nov. 2018)

BERENDE, M., *The potential of blockchain. From flight-delay to agriculture insurance*, 23 mai 2018, en ligne : <<https://medium.com/impact-insurance/the-potential-of-blockchain-from-flight-delay-to-agriculture-insurance-eb774e8f8508>> (consulté le 16 nov. 2018)

BERNERS-LEE, T., *Tim Berners-Lee on the Web at 25. The past, present and future*, 23 août 2014, en ligne : <<https://www.wired.co.uk/article/tim-berners-lee>> (consulté le 18 nov. 2018)

BIJON, L., *SBI veut adopter la technologie Ripple à une plus grande échelle via le consortium R3*, oct. 2018, en ligne : < <https://www.placecrypto.fr/cryptos/sbi-veut-adopter-la-technologie-ripple-a-une-plus-grande-echelle-via-le-consortium-r3.html> > (consulté le 4 nov. 2018)

BITMEX RESEARCH, *The Ripple story*, 06 fév. 2018, en ligne : < <https://blog.bitmex.com/the-ripple-story/> > (consulté le 19 sept. 2018)

BITSHARES. *Delegated Proof of Stake*, en ligne : < <http://docs.bitshares.org/bitshares/dpos.html> > (consulté le 2 nov. 2018)

BLOCKCHAIN FRANCE, *Qu'est-ce que la blockchain ?*, 2016, en ligne : <<https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/>> (consulté le 28 oct. 2018)

BROOKS, S., *Incentivised Distributed Computation for Registered Digital Content Search*, juill. 2017, (PDF) en ligne: <<https://goo.gl/fE1xHK>> (consulté le 06 nov. 2018)

BUTERIN, V., *On Public and Private Blockchains*, 6 août 2015, en ligne :
<<https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>> (consulté le 2 nov. 2018)

BUTERIN, V., *Ethereum White Paper. A next generation smart contract & decentralized application platform*, nov. 2013, (PDF) en ligne :
<http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf> (consulté le 26 oct. 2018)

B3I, *The Blockchain Insurance Industry Initiative*, en ligne : <<https://b3i.tech/home.html>>
(consulté le 16 nov. 2018)

CHAMBER OF DIGITAL COMMERCE, *“Smart Contracts” Legal Primer*, 2018, Washington DC, (PDF) en ligne : <<https://digitalchamber.org/wp-content/uploads/2018/02/Smart-Contracts-Legal-Primer-02.01.2018.pdf>> (consulté le 13 déc. 2018)

CHAPMAN, J., GARRATT, R., HENDRY, S. MCCORMACK, A., et MCMAHON, W., « Projet Jasper. Les systèmes de paiement de gros décentralisés sont-ils aujourd’hui chose faisable ? », *Banque du Canada*, juin 2017, en ligne : <<https://www.banqueducanada.ca/wp-content/uploads/2017/05/rsf-juin-2017-chapman.pdf>> (consulté le 04 nov. 2018)

CHARPENTIER, E., *Les Principes d’Unidroit: une codification de la lex mercatoria?*. Les Cahiers de Droit, vol. 46, n. 1-2, mars-juin 2005, en ligne : <<https://bit.ly/2F86OYe>>
(consulté le 26 janv. 2019)

CLEMENTONI, G., *The Difference Between Blockchain and Fintech*, 17 juill. 2018, en ligne : <<https://www.e-zigurat.com/digital/the-difference-between-blockchain-and-fintech>> (consulté le 04 nov 2018)

CHOHAN, U. W., *What Is a Ricardian Contract?*, UNSW Business School, 2017, en ligne : < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3085682 > (consulté le 12 janv. 2019)

COMMISSION DES NATIONS UNIES POUR LE DROIT COMMERCIAL INTERNATIONAL (CNUDCI), *Accueil*, en ligne : < <https://uncitral.un.org/fr> > (consulté le 20 janv. 2019)

_____, *Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux*, Vienne, Commission des Nations Unies pour le droit commercial international, 2007, en ligne : < http://www.uncitral.org/pdf/french/texts/electcom/06-57453_Ebook.pdf > (consulté le 20 janv. 2019)

CONG, L. W., et HE, Z., *Blockchain Disruption and Smart Contracts*, 10 sept. 2018, (PDF) en ligne : < <https://goo.gl/EdDRvo> > (consulté le 19 oct. 2018)

CONJOULE, en ligne : < <http://conjoule.de/de> > (consulté le 5 nov. 2018)

COPELAND, C., et ZHONG, H., *Tangaroa: a Byzantine Fault Tolerant Raft*, 2014, (PDF) en ligne : < http://www.scs.stanford.edu/14au-cs244b/labs/projects/copeland_zhong.pdf > (consulté le 03 nov. 2018)

DAI, W., *B-Money*, 1999, en ligne : < <http://www.weidai.com/bmoney.txt> > (consulté le 18 sept. 2018)

DELLOITTE. *The future is here. Project Ubin. SGD on Distributed Ledger*, 2017, en ligne : < [http://www.mas.gov.sg/~media/ProjectUbin/Project Ubin SGD on Distributed Ledger.pdf](http://www.mas.gov.sg/~media/ProjectUbin/Project%20Ubin%20SGD%20on%20Distributed%20Ledger.pdf) > (consulté le 04 nov. 2018)

DEMOCRACY EARTH, *Introducing the Social Smart Contract*, 06 oct. 2017, en ligne : < <https://words.democracy.earth/introducing-the-social-smart-contract-8c7aa1d19682> > (consulté le 19 oct. 2018)

ELECTRICCHAIN, en ligne : < <https://www.electricchain.org/> > (consulté le 5 nov. 2018)

ENERCHAIN, *The Enerchain Project*, en ligne : < <https://enerchain.ponton.de/> > (consulte le 5 nov. 2018)

ETHEREUM. *Blockchain App Platform*, en ligne : < <https://www.ethereum.org/> > (consulté le 28 oct. 2018)

FAIFE, C., *The Authors of “Blockchain and the Law” Want You to Rethink the Internet*, 17 septembre 2018, en ligne : < <https://breakermag.com/the-authors-of-blockchain-and-the-law-want-you-to-rethink-the-internet/> > (consulté le 16 nov. 2018)

FRAZ FINANCE CENTRE DE FORMATION FINANCIÈRE, *Blockchain. L'assurance indicielle. Nouvelle assurance agricole pour l'Afrique*, 30 nov. 2017, en ligne : < <http://centre-de-formation-financiere.over-blog.com/2017/11/blockchain-l-assurance-indicielle-nouvelle-assurance-agricole-pour-l-afrique.html> > (consulté le 16 nov. 2018)

GENERAL CULTURE, *Comment un distributeur reconnaît-il les pièces que j'insère?*, 2012, en ligne : < <https://goo.gl/d9336j> > (consulté le 20 oct. 2018)

GITHUB, *The Raft Consensus Algorithm*, en ligne : < <https://raft.github.io/> > (consulté le 2 nov. 2018)

GONÇALVES, M. E., et GAMEIRO, M. I., *Project : the Landscape and Isobars of European Values in Relation to Science and New Technology. A Critical Discussion of Soft Law in a Governance Perspective*, Community Research and Development Information Service (CORDIS), European Commission, septembre 2011, en ligne : < https://www.researchgate.net/publication/319065378_A_critical_discussion_of_soft_law_in_a_governance_perspective_Work_package_4_Authors_Maria_Ines_Gameiro_Maria_Eduarda_Goncalves > (consulté le 06 janv. 2019)

GREEN ENERGY CORP, *Microgrid Overview*, en ligne :

<<http://www.greenenergycorp.com/about-us/about-us/technology/>> (consulté le 2 nov. 2018)

HASHCASH.ORG, *Hashcash*, en ligne : <<http://www.hashcash.org/>> (consulté le 15 nov. 2018)

HIGGINS, S., 3 Pre-Bitcoin Virtual Currencies That Bit the Dust, 30 nov. 2014, en ligne: <<https://www.coindesk.com/3-pre-bitcoin-virtual-currencies-bit-dust>> (consulté le 15 sept. 2018)

IRRERA, A., « Bank-backed R3 launches new version of its blockchain », *Reuters*, 3 oct. 2017, en ligne : <<https://www.reuters.com/article/us-r3-blockchain/bank-backed-r3-launches-new-version-of-its-blockchain-idUSKCN1C80MS>> (consulté le 2 nov. 2018)

_____, *Blockchain startup Ripple signs up PNC as a customer for its payment tech*, 19 sept. 2018, en ligne : <<https://goo.gl/4tW9Me>> (consulté le 04 nov. 2018)

KOWALESKI, M. R., *Ohio to consider information stored in a blockchain valid and legal in SB 300*, 21 juin 2018, en ligne : <<https://www.ohiocpa.com/search/utilities/displaynewsitem/2018/06/21/ohio-to-consider-information-stored-in-a-blockchain-valid-and-legal-in-sb-300>> (consulté le 10 janv. 2019)

LUU, L., CHU, D.H., OLICKEL, H., SAXENA, P., et HOBOR, A., *Making Smart Contracts Smarter*, Vienna, oct. 2016, (PDF) en ligne : <<https://eprint.iacr.org/2016/633.pdf>> (consulté le 14 nov. 2018)

MARKCC. *Paxos, a really beautiful protocol for distributed consensus*, 30 janv. 2015, en ligne : <<http://www.goodmath.org/blog/2015/01/30/paxos-a-really-beautiful-protocol-for-distributed-consensus>> (consulté le 2 nov. 2018)

MEKKI, M., *Blockchain : l'exemple des smart contracts – Entre innovation et precaution*, 2018, en ligne : < <https://lesconferences.openum.ca/files/sites/97/2018/05/Smart-contracts.pdf> > (consulté le 01 oct. 2019)

MOHAN, N., *Solidity Smart contract Security best practices*, 07 août 2017, en ligne : https://consensys.github.io/smart-contract-best-practices/known_attacks/> (consulté le 12 nov. 2018)

MONEGRAPH, *How it works*, en ligne : < <https://monegraph.com/> > (consulté le 5 nov. 2018)

MURCK, P., *Code as law?*, 5 juill. 2014, en ligne : < <http://virtuallylaw.com/code-as-law> > (consulté le 20 déc. 2018)

NAKAMOTO, S., *Bitcoin: A Peer-to-peer Electronic Cash System*, 2008, en ligne : <<https://bitcoin.org/bitcoin.pdf>> (consulté le 12 août 2018)

OLIVER WYMAN, ANTHEMIS GROUP AND SANTANDER INNOVENTURES, *The Fintech 2.0 Paper. Rebooting financial services*, 2015, (PDF) en ligne : <<http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf>> (consulté le 04 nov. 2018)

OYENTE, *An Analysis Tool for Smart Contracts*, en ligne : < <https://www.comp.nus.edu.sg/~loiluu/oyente.html> > (consulté le 15 nov. 2018)

PICARD, R., *Cadre juridique des technologies de l'information au Québec*, Réseau juridique du Québec, 2013, en ligne : < <https://www.avocat.qc.ca/affaires/iicadre-ti-quebec.htm> > (consulté le 18 déc. 2019)

PILLOU, J.F., *Algorithme de chiffrement RSA*, 17 sept. 2012, en ligne : <<https://www.commentcamarche.com/contents/208-algorithme-de-chiffrement-rsa>> (consulté le 13 août)

POULLET, Y., DINANT, J-M., *L'autodétermination informationnelle à l'ère de l'Internet*, Conseil de l'Europe, Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 18 nov. 2004, en ligne : < <https://rm.coe.int/16806ae51f> > (consulté le 20 fév. 2019).

POWERLEDGER, en ligne : < <https://www.powerledger.io/> > (consulté le 5 nov. 2018)

PRISCO, G., *The DAO raises more than \$117 million in world's largest crowdfunding to date*, 16 mai 2016, en ligne : < <https://bitcoinmagazine.com/articles/the-dao-raises-more-thanmillion-in-world-s-largest-crowdfunding-to-date-1463422191> > (consulté le 12 nov. 2018)

PROJET DECODE, en ligne : < www.decodeproject.eu/ > (consulté le 09 janv. 2019)

RINGELHEIM, J., *Droit, contexte et changement social*, Revue interdisciplinaire d'études juridiques, 2013, en ligne: < <https://www.cairn.info/revue-interdisciplinaire-d-etudes-juridiques-2013-1-page-157.htm> > (consulté le 26 déc. 2018)

RIPPLE, *Today's Payment Rails Don't Cut It*, en ligne : < <https://ripple.com/> > (consulté le 04 nov. 2018)

ROCHE, S., ZUNDEL, J., JACQUOT, F., KURTH, A., JOUIN, E., *Traduction du Livre Blanc Ethereum. Plateforme de contrats autonomes et d'applications décentralisées de nouvelle génération*, 09 nov. 2016, en ligne : < <http://www.asseth.fr/2016/11/09/traduction-whitepaper-ethereum/> > (consulté le 18 oct. 2018)

ROSSTANDART FEDERAL AGENCY ON TECHNICAL REGULATING AND METROLOGY. *ISO/TC 307 "Blockchain and distributed ledger technologies" session took place in Moscow*, 30 oct. 2018, Moscow, en ligne : < <https://bit.ly/2J9nx1o> > (consulté le 08 janv. 2019)

ROULAND, M., « La normalisation technique (instrument de concurrence à la loi) », dans Emmanuel CLAUDEL et Béatrice THULLIER (dir.), *Le droit mou : une concurrence faite à la*

loi, Paris, Centre de Droit civil des Affaires et du Contentieux Économique de l'Université de Paris X-Nanterre, 2004, (PDF) en ligne : < <http://www.glose.org/CEDCACE7.pdf> > (consulté le 06 janv. 2019)

SANDRE, A., *7 social media startups powered by blockchain*, 03 avril 2018, en ligne : <<https://hackernoon.com/6-social-media-powered-by-blockchain-fdc41d16cb12>> (consulté le 28 sept. 2018)

SWANSON, T., *Consensus-as-a-Service. A Brief Report on the Emergence of Permissioned, Distributed Systems*, 6 avril 2015, en ligne : <<http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf>> (consulté le 08 sept. 2018)

SZABO, N., *Smart Contracts: Building Blocks for Digital Markets*, 1996, en ligne: < <https://goo.gl/wQH4PX> > (consulté le 10 avril 2018)

_____, *Bit gold*, 08 décembre 2008, en ligne : <<http://unenumerated.blogspot.com/2005/12/bit-gold.html>> (consulté le 10 sept. 2018)

TERUZZI, D., *Combien ça coûterait une attaque 51% ?*, 11 février 2016, en ligne : <<http://blogchaincafe.com/combien-ca-couterait-une-attaque-51>> (consulté le 12 nov. 2018)

UJO, *Empowering music*, en ligne : < <https://ujomusic.com> > (consulté le 6 nov. 2018)

UNIBRIGHT.IO, *Blockchain evolution: from 1.0 to 4.0*, 7 déc. 2017, en ligne : < <https://medium.com/@UnibrightIO/blockchain-evolution-from-1-0-to-4-0-3fbdbccfc666> > (consulté le 26 oct. 2018)

VEREDICTUM, *Decentralised anti-piracy & content distribution platform*, 2015, en ligne : < <https://www.veredictum.io/> > (consulté le 6 nov. 2018)

WITTEBORG, N., *Les Principes d'UNIDROIT relatifs aux contrats du commerce international comme source de connaissance du droit*, Séminaire L'harmonisation du droit du contrat en Europe – 38^e séminaire commun des Facultés de Droit des Universités de Montpellier et Heidelberg, (PDF), en ligne : < <https://www.ipr.uni-heidelberg.de/md/jura/ipr/montpellier/vortraege/38witteborg.pdf> > (consulté le 25 janv. 2019)

ANNEXE I – CERTAINES APPLICATIONS DE LA CHAÎNE DE BLOCS

« Authentification des œuvres d’art (Verisart); microcontrats (Czam); carters prépayées (BuyAnyCoin); chaîne d’approvisionnement (Skuchain, ThingChain, Caravaggio, Cognizant, Consentio, Fluent, Kouvola Innovation, Modum, Open Trade Docs, Synechron, Zerado); digitalisation de contrats (Colu); lutte contre la contrefaçon (TheRealMcCoy, Chainlink, BlockVerify); gestion de diamants (Everledger); authentification de diplômes (Keeex, dipl.me); authentification de documents, preuves d’existence, preuve de propriété de contenus numériques (Ascribe, Artplus, blockai.com, blockness.io, bitproof.io, ChaiyLing, crypto Public Notary, factom.org, Keeex, proofofexistence.com, remember.io, Stampery); bases de données publiques (Mayor Chains); énergie renouvelable et économie de partage (TransActive Grid, powerledger.com, SolarCoin); cartes de fidélité (Ribbit.me); identités digitales (Onename, Trustatom, FollowMyVote); Internet alternatif (ZeroNet); Internet des objets (IOTA, beAchain, Adept, Filament, Hyperledger); jeux (Spells of Genesis, Voxelnauts); gestion de dossiers médicaux (BitHealth); musique (Ujo, Peertracks, BitTunes Music on the Blockchain); gestion de noms de domaines (Namecoin); paiement en ligne simple et sécurisé (Alipay); prêts entre particuliers (MoneyCircles); propriété intellectuelle (Blockness.io, Monegraph, Bitproof); bâtiments intelligents (L03 Energy, Enerchain, ElectricChain); stockage décentralisé (Storj, BigchainDB, Sia.tech); signature électronique (BlockSign); traçabilité (Blockness.io, Blockpharma, Provenance); transport de personnes (aeCar, la’Zooz); vote (Voatz, Belem, Neutral Voting Bloc, civicdApp.com, cryptovoter.com, v-initiative.org, followmyvote.com, unchain.voting) »²⁷¹.

²⁷¹ LELOUP, L., *Blockchain. La deuxième révolution numérique*, Montréal : Éditions Edito, 2017, p. 125-128