

Université de Montréal

La responsabilité civile des acteurs du contrat intelligent

par
Clémence Francès

Faculté de Droit

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de Maîtrise
en Droit des Technologies de l'Information (LL.M)

Août, 2019

© Clémence Francès, 2019

Résumé

Les contrats intelligents sont des programmes informatiques qui s'exécutent d'eux-mêmes dès lors que certaines conditions, déterminées au préalable par les parties, sont remplies. Ce type de contrat est récemment entré dans une nouvelle ère suite à la démocratisation des cryptomonnaies, notamment le Bitcoin et sa technologie sous-jacente ; la chaîne de blocs. Celle-ci se définit comme un registre virtuel répertoriant des historiques de transactions, permettant entre autres de réaliser des transferts d'actifs de pair à pair, sans intermédiaire. Désormais, la chaîne de blocs est aussi capable de servir de support au contrat intelligent, ce qui soulève de nouvelles problématiques juridiques.

En raison de sa nature, il est possible que le contrat intelligent puisse causer un préjudice en cas de mauvaise ou de non-exécution. Le présent mémoire consiste à déterminer l'applicabilité du régime de responsabilité civile à ce type de contrat, au regard des dispositions du *Code civil du Québec* et de la *Loi concernant le cadre juridique des technologies de l'information*.

Mots-clés : Chaîne de blocs – Contrats intelligents – Responsabilité – Dommage – Contrats – Intelligence artificielle

Abstract

Smart contracts are computer programs that run on their own when conditions, previously determined by the parties, are met. This type of contract has recently entered a new era following the democratization of cryptocurrencies, especially Bitcoin and its underlying technology; the Blockchain. It's a virtual register listing transaction history, making it possible, among other things, to carry out asset transfers from peer to peer without any intermediary. Now, the blockchain is also able to support smart contracts, which raises new legal issues.

Due to its nature, it is possible that the smart contract may cause damage in case of bad or non-performance. The purpose of this paper is to determine the applicability of the civil liability regime to this type of contract, in light of the provisions of the *Civil Code of Quebec* and the *Act to establish a legal framework for information technology*.

Keywords: Blockchain – Smart contract – Liability – Damage – Contracts – Artificial Intelligence

Table des matières

Résumé.....	i
Abstract.....	ii
Table des matières.....	iii
Liste des figures	v
Liste des sigles et abréviations.....	vi
Introduction.....	1
I. Le contrat intelligent.....	8
A. La formation du contrat intelligent	8
1. La chaîne de blocs : une technologie de stockage et de transmission d’informations ou de transactions.....	9
a. La construction d’une chaîne de blocs.....	11
b. Différents types et usages de la chaîne de blocs	17
2. Un contrat à exécution automatique	25
a. Définition et applications du contrat intelligent.....	26
b. Les apports de la chaîne de blocs au contrat intelligent sur le plan juridique	31
B. Les acteurs du contrat intelligent	37
1. Contrat intelligent et statut juridique	38
a. La qualification juridique du contrat intelligent	38
b. Réglementation et contrat intelligent.....	45
2. Les intervenants à la réalisation du contrat intelligent.....	50
a. Les principaux intervenants au contrat intelligent	50
b. L’Oracle : un frein à la décentralisation ?.....	59
II. Le partage de responsabilité en cas de mauvaise exécution d’un contrat intelligent.....	61
A. Dans le cas d’un dommage causé par une erreur survenue lors de la mise en place du contrat intelligent	63
1. L’engagement de la responsabilité des parties dans le contrat intelligent	64
a. L’exemple de la machine distributrice.....	64
b. La responsabilité des cocontractants du contrat intelligent	69
2. L’engagement de la responsabilité du programmeur ou de l’auditeur	72

a.	L'engagement de la responsabilité du programmeur dans le contrat intelligent ..	72
b.	Le cas d'un contrat intelligent validé par un auditeur.....	81
B.	Dans le cas d'un dommage causé par une erreur d'exécution du contrat intelligent....	84
1.	L'engagement de la responsabilité de l'oracle dans le contrat intelligent	85
a.	Dans le cas où l'oracle donne une information erronée.....	86
b.	Le cas d'une entente réalisée entre les parties et l'oracle	91
2.	Les solutions envisageables pour l'encadrement juridique du contrat intelligent	94
a.	Vers quel type de réglementation pour le contrat intelligent ?	95
b.	La solution de l'ajout de clauses contractuelles dans le contrat intelligent	96
	Conclusion	99
	Bibliographie.....	104
	Table de la jurisprudence	110
	Table de la législation	112

Liste des figures

Figure 1.	Le processus d'envoi d'une transaction via la chaine de blocs	12
Figure 2.	La formation d'une chaine de blocs.....	15
Figure 3.	Arbre de décision entre les différents types de chaines de blocs.....	21
Figure 4.	Plusieurs applications décentralisées sur une plateforme Ethereum.....	24
Figure 5.	Exemple de codage simplifié d'un contrat de vote sur le logiciel EtherScripter..	53
Figure 6.	Schéma simplifié d'un contrat intelligent dans le cas d'un testament	57
Figure 7.	L'exemple de la machine distributrice en tant que contrat intelligent.....	65
Figure 8.	Exemple d'une procédure d'audit intégrée au contrat intelligent.....	82

Liste des sigles et abréviations

Termes relatifs à la législation et à la réglementation :

al. : Alinéa

art. : Article

C.c.Q. : Code civil du Québec

etc. : Et cætera

L.C. : Lois du Canada (depuis 1987)

L.C.C.J.T.I. : Loi concernant le cadre juridique des technologies de l'information

L.Q. : Lois du Québec (depuis 1969)

L.R.C. : Lois révisées du Canada (depuis 1985)

L.R.Q. : Lois refondues du Québec (depuis 1977)

no. : Numéro

R.G.P.D. : Règlement général sur la protection des données

U.E. : Union Européenne

Termes relatifs à la jurisprudence :

C.A. : Cour d'appel (du Québec)

C.Q. : Cour du Québec

C.S. : Cour supérieure

QCCA : Cour d'appel du Québec

QCCQ : Cour du Québec

QCCS : Cour supérieure du Québec

R.C.S. : Recueils de la Cour suprême du Canada

R.D.I. : Recueils de droit immobilier

R.R.A. : Recueils de droit en responsabilité et assurance

Revues juridiques et technologiques :

C.P.I. : Cahiers de propriété intellectuelle

R. de J. : Revue de jurisprudence

R. du B. : Revue du barreau du Québec

R.D.J. : Revue de droit juridique

R.J.T. : Revue juridique Thémis

R.L.D.I : Revue Lamy droit de l'immatériel

SSRN Electronic Journal : Social Science Research Network Electronic Journal

Termes relatifs aux technologies de l'information :

D.A.p.p. : Data Acquisition and Processing Program

D.L.T. : Distributed Ledger Technology

I.C.O. : Initial Coin Offering

Autres termes :

I.S.D.A. : International Swaps and Derivates Associations

I.R.D.A.: Institut de recherche de droit des affaires

Introduction

La technologie de la chaîne de blocs¹ suscite depuis quelques années une grande curiosité, que ce soit par les particuliers, les entreprises, ou encore les États. Si elle est parfois présentée comme « la machine de confiance qui, au-delà du Bitcoin, pourrait changer le monde »², d'autres l'envisagent au mieux comme un effet de mode ou au pire comme un « grand mensonge »³.

Aujourd'hui la confiance présente dans les transactions entre acteurs repose principalement sur un système centralisé. En effet les acteurs placent leur confiance dans une entité reconnue par tous (le notaire, l'État, une institution bancaire, etc). Le tiers de confiance choisi par les acteurs est alors le seul à pouvoir modifier ou mettre à jour le registre de transactions qu'il détient afin de garantir la sécurité et limiter la fraude⁴. Avec l'apparition des monnaies virtuelles⁵, on a constaté que le règlement des transactions pouvait se faire de manière décentralisée, et ce grâce à la technologie de la chaîne de blocs. Comme le mentionne Drescher dans son ouvrage⁶, ce qui suscite l'intérêt grandissant pour la chaîne de blocs, c'est cette possibilité de désintermédiation des transactions :

« The relation between purely distributed peer-to-peer systems to the blockchain is that the former uses the latter as a tool to achieve and maintain integrity. Hence, the argument that explains the excitement about and the potential of the blockchain is: Purely distributed

¹ La chaîne de blocs est définie par l'institut Blockchain France comme « une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle ». Définition disponible sur le site <https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/>. Les auteurs utilisent communément la traduction anglaise « blockchain » pour désigner cette technologie. Dans ce travail, nous utiliserons le terme de « chaîne de blocs ».

² The Economist, « The Trust Machine, How the technology behind bitcoin could change the world », 31 octobre, 6 novembre 2015, n° 44.

³ Nouriel NOURIBI, « Le grand mensonge de la blockchain », Project Syndicate, 15 octobre 2018

⁴ Côme BERBAIN, « La blockchain : concept, technologies, acteurs et usages », *Annales des Mines - Realites industrielles* Août 2017, n° 3 (26 juillet 2017): 6-9.

⁵ Communément appelées aussi « crypto monnaies » : Bitcoin, Ethereum, Ripple, Litecoin, Dash, etc.

⁶ Daniel DRESCHER, *Blockchain basics*. Berkeley, CA : Apress, 2017.

peer-to-peer systems have a huge commercial potential as they can replace centralized systems and change whole industries due to disintermediation. »⁷

La première utilisation d'une chaîne de blocs, et aujourd'hui la plus connue, est apparue en 2009 avec la cryptomonnaie Bitcoin⁸. Connus sous le pseudonyme de Satoshi Nakamoto⁹, le ou les initiateurs de ce réseau avaient pour intention de créer une monnaie qui puisse contourner le système bancaire et plus largement le domaine financier qui avait perdu en crédibilité depuis la crise financière de deux mille huit¹⁰ dans le but de contourner le problème de la double dépense comme le mentionne son créateur lors de la description de son invention¹¹ :

« What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. » - Satoshi Nakamoto.

Cette cryptomonnaie repose sur un système de transactions enregistrées sur un grand livre de compte accessibles à tous sur le réseau : une chaîne de blocs. Pour utiliser ce réseau, il suffit pour un utilisateur d'accéder à un logiciel, de se créer un compte, et d'échanger sa monnaie traditionnelles (dollars, euros ou autres) contre des bitcoins afin de pouvoir commencer les transactions¹². Il peut conserver ou utiliser ses bitcoins à partir d'une « adresse », c'est-à-dire une chaîne de caractères qui correspond en quelque sorte à un numéro de compte, auquel sont associés une clé privée qui permet à son détenteur de dépenser les bitcoins, et une clé publique

⁷ Ibid.

⁸ « Unité monétaire d'un système de paiement virtuel permettant à une communauté d'utilisateurs d'échanger entre eux des biens et des services sur Internet » <https://www.larousse.fr/dictionnaires/francais/bitcoin/10911016>

⁹ Consulter le site https://fr.wikipedia.org/wiki/Satoshi_Nakamoto

¹⁰ Consulter le site <https://www.thecanadianencyclopedia.ca/fr/article/recession-of-200809-in-canada>

¹¹ Satoshi NAKAMOTO, « Bitcoin : A Peer-to-Peer Electronic Cash System ». En ligne : <https://bitcoin.org/bitcoin.pdf>

¹² Pierre-Henri FAURE, « Le bitcoin peut-il être assimilé à une monnaie ? Un examen à partir des différentes grilles de lecture de la science économique » (2016), <https://hal.archives-ouvertes.fr/hal-01337694>.

destinée à recevoir des paiements¹³. Une fois la transaction validée par l'ensemble du réseau à l'aide de la résolution de calculs cryptographiques complexes, elle est ajoutée sur la chaîne de blocs.

A ses débuts, la chaîne de blocs était uniquement considérée comme la technologie supportant le réseau bitcoin¹⁴ mais il ne fallut que très peu de temps pour voir évoluer la chaîne de blocs vers d'autres utilisations que les cryptomonnaies, tel que le stockage sécurisé de dossiers sensibles, ou encore la création de contrats intelligents, notamment à l'aide de la plateforme Ethereum ; une autre cryptomonnaie permettant, en plus du transfert d'actifs, de mettre en place ce nouveau type de contrats. C'est précisément sur cette forme d'utilisation de la chaîne de blocs, à savoir la création de contrats intelligents, que ce mémoire portera.

En 1997, le cryptographe américain Nick Szabo publiait un article intitulé « *The idea of Smart Contracts* »¹⁵ où il développait l'idée des contrats intelligents, à savoir des clauses contractuelles traduites dans des programmes informatiques. Pour expliquer son idée, il donne l'exemple de la machine distributrice ; un contrat qui s'exécute de façon automatisée et sans intermédiaire¹⁶. En effet, nous verrons que la machine distributrice est un contrat intelligent. Pour reprendre la définition officielle de l'entité Blockchain Partner, une société de conseil et de recherche sur les technologies de la chaîne de blocs, les contrats intelligents sont :

« Des programmes autonomes qui, une fois démarrés, exécutent automatiquement des conditions définies au préalable et inscrites dans la chaîne de blocs. Ils fonctionnent comme toute instruction conditionnelle de type « if – then » (si telle condition est vérifiée, alors telle conséquence s'exécute) »¹⁷.

¹³ En consultation sur le site <https://bitcoin.fr/Qu-est-ce-que-Bitcoin/>

¹⁴ Ce site monte le réseau bitcoin en temps réel : <https://www.blockchain.com/explorer>

¹⁵ Nick SZABO, "The idea of smart contracts". Nick Szabo's Papers and Concise Tutorials, 1997, vol. 6.

¹⁶ Ibid.

¹⁷ Définition issue du site officiel de l'entité Blockchain Partner : <https://blockchainfrance.net/nos-experts-blockchain/>

Dans notre quotidien nous contractualisons sans même nous en rendre compte. Cette technologie permet aux cocontractants de réaliser des transactions de façon anonyme s'ils le souhaitent et sans intermédiaire¹⁸. Un contrat intelligent peut être enregistré sur une chaîne de blocs, ce qui permet de rendre non modifiable le contrat (du moins plus difficilement), et les termes du contrat sont alors protégés selon le système de vérification intrinsèque à la chaîne de blocs¹⁹ comme nous le verrons ci-après²⁰. Ainsi, mettre en place des contrats intelligents pourrait réduire le risque de fraude, les coûts d'exécution et de suivi, mais surtout en faciliter l'exécution puisque celle-ci devient entièrement autonome. En effet, l'automatisation constitue l'une des forces de ce type de contrat puisqu'elle permet de limiter le risque d'erreur humaine dans l'exécution des clauses contractuelles, et donc limiterait le risque de contentieux. Aussi, la résiliation d'un contrat intelligent reposant sur la chaîne de blocs est théoriquement impossible, sauf si le motif de rupture a été préalablement envisagé et codifié dans le contrat ; ce qui permet de limiter les révocations injustifiées. Cependant, comme toute autre technologie, celle-ci n'est pas parfaite et nous verrons qu'elle présente certaines failles. Par exemple, la difficile résiliation présentée comme un avantage pour certains, sera considérée comme un inconvénient, notamment si les parties souhaitent modifier les termes du contrat.

Aux États-Unis, certains états²¹ ont récemment choisi d'adopter quelques dispositions légales pour le contrat intelligent. Par exemple l'art. 47-10-201 al. 2 du Tennessee Code²² définit le « smart contract » comme :

¹⁸ Alexander SAVELYEV, « Contract Law 2.0: “Smart” Contracts as the Beginning of the End of Classic Contract Law », (2017)

¹⁹ Vincenzo MORABITO, « Smart Contracts and Licensing », dans *Business Innovation Through Blockchain*, Springer International Publishing AG 2017, c. 6, p. 121.

²⁰ Se référer au paragraphe 1.a de la première partie : la construction d'une chaîne de blocs.

²¹ Notamment le Tennessee, l'Arizona, l'Ohio.

²² Tenn. Code Ann. § 47-10-201 (Lexis Advance through the 2018 Regular Session)

« An event-driven computer program, that executes on an electronic, distributed, decentralized, shared, and replicated ledger that is used to automate transactions, including, but not limited to, transactions that: (A) Take custody over and instruct transfer of assets on that ledger; (B) Create and distribute electronic assets; (C) Synchronize information; or (D) Manage identity and user access to software applications. ».

Ce qui rend ce type de contrat intelligent innovant et différent de la machine distributrice que mentionne Nick Szabo²³, c'est que les cocontractants peuvent user de la technologie de la chaîne de blocs pour tenter de rendre le contrat plus sécurisé et non modifiable. En effet, nous verrons dans ce mémoire que certains contrats intelligents utilisent la cryptographie via la chaîne de blocs, d'autres non²⁴. Dans certains cas, pour s'exécuter, le contrat intelligent aura besoin d'intégrer une variable externe et les répercussions de son exécution sera implémenté à la chaîne de blocs. Dans l'exemple d'un contrat intelligent programmé pour mettre en place une assurance en cas de retard d'avion, le contrat aura besoin d'aller chercher la variable externe qui déclenchera le contrat, à savoir les horaires d'arrivées sur le site officiel de la compagnie aérienne concernée ; c'est le rôle de l'oracle qui intégrera l'information extérieure à la chaîne de blocs et permettra au contrat, lié à cette dernière, de s'exécuter²⁵. Nous y reviendrons lorsque nous aborderons les différents intermédiaires dans le contrat intelligent.

L'avènement de la technologie de la chaîne de blocs et des registres distribués a mis en lumière les opportunités que peuvent apporter les contrats intelligents. Nous prenons le parti de traiter principalement, dans ce mémoire, des contrats intelligents qui reposent sur une chaîne de blocs car ils sont une réalité qui soulève de nouvelles questions juridiques que les contrats intelligents classiques ne posaient pas. Comme le font remarquer Wright et De Filippi, les utilisations du contrat intelligent ne cessent d'évoluer :

²³ Nick SZABO, préc.. note 15

²⁴ Cette distinction est expliquée en partie I. À noter que nous évoquerons exclusivement les contrats intelligents utilisant la cryptographie, à la différence des contrats intelligents classiques tels que la machine distributrice.

²⁵ ANTONOPOULOS, Andreas M. et WOOD, Gavin. "Mastering ethereum: building smart contracts and dapps." O'Reilly Media, 2018.

« To date, smart contracts have mostly been created to automatically execute derivatives, futures, swaps, and options. Yet, they are also being used to facilitate the sale of goods between unrelated people on the Internet without the need for a centralized organization. »²⁶

Au regard de l'émergence considérable de ce type de technologie de plus en plus complexe et pouvant prendre des décisions autonomes, les tribunaux ne se sont pas encore positionnés sur la question de savoir s'il devient nécessaire, en cas de dommage causé, de faire évoluer le droit ou s'il est possible de l'appliquer en l'état. En effet, en cas de litige concernant un contrat traditionnel, les juges se tournent normalement vers les clauses inscrites dans le contrat. Or dans un contrat intelligent, ces clauses sont écrites sous la forme de données numériques. Dans sa décision, le juge doit non seulement prendre en compte les composantes purement technologiques du contrat, mais aussi déterminer les principes du droit applicables au cas d'espèce. Pour les juges, l'un des principaux défis à relever est la question de la responsabilité lorsque la chaîne de blocs ou un contrat intelligent est impliqué. Leur caractère décentralisé, c'est-à-dire sans intermédiaire ni gouvernance, soulève la question de savoir à qui revient la responsabilité en cas de litige. À première vue, puisqu'une multitude d'agents ont le contrôle de la chaîne de blocs, personne ne peut être tenu responsable, ce qui constitue une position juridique difficilement tenable.

Notre étude consistera, dans un premier temps, à définir le contrat intelligent ainsi que la chaîne de blocs, technologie sur laquelle celui-ci peut être implémenté. Dans un second temps, nous nous pencherons exclusivement sur les principes de responsabilité civile applicables aux cas de dommages causés par la mauvaise exécution ou l'inexécution d'un contrat intelligent. En effet, plusieurs acteurs peuvent prendre part à l'élaboration d'un contrat intelligent : les parties contractantes, le programmeur, l'auditeur, l'oracle, les avocats²⁷, etc. Cette énumération non

²⁶Aaron WRIGHT et Primavera DE FILIPPI, « Decentralized Blockchain Technology and the Rise of Lex Cryptographia », SSRN Electronic Journal, 2015, <https://doi.org/10.2139/ssrn.2580664>. À noter que le terme de « registre décentralisé » est utilisé pour la chaîne de blocs dans le sens où les données échangées ne transitent pas par une seule entité ou ordinateur central et sont enregistrées dans des blocs stockés au sein d'une chaîne.

²⁷ Nous ne mentionnerons pas la responsabilité des avocats dans ce mémoire car le droit positif relatif à la responsabilité professionnelle s'appliquera en cas de manquement.

exhaustive constitue les intermédiaires susceptibles d'être responsables d'un préjudice subi par un cocontractant ou un tiers dans le cadre d'un contrat intelligent.

Dans un premier temps nous présenterons les technologies de la chaîne de blocs et du contrat intelligent (lorsqu'il est associé à cette dernière) dans leur aspect technique. Puis nous déterminerons le droit applicable au Québec au regard du *Code civil du Québec* et de la *Loi concernant le cadre juridique des technologies de l'information*. Pour cela, l'émission de différentes hypothèses permettra répondre à la question de savoir si, à défaut d'un cadre juridique clairement établi au sujet des contrats intelligents, le droit positif serait applicable en termes de responsabilité des intermédiaires participants à l'élaboration du contrat intelligent.

I. Le contrat intelligent

Les chaînes de blocs et les contrats intelligents ne sont que le résultat de l'évolution de technologies préexistantes. Si la chaîne de blocs a pris son essor en partie grâce à la monnaie numérique bitcoin²⁸, elle est aujourd'hui envisagée par les entreprises, les États, ou même les particuliers, pour d'autres utilisations que le transfert d'actifs comme, par exemple, la traçabilité de produits alimentaires²⁹. Le contrat intelligent³⁰, et la possibilité d'intégration de ses répercussions sur une chaîne de blocs, permet de créer des programmes autonomes qui exécutent les termes d'un contrat, sans nécessiter d'intervention humaine une fois déclenchés³¹. Afin de mieux cerner le contexte dans lequel ceux-ci évoluent, il semble nécessaire, dans les cas où les parties décident d'associer le contrat intelligent à une chaîne de blocs, de connaître le fonctionnement et les apports de cette nouvelle technologie aux contrats intelligents. Nous identifierons ensuite les acteurs intervenants dans l'élaboration d'un contrat intelligent et nous intéresserons à sa formation pour connaître les enjeux technologiques et juridiques que l'utilisation du contrat intelligent implique, notamment en termes de responsabilité.

A. La formation du contrat intelligent

C'est en grande partie en raison de la popularité du réseau Bitcoin que la chaîne de blocs³², technologie de stockage et de transmission d'informations ou de transactions³³, s'est faite

²⁸ Satoshi NAKAMOTO, préc., note 11

²⁹ Le géant de la distribution Walmart aux États-Unis, a décidé d'assurer, d'ici septembre 2019, la traçabilité des fruits et légumes avec l'aide de la technologie blockchain. Plus de précisions en ligne sur le site <https://www.placecrypto.fr/blockchain/walmart-mise-sur-la-blockchain-pour-ameliorer-la-tracabilite-des-fruits-et-legumes-10972/>

³⁰ Le terme anglophone de « *Smart Contract* » est aussi souvent utilisé par les auteurs pour décrire cette technologie.

³¹ Consulter le site <https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/>

³² Pour rappel, la chaîne de blocs est une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle (définition de l'Institut Blockchain France).

³³ Côme BERBAIN, « La blockchain : concept, technologies, acteurs et usages », *Annales des Mines - Réalités industrielles* Août 2017, no 3 (26 juillet 2017): 6-9.

connaître. Rappelons que celle-ci ne se limite pourtant pas à la transaction monétaire, et peut aussi servir d'infrastructure pour les contrats intelligents. Afin de mieux envisager les problématiques nouvelles que soulève ce type de contrat lorsque lié à une chaîne de blocs, nous décrirons les enjeux qu'apportent la chaîne de blocs au contrat intelligent, puis nous verrons en quoi cette technologie offre une plateforme intéressante pour le contrat intelligent et quelles en sont les limites associées.

1. La chaîne de blocs : une technologie de stockage et de transmission d'informations ou de transactions

La chaîne de blocs est assimilée à un registre³⁴, répertoriant un historique de transactions ou d'informations, de façon transparente, sécuritaire, et dans plusieurs cas, accessible à tous³⁵. Les transactions sont validées puis enregistrées sous forme de blocs, qui se lient les uns et autres chronologiquement³⁶. Bien qu'elle soit présentée par certains comme une « révolution blockchain »³⁷, on s'aperçoit que cette technologie n'est pas parfaite et soulève plusieurs questions, aussi bien sur le plan technique que juridique³⁸. Afin de mieux comprendre les enjeux et les débats que soulèvent actuellement la technologie de la chaîne de blocs, il est important de comprendre pourquoi certains auteurs³⁹ sont si réfractaires à cette technologie.

³⁴ Souvent mentionné par les auteurs par le terme de « *ledger* » en anglais.

³⁵ Nous verrons qu'il existe trois différents types de chaînes de blocs (privée, publique et de consortium) et que c'est dans le cadre de l'utilisation d'une chaîne de blocs publique que les données sont accessibles à tous.

³⁶ SILLABER, Christian et WALTL, Bernhard. *Life cycle of smart contracts in blockchain ecosystems*, 2017, vol. 41, no 8, p. 497-500.

³⁷ Philippe RODRIGUEZ, "La révolution blockchain: algorithmes ou institutions, à qui donnerez-vous votre confiance?", 2017.

³⁸ Plusieurs questions sont mises en avant, tant sur l'impact écologique de la chaîne de blocs, que sur la protection des données personnelles, ou l'identité numérique.

³⁹ Notamment au regard de l'inaltérabilité de certains contenus ; VOGEL, Nick. « The Great Decentralization: How Web 3.0 Will Weaken » Copyrights. *J. Marshall Rev. Intell. Prop. L.*, 2015, vol. 15, p. 136.

Sur le plan juridique, pour Primavera de Filippi⁴⁰, la chaîne de blocs soulève des questions de responsabilité et de régulation face à ces nouvelles organisations décentralisées qui sont gérées de façon autonome par les individus. En effet, qui est responsable dans le cadre d'une organisation qui n'a pas d'administrateur⁴¹? Nous verrons que la chaîne de blocs rend plus difficile l'attribution des responsabilités en raison de l'anonymat de ses utilisateurs, mais complique aussi le blocage des opérations en raison de son fonctionnement autonome.

Ensuite, il est certain que, sur le plan écologique, la chaîne de blocs a encore des progrès à faire. Par exemple, la cryptomonnaie Bitcoin, dont le cours ne cesse d'augmenter depuis sa création⁴², est pilotée par un algorithme qui s'appuie sur un réseau mondial d'ordinateurs archivant l'intégralité des transactions réalisées, ce qui nécessite l'utilisation simultanée de milliers d'ordinateurs et crée une consommation accrue d'électricité dans le monde⁴³.

Aussi, certains évoquent que techniquement la chaîne de blocs ne serait pas capable de faire face à une augmentation massive de son nombre d'utilisateurs. À titre de comparaison, la plateforme Ethereum⁴⁴ est aujourd'hui capable de traiter environ 15 transactions par seconde, tandis que l'opérateur Visa est capable d'en traiter 45 000 à la seconde. Au-delà du problème de rapidité de transaction, au fur et à mesure qu'elle est utilisée par le plus grand nombre, la chaîne de blocs nécessite une puissance de calcul qui croît au fil du temps. Jusqu'où la chaîne de blocs pourra supporter cette augmentation, et surtout à quel coût ? L'entreprise Bitfury⁴⁵, basée à Amsterdam, réputée pour le développement et la délivrance de matériel de minage pour

⁴⁰ Propos tenus par Primavera DE FILIPPI, chercheuse au CNRS et à l'université d'Harvard, lors de la conférence « Big Bang Blockchain » organisée par l'Institut Blockchain France le 14 février 2016. Consultation en ligne sur le site https://blockchainfrance.net/2016/02/14/droit_blockchain_contrats/

⁴¹ Cette question sera abordée en deuxième partie de ce mémoire avec la notion de gardien en responsabilité civile.

⁴² Pour information, aujourd'hui 1 Bitcoin vaut 13581 \$CAD (en date du 21 août 2019). Consultation en ligne de l'évolution du cours du Bitcoin sur <https://www.coingecko.com/fr/pièces/bitcoin/cad>

⁴³ A ce propos consulter l'article « L'impact écologique désastreux du Bitcoin », Le point, publié le 29/11/2017. Disponible en ligne sur https://www.lepoint.fr/argent/l-impact-ecologique-desastreux-du-bitcoin-29-11-2017-2176015_29.php

⁴⁴ Cette plateforme permet de créer et de gérer des contrats intelligents. Son utilisation et son fonctionnement seront abordés plus loin dans ce mémoire.

⁴⁵ Consultation du site officiel de l'entreprise Bitfury disponible sur <https://bitfury.com/about>

travailler avec la chaîne de blocs de Bitcoin, rappelle à ce titre que « si on prend en compte l'électricité, l'équipement et les centres de données, au total la "blockchain" publique du bitcoin coûte dans les 400 millions d'euros par an ». S'il est clair que la chaîne de blocs peut encore largement évoluer pour corriger ces quelques aspects négatifs, il n'en reste pas moins qu'elle est une technologie grandissante, qui ne cesse d'acquérir de nouveaux utilisateurs, et à l'origine de diverses avancées technologiques touchant divers secteurs d'activités⁴⁶.

a. La construction d'une chaîne de blocs

La chaîne de blocs est avant tout un outil de désintermédiation qui propose aux participants du réseau poste-à-poste de vérifier eux-mêmes les transactions⁴⁷.

Comprendre la construction d'une chaîne de blocs dans son aspect plus technique permet d'en définir les usages afin de pouvoir analyser ensuite en quoi les contrats intelligents et une chaîne de blocs peuvent être liés dans certains cas.

i- La chaîne de blocs, un registre décentralisé

L'institut Blockchain France définit la chaîne de blocs comme « une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle »⁴⁸. A première vue, cette définition ne semble pas apporter une grande nouveauté à ce qui existe déjà en termes de stockage et de transmission d'information. La nouveauté réside dans le fait de pouvoir transférer des informations ou des actifs, sans « organe central de

⁴⁶ Par exemple dans le secteur de la musique, la chaîne de blocs permet de supprimer les intermédiaires et ainsi rémunérer directement les artistes et réduire les coûts. Autre exemple, dans les chaînes de productions alimentaires, la chaîne de blocs est utilisée pour assurer une meilleure traçabilité des aliments. Consulter le site <https://medium.com/@matteozago/50-examples-of-how-blockchains-are-taking-over-the-world-4276bf488a4b> qui réfère aux différents secteurs qui utilisent la chaîne de blocs.

⁴⁷ Satoshi NAKAMOTO, et al. "Bitcoin: A peer-to-peer electronic cash system." 2008.

⁴⁸ <https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/>

contrôle », c'est-à-dire sans l'intermédiaire des banques, de l'État, des notaires ou des plateformes internet. Le schéma ci-dessous démontre comment une transaction peut être réalisée sans intermédiaire.

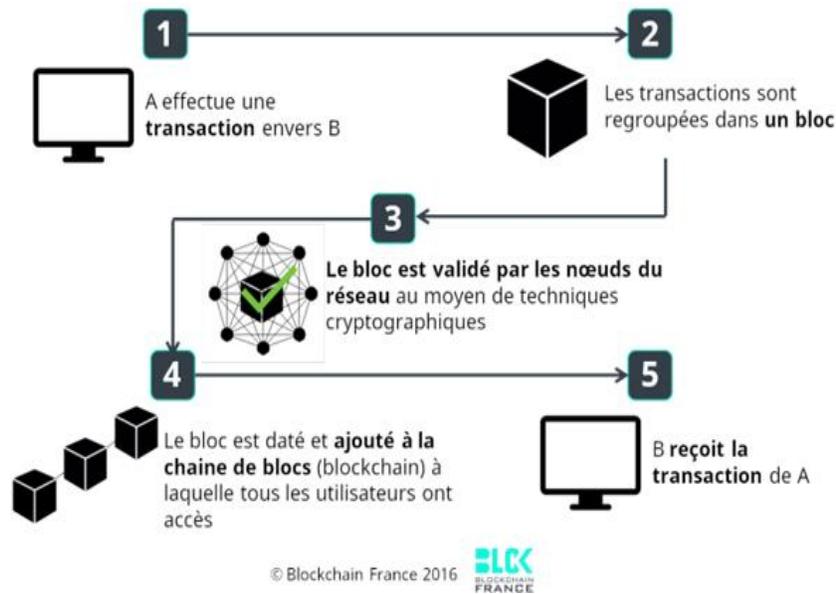


Figure 1. Le processus d'envoi d'une transaction via la chaîne de blocs⁴⁹

Dans un premier temps, les transactions réalisées sur le réseau par les utilisateurs sont regroupées par blocs de façon chronologique. Un bloc contient plusieurs informations, à savoir la signature du propriétaire, les informations de la dernière transaction, le moment de la création du bloc (on parle d'horodatage⁵⁰), et la clé publique du destinataire⁵¹. Chaque bloc est validé par les « nœuds du réseau » selon la résolution de problèmes algorithmiques⁵², puis ajouté à la chaîne de blocs et visible par tous⁵³.

⁴⁹ Source : Institut Blockchain France, 2016. En ligne : <https://blockchainfrance.net/>

⁵⁰ Se référer aux explications ci-après concernant cette notion.

⁵¹ Satoshi NAKAMOTO, et al. préc., note 47

⁵² Les termes de « nœuds du réseau » et « problèmes algorithmiques » sont explicités ci-après.

⁵³ Blockchain France, en ligne : <https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/>

Aujourd'hui, les intermédiaires tels que l'État, les notaires, les avocats, les banques et bien d'autres encore, sont au cœur de nos transactions réalisées quotidiennement, et pourtant ils ne font pas tous l'unanimité, notamment en termes de coûts. En effet, nous sommes dans une société qui se veut de plus en plus individualiste et rapide, où le traitement des transactions et leurs coûts parfois excessifs⁵⁴ freinent de nombreux utilisateurs. Le défi de la chaîne de blocs est de continuer à réaliser ces transactions, en créant la confiance que les intermédiaires produisent aujourd'hui, tout en supprimant leur intervention. La chaîne de blocs permet alors de s'échanger de la valeur de pair à pair, sans intermédiaire. La notion de registre distribué des transactions est souvent utilisée pour décrire la chaîne de blocs mais celle-ci n'est en fait qu'une de ses propriétés⁵⁵. En effet, la technologie de la chaîne de blocs correspond à un type particulier de registre distribué⁵⁶. Par définition, un registre distribué est une base de données décentralisée, gérée par plusieurs participants, et enregistre des transactions sur des nœuds de manière décentralisée⁵⁷.

Afin de mieux comprendre l'enjeu de la chaîne de blocs, imaginons une personne A qui souhaite transmettre une information à son ami B. Certes elle peut déjà le faire avec internet, mais cette information envoyée sera obligatoirement dupliquée pour arriver à B. Cela ne pose pas de problème tant que cette information envoyée correspond à autre chose que de la valeur monétaire. En effet aujourd'hui, via internet, on sait transférer une information d'une personne A à une personne B par exemple en envoyant un courriel avec un fichier en pièce jointe⁵⁸. Mais si A veut envoyer de la valeur monétaire à B, il est important que cette valeur envoyée ne soit pas dupliquée et ne reste pas à l'actif de A une fois qu'elle a été envoyée. L'idéal serait donc que A puisse transférer cette information à B directement via son ordinateur, sans que A ne

⁵⁴ On pense notamment, dans le système bancaire, aux délais et aux coûts parfois élevés des virements internationaux.

⁵⁵ William MOUGAYAR, *Business Blockchain, Pratiques et applications professionnelles*, 2017 éditions Dicoland, p47

⁵⁶ Connue sous son acronyme anglais *Distributed Ledger Technology* (ci-après nommé DLT).

⁵⁷ Consultation en ligne sur <https://www.tokens24.com/fr/cryptopedia/basics/ledger-distribue-blockchain-la-difference-entre-eux>

⁵⁸ Exemple issu de la vidéo explicative de Claire BALVA, co-fondatrice de la start-up Blockchain France, intitulée « *La Blockchain : réinventer les rapports de confiance* ». En ligne : <https://www.youtube.com/watch?v=JID9c-MABis>

garde cette valeur à son actif. Mais la seule solution pour transférer de la valeur sans que A n'y garde un accès, c'est d'utiliser une entité intermédiaire chargée de garder et sécuriser l'information (une banque, l'État, un professionnel agréé...). Finalement la chaîne de blocs répond à la question de savoir comment transférer des actifs et des informations entre particuliers, sans qu'une entité intermédiaire de confiance n'ait besoin d'intervenir.

ii- La sécurisation des données sur la chaîne de blocs

La question récurrente à ce sujet est de savoir comment sécuriser des informations ou des transactions sans organe central. Sur la chaîne de blocs, la transaction entre dans le système, et au lieu d'être validée par un organe central, elle doit être validée par « les nœuds du réseau » au regard des écritures précédentes présentes sur la chaîne de blocs. Les « nœuds du réseau »⁵⁹ sont des personnes ou groupes de personnes accréditées qui se connectent au réseau de manière indépendante et vérifient que, par exemple dans le cas d'un transfert de bitcoins, le compte en question a été alimenté en amont (au regard des écritures enregistrées précédemment) et que l'auteur de la transaction est habilité à utiliser cet argent. Puis chaque nœud qui reçoit le message de cette transaction vérifie à son tour la structure et la légitimité de la transaction.

Une fois cette étape réalisée, les transactions valides sont copiées sur chaque ordinateur du réseau afin d'être enregistrées au sein de blocs qui constitueront la chaîne de blocs. La construction de ces blocs est appelée le « minage »⁶⁰. Chaque bloc contient sa date de création, les données à stocker, la position du bloc dans la chaîne, un code de hashage (communément appelé « *hash* ») généré à partir des données contenues dans le bloc, ainsi que le *hash* du bloc

⁵⁹ Lexique de Blockchain France : « Nœud : ordinateur relié au réseau blockchain et utilisant un programme relayant les transactions. Les nœuds conservent une copie du registre blockchain et sont répartis partout dans le monde. » En ligne : <https://blockchainfrance.net/le-lexique-de-la-blockchain/>

⁶⁰ Lexique de Blockchain France : « Minage : utilisation de la puissance de calcul informatique afin de traiter des transactions, sécuriser le réseau et permettre à tous les utilisateurs du système de rester synchronisés. » En ligne : <https://blockchainfrance.net/le-lexique-de-la-blockchain/>

précédent⁶¹. La partie la plus importante du bloc est le *hash* car il garantit l'intégrité du bloc⁶². C'est celui-ci qui permet de s'assurer que les blocs sont dans le bon ordre. Un *hash* est calculé à partir du *hash* du bloc précédent, et chaque nœud du réseau conserve une copie de la chaîne. La modification d'un bloc n'invalide pas seulement celui-ci mais aussi tous les blocs de la chaîne, ce qui améliore la sécurité et l'intégrité de l'information contenue dans les blocs⁶³.

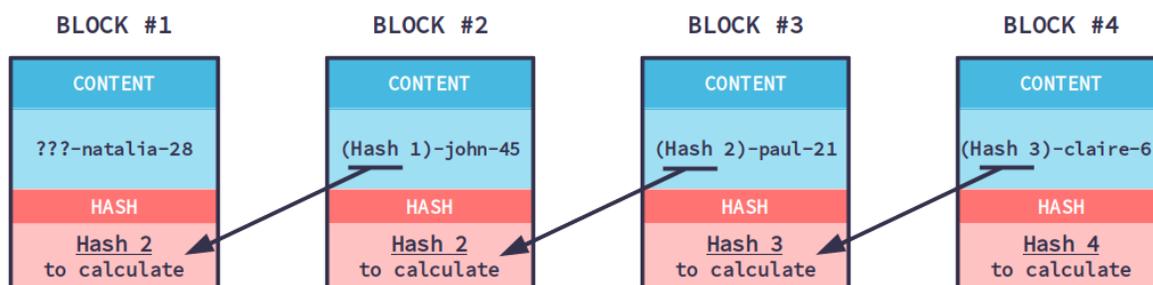


Figure 2. La formation d'une chaîne de blocs⁶⁴

Chaque transaction est horodatée, c'est-à-dire que l'heure de chaque transaction effectuée est enregistrée sur la chaîne de blocs. Outre les transactions financières, le changement de propriété ou toute autre opération enregistrée fait aussi l'objet d'un horodatage⁶⁵, ce qui donne à la chaîne de blocs une fonction de preuve non négligeable.

Une fois le bloc constitué, il est ajouté à la chaîne de blocs qui doit alors être certifiée à l'aide d'un mécanisme de consensus⁶⁶. Ce travail de certification est réalisé par les nœuds du réseau

⁶¹ Souvent évoqué par les auteurs sous le terme anglophone de *PreviousHash* ; William MOUGAYAR, préc., note 55

⁶² Le *hash* sert d'empreinte digitale à la transaction car le *hash* du nouveau bloc doit incorporer le *hash* du bloc précédent ; DWYER, Gerald P., *Blockchain: a primer*, The Most Important Concepts in Finance, Edward Elgar Publishing, 2017, p. 12-27.

⁶³ <https://www.welivesecurity.com/fr/2018/10/09/blockchain-definition-fonctionnement-utilisations/>

⁶⁴ Source en ligne : <http://www.ledgerprojects.com/how-a-blockchain-works-lets-make-one/>

⁶⁵ William MOUGAYAR, préc., note 55, p.66

⁶⁶ Il existe plusieurs mécanismes de consensus qui permettent de certifier la chaîne de bloc cryptée : « Proof of Stake » (PoS) preuve d'enjeu ou de possession, « Proof of Service » (PoS) preuve d'identité, « Proof of Elapsed Time » (PoET) et d'autres encore. En ligne : <https://medium.com/@godefroy.galas/analyse-et-comparaison-des-mecanismes-de-consensus-dans-la-blockchain-f91aee511ea3>

qui, par la résolution de problèmes cryptographiques, s'accordent sur la validité et sur l'ajout de nouveaux blocs à l'historique de transactions⁶⁷, sans entité centralisée qui doit mettre à jour le registre, et sans confiance établie entre les nœuds du réseau. Ce travail de certification par les nœuds du réseau, appelé « preuve de travail », est essentiel pour assurer l'intégrité d'une chaîne de blocs⁶⁸. En cas de panne, de piratage, ou de nœud du réseau inopérant, il permet de garantir l'intégrité des données stockées puisque les autres nœuds du réseau pourront continuer le travail de validation. Par exemple, sur le réseau Bitcoin, le mécanisme de consensus utilisé est le « Proof of Work » (PoW). Pour pouvoir ajouter un bloc à la chaîne de blocs, chaque nœud doit montrer qu'il a réalisé une certaine quantité de travail. Il s'agit pour les « mineurs »⁶⁹, les personnes qui travaillent sur la certification des transactions, de résoudre un problème mathématique complexe qui nécessite une grande puissance de calculs, mais pouvant être facilement vérifié par les autres nœuds du réseau⁷⁰. Le premier mineur qui arrive à résoudre le problème mathématique obtient le droit d'ajouter son bloc à la chaîne, moyennant une récompense en cryptomonnaie.

Aujourd'hui, au regard de l'évolution grandissante de la technologie de la chaîne de blocs, la taille des chaînes augmente, ce qui nécessite d'autant plus de puissance de calcul. Ce ne sont donc plus des particuliers qui effectuent le travail de certification, mais des institutions ou encore des sociétés de *cloud mining*⁷¹ qui se multiplient. Le principe consiste, pour une entreprise, à investir dans le matériel nécessaire pour miner, et ainsi permettre à des personnes de participer au minage moyennant un coût⁷². Cela revient à une location de matériel de minage ou de puissance de calcul, ce qui évite l'installation et la maintenance du matériel ainsi que des coûts

⁶⁷ Yves CASEAU, and Serge SOUDOPLATOFF. «La blockchain, ou la confiance distribuée. », Fondation pour l'innovation politique, 2016.

⁶⁸ Claire FÉNERON PLISSON, *La blockchain, un bouleversement économique, juridique voire sociétal*, I2D Information, données documents Volume 54, n° 3 (2 octobre 2017): 20-22.

⁶⁹ Définition sur Blockchain France : « Mineur : personnes (particuliers ou sociétés) qui connectent sur le réseau une ou plusieurs machines équipées pour effectuer du minage. Chaque mineur est rémunéré au prorata de la puissance de calcul qu'il apporte au réseau. » En ligne : <https://blockchainfrance.net/le-lexique-de-la-blockchain/>

⁷⁰ Source en ligne : <https://medium.com/@godefroy.galas/analyse-et-comparaison-des-mecanismes-de-consensus-dans-la-blockchain-f91aee511ea3>

⁷¹ « Hashnest » est un exemple de site de cloud mining : <https://www.hashnest.com>

⁷² Pour plus de précisions à ce sujet, consulter le site <https://www.cloudmining.fr/obtenir-des-bitcoins-et-autres-altcoins/>

énergétiques élevés⁷³. Il semble que ce mode de fonctionnement laisse finalement entrevoir une forme de corporisation et donc une certaine centralisation. Or tout l'enjeu de la chaîne de blocs gravitait initialement autour de la décentralisation et de la désintermédiation.

b. Différents types et usages de la chaîne de blocs

Il existe différents types de chaîne de blocs : publique (dite « ouverte »), privée (dite « fermée ») ou de consortium. L'une des différences majeures entre la chaîne de blocs privée et publique est liée à la confidentialité des transactions, des données, et, comme nous le verrons ci-après, des contrats intelligents qui y sont attachés. Il est important de distinguer ces trois types de chaînes de blocs qui diffèrent sur certains points. En effet, si la chaîne de blocs publique représente une solution de confiance décentralisée, la chaîne de blocs privée quant à elle peut être complètement centralisée⁷⁴ et ne répond pas aux mêmes besoins que la chaîne de blocs publique. Une fois les besoins et le type de chaîne de blocs déterminés, les transactions se font à l'aide d'une application décentralisée⁷⁵ et de jetons, ceux-ci constituent respectivement le support pour la transaction, et la monnaie d'échange⁷⁶.

i- La distinction entre chaîne de bloc publique, privée et de consortium

⁷³ Ibid.

⁷⁴ Patrick WAELBROECK, « Les enjeux économiques de la blockchain. », *Annales des Mines-Réalités industrielles*. FFE, 2017. p. 10-19.

⁷⁵ Appelées aussi « decentralized application » ou « DApp ». Définition du Lexique Blockchain France : « Une DApp, ou application décentralisée, est une application qui fonctionne sur un réseau décentralisé. Elle n'a pas besoin d'autorité centrale pour fonctionner : elle rend ainsi possible des interactions directes, pair-à-pair, entre utilisateurs via des smart contracts. Elle utilise une cryptomonnaie ou un token. Les données sont stockées de façon chiffrée et transparente sur une blockchain. » Consultation en ligne : <https://blockchainfrance.net/2018/09/14/quest-ce-que-une-application-decentralisee-dapp/>

⁷⁶ Chris DANNEN, « *Introducing Ethereum and Solidity* », Berkeley : Apress, 2017.

Pour appréhender au mieux toutes les opportunités offertes par la technologie de la chaîne de blocs, il est nécessaire de bien en distinguer les trois différents types⁷⁷. Au moyen de différentes questions fermées, la figure ci-dessous résume très schématiquement les usages et l'intérêt pour un utilisateur de mettre en place un type de chaîne de blocs plutôt qu'un autre.

En effet, une chaîne de blocs publique est accessible à tous, son accès nécessite uniquement une connexion internet ainsi que le téléchargement du protocole informatique qui définit les règles de fonctionnement du réseau concerné, notamment le mécanisme de consensus, le minage et la rémunération en cryptomonnaie⁷⁸. Le réseau bitcoin est l'exemple même d'une chaîne de blocs publique dans le sens où n'importe quel utilisateur peut consulter et participer au réseau sans conditions spécifiques d'admission. Ce type de chaîne de blocs est considéré comme « totalement décentralisé »⁷⁹ puisque la confiance émane d'un consensus des nœuds du réseau et la réalisation de la transaction se passe de tiers intermédiaire. La gouvernance d'une chaîne de blocs publique nécessite un accord de l'ensemble des nœuds du réseau pour valider le protocole de validation des données⁸⁰.

La chaîne de blocs privée quant à elle ne fonctionne pas avec le même système de preuve de travail et de minage, mais avec des agents clairement identifiés, autorisés, et sélectionnés au préalable pour accéder au réseau⁸¹. Contrairement à la chaîne de blocs publique, la décision de la validation des données peut alors être prise par un petit nombre de nœuds. Quelques entreprises privées et institutions bancaires utilisent la chaîne de blocs privée pour partager des bases de données en interne afin de progresser en rapidité d'exécution, et diminuer le coût de

⁷⁷Article en ligne de Vitalik BUTERIN (6 août 2015), co-fondateur de la plateforme Ethereum : <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>

⁷⁸ Ces composantes sont expliquées plus en détail plus haut dans ce papier ainsi que sur <https://www.blockchains-expert.com/blockchain-privee-vs-blockchain-publique/>

⁷⁹ Consulter le site <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>

⁸⁰ Pour plus de précisions sur ce point, revenir sur la section précédente intitulée « La construction d'une chaîne de blocs ».

⁸¹ Don TAPSCOTT et Alex TAPSCOTT, "Blockchain Revolution How the Technology behind Bitcoin Is Changing Money", Business and the World, 2016.

leurs transactions. Aussi, pour les institutions bancaires, l'utilisation d'une chaîne de blocs privée a pour avantage d'être plus en adéquation avec les questions de responsabilité juridique et de gouvernance puisque la chaîne de blocs est en quelque sorte « centralisée » et interne à une organisation.

Souvent les entreprises utilisent la chaîne de blocs privée afin d'optimiser un processus déjà existant. Les banques sont notamment intéressées par cette technologie afin de réduire les coûts d'exploitation liés aux échanges internationaux ou mettre en place de nouveaux services⁸². Outre le secteur financier, les entreprises de l'agro-alimentaire s'y mettent aussi; c'est le cas du groupe Carrefour⁸³ en France, qui annonçait dans son communiqué de presse le six mars deux mille dix-huit⁸⁴, l'utilisation de la technologie chaîne de blocs pour garantir à ses clients la traçabilité de ses produits en arguant plus de transparence. Ainsi, à l'aide d'un code barre, le client peut accéder aux informations du produit sur son téléphone intelligent et donc en suivre la traçabilité, depuis la production jusqu'à la mise en rayon du produit (lieu et le mode d'élevage, traitement utilisé, alimentation reçue, etc.)⁸⁵. La chaîne de blocs offre alors une très grande transparence pour les acteurs de la chaîne agro-alimentaire, que ce soit le consommateur, l'éleveur, le transformateur, le distributeur, ou les contrôleurs sanitaires, tous auront librement accès aux informations du produit et à son entière traçabilité.

Le fait que ce type de chaîne de blocs « réglementé » soit géré par un organe central (en l'occurrence « Carrefour »), supprime les deux fonctions clés de la chaîne de blocs initiale du réseau bitcoin que sont la décentralisation et l'absence de tiers de confiance. Notons qu'il est

⁸² Un article de L'Usine Digitale paru le 22 mars 2018 en France est intitulé « Blockchain : comment ces trois grandes banques l'utilisent déjà » En ligne : <https://www.usine-digitale.fr/article/blockchain-comment-ces-trois-grandes-banques-l-utilisent-deja.N670389>. A ce propos, la Banque Nationale du Canada et J.P Morgan ont lancé leur propre chaîne de blocs nommée Quorum pour tester l'émission de dette sur chaîne de blocs : Dans un article de presse de la revue Finance et Investissement du 20 avril 2018 intitulé : « La Banque Nationale et JP Morgan testent la technologie des chaînes de blocs ». En ligne : <https://www.finance-investissement.com/nouvelles/actualites/la-banque-nationale-et-j-p-morgan-testent-la-technologie-des-chaines-de-blocs/>

⁸³ Groupe spécialisé dans la grande distribution. Site officiel <http://www.carrefour.com/fr>

⁸⁴ Consulter le site http://www.carrefour.com/sites/cp_carrefour_blockchain_alimentaire_06032018_vf.pdf

⁸⁵ Consulter le site <https://www.crypto-france.com/carrefour-blockchain-clientele-transparence/>

relativement facile de garantir la confidentialité des données stockées dans une chaîne de blocs privée car seul un nombre limité d'acteurs peut y avoir accès, ce qui explique aussi leur développement rapide en comparaison à la chaîne de blocs publique⁸⁶.

Enfin, il existe la chaîne de blocs de consortium, qui consiste à contrôler le mécanisme de consensus par un ensemble de nœuds sélectionnés au préalable⁸⁷. C'est l'exemple du projet R3⁸⁸, créé en deux mille quinze,⁸⁹ qui regroupe plusieurs institutions bancaires du monde au sein d'un consortium pour explorer ensemble les opportunités dans le secteur de la finance, notamment en ce qui concerne les échanges interbancaires ou les questions de mise en conformité par exemple⁹⁰.

Le choix entre ces trois types de chaînes de blocs dépend de l'utilisation et des objectifs de son créateur : s'il souhaite que les participants à la chaîne ne soient pas connus publiquement, mieux vaut opter pour une chaîne publique, tandis que si connaître l'identité des nœuds du réseau est nécessaire, alors mieux vaut opter pour une chaîne privée ou de consortium⁹¹ selon le niveau d'accessibilité au public souhaité. C'est ce qu'explique de façon schématisée, sous forme d'arbre de décision, la figure suivante.

⁸⁶ Patrick WAELBROECK, préc., note 74. p. 15.

⁸⁷ <https://blogs.alternatives-economiques.fr/vauplane/2016/02/14/la-blockchain-et-la-loi>

⁸⁸ Lire l'article du Journal du net paru le 18 juillet 2017 intitulé « R3, le consortium blockchain qui divise les banques » pour en savoir plus sur la création de ce projet et ses limites : <https://www.journaldunet.com/economie/finance/1196309-r3-le-consortium-blockchain-qui-divise-les-banques/>

⁸⁹ Ce projet fonctionne via une plateforme nommée Corda. Consultation en ligne sur <https://www.r3.com>

⁹⁰ Primavera DE FILIPPI, « Chapitre III. Applications de la blockchain », *Que sais-je ?*, 5 octobre 2018, 74-103.

⁹¹ Voir la figure intitulée « Comment choisir son type de blockchain ? » dans l'ouvrage de Jean-Guillaume DUMAS et al., *Les blockchains en 50 questions: Comprendre le fonctionnement et les enjeux de cette technologie* (Dunod, 2018), 10.

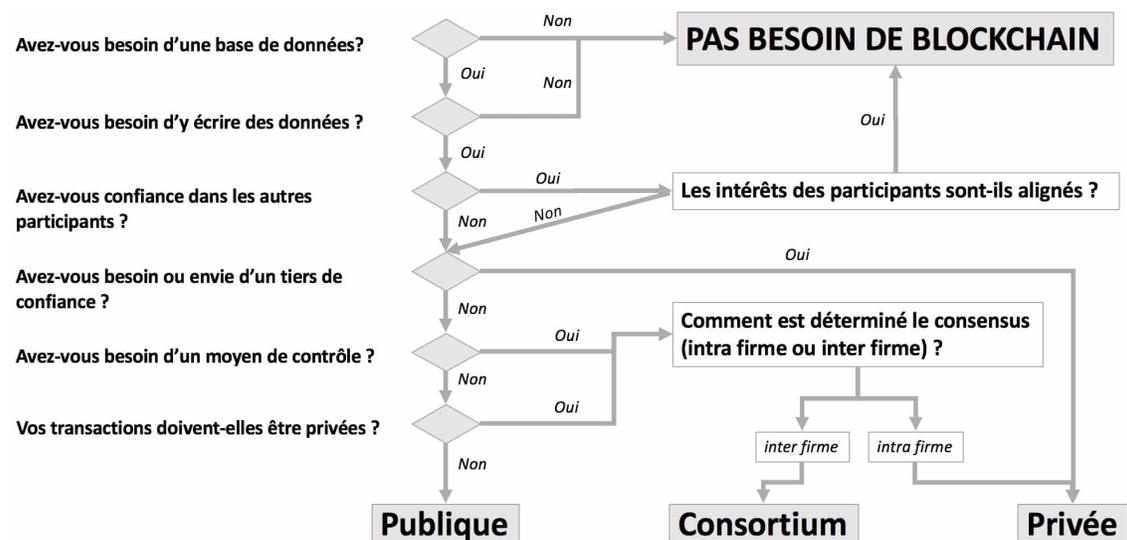


Figure 3. Arbre de décision entre les différents types de chaînes de blocs⁹²

Enfin, dans le cas où l'utilisateur ne ressent pas le besoin de rendre privées ses transactions, ni d'utiliser un moyen de contrôle,⁹³ alors il peut s'orienter vers une chaîne de blocs publique. En revanche, s'il nécessite d'avoir un tiers de confiance ou un moyen de contrôle centralisé et que les transactions doivent rester privées, alors mieux vaut s'orienter vers une chaîne de blocs privée⁹⁴.

ii- Jetons et applications décentralisées

« Today, it is possible to build blockchain applications with minimal knowledge of cryptography, game theory, mathematics or complex coding, and computer science fundamentals, thanks to Ethereum. »⁹⁵

⁹² Sébastien BOURGUIGNON, « Part V : Blockchain privée ou publique, quelle différence ? », Les Echos Solutions, 17 janvier 2018.

⁹³ On entend ici un moyen de contrôle centralisé.

⁹⁴ Sébastien BOURGUIGNON, préc., note 92

⁹⁵ B. SINGHAL et al., « Beginning Blockchain », p.219. Ressource en ligne: https://doi.org/10.1007/978-1-4842-3444-0_4

En 2013, Vitalik Buterin, programmeur et co-fondateur de la plateforme Ethereum⁹⁶, définit son projet comme « une blockchain qui comprend un langage de programmation, c'est à dire une plateforme très libre sur laquelle on peut faire n'importe quelle chose et bénéficier des avantages que la blockchain offre (décentralisation, transparence, auditabilité, etc.) »⁹⁷.

Ce qui différencie Ethereum du Bitcoin, c'est que ce dernier est une cryptomonnaie qui consiste uniquement à transférer des actifs en pair à pair sans intermédiaire. Drescher définit le fonctionnement du système Bitcoin comme suit :

« Peer-to-peer systems are distributed software systems that consist of nodes (individual computers), which make their computational resources (e.g., processing power, storage capacity, or information distribution) directly available to another. When joining a peer-to-peer system, users turn their computers into nodes of the system that are equal concerning their rights and roles. »⁹⁸

Ethereum, en plus de la création de monnaie et de l'échange de transactions, fonctionne comme une plateforme qui permet à des utilisateurs d'utiliser des jetons dits « tokens »⁹⁹ pour créer des applications décentralisées et réaliser des contrats intelligents.

« Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference »¹⁰⁰.

⁹⁶ Cette plateforme fonctionne sur la cryptomonnaie nommée « Ether » et propose à ses utilisateurs de mettre en place des contrats intelligents. <https://www.ethereum-france.com/quest-ce-que-lethereum/>

⁹⁷<https://www.ethereum-france.com/interview-de-vitalik-buterin-createur-dethereum-et-president-de-la-fondation-partie-1-sur-2/>

⁹⁸ Daniel DRESCHER, préc., note 6

⁹⁹ Le Bitcoin est le premier jeton ayant été créé en 2009 dans le but de transférer de la valeur sur internet. De nombreux autres types de jetons ont émergés par la suite : la plateforme Status, lancée en juillet 2017, est une interface mobile permettant d'accéder à des applications décentralisées de la chaîne de blocs Ethereum. Pour cela, le jeton SNT permet de réaliser certaines opérations sur l'application (<https://cryptoactu.com/quest-ce-que-status-snt/>). Dans le même registre, Storj est un service de stockage cloud décentralisé qui permet à un utilisateur de mettre en location l'espace libre qu'il possède sur son ordinateur ou au contraire acheter de l'espace à un autre utilisateur, et ce en échange du token appelé « Storjcoin » (<https://blockchainfrance.net/2018/05/22/comprendre-les-tokens/>).

¹⁰⁰ Définition issue du site officiel Ethereum : <https://www.ethereum.org>

Le plus souvent les contrats intelligents¹⁰¹ créent ce qu'on appelle des jetons¹⁰² sur la chaîne de blocs Ethereum. Ce sont « des actifs numériques émis et échangeables sur une blockchain »¹⁰³ selon l'institut Blockchain France. Le jeton peut permettre de faire fonctionner les applications décentralisées et peut aussi avoir une fonction monétaire tel qu'un moyen de paiement, ou représenter un droit d'accès à une application. Il est créé par n'importe quel internaute et possède les caractéristiques d'une crypto monnaie¹⁰⁴, à savoir qu'il peut être transféré en pair à pair sans nécessiter de tiers intermédiaire ni d'autorisation préalable, et la transaction est enregistrée sur un registre immuable.

Ainsi, Vitalik Buterin a introduit Ethereum pour faciliter les transactions non seulement en argent mais aussi toutes celles ayant une valeur intrinsèque ; terrains, actions, véhicules ou encore contenus numériques, etc¹⁰⁵. La figure ci-dessous présente les possibilités apportées par les applications décentralisées que la plateforme Ethereum peut contenir.

¹⁰¹ Le contrat intelligent sera défini dans le titre I.A.2 de ce mémoire. C'est un contrat programmé (sous forme de code informatique) qui s'exécute automatiquement selon des conditions définies au préalable par les parties au contrat.

¹⁰²Définition du lexique Blockchain France : « Token : actif numérique personnalisé par son auteur, émis et échangeable sur une blockchain, et possédant les caractéristiques d'une cryptomonnaie : infalsifiabilité, unicité, enregistrement des échanges dans un registre immuable, sécurité des échanges, etc. En particulier, un token est transférable (et non duplicable) entre deux parties sur Internet, sans nécessiter l'accord d'un tiers. » En ligne : <https://blockchainfrance.net/le-lexique-de-la-blockchain/>

¹⁰³ <https://blockchainfrance.net/2018/05/22/comprendre-les-tokens/>

¹⁰⁴Définition de Blockchain France : « Monnaie électronique, échangeable en pair-à-pair (c'est-à-dire sans intermédiaire), se basant sur des principes cryptographiques et des mécanismes d'incitation économique pour la validation des transactions et la génération de la monnaie elle-même. » En ligne : <https://blockchainfrance.net/le-lexique-de-la-blockchain/>

¹⁰⁵ B. SINGHAL et al., préc., note 95 p.221

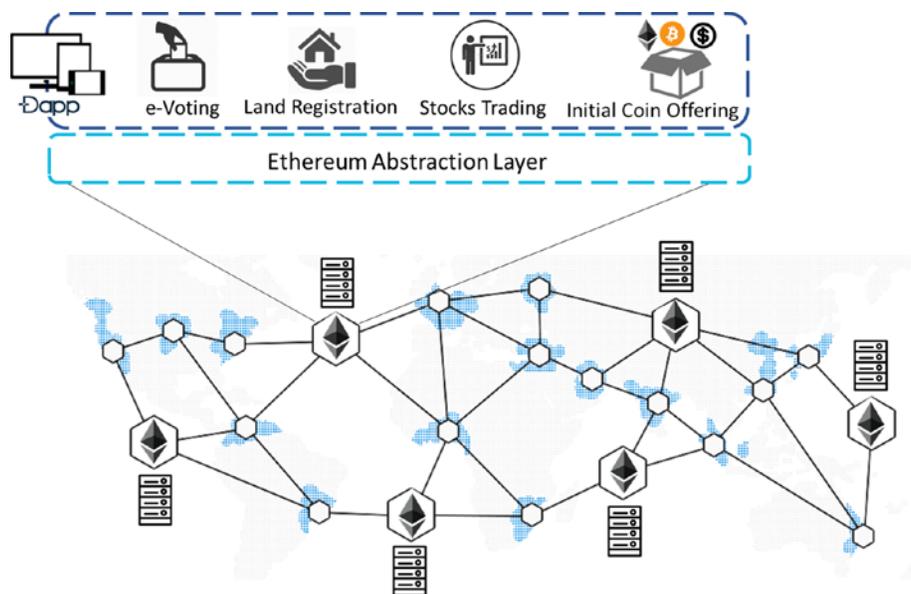


Figure 4. Plusieurs applications décentralisées sur une plateforme Ethereum¹⁰⁶

À propos des contenus numériques, nombreux sont les services de documents en ligne où les données sont stockées et gérées par des serveurs tel que Google Drive¹⁰⁷ ou Icloud¹⁰⁸ par exemple. Ethereum ajoute à ce type de service une gestion des données par des « nœuds » décentralisés sur le réseau. Ainsi, seul l’auteur des données pourra les contrôler et les modifier, ce qui amoindri le risque qu’une application puisse disparaître au détriment de son utilisateur. Certains auteurs voient cette forme de « rigidité » du contrat intelligent comme un gage de sécurité¹⁰⁹, tandis que d’autres l’entendent comme un renforcement des obligations entre cocontractants puisque le contrat les lie d’autant plus. De la même façon, aucun retour en arrière n’est envisageable si une personne loue un véhicule à une société utilisant Ethereum et conclu un contrat intelligent qui se déclenche en envoyant une clé numérique pour déverrouiller le véhicule une fois que le client a payé la somme convenue.

¹⁰⁶ Ibid.

¹⁰⁷ Site officiel de Google Drive : https://www.google.com/intl/fr_ALL/drive/

¹⁰⁸ Présentation du serveur sur https://support.apple.com/kb/PH2608?locale=fr_FR

¹⁰⁹ Patrick WAELBROECK, préc., note 86 p.19

A cet effet, la plateforme HireGo¹¹⁰ a lancé son application décentralisée (DApp) permettant le partage de voitures de particulier à particulier, sans entité intermédiaire et via un paiement en cryptomonnaie à l'aide des jetons appelés « HGO ». Les termes de la charte de l'application HireGo mentionnent que « lorsqu'une transaction de location est conclue, l'utilisateur de location émet une transaction payée au contrat de location. Les fonds sont détenus par le contrat jusqu'à ce que la période de location soit écoulée et que les deux utilisateurs aient indiqué une transaction réussie »¹¹¹. L'identité ainsi que toutes activités de l'utilisateur sont basées sur la chaîne de blocs, ce qui permet de s'assurer de son authenticité et d'en garder une trace. Cette application est disponible sur tous types de téléphones intelligents,¹¹² et permet une utilisation facile de la plateforme de location pour des personnes ne connaissant que très peu ou pas la technologie de la chaîne de blocs.

2. Un contrat à exécution automatique

Le fonctionnement de la technologie de la chaîne de blocs ayant été éclairci, nous pouvons désormais aborder ce qui constitue le cœur de ce mémoire, à savoir le contrat intelligent. Rappelons que le contrat intelligent n'est pas nécessairement lié à la chaîne de blocs; il peut tout à fait fonctionner indépendamment de celle-ci. En effet, la chaîne de blocs présente l'avantage de pouvoir stocker les données et les répercussions du contrat, ce qui limite les fraudes, les erreurs, et oblige chaque partie à répondre de ses obligations en vertu du contrat. Aussi, puisque les intervenants diffèrent,¹¹³ les questions de responsabilité en cas de dommage causé par l'exécution d'un contrat intelligent ne seront pas les mêmes avec ou sans chaîne de blocs.

¹¹⁰ Site officiel de la plateforme HireGo, en ligne <https://hirego.io/?culture=fr>

¹¹¹ Issu du livre blanc d'HireGo, à consulter en ligne sur le site https://hirego.io/lib/HireGo_Whitepaper-fr.pdf

¹¹² Disponible depuis les téléphones IOS, Android ainsi que sur le Web.

¹¹³ Par exemple nous verrons plus loin dans ce mémoire les problématiques liées à l'intervention de l'Oracle (l'Oracle permet d'intégrer à la chaîne de blocs des facteurs externes). Or cet intervenant n'a pas lieu d'exister dans le cadre un contrat intelligent qui ne repose pas sur une chaîne de blocs.

Le contrat intelligent permet de programmer des codes qui s'exécuteront automatiquement sans nécessiter d'intermédiaire. Par exemple, dans le cadre d'un contrat intelligent qui prévoit une transaction avec une remise d'une somme d'argent, le code est intégré dans la chaîne de blocs sous la forme d'un nouveau bloc de transaction, et une fois que les conditions sont réunies le contrat s'exécute de lui-même pour envoyer la somme d'argent. Ceci est un exemple très simplifié mais nous verrons dans ce chapitre que le contrat intelligent peut revêtir différentes formes d'applications.

a. Définition et applications du contrat intelligent

Le contrat est défini à l'article 1378 *Code civil du Québec* comme « (...) un accord de volonté, par lequel une ou plusieurs personnes s'obligent envers une ou plusieurs autres à exécuter une prestation »¹¹⁴. Tout comme le contrat traditionnel, le contrat intelligent se négocie entre cocontractants qui doivent respecter leurs obligations. L'expression de « contrat intelligent » a été introduite par Nick Szabo en 1997¹¹⁵ qui le définit comme un « protocole de transaction informatisé qui exécute les termes d'un contrat »¹¹⁶. Il propose les mécanismes numériques qui peuvent être employés pour s'assurer que les parties respectent leurs obligations¹¹⁷. Dans un premier temps, il est nécessaire de comprendre la définition et l'intérêt que cette nouvelle technologie peut apporter, avant d'en déterminer les usages envisageables.

¹¹⁴Art. 1378 C.C.Q

¹¹⁵Nick SZABO, « The Idea of Smart Contracts »

¹¹⁶Philippe RODRIGUEZ, *La Révolution Blockchain: Algorithmes ou institutions, à qui donnerez-vous votre confiance?*, Dunod, 2017 ; Kai ZHENG, Ying LIU, Chuanyu DAI, Yanli DUAN, Xin HUANG, "Model Checking PBFT Consensus Mechanism in Healthcare Blockchain Network", *Information Technology in Medicine and Education (ITME) 2018 9th International Conference on*, p. 880, 2018.

¹¹⁷Ibid.

i – Qu'est-ce qu'un contrat intelligent ?

Le contrat intelligent est un contrat programmable via le code informatique, qui s'exécute automatiquement selon des conditions (le code du contrat intelligent se base sur la formule : *si... alors...*) définies au préalable par les cocontractants¹¹⁸. Ce sont donc des clauses programmées pour réaliser des actions spécifiques lorsqu'une condition est remplie.

Le contrat intelligent permet de s'assurer de l'exécution des obligations des cocontractants sans qu'ils ne se connaissent au préalable et n'aient besoin de l'intervention d'un intermédiaire dans la transaction. Par exemple, dans le cas où Madame A doit envoyer par courrier un colis à Monsieur B qui doit alors payer Madame A en retour une fois que celle-ci a envoyé le colis. Madame A et Monsieur B ne s'étant jamais rencontrés auparavant, il est possible que Madame A n'ose pas envoyer le colis de peur que Monsieur B ne la paye pas en retour, ou que ce dernier n'ose pas envoyer l'argent tant qu'il n'est pas sûr que madame A ait bien envoyé le colis. Dans ce cas, le recours à la cryptographie via le contrat intelligent va leur permettre de réaliser leur transaction en s'assurant que Madame A sera payée dès lors que Monsieur B aura reçu son colis. En d'autres mots, cela empêche qu'une partie ayant reçu un paiement de son cocontractant décide de façon unilatérale de ne pas remplir son obligation en retour puisque le programme le fait automatiquement à sa place¹¹⁹.

ii – Le contrat intelligent et ses usages

Plusieurs auteurs se questionnent sur le fait de savoir si le contrat intelligent est réellement « intelligent ». L'intelligence est définie par le Centre National de Ressources Textuelles et

¹¹⁸ Benjamin JEAN et Primavera DE FILIPPI, « Les Smart Contracts, les nouveaux contrats augmentés ? », *Conseils et Entreprises*, décembre 2016, <https://hal.archives-ouvertes.fr/hal-01676878>.

¹¹⁹ BERGERON-DROLET, E., et CAPOGROSSO, B. J., « Introduction au blockchain pour les avocats en propriété intellectuelle », dans *Barreau du Québec, Service de la formation continue, Développements récents en droit de la propriété intellectuelle* (2017), volume 437, Montréal, Éditions Yvon Blais, 2017

Lexicales comme un être « *doué de la fonction mentale d'organisation du réel en pensées (chez l'homme), en actes (chez l'homme et l'animal)* »¹²⁰. Or il est aujourd'hui difficile d'imaginer qu'un contrat puisse être doté de cette fonction mentale d'organisation du réel en pensées et en actes. Le contrat intelligent est un programme autonome qui, une fois démarré, ne nécessite plus l'intervention de l'homme.

A ce titre, certains auteurs préfèrent employer les termes de contrat « auto-exécutant », « à exécution automatique », ou de « déclenchements intelligents (Smart Triggers) » puisque sa structure est plus algorithmique que juridique¹²¹. Finalement, l'intelligence du contrat intelligent tient seulement en sa capacité à pouvoir auto-exécuter des obligations contractuelles. Les contrats intelligents sont donc à distinguer de l'intelligence artificielle comme le conçoit par exemple Alan Turing¹²² c'est à dire concevoir la capacité des machines à penser¹²³. Cependant nous verrons plus loin dans ce mémoire¹²⁴ que certains auteurs n'excluent pas l'idée que le contrat intelligent puisse un jour être capable de choisir une base de données plutôt qu'une autre (qu'il considère plus fiable par exemple) et qui déclenchera l'exécution du contrat intelligent avec un risque d'erreur plus faible.

Beaucoup d'actions courantes de notre société pourraient être contractualisées et automatisées via le contrat intelligent. Par exemple, dans le domaine de l'assurance, le contrat intelligent peut servir à l'indemnisation de clients si un contrat est conclu sur la base d'un facteur météorologique défini au préalable. En effet, certaines compagnies d'assurance se sont lancées sur la garantie de sécheresse. Pour cela, ils ont paramétré sur une chaîne de blocs la condition « si il n'a pas plu depuis X jours sur X région, alors il y a indemnisation » certifiée par le croisement de sources fiables (sites météorologiques, experts, syndicats des agriculteurs, etc.).

¹²⁰ <http://www.cnrtl.fr/definition/intelligent>

¹²¹ Pierre-Marie LORE, « Evolution ou révolution pour les contrats en France ? », s. d., 52.

¹²² Alan M. TURING, « Computing Machinery and Intelligence », in *Parsing the Turing Test: Philosophical and Methodological Issues in the Quest for the Thinking Computer*, éd. par Robert Epstein, Gary Roberts, et Grace Beber (Dordrecht: Springer Netherlands, 2009), 23-65, En ligne: https://doi.org/10.1007/978-1-4020-6710-5_3.

¹²³ Pour plus d'information, consulter le Test de TURING dans MOOR, James (ed.). « The Turing test: the elusive standard of artificial intelligence. », Springer Science & Business Media, 2003.

¹²⁴ Consulter à ce propos l'engagement de la responsabilité de l'oracle en partie II de ce mémoire.

Ainsi, les indemnités sont déclenchées automatiquement lorsque les facteurs programmés sont réunis¹²⁵.

Un autre exemple est souvent employé, dans le domaine assurantiel, pour décrire le fonctionnement d'un contrat intelligent : l'indemnité automatisée en cas de retard d'avion dépassant un certain nombre d'heures¹²⁶. Pour bénéficier de cette politique, l'acheteur d'un billet d'avion doit souscrire à l'assurance proposée, dont la solution est reliée au trafic aérien mondial afin de connaître les heures d'atterrissages des vols. Si un retard de plus de deux heures est constaté¹²⁷, le voyageur est alors remboursé automatiquement.

D'autre part, en immobilier, le contrat intelligent peut apporter une preuve de propriété tel qu'un certificat ou une attestation¹²⁸, mais aussi faciliter les transactions lors de l'achat ou la location d'un bien immobilier. Certaines entreprises¹²⁹ s'intéressent notamment à l'automatisation de la location saisonnière au moyen d'une réservation en ligne et de la remise d'une clé électronique qui permettrait au client d'accéder aux lieux uniquement durant la durée de sa réservation. Il est vrai que le processus d'achat ou de location d'un bien peut aujourd'hui faire intervenir plusieurs personnes telles que le notaire, l'assureur, le vendeur, etc. Intégrer le contrat intelligent dans le secteur de l'immobilier permettrait alors de réduire le nombre d'intervenants dans le processus

¹²⁵ Exemple issu de l'article « Smart contracts : quels impacts pour le business model des assureurs ? », disponible sur le site <https://www.insurancespeaker-wavestone.com/2016/11/smart-contracts-impacts-business-model-assureurs/>

¹²⁶ En France, la compagnie d'assurance Axa a lancé une nouvelle assurance paramétrique, appelée Fizzy, permettant de couvrir les retards d'avions au moyen de la chaîne de blocs. Consultation en ligne sur le site <https://www.usine-digitale.fr/article/axa-lance-une-assurance-contre-les-retards-d-avions-avec-la-blockchain-ethereum.N588233>. Lire aussi GATTESCHI, Valentina, LAMBERTI, Fabrizio, DEMARTINI, Claudio, et al. *Blockchain and smart contracts for insurance: Is the technology mature enough?*. Future Internet, 2018, vol. 10, no 2, p. 20.

¹²⁷ Ce délai de 2h s'applique dans le cas de l'assurance Fizzy proposée par la compagnie Axa en France. Les conditions d'indemnité peuvent varier d'une compagnie à l'autre, comme dans tout contrat d'assurance classique.

¹²⁸ Jérôme PONS, « La mise en œuvre de la blockchain et des smart contracts par les industries culturelles », s. d., 10.

¹²⁹ La plateforme immobilière internationale *Propy* intègre les contrats intelligents et la chaîne de blocs dans ses transactions. Site officiel de la plateforme Propy : <http://snip.ly/jno33p#https://propy.com/>

d'acquisition d'une propriété, et rendrait transparentes les informations relatives aux transactions réalisées¹³⁰.

Aussi, dans un article intitulé « Validation and verification of smart contracts : A research agenda »¹³¹, les auteurs donnent un exemple pertinent de l'utilisation du contrat intelligent dans le domaine de l'import-export :

« For example, the legal movement of physical goods from one country to another typically requires export and import permissions from the countries involved. Associated with these permissions might be taxes or duties, evidence of payment of which is required for the relevant permissions to be granted. The vendors and buyers of these goods might require bridging finance to cover delays in receipt of payments or goods, and they might purchase insurances of various forms along the chain. There may be multiple parties: vendors and buyers of the goods, transporters, banks providing trade finance, insurance companies, different countries' customs departments, and so on. The workflow could—at least, in theory—be managed by a sequence of computer programs that execute automatically as successive intermediate milestones in the physical goods' journey are reached. »¹³²

Comme les auteurs le précisent dans cet exemple, c'est un enchaînement d'opérations que les contrats intelligents pourraient théoriquement prendre en charge, mais leur utilisation n'est pas encore répandue et nous verrons par la suite que des incertitudes demeurent quant à leur validité et leurs statut juridique¹³³.

¹³⁰ Cela nécessiterait toutefois certains ajustements législatifs puisque, par exemple, le transfert de propriété d'un immeuble doit être constaté par un notaire sur le fondement de l'article 2970 C.c.Q. C'est donc une possibilité envisageable sur le plan technologique, mais pas juridiquement.

¹³¹ Daniele MAGAZZENI; Peter MCBURNEY; William NASH, "Validation and Verification of Smart Contracts: A Research Agenda", Computer Magazine, IEEE, 2017, p50-57

¹³² Ibid.

¹³³ Réf. partie I,B,1,a. Le statut juridique du contrat intelligent

b. Les apports de la chaîne de blocs au contrat intelligent sur le plan juridique

L'application de la chaîne de blocs, telle que nous y avons fait référence, ne se limite pas à des transactions monétaires; elle peut aussi servir d'infrastructure pour des contrats intelligents. En effet les parties au contrat peuvent choisir de faire exécuter ou non leur contrat intelligent sur la chaîne de blocs ou tout autre registre distribué. Dans ce chapitre nous faisons le choix de distinguer les contrats intelligents attachés à une chaîne de blocs de ceux qui ne le sont pas, car les notions d'intégrité¹³⁴ et de réversibilité ne seront pas abordées de la même façon selon le cas.

i- Intégrité et contrat intelligent

Le terme de « contrat intelligent » ne permet pas d'imaginer immédiatement toutes les applications pratiques que l'on pourrait en faire. Partons de l'exemple d'Uber¹³⁵, cette entreprise néerlandaise qui a vu le jour en 2009 en développant et exploitant des applications mobiles de mise en contact d'utilisateurs avec des conducteurs réalisant des services de transport¹³⁶ pour les personnes souhaitant se rendre d'un point A à un point B, mais aussi pour des livraisons de colis ou de plats provenant d'entreprises locales. Quand un client paie son trajet en dollars via l'application Uber, l'application en verse une partie au chauffeur et l'entreprise Uber garde une commission. Imaginons maintenant une application décentralisée (DApp) de véhicules de tourisme avec chauffeur (VTC) fonctionnant via Ethereum avec un contrat intelligent. Ici il n'y a pas d'entité centrale intermédiaire puisque le code du contrat est exécuté par la Machine Virtuelle Ethereum (ou « EVM »)¹³⁷ du réseau. Quand le client paie sa course, les Ethers sont

¹³⁴ « État d'une chose qui est intacte, à laquelle rien ne manque » ; REID, Hubert. *Dictionnaire de droit québécois et canadien: avec table des abréviations et lexique anglais-français*. Montréal: Wilson & Lafleur, 2001.

¹³⁵ Site officiel d'Uber : <https://www.uber.com/>

¹³⁶ [https://fr.wikipedia.org/wiki/Uber_\(entreprise\)](https://fr.wikipedia.org/wiki/Uber_(entreprise))

¹³⁷ « L'EVM (Ethereum Virtual Machine) est le réseau d'ordinateurs qui constitue le réseau Ethereum en stockant ou transférant des données et en effectuant des calculs. » Enée BUSSAC, *Bitcoin, ether & Cie: Guide pratique pour comprendre, anticiper et investir 2019* (Dunod, 2018).

alors directement transférés sur le compte du chauffeur, sans passer par une entité centrale gérante et donc sans commission prélevée. À noter tout de même la présence de frais de transactions Ethereum que l'on appelle du gaz¹³⁸, ainsi que la nécessité pour l'utilisateur d'adopter un logiciel ou une application¹³⁹ pour pouvoir utiliser facilement le réseau décentralisé sans pour autant être un expert de la technologie de la chaîne de blocs.

Dans un système traditionnel, ce sont aujourd'hui les entités centrales qui créent la confiance. On pense notamment aux institutions bancaires ou aux plateformes telles que Uber comme évoqué ci-dessus ou Airbnb¹⁴⁰ qui mettent en relation les particuliers et se rémunèrent par ce biais. La chaîne de blocs permet à son tour de créer cette confiance, sans intermédiaire. Grâce au modèle du consensus que nous avons évoqué plus tôt dans ce mémoire¹⁴¹, ce sont les nœuds du réseau qui véhiculent la confiance par leurs prises de décisions collectives.

Initialement, il n'est pas nécessaire d'introduire une chaîne de bloc dans le processus du contrat intelligent. Notons que le registre distribué sur lequel repose le contrat intelligent permet uniquement d'assurer l'intégrité du document. Logiquement, le contrat intelligent étant assimilable à un écrit électronique, il se doit de répondre au critère d'intégrité que pose la *Loi concernant le cadre juridique des technologies de l'information*¹⁴² en son article 6 :

« L'intégrité du document est assurée, lorsqu'il est possible de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité, et que le support qui porte

¹³⁸ <https://www.ethereum-france.com/comptes-transactions-gaz-et-limites-de-gaz-par-bloc-sur-ethereum/> : « Le fait que l'exécution du contrat est répliquée de façon redondante auprès de chaque nœud rend naturellement l'exécution coûteuse en termes de puissance de calcul, ce qui doit inciter à ne pas utiliser la blockchain pour des calculs qui pourraient être effectués hors de la chaîne. Pour chaque opération exécutée, un coût est identifié, qui est exprimé en un nombre d'unité de gaz. Chaque opération qu'un contrat contient une valeur en gaz définie. »

¹³⁹ En effet cela nécessite le développement d'une application, comme l'a fait l'entreprise Hirego mentionnée dans la section précédente de ce mémoire.

¹⁴⁰ Airbnb présente les valeurs de sa communauté en évoquant « les bases d'une relation de confiance solide » : <https://www.airbnb.fr/trust/standards>

¹⁴¹ Se référer à la partie I.A.1.a. La construction d'une chaîne de blocs

¹⁴² L.R.Q., chapitre C-1.1.

cette information lui procure la stabilité et la pérennité voulue. L'intégrité du document doit être maintenue au cours de son cycle de vie (...) »¹⁴³.

Or, en plaçant le contrat intelligent sur la chaîne de blocs, la validation de la transaction étant réalisée par un très grand nombre de participants, ceci rend les informations non modifiables ou du moins difficilement. C'est l'image d'un cercle vertueux dans lequel le sentiment de collectivité apporte la confiance entre individus, ce qui facilite le consensus, et le consensus apporte la confiance¹⁴⁴.

Comme mentionné précédemment, le contrat intelligent présente l'avantage de pouvoir garder un historique de la volonté des parties. Puisqu'il peut être associé à un registre distribué, le contrat intelligent empêchera un cocontractant de mauvaise foi de revenir sur sa décision et de nier le fait qu'il ait manifesté son consentement pour ledit contrat. Le fait d'intégrer le contrat intelligent à la chaîne de blocs permettrait donc de s'assurer que les clauses du contrat ne seront pas modifiées et qu'elles se réaliseront à la réalisation de la condition prédéterminée par les parties. La chaîne de blocs apporte au contrat intelligent l'assurance que les termes du contrat et les faits relatifs à l'exécution du contrat ne peuvent pas être annulés par un nœud individuel erroné ou malveillant¹⁴⁵.

ii- Interprétation du juge et contrat intelligent

L'exécution du contrat intelligent sur le réseau de la chaîne de blocs a pour particularité d'être irréversible¹⁴⁶. Pourtant, l'article 35 de la *Loi concernant le cadre juridique des technologies de*

¹⁴³ Art. 6 de la *Loi concernant le cadre des technologies de l'information*, *Id.*

¹⁴⁴ <http://www.droit-blockchain.fr/definition-blockchain/>

¹⁴⁵ « The Law and Legality of Smart Contracts », *Georgetown Law Technology Review* (blog), 17 avril 2017, <https://www.georgetownlawtechreview.org/the-law-and-legality-of-smart-contracts/GLTR-04-2017/>.

¹⁴⁶ TAPSCOTT, Don et TAPSCOTT, Alex. *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. Penguin, 2016.

*l'information*¹⁴⁷ pose la nécessité de pouvoir revenir sur les termes du contrat en cas d'erreur technique dans le cadre de l'utilisation d'un document préprogrammé.

« La partie qui offre un produit ou un service au moyen d'un document préprogrammé doit (...) faire en sorte que le document fournisse les instructions nécessaires pour que la partie qui utilise un tel document puisse dans les meilleurs délais l'aviser d'une erreur commise ou disposer des moyens pour prévenir ou corriger une erreur ».

Or dans le contrat intelligent, celui-ci s'exécutant automatiquement, un retour en arrière n'est pas envisageable si aucun moyen n'a été mis en place par les cocontractants au préalable afin de pouvoir corriger ou prévenir une erreur. Dans ce cas, peut-on affirmer que le contrat intelligent est réellement légal ?

La solution au problème de l'immutabilité des données serait de pouvoir intégrer aux contrats intelligents des variables telles une clause considérant une prise en charge de certains risques, ou encore une clause limitative de responsabilité¹⁴⁸ afin de gérer le risque et de le répartir pour palier au mieux à l'irréversibilité du dommage causé. En effet, : « [...] la loi permet aux parties contractantes de fixer par avance le quantum des dommages-intérêts au moyen soit d'une clause limitative de responsabilité, soit d'une clause pénale ».¹⁴⁹ En autres mots, si le contrat intelligent réduit certains risques (par exemple le risque de non-exécution de la part d'une partie), il en crée de nouveaux qu'il est nécessaire d'encadrer au moyen de clauses contractuelles qui ne peuvent être algorithmées. Comme nous le verrons par la suite, il est alors nécessaire d'intégrer au contrat traditionnel qui accompagne le contrat intelligent différentes clauses permettant de gérer notamment le risque, l'imprévu et la force majeure.

¹⁴⁷ Art.35 de la Loi concernant le cadre juridique des technologies de l'information, préc., note 142

¹⁴⁸ En ligne, précisions sur la clause limitative de responsabilité : <https://www.educaloi.qc.ca/capsules/les-clauses-de-limitation-et-d'exclusion-de-responsabilite>

¹⁴⁹ Paul-André CRÉPEAU, (1962) 22 R. du B. 501, p. 507

Dans l'affaire *Samen Investments Inc. c. Monit Management Limited*¹⁵⁰ le juge interprète et détermine la limite de la clause limitative de responsabilité. En l'espèce, la demanderesse Samen Investments est une compagnie Québécoise propriétaire d'immeubles commerciaux, fait le constat que la partie défenderesse, le groupe Monit, ancien gestionnaire d'un immeuble, a négligé l'entretien du stationnement intérieur durant vingt ans, alors qu'en vertu de leur entente Monit s'engageait à gérer l'immeuble appartenant à Samen. Cette négligence a engendré d'importants travaux de démolition puis de reconstruction. Pour sa défense, Monit mentionne l'existence d'une clause de limitation de responsabilité. Le juge écarte l'application de cette clause en mentionnant que :

« [77] La limite à l'applicabilité d'une clause d'exclusion de responsabilité s'impose à l'égard des obligations qui sont de l'essence même du contrat. » Il ajoute à cela que « le défaut d'exécuter les obligations fondamentales d'un contrat ne peut jamais former l'objet d'une clause de non-responsabilité. Bien que ce principe n'ait pas été extrêmement développé par nos tribunaux, la jurisprudence québécoise est constante à l'effet que l'on ne peut s'exonérer des dommages découlant de son défaut d'exécuter l'obligation principale d'un contrat et que le principe constitue une règle de droit et non d'interprétation ».

Aussi, dans ce cas d'espèce, le juge s'appuie sur l'article 1437 alinéa 2 du *Code civil du Québec*¹⁵¹ qui énonce notamment qu'est « abusive, notamment, la clause si éloignée des obligations essentielles qui découlent des règles gouvernant habituellement le contrat qu'elle dénature celui-ci ». Cette notion d'obligation essentielle a été entièrement consacrée par le législateur en matière de clauses abusives.

¹⁵⁰ *Samen Investments Inc. c. Monit Management Ltd.* (2618 QCCS 17 juin 2010).

¹⁵¹ Art 1437 C.c.Q « La clause abusive d'un contrat de consommation ou d'adhésion est nulle ou l'obligation qui en découle, réductible. Est abusive toute clause qui désavantage le consommateur ou l'adhérent d'une manière excessive et déraisonnable, allant ainsi à l'encontre de ce qu'exige la bonne foi; est abusive, notamment, la clause si éloignée des obligations essentielles qui découlent des règles gouvernant habituellement le contrat qu'elle dénature celui-ci. »

Le professeur Paul-André Crépeau considérait que la clause essentielle au contrat était celle qui « doit nécessairement s’y trouver »¹⁵². Les définitions doctrinales sont nombreuses à ce sujet¹⁵³ et cette notion semble largement considérée par les juges pour déterminer le contenu implicite du contrat. Cette notion a été développée par la jurisprudence¹⁵⁴ pour répondre à la nécessité de protéger l’engagement contractuel et la force obligatoire du contrat. Or, appliqué au contrat intelligent, peut-on réellement juger applicable la notion d’obligation essentielle issue du contrat traditionnel ? En effet le contrat intelligent peut, dans certains cas, ne pas refléter la volonté originale du contractant. Pour autant, il n’y a pas forcément une « erreur sur la qualité essentielle » de la prestation qui entrainerait la nullité du contrat. Finalement, les cocontractants au contrat intelligent sont déjà dans l’obligation de respecter leurs engagements et la force obligatoire du contrat du fait de son exécution automatique et de l’enregistrement de ses effets sur la chaîne de blocs.

De plus, l’article 1434 du *Code civil du Québec*¹⁵⁵ prévoit que les parties au contrat s’engagent non seulement pour ce qui y est exprimé, mais aussi pour ce qui en découle « d’après sa nature et suivant les usages, l’équité ou la loi »¹⁵⁶. Or, nous verrons que pour un contrat intelligent utilisant la chaîne de blocs, l’interprétation ainsi que les événements extérieurs au contrat et non prévisibles semblent difficiles à envisager dû au fait que les événements doivent être codifiables

¹⁵² Paul-André CRÉPEAU, « Le contenu obligationnel d’un contrat », (1965) 43 R. du B. can. 1, p. 24

¹⁵³ Le professeur TANCELIN la définit comme « l’obligation qui transcende toutes les autres et tient à l’essence même du contrat » ; Maurice TANCELIN, *Des obligations en droit mixte du Québec*, 7e éd., Montréal, Éditions Wilson & Lafleur, 2009, no 1107, p. 793-795. Le professeur GRAMMOND estime que ce concept « d’ailleurs mentionné à l’article 1437, semble se référer aux obligations les plus caractéristiques du contrat en cause » ; Sébastien GRAMMOND, « La règle sur les clauses abusives sous l’éclairage du droit comparé », (2010) 51 C. de D. 83, 108.

¹⁵⁴ Sur l’application de l’article 1437 al.2 par la jurisprudence, consulter les affaires *Demers c. Roy*, 2008 QCCQ 4708, par. 54 (CanLII) ; *Reichenbach c. Moto Internationale*, 2010 QCCQ 4128, par. 28 et 29 (CanLII).

¹⁵⁵ Art. 1434 C.C.Q

¹⁵⁶ Dans ces deux affaires le juge considère qu’une obligation essentielle découle de la nature et des usages du contrat : *Union canadienne (L’), compagnie d’assurances c. Mini-entrepôt Longueuil inc.*, 2011 QCCQ 7058, par. 7-10 ; *Syndicat des employées et employés professionnels et de bureau, section locale 571, CTC-FTQ (SEPB) c. Barreau du Québec*, 2007 QCCA 64, par. 30.

et ne tiennent pas compte des éléments humains et imprévisibles¹⁵⁷. La technologie du contrat intelligent étant peu propice aux interprétations, ces deux types de fondements utilisés dans l'interprétation des juges en droit des contrats traditionnels ne pourront pas forcément être applicables aux cas de contrats conclus sous forme de contrats intelligents.

B. Les acteurs du contrat intelligent

Comme évoqué ci-dessus, le contrat intelligent pose plusieurs questions non encore résolues, notamment sur le plan juridique. Lorsqu'il est enregistré sur une chaîne de blocs, il peut être difficile d'identifier les parties au contrat puisque la chaîne de blocs repose sur un principe d'anonymat¹⁵⁸. De plus, nous verrons que le contrat intelligent est un contrat électronique. Ce constat permet déjà de répondre à plusieurs problématiques que soulèvent le contrat intelligent, mais il en apporte aussi de nouvelles. De plus, les clauses du contrat étant codées informatiquement, cela rend d'autant plus difficile l'exercice pour un juge devant interpréter les clauses du contrat en cas de litige. Le contrat intelligent, en tant que logiciel dit « autonome », ne nécessite pas d'intervention humaine lors de son exécution. En revanche, plusieurs intervenants participent à sa rédaction et son élaboration. Ainsi, les choix générés dans la construction du contrat intelligent par les parties conditionnent l'intervention des différents protagonistes et intermédiaires à la formation du contrat intelligent.

¹⁵⁷ BERGERON-DROLET, E., et CAPOGROSSO, B. J., « Introduction au blockchain pour les avocats en propriété intellectuelle », dans Barreau du Québec, Service de la formation continue, Développements récents en droit de la propriété intellectuelle (2017), volume 437, Montréal, Éditions Yvon Blais, 2017

¹⁵⁸ Alexander SAVELYEV, « Contract Law 2.0: “Smart” Contracts as the Beginning of the End of Classic Contract Law », (2017)

1. Contrat intelligent et statut juridique

Le contrat intelligent suscite des positions doctrinales divergentes autour de son statut juridique. Beaucoup assimilent le contrat intelligent à l'intelligence artificielle¹⁵⁹. Or le contrat intelligent est avant tout un programme d'ordinateur, « un script représentant une promesse unilatérale d'assurer une exécution fondée sur des transactions qui sont envoyées au script »¹⁶⁰. D'autres idées gravitent autour du contrat intelligent, tel que le « Smart Contract Code » et le « Smart Legal Contract »¹⁶¹. Le premier fait référence au programme d'ordinateur en lui-même, tandis que le second réfère au contexte juridique dans lequel il évolue¹⁶². Exposer les débats que suscite le contrat intelligent autour de ces questions permettra d'en apprendre davantage sur les différentes possibilités de formation du contrat intelligent.

a. La qualification juridique du contrat intelligent

La technologie de la chaîne de blocs a suscité un rapide engouement et pourrait bouleverser le rôle des tiers de confiance dans divers domaines allant de l'audit des entreprises, aux systèmes de votes, aux ventes immobilières réalisées par les notaires, aux transferts de titres de propriété, aux compagnies d'assurances¹⁶³, ou encore en termes de propriété intellectuelle¹⁶⁴, de vente

¹⁵⁹ Définition issue de la revue en ligne Futura Tech : L'intelligence artificielle (IA, ou AI en anglais pour Artificial Intelligence) consiste à mettre en œuvre un certain nombre de techniques visant à permettre aux machines d'imiter une forme d'intelligence réelle. L'IA se retrouve implémentée dans un nombre grandissant de domaines d'application. Lien internet : Futura-sciences.com

¹⁶⁰ Issu du site internet <https://www.blockchains-expert.com/smart-contracts-peuvent-etre-appliques-a-nos-vies-de-jours/>

¹⁶¹ Ces deux notions seront définies et commentées ci-après

¹⁶² Concernant cette distinction, consulter le site <https://www.blockchains-expert.com/smart-contracts-peuvent-etre-appliques-a-nos-vies-de-jours/>

¹⁶³ Comme mentionné précédemment, c'est par exemple le cas de la compagnie française d'assurance Axa qui a lancé l'assurance *Fizzy* afin d'indemniser les retards d'avions.

¹⁶⁴ Par exemple un nouveau protocole décentralisé et indépendant nommé *Ariane* utilise la chaîne de blocs pour permettre aux marques de délivrer un certificat d'identité numérique à un produit de luxe, qui permettra à l'acheteur d'avoir l'assurance de détenir un produit original.

d'œuvres d'art ou de musique¹⁶⁵, ou pour les objets connectés¹⁶⁶. Rappelons que le contrat intelligent ne pose pas les mêmes interrogations juridiques que l'intelligence artificielle. En effet, ce type de contrat soulève de nouvelles problématiques, notamment en raison de ses multiples usages et applications possibles. Ainsi, ce n'est pas parce qu'on parle de contrat « intelligent » qu'il doit être assimilé à un robot issu de l'intelligence artificielle¹⁶⁷.

i- Contrat intelligent et intelligence artificielle

L'intelligence artificielle se définit comme un « ensemble de théories et de techniques mises en œuvre en vue de réaliser des machines capables de simuler l'intelligence humaine »¹⁶⁸. A ce propos, Alexandre De Streel et Hervé Jacquemin énoncent dans leur ouvrage intitulé *L'intelligence artificielle et le droit*, que « pour devenir capable de détecter les corrélations utiles (prédictives) dans les masses de données, les algorithmes doivent apprendre »¹⁶⁹. Selon eux, il existe deux formes d'apprentissage : l'apprentissage « supervisé » par l'humain qui fournit à l'algorithme des données et des résultats attendus afin d'entraîner ce dernier à se tourner vers la bonne solution souhaitée, et l'apprentissage « non supervisé » qui ne fournit pas de « bonne solution » à l'algorithme mais le laisse identifier et analyser les corrélations entre différentes données dans le but de voir apparaître des solutions inattendues ou non perceptibles par l'humain¹⁷⁰.

Il semble donc que le code informatique puisse venir peu à peu à cette forme d'« intelligence », notamment avec la notion d'apprentissage profond (*deep learning*) qui correspond à une

¹⁶⁵ La chaîne de blocs pourrait rétablir dans ce domaine la confiance en permettant de retracer de manière transparente et irréfutable le parcours d'une œuvre.

¹⁶⁶ Par exemple ce serait le cas d'une voiture connectée qui, une fois le paiement reçu, via un contrat intelligent, se déverrouillerait automatiquement et débloquerait un certain nombre de kilomètres pour son utilisateur.

¹⁶⁷ Alain BENSOUSSAN et Jérémy BENSOUSSAN, *Droit des robots*. Éditions Larcier, 2015.

¹⁶⁸ Encyclopédie Larousse. En ligne : https://www.larousse.fr/encyclopedie/divers/intelligence_artificielle/187257

¹⁶⁹ Alexandre DE STREEL, et Hervé JACQUEMIN, *L'intelligence artificielle et le droit*. Éditions Larcier, 2017.

¹⁷⁰ Notons à cet égard que, pour d'autres auteurs, il existe d'autres formes d'apprentissage à savoir l'apprentissage semi-supervisé, ou encore l'apprentissage transductif mis en avant en 1998 par Vapnik. Toutefois dans le cadre du présent mémoire, il n'est pas nécessaire d'étendre le sujet.

technique d'apprentissage automatique (*machine learning*) qui s'inspire du fonctionnement du cerveau humain pour permettre à un ordinateur d'apprendre par lui-même en se basant sur des réseaux de neurones artificiels¹⁷¹.

Si un algorithme est capable d'apprendre, il serait possible d'imaginer que le contrat intelligent intègre le fait qu'un Oracle¹⁷² puisse se tromper, et donc s'orienter vers un second Oracle, plus fiable¹⁷³. Cependant, même si grâce à l'apprentissage profond l'intelligence artificielle forte arrive aujourd'hui à prendre en compte une part d'imprévu¹⁷⁴, le recours aux algorithmes a permis de développer la sécurité et l'efficacité du code informatique, sans pour autant qu'il soit sans failles¹⁷⁵. Dans l'exemple du contrat intelligent, il n'est pas encore arrivé à gérer de façon autonome la force majeure que le *Code civil du Québec* définit comme « un événement imprévisible et irrésistible »¹⁷⁶. Puisque la technologie de la chaîne de blocs permet au contrat intelligent de ne pas pouvoir être modifié ou contourné car ceci est gage de sécurité, que se passe-t-il si les cocontractants souhaitent rompre le contrat ? Quelle place est laissée à l'humain dans la conclusion d'un contrat intelligent ?

Nombreux sont les contrats basés sur des composantes variables autres que l'imprévisibilité telles que la bonne foi, la capacité, le raisonnable, la légitimité, ou encore ce qui est considéré comme manifestement disproportionné.¹⁷⁷ Toutes ces notions juridiques ont pour particularité

¹⁷¹ Pour plus de précisions sur le sujet : Yann LECUN, Yoshua BENGIO, et Geoffrey HINTON, « Deep Learning », *Nature* 521, n° 7553 (mai 2015): 436-44, <https://doi.org/10.1038/nature14539>.

¹⁷² La notion d'Oracle sera définie lorsque nous aborderons les acteurs du contrat intelligent (I.B.2). Il permet d'implémenter sur la chaîne de blocs l'information externe nécessaire au déclenchement de l'exécution automatique du contrat intelligent.

¹⁷³ Cette idée est développée plus en détail en seconde partie de ce mémoire, relativement aux questions de responsabilité de l'Oracle.

¹⁷⁴ Philippe PERRENOUD, *Gestion de l'imprévu, analyse de l'action et construction de compétences*. Éducation permanente, 1999, vol. 140, no 3, p. 123-144.

¹⁷⁵ Nous faisons référence ici aux différentes attaques informatiques importantes survenues au cours de ces dernières années.

¹⁷⁶ Art.1470 C.c.Q

¹⁷⁷ Site internet <https://lesconferences.openum.ca/files/sites/97/2018/05/Smart-contracts.pdf>.

d'être entièrement soumises à l'interprétation du juge en cas de litige¹⁷⁸. Il est alors difficile d'imaginer qu'une ligne de code informatique puisse envisager l'imprévisibilité ou la légitimité. Le contrat intelligent ne fait qu'exécuter les clauses du contrat. Ainsi, celui-ci ne peut intégrer des éléments imprévisibles tel que la force majeure prévue à l'article 1470 *Code civil du Québec*¹⁷⁹ qui la définit comme « un événement imprévisible et irrésistible ». Ce type de clause pose un problème de programmation et d'interprétation dans le contrat intelligent. En effet, l'imprévisibilité nécessite d'établir si l'évènement pouvait être anticipé au regard des connaissances communes et des circonstances en l'espèce. C'est donc une condition très subjective qui repose entièrement sur l'interprétation du juge. Comme pour un contrat classique, il est toujours possible de contester la validité de la relation contractuelle devant une juridiction, par exemple pour la faire annuler sur le fondement d'un vice de consentement, l'erreur, ou le dol¹⁸⁰. La conséquence de l'annulation d'un contrat traditionnel est le statu quo ante, dans le sens où les parties se retrouvent dans la situation dans laquelle elles se trouvaient avant d'avoir contracté¹⁸¹. Le contrat intelligent devrait prévoir ce type d'éventualité dans son code.

Si le code informatique n'est pas capable, à lui seul, de traduire les évènements imprévisibles¹⁸², il existe cependant un moyen de contourner cet obstacle : l'intervention de l'oracle, comme mentionné ci-dessus. En effet, dans le cas où la condition d'exécution du contrat repose sur un évènement extérieur imprévisible à la signature, ce dernier sera capable de le constater a posteriori. C'est ce constat qui sera contractualisé, et non l'évènement imprévisible en lui-même. Mustapha Mekki décrit ci-dessous le fonctionnement d'un contrat intelligent intégrant une part d'imprévu: « une clause contractuelle fiat peut prévoir qu'un tel évènement imprévisible, constaté par un tiers (un Oracle) et dont l'existence est intégrée à la chaîne de

¹⁷⁸ Affaire *Bérubé c. Bois Rocam inc.* (C.Q., 2004-12-13), SOQUIJ AZ-50286464, J.E. 2005-547, sur l'interprétation du contrat et la recherche de la bonne foi et de l'intention des parties au moment où elles ont contracté.

¹⁷⁹ Article 1470 C.c.Q

¹⁸⁰ Article 1416 C.c.Q et s. sur la nullité du contrat : « Tout contrat qui n'est pas conforme aux conditions nécessaires à sa formation peut être frappé de nullité. »

¹⁸¹ Article 1699 et s. C.c.Q : « La restitution des prestations a lieu chaque fois qu'une personne est, en vertu de la loi, tenue de rendre à une autre des biens qu'elle a reçus sans droit ou par erreur, ou encore en vertu d'un acte juridique qui est subséquemment anéanti de façon rétroactive ou dont les obligations deviennent impossibles à exécuter en raison d'une force majeure. »

¹⁸² Se référer en amont à la partie relative à la qualification juridique du contrat intelligent.

blocs, entraîne le déclenchement d'un autre contrat intelligent venant contrecarrer le fonctionnement du premier. On aurait ainsi une « suicide clause » faisant elle-même l'objet d'un smart contract. »¹⁸³.

Pour pallier à cette contrainte, ce sera aux parties d'être plus vigilants au moment de la conclusion du contrat afin d'ajouter les clauses nécessaires, parallèlement à la programmation du contrat intelligent. Si on reprend l'exemple de la notion d'imprévisibilité évoquée ci-dessus, la solution serait d'intégrer au contrat intelligent non pas l'imprévu en lui-même, mais les effets qu'il causerait. Il s'agirait alors d'ajouter au contrat une clause « traditionnelle » qui prévoit que si un évènement imprévisible survient (constaté par un Oracle relié à la chaîne de blocs par exemple), alors un second contrat intelligent se déclenche et viendra faire l'inverse de ce qui était prévu dans le premier contrat afin d'annuler les effets de ce dernier¹⁸⁴.

ii- « Smart Legal Contract » ou « Smart Contract Code »

Le contrat intelligent peut découler d'un contrat papier entièrement traduit en code, on parle de modèle externe. Le modèle interne du contrat intelligent est quant à lui composé de certaines clauses dites opérationnelles qui sont susceptibles d'automatisation et d'application directe, complétées par des clauses non-opérationnelles qui nécessitent quant à elles une interprétation et une prise de décision humaine préalable¹⁸⁵. Ainsi, sur le schéma classique du contrat intelligent qu'on connaît aujourd'hui, ne sont codées informatiquement que certaines étapes du contrat, à savoir la remise de fonds, la remise de documents ou encore la fin de l'engagement. Afin de conclure un contrat intelligent, les parties ont donc deux possibilités : traduire un contrat « traditionnel » conclu à l'oral ou à l'écrit dans le monde physique, en code informatique et

¹⁸³ Mustapha MEKKI, « Blockchain : l'exemple des smart contracts. Entre innovation et précaution ». En ligne : <https://www.mekki.fr/files/sites/37/2018/05/Smart-contracts.pdf>

¹⁸⁴ Ibid.

¹⁸⁵ Voir au sujet des clauses opérationnelles et non-opérationnelles le *white paper* de l'International Swaps and Derivatives Association (ISDA), en collaboration avec Linklaters, Mark Gates, *Blockchain ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money*, 2017.

choisir d'utiliser ou non la chaîne de blocs comme moyen d'exécution du contrat. Ou bien programmer le contrat directement via le contrat intelligent, en dehors de tout contrat dans le domaine physique¹⁸⁶.

Une partie de la doctrine considère que le contrat intelligent doit évoluer dans un environnement juridique et parle de « Smart legal contract ». C'est l'adage qui résume la première solution proposée ci-dessus, à savoir la transcription d'un contrat papier par un outil technologique qui va appliquer ce contrat préalablement conclu classiquement entre deux individus. Guerlin évoque très justement à ce propos que le contrat intelligent n'est pour l'instant qu'un « *algorithme de gestion des opérations contractuelles* »¹⁸⁷. Grâce au principe de décentralisation et de registre public, la transcription du contrat physique dans la chaîne de blocs présente l'avantage de pouvoir sécuriser et fiabiliser le contrat, en conserver la preuve et garantir son authenticité, mais aussi palier d'éventuels litiges relatifs à des questions de preuve, de détérioration physique du contrat, de contestation de sa conclusion ou de son contenu.

D'autres revendiquent le « Smart contract code », c'est-à-dire un contrat entièrement composé d'algorithmes. Il désigne un logiciel écrit dans un langage de programmation¹⁸⁸ agissant pour les parties afin de remplir des obligations ou d'exercer certains droits. Ce n'est donc pas un contrat comme on l'entend juridiquement, mais un contrat créé de façon purement technologique, sans passer par l'écriture d'un contrat physique au préalable. Le fait que le « Smart contract code » soit considéré comme un contrat juridiquement parlant, porte à débat. Dans le droit positif, l'application de la loi passe par l'interprétation du juge et l'adaptation de la règle de droit aux circonstances particulières du litige. Le code informatique, quant à lui, ne possède pas cette capacité d'adaptation et définit les modalités d'exécution du contrat sur un modèle binaire « Si... Alors... », ce qui ne laisse pas de place à l'interprétation.

¹⁸⁶ Daniele MAGAZZENI; Peter MCBURNEY; William NASH, "Validation and Verification of Smart Contracts: A Research Agenda", Computer Magazine, IEEE, 2017, p50-57

¹⁸⁷ GUERLIN, G. « Considérations sur les smart contracts ». Dalloz IP/IT, 2017.

¹⁸⁸ Martin VALENTA et Philipp SANDNER, « Comparison of Ethereum, Hyperledger Fabric and Corda », s. d., 6.

Traditionnellement, en droit des contrats, la loi impose des conditions de forme et de fond à certains types de contrats pour qu'ils soient valides juridiquement¹⁸⁹. Par exemple, l'acte authentique énoncé à l'article 2813 du *Code Civil du Québec*¹⁹⁰ doit avoir été « reçu ou attesté par un officier public compétent selon les lois du Québec ou du Canada, avec les formalités requises par la loi ». Ainsi, le contrat de vente immobilière ou le contrat de mariage doivent être conclus par une autorité comme le notaire. Mais qu'en est-il alors dans le cas de l'utilisation d'un contrat intelligent ? Est-ce qu'on peut considérer qu'il respecte les conditions de formes et de fonds nécessaires à sa validité ? Aujourd'hui, le droit positif a été adapté pour faciliter le recours au numérique en permettant la conclusion de contrats par voie électronique, notamment via l'article 2 de la *Loi concernant le cadre juridique des technologies de l'information*¹⁹¹ qui établit un principe de liberté de choix quant au support et à la technologie utilisée. Cet article prévoit que :

« À moins que la loi n'exige l'emploi exclusif d'un support ou d'une technologie spécifique, chacun peut utiliser le support ou la technologie de son choix, dans la mesure où ce choix respecte les règles de droit, notamment celles prévues au Code civil.

Ainsi, les supports qui portent l'information du document sont interchangeables et, l'exigence d'un écrit n'emporte pas l'obligation d'utiliser un support ou une technologie spécifique. »

Au regard de cette disposition, dans le cas où la loi n'exigerait pas de support particulier, l'utilisation du contrat intelligent sur une chaîne de blocs serait donc applicable. Cependant, dans le cas où la loi exigerait l'utilisation d'un support exclusif, en application de l'article 2 de la LCCJTI, l'utilisation de la chaîne de blocs en tant que support ne serait pas autorisée. Si on

¹⁸⁹ En droit français, l'article 1128 du Code Civil énonce que « sont nécessaires à la validité d'un contrat : 1° Le consentement des parties ; 2° Leur capacité de contracter ; 3° Un contenu licite et certain ». En ligne : <https://www.legifrance.gouv.fr/>

¹⁹⁰ Art. 2813 C.c.Q

¹⁹¹ Art. 2 de la Loi concernant le cadre juridique des technologies de l'information, préc., note 142

revient aux deux exemples cités ci-dessus (le contrat de vente immobilière ou le contrat de mariage), l'utilisation d'un contrat intelligent basé sur une chaîne de blocs ne serait alors pas valide puisque le *Code civil du Québec* exige l'intervention d'une personne physique (le notaire) pour valider le contrat¹⁹².

D'autre part, le contrat intelligent requiert des solutions plus technologiques que les contrats classiques¹⁹³. En effet, l'utilisation de la cryptographie n'est pas à la portée de tous, il est nécessaire d'y être formé pour pouvoir maîtriser ce langage. En cas de litige, il est probable que le processus de résolution soit ralenti du fait, pour le juge, de la nécessité de prendre en compte à la fois les clauses contractuelles codées dans le contrat intelligent (le programme) et les clauses contractuelles originales et naturelles telles que définies par les parties. La preuve d'expert, tels que des programmeurs équipés pour déchiffrer le code d'un contrat intelligent, pourra être requise¹⁹⁴. Ou bien, pour gagner en efficacité, peut-être que les professions juridiques devront s'affranchir d'une double compétence dans le code informatique et la programmation, en addition à leur formation juridique.

b. Règlementation et contrat intelligent

Les institutions européennes montrent de plus en plus d'intérêt pour la chaîne de blocs. Un comité des *Sciences and Technology Option Assessment* (STOA) a été créé au Parlement Européen¹⁹⁵ pour mettre en place un groupe de travail autour de la DLT¹⁹⁶, surveiller l'évolution de cette technologie et ainsi pouvoir décider s'il faut légiférer ou non¹⁹⁷. Sur la qualification du

¹⁹² En vertu de l'Art. 2245 C.c.Q

¹⁹³ Catherine BARREAU, « La régulation des smart contracts et les smart contracts des régulateurs », *Annales des Mines - Réalités industrielles* Août 2017, n° 3 (26 juillet 2017): 74-76.

¹⁹⁴ Mark GIANCASPRO, "Is a 'smart contract' really a smart idea? Insights from a legal perspective". *Computer law & security review*, 2017, vol. 33, no 6, p. 833

¹⁹⁵ Le comité STOA a rédigé une publication intitulée « How blockchain could change our lives » en février 2017. En consultation sur [http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA\(2017\)581948_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf)

¹⁹⁶ Préc. note 56 ; La DLT correspond à la technologie du registre distribué définie en amont.

¹⁹⁷ Issu du livre blanc publié par Paris Europlace : « Les impacts des réseaux distribués de la Technologie Blockchain dans les activités de marché ». En ligne : <https://www.paris-europlace.com>

statut du contrat intelligent, en France, un projet d'amendement n°227 du 1^{er} juin 2016 relatif à la *Loi sur la transparence, la lutte contre la corruption et la modernisation de la vie économique*¹⁹⁸, avait pour objet d'insérer un alinéa supplémentaire au sein du code monétaire et financier afin de considérer le contrat intelligent en tant qu'acte juridique : « Les opérations effectuées au sein d'un système organisé selon un registre décentralisé permanent et infalsifiable de chaîne de blocs de transactions constituent des actes authentiques au sens du deuxième alinéa de l'article 1317 du Code Civil¹⁹⁹. »²⁰⁰.

Pour motiver ce projet, les rédacteurs affirment que les transactions utilisant la technologie de la chaîne de blocs ont toutes les caractéristiques d'un acte authentique, à savoir une date certaine et incontestable, un contenu garantissant la validité du fond et la forme de l'acte, une force probante, ainsi qu'une force exécutoire de plein droit²⁰¹. Ce projet n'a cependant pas été retenu par la suite. Le droit français a tout de même pris en compte l'existence de la chaîne de blocs en droit financier en la définissant comme un « dispositif électronique partagé ».²⁰² Pourtant les grands principes posés par le *Règlement général sur la protection des données personnelles* (ci-après nommé « RGPD ») ne semblent pas adaptés à l'utilisation de cette technologie. Depuis l'entrée en vigueur le 25 mai 2018 du RGPD, plusieurs auteurs ont souligné une incompatibilité entre l'utilisation de la chaîne de blocs pour le contrat intelligent, et le RGPD. En effet, la chaîne de blocs souhaite rendre les informations immuables, tandis que le RGPD souhaite les rendre modifiables et effaçables. Par exemple, en ce qui concerne la chaîne de blocs et donc les contrats intelligents qui y sont liés, il est impossible de modifier quoi que ce soit ou de revenir sur une clause abusive.

¹⁹⁸ « Assemblée nationale ~ RELATIF À LA TRANSPARENCE, À LA LUTTE CONTRE LA CORRUPTION ET À LA MODERNISATION DE LA VIE ÉCONOMIQUE (no 3785) - Amendement no 227 », consulté le 20 janvier 2019, <http://www.assemblee-nationale.fr/14/amendements/3785/AN/227.asp>.

¹⁹⁹ À titre d'information, l'article 1317 du Code Civil français prévoit que : « Entre eux, les codébiteurs solidaires ne contribuent à la dette que chacun pour sa part. Celui qui a payé au-delà de sa part dispose d'un recours contre les autres à proportion de leur propre part. Si l'un d'eux est insolvable, sa part se répartit, par contribution, entre les codébiteurs solvables, y compris celui qui a fait le paiement et celui qui a bénéficié d'une remise de solidarité. »

²⁰⁰ Préc. note 198

²⁰¹ *Id.*

²⁰² Ordonnance n° 2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers.

L'architecture de la chaîne de blocs repose sur un registre où chaque information détient une place qui conditionne celle de toutes les informations suivantes. Ainsi on ne peut retirer une seule information de la chaîne de blocs sans impacter toutes les autres. Parallèlement, le RGPD attache une grande importance à la limitation du délai de conservation des données²⁰³ et prévoit que ces données doivent être effacées dès lors qu'elles ne présentent plus d'intérêt direct pour celui qui les conserve. A ce titre, l'article 5.e du RGPD²⁰⁴ prévoit :

« Les données à caractère personnel doivent être (...) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ».

Or, dans le cas où un contrat intelligent serait appliqué sur une chaîne de blocs publique, la possible identification de la personne concernée ne peut être supprimée une fois que l'information est sur la chaîne de blocs.

De plus, le RGPD souhaite protéger les données à caractère personnelles or l'identité d'un utilisateur de la chaîne de blocs est automatiquement dévoilée. Il s'agit d'une « clé publique » (appelée aussi « clé de chiffrement ») qui prendra la forme d'une suite de chiffres et qui permettra de remonter à une personne physique. La Cour de cassation a jugé en 2016 que « les adresses IP, qui permettent d'identifier indirectement une personne physique, sont des données à caractère personnel »²⁰⁵. Ainsi, le code inscrit dans la chaîne de blocs permettant d'identifier la personne physique, constitue une donnée personnelle, ce qui va à l'encontre des dispositions du RGPD. Cependant, ce cas de figure est envisageable seulement si l'utilisateur du réseau

²⁰³ Art.5 §1. e, R.G.P.D

²⁰⁴ « Règlement (UE) 2016/ 679 Du Parlement Européen Et Du Conseil - du 27 avril 2016 - relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/ 46/ CE (règlement général sur la protection des données) », s. d., 88.

²⁰⁵ Cass. 1^{ère} civ., 3 nov. 2016, n° 15.22-595

détient déjà un bon niveau en informatique. En effet, retrouver l'identité d'une personne à partir d'une « clé publique » est certes possible, mais réservée qu'à un cercle de connaisseurs.

Aussi, la clé publique constitue à notre avis un renseignement personnel au sens de la *Loi sur la protection des renseignements personnels et les documents électroniques*, puisqu'elle correspond à « tout renseignement concernant un individu identifiable, à l'exclusion du nom et du titre d'un employé d'une organisation et des adresse et numéro de téléphone de son lieu de travail »²⁰⁶. En effet, pour qu'une clé chiffrée soit considérée comme étant un renseignement personnel, il est nécessaire d'apprécier la possibilité d'identification, c'est-à-dire que la clé doit permettre d'identifier une personne. La décision *Gordon c. Canada (Health)*²⁰⁷ interprète la notion de caractère « identifiable » de la personne :

« Thus, information recorded in any form is information “about” a particular individual if it “permits” or “leads” to the possible identification of the individual, whether alone or when combined with information from sources “otherwise available” including sources publicly available. »

Ainsi, pour qu'un renseignement soit considéré comme un renseignement personnel au sens de la loi, il faut que celui-ci permette clairement d'identifier l'individu, ou rende possible son identification, que ce soit un renseignement seul ou combiné avec d'autres informations.

Sur ce même sujet, en Europe, un groupe de travail établi par l'article 29 de la directive 95/46/CE²⁰⁸ a rendu un avis énonçant que :

²⁰⁶ Art 2 de la Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000

²⁰⁷ *Gordon v. Canada (Health)*, 2008 FC 258 (CanLII)

²⁰⁸ La directive 95/46/CE définit en son article 2 la notion de « données à caractère personnel » comme étant « toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale. »

« Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne »²⁰⁹.

Selon eux, si compte tenu de l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, la personne n'est pas clairement identifiable, alors la simple hypothèse de pouvoir distinguer une personne ne suffit pas pour la considérer comme « identifiable » et n'entre donc pas dans la définition de « données à caractère personnel ». Par contre, une entreprise qui détient un logiciel permettant de décrypter la clé publique dispose clairement d'un moyen d'identifier la personne. C'est ce qui est envisagé sur la chaîne de blocs, plus particulièrement une chaîne de blocs privée, où les utilisateurs sont capables d'identifier une personne au regard de sa clé publique²¹⁰.

Au-delà de la question relative aux renseignements personnels via la clé publique, rappelons que tout l'intérêt du contrat intelligent se trouve dans la désintermédiation et l'anonymat²¹¹. Il est donc difficile pour les cocontractants d'agir en justice s'ils ne connaissent pas l'identité des personnes avec qui ils ont contracté. Là encore, au sein d'une chaîne de blocs privée, le problème est moindre car, dans la plupart des cas, les cocontractants se connaissent au préalable et utilisent le contrat intelligent afin que la transaction reste anonyme et confidentielle aux yeux des acteurs du réseau, mais en gardant la possibilité de faire correspondre facilement l'adresse au cocontractant.

²⁰⁹ Avis 4/2007 sur le concept de données à caractère personnel. Groupe de travail « article 29 » sur la protection des données. Avis disponible sur https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp136_fr.pdf

²¹⁰ Sur ce sujet, consulter le site <https://www.loyensloeff.com/be/en/news/articles-and-newsflashes/blockchain-and-gdpr-is-a-clash-really-inevitable-n11588/> qui réfère au groupe de travail sur l'article 29 concernant l'avis 05/2014 sur des techniques d'anonymisation : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf

²¹¹ Alexander SAVELYEV, « Contract Law 2.0: "Smart" Contracts as the Beginning of the End of Classic Contract Law », (2017)

2. Les intervenants à la réalisation du contrat intelligent

Le contrat intelligent est le produit d'une cohabitation entre les codes juridique et informatique. Si notre système juridique repose sur l'idée que la loi doit être interprétée par un juge pour savoir comment elle doit être appliquée, le code informatique est quant à lui plus strict. Il s'applique uniquement aux cas qui ont été anticipés, et ne possède pas la souplesse nécessaire pour faire face à l'imprévu²¹². Afin de mieux cerner les hypothèses d'engagement de responsabilité des acteurs participants à l'élaboration ou à l'exécution du contrat intelligent, il convient d'établir un ordre d'intervention de ces principaux acteurs lors de la mise en place d'un contrat intelligent. Rappelons que cette énumération n'est surement pas exhaustive et reprend uniquement les agents dont la responsabilité civile pourrait être engagée en cas de litige.

a. Les principaux intervenants au contrat intelligent

Dans une vision globale et simplifiée, un contrat intelligent est issu d'un accord de volonté entre deux cocontractants²¹³, pouvant être officialisé par un professionnel du droit, programmé par des développeurs, audité selon les cas, et qui peut se fier à un oracle lors de son exécution. Ces intervenants sont autant de responsables potentiels en cas de dommage causé par l'exécution d'un contrat intelligent.

i- Les cocontractants

Le cocontractant est « celui qui s'engage avec d'autres par un contrat »²¹⁴. Notre société est basée sur la conclusion de contrats au quotidien, parfois même sans s'en rendre compte. Il

²¹² Cette notion sera développée ci-après en évoquant l'intervention humaine dans le contrat intelligent ; JEAN et DE FILIPPI, préc., note 118

²¹³ Art. 1378 C.c.Q : « Le contrat est un accord de volonté, par lequel une ou plusieurs personnes s'obligent envers une ou plusieurs autres à exécuter une prestation ».

²¹⁴ « Se dit d'une personne qui se lie par contrat, qui est partie à un contrat » : REID, H., Dictionnaire de droit québécois et canadien, 3e édition, Montréal, Wilson & Lafleur, 2004, 828 p.

correspond à l'engagement de plusieurs personnes, appelées les cocontractants, à réaliser quelque chose pour l'autre. Comme tout contrat traditionnel, un contrat intelligent correspond lui aussi au produit d'un accord de volonté entre deux ou plusieurs parties²¹⁵. Ces individus à l'origine de l'élaboration du contrat traditionnel, comme du contrat intelligent, peuvent être des personnes physiques, un groupe de personnes, une personne morale, ou un représentant de cette dernière.

ii- Les professionnels du droit

La loi continue d'exiger l'intervention d'un professionnel du droit pour valider certains actes²¹⁶. C'est notamment le cas de l'avocat pour les actes contresignés (par exemple dans le cas de cessions de parts sociales²¹⁷, ou la rédaction des statuts d'une société²¹⁸), ou encore le notaire pour les actes notariés (le contrat de mariage²¹⁹, la dissolution d'une union civile²²⁰, la donation de meubles ou d'immeubles²²¹, etc.). En effet, même si le contrat intelligent et la chaîne de bloc ont pour caractéristique première d'évoluer dans un monde sans intermédiaire, l'avocat ou le notaire restent des protagonistes pouvant participer à l'élaboration du contrat intelligent. Le professionnel du droit consacre ainsi l'information des parties de façon officielle et atteste que les parties reconnaissent les conséquences juridiques de l'acte. Leur intervention est donc un gage de meilleure qualité des actes signés et d'une plus grande sécurité juridique.

²¹⁵ Art. 1378 al1 C.c.Q : « Le contrat est un accord de volonté, par lequel une ou plusieurs personnes s'obligent envers une ou plusieurs autres à exécuter une prestation. »

²¹⁶ Art. 2813 C.c.Q: « L'acte authentique est celui qui a été reçu ou attesté par un officier public compétent selon les lois du Québec ou du Canada, avec les formalités requises par la loi. »

²¹⁷ En vertu de la Loi sur les sociétés par actions, RLRQ c S-31.1

²¹⁸ En vertu de l'Art. 2250 C.c.Q

²¹⁹ En vertu de l'Art. 440 C.c.Q

²²⁰ En vertu de l'Art. 521.13 C.c.Q

²²¹ En vertu de l'Art. 1824 C.c.Q

Que le contrat intelligent soit le résultat d’un contrat traditionnel traduit en code, ou soit directement mis sous forme de code, le programmeur²²² doit traduire certaines clauses du contrat en langage de programmation selon la logique « if... then » (si x condition se réalise, alors l’action y s’enclenchera). Ce dernier s’auto-exécutera lorsque les conditions définies dans le contrat par les parties seront réunies. Ensuite, dans le contexte de la chaîne de blocs, le programme informatique du contrat intelligent y sera enregistré²²³.

Prenons l’exemple du logiciel « Ether Scriptor »²²⁴ qui propose différents exemples de codage pour plusieurs types de contrats (contrat de vote, contrat de mariage, contrat d’assurance, etc). Dans la figure ci-dessous, le logiciel propose un exemple de contrat d’enregistrement d’un vote (dans le cas proposé, les utilisateurs peuvent voter pour « COKE » ou « PEPSI »).

²²² Définition selon l’office québécois de la langue française : « Spécialiste qui traduit les opérations que l’ordinateur doit effectuer en une instruction que ce dernier peut comprendre. »

²²³ Le langage de script utilisé par Ethereum est le langage EVM (Ethereum Virtual Machine). Il est aussi possible d’utiliser un langage de plus haut niveau : le script « Solidity », « Serpent » ou « LLL ». Il existe des logiciels éditeurs de contrats intelligents qui transposent en code les clauses d’un contrat traditionnel de façon simplifiée.

²²⁴ Lien d’accès au logiciel Ether Scriptor : <https://etherscriptor.com/0-5-1/>

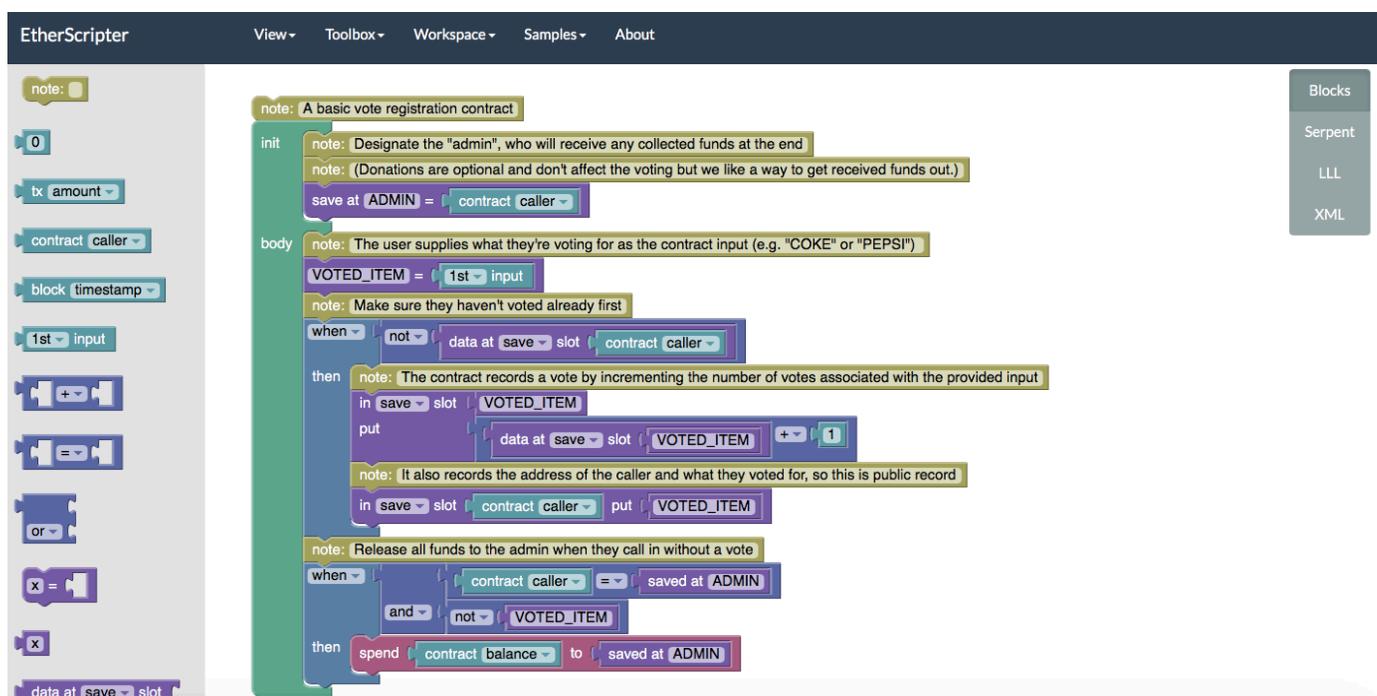


Figure 5. Exemple de codage simplifié d'un contrat de vote sur le logiciel EtherScripter²²⁵

Ce logiciel permet de construire des contrats intelligents sur Ethereum à partir de modèles proposés sous forme d'échantillons. Après avoir choisi le langage de programmation²²⁶ et le type de contrat souhaité²²⁷ (un échange d'actifs, un contrat de vente, un pari en ligne, etc.), un codage simplifié apparaît à l'écran. L'utilisateur peut ensuite cliquer sur les encadrés afin de personnaliser son contrat intelligent et y insérer tout d'abord l'identité de la personne « administrateur » qui doit recevoir les fonds lors de l'exécution du contrat, puis l'objet et les conditions du vote (définir l'objet du vote (en l'occurrence « Coke » ou « Pepsi »), et vérifier que la même personne ne puisse pas voter deux fois). Ensuite, le contrat enregistre un vote en incrémentant le nombre de votes associé à l'entrée fournie. Il enregistre également l'adresse de

²²⁵ <https://etherscripter.com/0-5-1/>

²²⁶ Ce logiciel propose différents types de langages de programmation : Blocks, Serpent, LLL et XML (en haut à droite de la figure).

²²⁷ Dans la figure ci-dessus, nous avons choisi le cas d'un enregistrement de vote.

l'appelant et ce pour quoi ils ont voté pour que ce soit un vote public, puis le contrat se termine en libérant les fonds à l'administrateur.

iv- L'auditeur

Il est très utile de vérifier que le contrat intelligent ainsi nouvellement codé soit conforme au contrat traditionnel, et plus particulièrement à la volonté des parties : c'est le rôle de l'auditeur. En effet, afin de s'assurer de la bonne programmation du contrat intelligent selon la volonté des parties, celles-ci peuvent choisir de faire auditer le contrat intelligent après qu'il ait été programmé. L'auditeur sera peut-être amené à faire évoluer son champ de compétences pour se porter vers les technologies de l'information et devrait notamment être capable de vérifier la structure et le code d'une chaîne de blocs ou d'un contrat intelligent²²⁸.

Comme pour le contrat traditionnel, il est important de pouvoir s'assurer que les risques encourus dans le contrat intelligent sont maîtrisés. Le contrat intelligent pourrait intégrer une procédure de suivi et de vérification de son élaboration. On l'imagine facilement dans une chaîne de blocs privée, mais ceci est plus difficile dans une chaîne de blocs publique. Comme l'évoque Mustapha Mekki²²⁹, une obligation de transparence serait mise à la charge des parties, et les acteurs se verraient imputer les dommages causés par un dysfonctionnement du contrat intelligent. Ce qui nous amène à intégrer diverses clauses de répartition des risques dans le contrat, tel que des clauses limitatives de responsabilité par exemple²³⁰.

²²⁸ Olivier DESPLEBIN et Gulliver LUX, « The evolution of accounting, control, audit and their practices through the prism of the Blockchain: a prospective reflection », in *Transitions numériques et informations comptables*, 39^{ème} Congrès de l'AFC (Nantes, France, 2018), cd-rom, <https://hal.archives-ouvertes.fr/hal-01907902>.

²²⁹ Mustapha MEKKI, préc., note 183

²³⁰ Cet aspect sera développé en seconde partie de ce mémoire.

v- L'oracle

Pour que le contrat intelligent puisse être employé dans le monde professionnel, il était nécessaire de résoudre le problème de la certification de la véracité des informations provenant de l'extérieur du réseau²³¹. L'exécution d'un contrat intelligent peut être immédiatement déclenchée (dans le cas d'un contrat de paiement électronique par exemple), ou s'exécuter suite à la réalisation d'une condition qui peut être interne au contrat intelligent (un déclenchement de l'exécution du contrat par l'arrivée à échéance par une date fixée au préalable par les parties), ou externe au contrat intelligent (le remboursement d'un voyageur si son avion est annulé).

La solution apportée au problème de certification de l'information dans le cas où celle-ci proviendrait de l'extérieur a été celle des oracles²³² ; il s'agit de placer sur le réseau des entités qui auront pour rôle de vérifier et de certifier les informations issues de l'extérieur, puis l'information sera ensuite intégrée à la chaîne de blocs.

L'exemple le plus souvent utilisé pour décrire le fonctionnement du contrat intelligent et de l'oracle est le contrat d'assurance contre une annulation de vol. Le contrat intelligent formé sur la base d'un contrat de police d'assurance sous la forme *if... then* (exemple : si le vol est retardé de deux heures ou plus, alors le client est indemnisé) est inscrit sur une chaîne de blocs. A partir d'un oracle, sont également intégrés à la chaîne de bloc les renseignements relatifs aux heures de vols de la compagnie aérienne (par exemple à partir du site internet de la compagnie aérienne concernée). Quand les informations de vols sont intégrées dans la chaîne de blocs, le programme du contrat intelligent vérifie si le retard du vol est supérieur à la limite de deux heures fixée dans le contrat, et enclenche l'assurance et le versement de l'indemnité si la condition se vérifie.²³³

²³¹ ANTONOPOULOS, Andreas M. et WOOD, Gavin. Préc., note 25

²³² L'oracle est un concept imaginé dans les années mille neuf cent cinquante par le mathématicien et programmeur britannique Alan TURING.

²³³ Exemple inspiré de l'article intitulé « Que peut apporter l'industrie de la chaîne de blocs à l'industrie de l'assurance ? » rédigé par Ingrid SAPONA. Consultation en ligne : <https://www.insuranceinstitute.ca/fr/cipsociety>

Ainsi, l'exécution du contrat sera générée par un oracle qui peut se présenter sous deux formes distinctes selon les cas²³⁴. Il peut être un tiers connu des deux parties et identifié dans le contrat au préalable, ou bien une base de données externe qui aura été choisie par les parties et à laquelle le contrat intelligent se réfèrera.

Tout d'abord, l'oracle peut constituer un ou plusieurs agents, approuvés par les participants de la chaîne de blocs, qui iront chercher l'information au moment opportun. Celui-ci surveille donc les paramètres externes conçus dans le contrat intelligent et donne les directives ou son approbation pour exécuter le contrat si les paramètres sont respectés²³⁵. En d'autres termes, il effectue le lien entre la chaîne de blocs et le monde « réel » afin d'attester des événements extérieurs. Ce type d'oracle sera utilisé par exemple dans un contrat intelligent conclu pour la réalisation de travaux de rénovation d'une maison. Cette information ne peut être obtenue par un algorithme seul et nécessite l'intervention d'un agent sur place pour attester de la bonne avancée des travaux ou non.

Dans d'autres cas, l'intervention d'un agent ne sera pas nécessaire pour relayer l'information au contrat intelligent; un algorithme seul sera capable de réaliser ce relais, et c'est vers l'utilisation de cette autre forme d'oracle que les concepteurs du contrat intelligent veulent tendre. En effet, l'oracle peut aussi prendre la forme d'une base de données externe, identifiée et sélectionnée au préalable par les parties, que le contrat intelligent consultera au moment opportun pour s'exécuter ensuite.

Pour mieux comprendre, imaginons une DApp développée sur Ethereum permettant de réaliser des paris sportifs. Dans ce cas, à la fin du match, la personne qui pari est prélevée ou rémunérée automatiquement en fonction du résultat. Cependant, une chaîne de blocs ne peut pas, à elle

²³⁴ Boris BARRAUD, « Les blockchains et le droit », *Revue Lamy Droit de l'immatériel*, n° 147 (2018): 48-62.

²³⁵ Alan COHN, Travis WEST, et Chelsea PARKER, « Smart after all: blockchain, smart contracts, parametric insurance, and smart energy grids » 1 (2017): 32.

seule, aller chercher l'information du résultat du match. Il est donc nécessaire de recourir à un facteur externe qui pourra trouver l'information, l'inclure dans le contrat, et en déterminer l'issue. Dans ce cas, l'oracle constituera le lien avec une base de données (le site officiel de la NHL par exemple), qui communiquera au contrat intelligent à qui appartient la victoire. L'oracle est donc un intermédiaire externe à la chaîne de blocs, mais y est lié et permet de fournir au contrat intelligent la donnée externe nécessaire.

Autre exemple d'un oracle qui prend la forme d'un algorithme relié à une base de données ; le cas d'un testament conclu via un contrat intelligent : l'oracle pourra aller chercher dans le registre des décès la certification qu'une personne est décédée ou non et ainsi déclencher le virement de fonds selon le testament.

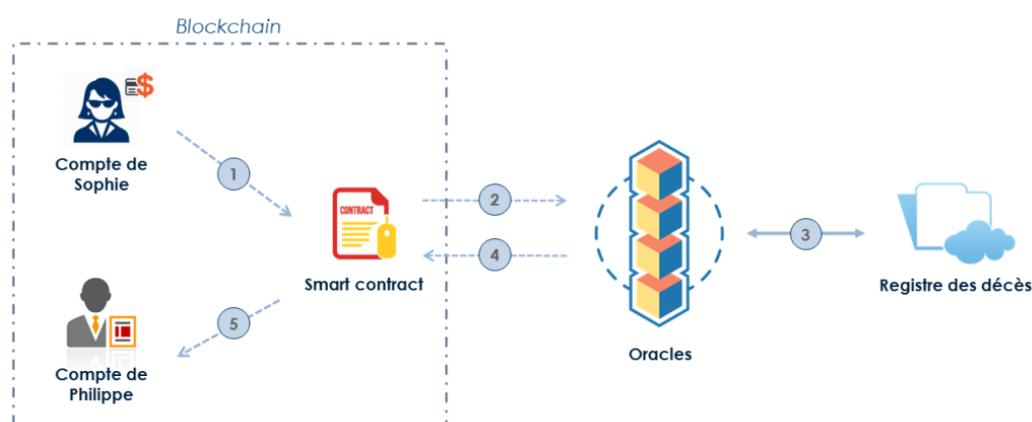


Figure 6. Schéma simplifié d'un contrat intelligent dans le cas d'un testament²³⁶

Dans cet exemple, Sophie crée un contrat car elle souhaite transférer des fonds à Philippe si elle décède. Le contrat intelligent se réfère alors à un oracle ayant pour rôle de consulter le registre

²³⁶ Source : <https://www.insurancespeaker-wavestone.com/2016/03/dossier-blockchain-futur-tiers-de-confiance-utilisations-possibles-de-blockchain-assurance/>

officiel des décès²³⁷ et retransmet l'information au contrat intelligent. Les mineurs valident la transaction puis celle-ci est inscrite dans la chaîne de blocs et Philippe reçoit les fonds.

Il existe aujourd'hui des entreprises²³⁸ qui offrent des services permettant de créer des oracles pour vérifier des informations extérieures pertinentes à l'exécution des contrats intelligents, comme par exemple les données météorologiques, le cours des actions en bourse, le taux d'intérêt pratiqué par les banques, etc.

Cependant, comme le rappelle Antonopoulos et Wood, l'utilisation d'un oracle n'est pas sans risques pour le contrat intelligent :

« Of course, oracles also introduce a significant risk—if they are trusted sources and can be compromised, they can result in compromised execution of the smart contracts they feed. (...) If you assume the oracle can be trusted, you may be undermining the security of your smart contract by exposing it to potentially false inputs. That said, oracles can be very useful if the security assumptions are carefully considered ».²³⁹

En effet le risque relatif à l'utilisation de l'oracle dans le contrat intelligent serait que celui-ci ne donne pas l'information, ou donne une mauvaise information qui elle-même entraînerait une mauvaise exécution du contrat intelligent. S'il n'envoie aucune information sur la chaîne de blocs alors le contrat ne va jamais s'exécuter. Les concepteurs du contrat doivent donc prévoir une clause annexe afin que si aucune information n'est entrée, le contrat est nul et chacun récupère ses fonds²⁴⁰. Si une mauvaise information est donnée, alors le contrat ne s'exécutera pas comme

²³⁷ Par exemple le Répertoire National d'Identification des Personnes Physique (RNIPP) en France.

²³⁸ Rhombus est une entreprise dont la devise est "Connect your smart contract with real-world data" consultable sur le site <https://rhombus.network>; Verity est une autre entreprise qui se présente comme une solution d'oracle et énonce : « Use Verity to verify real-world information for your smart contracts. Examples include: sports and eSports data feeds, fake news detection, real-time content moderation, image recognition, insurance claims, sentiment analysis, live events data, real-time market research and more. », En consultation sur le site <https://verity.network>

²³⁹ ANTONOPOULOS, Andreas M. et WOOD, Gavin. Préc., note 25

²⁴⁰ Site officiel Ethereum France, en ligne : <https://www.ethereum-france.com/les-oracles-lien-entre-la-blockchain-et-le-monde/>

prévu et aucun retour en arrière ne sera possible. Les questions de responsabilités face à ce type d'hypothèses seront abordées en seconde partie de ce mémoire.

b. L'Oracle : un frein à la décentralisation ?

Comme le précise Ethereum France, « le système d'Oracle implique le recours à une personne ou une société tierce dont le rôle est de rechercher et d'insérer l'information demandée »²⁴¹. Or la décentralisation est au cœur du concept de contrat intelligent afin de pouvoir intégrer dans le monde des affaires et de la contractualisation une sécurité optimale. Selon certains auteurs, les oracles réincarnent alors le « tiers de confiance » que la technologie de la chaîne de bloc a souhaité écartier afin d'évoluer dans un monde qui se voudrait entièrement décentralisé²⁴².

Peut-on parler de décentralisation quand un contrat intelligent nécessite l'intervention d'un oracle pour s'exécuter ? En effet, avec l'intervention des oracles, on revient finalement à une forme de réintroduction des intermédiaires au sein du processus de la chaîne de blocs, puisque l'oracle représente cette information considérée comme une vérité et donc un élément de confiance dans la relation d'affaire entre les contractants. A l'aide de données cryptographiques, l'oracle basé sur une information disponible en ligne, peut vérifier et certifier la source de l'information puis l'intégrer dans le contrat intelligent²⁴³. S'il semble facile de recueillir certaines informations concrètes sur des sites certifiés telles que l'horaire d'un avion sur le site officiel d'une compagnie aérienne, la météo du jour sur un site météorologique national, ou le résultat d'un match sportif sur le site officiel d'une ligue, il semble plus compliqué de certifier les informations concernant d'autres types de recherches plus complexes qui peuvent donner lieu à plusieurs vérités²⁴⁴.

²⁴¹ *Id.*

²⁴² Mustapha MEKKI, Préc., note 229

²⁴³ Vanessa RABESANDRATANA et Nicolas BACCA, « L'Oracle hardware : la couche de confiance entre les blockchains et le monde physique », *Annales des Mines - Réalités industrielles* Août 2017, n° 3 (26 juillet 2017): 91.

²⁴⁴ *Id.*

Si l'objectif de l'oracle est de trouver la « bonne » information de source certifiée et officielle, encore faut-il que cette source ne soit pas erronée, falsifiée ou désuète. Si on reprend l'exemple cité plus haut²⁴⁵ relatif à la conclusion d'un testament via un contrat intelligent, il se peut que l'oracle ne puisse aller chercher l'information souhaitée si, par exemple, le registre officiel des décès, sur lequel il devait se baser, n'est pas mis à jour ou donne des informations erronées. L'oracle n'aura pas la capacité de juger si les résultats qu'il fournit sont cohérents ou non ; il les restituera comme tel et exécutera le contrat à tort, ce qui peut engendrer des erreurs de transmission de fonds. Or, rappelons-le, un contrat qui s'exécute sur une chaîne de bloc ne peut être modifié²⁴⁶ :

« It is important to remember that a contract's code cannot be changed. However, a contract can be "deleted," removing the code and its internal state (storage) from its address, leaving a blank account. Any transactions sent to that account address after the contract has been deleted do not result in any code execution, because there is no longer any code there to execute. »²⁴⁷

Pour assurer la sécurité des données fournies par l'oracle, on pourrait choisir de combiner plusieurs oracles afin de réaliser une « moyenne » et ainsi assurer la fiabilité de l'information fournie dans le contrat intelligent. Cependant en cas de litige, le fait que les parties ne se soient pas accordés au préalable sur un oracle en particulier mais que ce soit finalement un ordinateur qui fasse le choix de l'oracle à partir d'une moyenne, peut poser une difficulté à propos de la validité du contrat intelligent dans le sens où ce n'est plus un « accord de volonté »²⁴⁸ au sens de l'article 1378 alinéa 1 du *Code civil du Québec*²⁴⁹.

²⁴⁵ Se référer à la figure n°6 de ce mémoire.

²⁴⁶ Wright, AARON, and Primavera DE FILIPPI. "Decentralized blockchain technology and the rise of lex cryptographia." (2015).

²⁴⁷ ANTONOPOULOS, Andreas M. et WOOD, Gavin. Préc., note 25

²⁴⁸ LORE, « Evolution ou révolution pour les contrats en France ? »

²⁴⁹ Art 1378 C.c.Q

II. Le partage de responsabilité en cas de mauvaise exécution d'un contrat intelligent

Il est certain que les contrats intelligents ne peuvent offrir qu'une approche approximative du droit des contrats car il est par exemple difficile de prendre en compte les règles de droit touchant à la suspension de l'exécution de l'obligation, tel que les circonstances imprévues, ou encore faire intervenir un jugement humain tel que le raisonnable ou la bonne foi²⁵⁰. Aussi, le fait de se fier à des oracles constitue à la fois une force car ils sont le lien nécessaire entre la chaîne de blocs et le monde réel²⁵¹, et une faiblesse car c'est l'exécution automatique du contrat intelligent qui sera touchée en cas d'informations erronées véhiculée par le ou les oracles²⁵². En effet il faut prendre en compte le fait que la non-exécution ou la mauvaise exécution du contrat intelligent initialement prévu par les parties peut engendrer un préjudice pour une des parties au contrat ou un tiers. Qui doit alors répondre de ce dommage engendré par le contrat intelligent ? Est-ce le créateur du logiciel, les programmeurs, les professionnels du droit, ou les tiers de confiance ?

N'ayant pas de fondements juridiques propres, les questions de responsabilité relatives aux contrats intelligents nécessitent d'être évaluées au regard du régime classique du droit des obligations. Ces dispositions sont-elles adaptées dans le cadre du contrat intelligent ? Pour répondre à ces interrogations, nous nous intéressons à la question de savoir comment peut-on appliquer le cadre législatif en vigueur, à savoir principalement les dispositions du *Code Civil du Québec*, aux évolutions technologiques telles que la mise en place du contrat intelligent au

²⁵⁰Philippe PERRENOUD, *Gestion de l'imprévu, analyse de l'action et construction de compétences*, Éducation permanente, 1999, vol. 140, no 3, p. 144.

²⁵¹ ANTONOPOULOS, Andreas M. et WOOD, Gavin. Préc., note 25

²⁵² TAI, Eric et TJONG Tjin. "Force Majeure and Excuses in Smart Contracts.", *European Review of Private Law*, 2018, vol. 26, no 6, p. 804.

Québec. Pour cela, il est nécessaire d'identifier les dispositions applicables aux dommages causés par l'utilisation d'un contrat intelligent.

Dans le contrat traditionnel, le fait que le contenu puisse être corrompu de façon spontanée n'est pas une chose commune, alors que le code d'un contrat intelligent peut, à tout moment, changer et affecter le mode de fonctionnement de ce dernier²⁵³. Dans ce cas précis, la responsabilité ne peut être attribuée à aucune des parties, sauf si c'est un tiers qui commet l'erreur. En effet, il est possible que le programmeur code de manière incorrecte les conditions convenues par les parties, ou bien que la source d'information externe (les oracles) sur laquelle le contrat intelligent se base, soit erronée²⁵⁴.

Le régime de responsabilité applicable diffèrera selon l'origine de la faute commise ainsi que les acteurs impliqués. En effet, s'il s'avère que l'audit commet une faute dans la traduction de l'intention des parties au contrat, l'applicabilité d'une responsabilité contractuelle sera évidente. Tandis que la responsabilité des acteurs engagés non contractuellement dans l'élaboration du contrat intelligent sera plus difficile à définir²⁵⁵. Pour cette raison, dans cette étude, nous ferons le choix de traiter dans un premier temps le cas d'un dommage causé par une erreur réalisée lors de la création du contrat intelligent à savoir par les parties, le programmeur ou l'audit, puis dans un second temps nous évaluerons le cas d'un dommage causé par l'exécution du contrat intelligent en abordant notamment l'applicabilité de la responsabilité de l'oracle.

²⁵³ Mark GIANCASPRO, préc., note 194

²⁵⁴ *Id.*

²⁵⁵ LAUSLAHTI, Kristian, MATTILA, Juri, et SEPPALA, Timo. "Smart Contracts—How will blockchain technology affect contractual practices?", 2017.

A. Dans le cas d'un dommage causé par une erreur survenue lors de la mise en place du contrat intelligent

Cette partie consiste à déterminer les cas d'engagement de responsabilité lors de la mise en place du contrat intelligent; les acteurs impliqués dans cette étape du processus sont essentiellement les cocontractants, et les programmeurs. À noter que les avocats participant au processus peuvent aussi avoir leur part de responsabilité, mais cette éventualité ne sera pas mentionnée dans ce mémoire car la jurisprudence²⁵⁶ en termes de responsabilité professionnelle des avocats est déjà bien établie en droit²⁵⁷.

D'une part, il est possible que l'origine du dommage provienne d'une faute commise par les parties, ou leurs représentants, ayant par exemple mal transmis leurs intentions au programmeur. D'autre part, le programmeur peut aussi commettre une erreur d'interprétation de la volonté des parties, tout comme l'auditeur peut aussi commettre une erreur lors de la validation des termes du contrat. C'est donc ici la bonne transmission de la volonté des parties, la bonne compréhension de la part du programmeur, ainsi que la qualité de la validation de l'auditeur qui définiront la part de responsabilité de chacun dans le cas d'une éventuelle mauvaise conception d'un contrat intelligent.

²⁵⁶ Sur ce point, ces deux décisions traitent de l'étendue du devoir de conseil de l'avocat : *Labrie c. Tremblay*, Cour d'appel, Québec, 200-09-001084-987, 7 décembre 1999. Consulter aussi l'affaire *Côté et Les entreprises générales Rimo c. Rancourt*, Cour supérieure, St-François, 450-05-001065-966, 25 novembre 1999, en appel.

²⁵⁷ Denis BORGIA, « *La responsabilité professionnelle de l'avocat.* » Service de la formation permanente du Barreau du Québec, *Développements récents en droit immobilier* (1996), Cowansville, Éditions Yvon Blais, p.3

1. L'engagement de la responsabilité des parties dans le contrat intelligent

Comme évoqué en première partie, le statut juridique du contrat intelligent n'est pas explicité dans les textes de lois. Son statut découle d'interprétations diverses au travers des dispositions existantes contenues notamment dans le *Code civil du Québec* ainsi que la *Loi concernant le cadre juridique des technologies de l'information*. Les parties se doivent d'être les plus claires possible dans l'émission de leurs intentions concernant la relation d'affaires afin que le programmeur puisse traduire les clauses sous forme de code informatique. Partant de ce constat, nous évaluerons les cas de responsabilité des cocontractants par analogie à la machine distributrice, puis l'engagement de la responsabilité du programmeur et de l'auditeur car tous deux interviennent, au même titre que les cocontractants, lors de l'élaboration du contrat intelligent.

a. L'exemple de la machine distributrice

Le concept d'exécution automatique d'une obligation contractuelle qui se trouve derrière le contrat intelligent n'est pas entièrement nouveau ; c'est ce que nous avons vu en introduction lorsque Nick Szabo donne l'exemple de la machine distributrice²⁵⁸ pour expliquer le concept de contrat intelligent. Selon lui, la machine distributrice est une forme de contrat entre un consommateur et un marchand, qui s'exécute sans l'intervention d'un tiers²⁵⁹ ; n'importe quelle personne qui détient des pièces de monnaies ou une carte de crédit peut contracter avec le vendeur par l'intermédiaire de la machine.

²⁵⁸ SZABO, Nick. "Formalizing and securing relationships on public networks". *First Monday*, 1997, vol. 2, no 9.

²⁵⁹ *Ibid.*

Comme le démontre la figure ci-dessous, une machine distributrice correspond à un contrat intelligent entre un client et un fournisseur, dans le sens où elle est conçue pour réaliser un transfert de propriété en fonction de règles prédéfinies²⁶⁰.

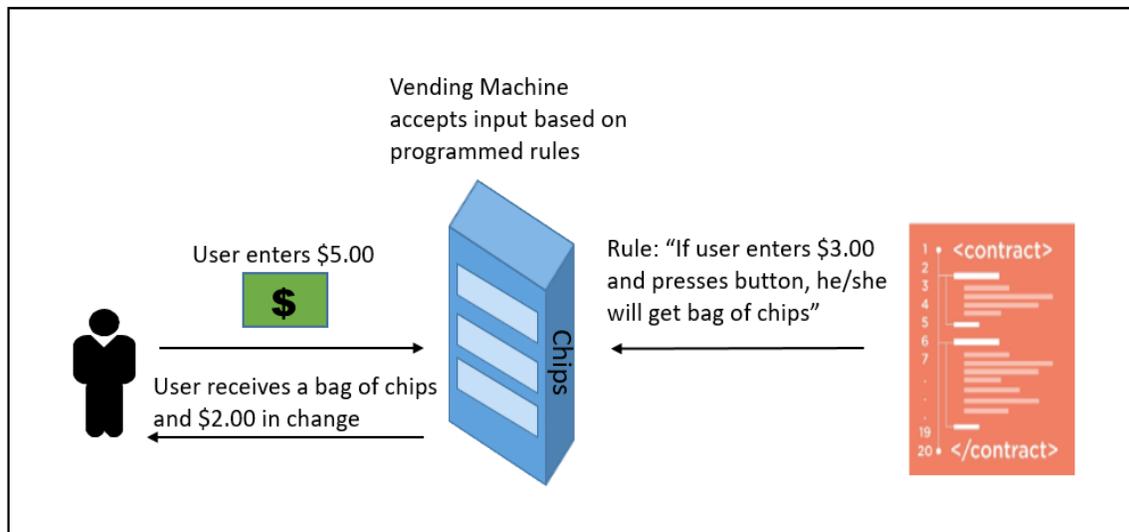


Figure 7. L'exemple de la machine distributrice en tant que contrat intelligent²⁶¹

Dans cet exemple, un client entre 5\$ dans la machine pour un paquet de chips qui coûte 3\$. La machine agit alors en fonction de différents scénarios définis au préalable : si le montant donné par le client correspond au prix du paquet de chips, alors la machine délivre le produit. Si le montant donné est supérieur au prix du produit, alors la machine délivrera le produit, ainsi que la monnaie de 2\$. Si le client ne délivre pas assez d'argent, alors la machine ne délivrera pas le produit et rendra la monnaie insérée par le client dans la machine. Cette dernière est un intermédiaire parfaitement fiable entre le fabricant de boissons et l'acheteur.²⁶²

²⁶⁰ Andrea M. ROZARIO and Miklos A. VASARHELYI, "Auditing with smart contracts", The International Journal of Digital Accounting Research Vol. 18, 2018, pp. 1-27

²⁶¹ Ibid.

²⁶² MILLER, Mark S. et STIEGLER, Marc. « The digital path: smart contracts and the Third World », Markets, Information and Communication. Routledge, 2003. p. 79.

Si la machine distributrice est un exemple éclairant du concept de contrat intelligent, son régime de responsabilité est plus simple à définir que celui d'un contrat intelligent basé sur la chaîne de blocs puisque les deux outils sont très différents sur un point : leur niveau d'automatisme ainsi que le caractère décentralisé et anonyme que possède la chaîne de blocs. En effet, là où la machine n'est que partiellement automatique (dans le sens où l'acheteur doit insérer une pièce de monnaie pour activer la livraison du produit), le déclenchement du contrat intelligent est entièrement automatique : c'est un événement extérieur ou interne au contrat, prévu en amont, qui déclenche le contrat sans aucune intervention de l'acheteur.

Notons toutefois que le niveau de capacité à identifier les intermédiaires ne sera pas le même entre la machine distributrice et le contrat intelligent dont les répercussions sont implémentées sur une chaîne de blocs. En effet la caractéristique première de la chaîne de blocs tient en sa capacité à décentraliser les informations qu'elle détient²⁶³. L'anonymat ainsi instauré par la chaîne de blocs rend plus difficile la détermination des responsabilités en cas de dommage subi. Dans plusieurs affaires²⁶⁴ relatives aux technologies de l'information, les juges énoncent l'article 22 de la *Loi concernant le cadre juridique des technologies de l'information* qui vient limiter la responsabilité des intermédiaires techniques²⁶⁵ :

« Le prestataire de services qui agit à titre d'intermédiaire pour offrir des services de conservation de documents technologiques sur un réseau de communication n'est pas responsable des activités accomplies par l'utilisateur du service au moyen des documents remisés par ce dernier ou à la demande de celui-ci.

Cependant, il peut engager sa responsabilité, notamment s'il a de fait connaissance que les documents conservés servent à la réalisation d'une activité à caractère illicite ou s'il a

²⁶³ Côte BERBAIN, préc., note 33

²⁶⁴ *Ibid.* ; *Warman c. Lemire*, 2009 TCDP 26 ; *Corriveau c. Canoe inc.*, 2010 QCCS 3396

²⁶⁵ Nicolas VERMEYS, « C-11, la Loi concernant le cadre juridique des technologies de l'information et la responsabilité des intermédiaires techniques québécois : une dualité de régimes (in)utile(s) ? », (2013) 25(3) CPI 1051.

connaissance de circonstances qui la rendent apparente et qu'il n'agit pas promptement pour rendre l'accès aux documents impossible ou pour autrement empêcher la poursuite de cette activité. »²⁶⁶

Dans l'affaire *Vaillancourt c. Lagacé*²⁶⁷, relative à la diffusion de propos diffamatoires sur Internet²⁶⁸, les tribunaux auraient pu recourir à l'article 22 LCCJTI qui vient limiter la responsabilité de l'intermédiaire technique²⁶⁹. En l'espèce, madame Vaillancourt fonde en 2003 le Centre aviaire Johanne Vaillancourt (ci-après nommé « CAJV »). Vaillancourt signe une première entente en 2004 avec madame Lagacé pour que cette dernière puisse donner des cours de formation à Québec pour le CAJV, puis décide en 2005 de créer un site web pour diffuser le contenu de ses cours. Les deux femmes signent une seconde entente en 2005 dans laquelle Vaillancourt permet à Lagacé de dispenser ses cours et de se servir de son nom et de son matériel à des fins professionnelles. Quelques mois plus tard, Lagacé crée le Club d'étude de comportement aviaire (ci-après « CECA ») auquel s'ajoute son propre site web qui donne notamment accès à un blogue. Lagacé annonce aux membres de CAJV que les cours seront désormais dispensés par elle et en son nom via le CECA. Vaillancourt allègue une violation de droits d'auteurs, et que ce blogue contient des propos diffamatoires et mensongers à son égard. L'une des questions en litige était alors de savoir quel intermédiaire devait être en capacité de garder le contrôle des propos tenus sur internet. Les juges estiment « [31] Aucune preuve technique n'a été déposée expliquant le fonctionnement d'un blogue. D'après la définition de l'Office de la langue française, les internautes communiquent leurs idées directement sur le site. Aucune preuve n'indique qu'un ou plusieurs des défendeurs ont le contrôle sur les propos qui y sont tenus, ni qu'ils ont la capacité technique de supprimer certains commentaires. ».

²⁶⁶ Art. 22 de la Loi concernant le cadre des technologies de l'information, préc., note 142

²⁶⁷ *Vaillancourt c. Lagacé*, 2005 QCCS 29333. Décision citée par Pierre TRUDEL dans son rapport « La responsabilité sur internet en droit civil ».

Extrait de la décision en ligne : <https://www.lccjti.ca/decisions/vaillancourt-c-lagace-2005-qccs-29333/>

²⁶⁸ Voir de rapport de Pierre TRUDEL, « La responsabilité sur internet en droit civil québécois ». Rapport préparé pour le colloque de droit civil 2008 de l'institut national de la magistrature, Ottawa, 13 juin 2008. En ligne : https://www.pierretrudel.net/files/sites/6/2015/01/TRUDEL_resp_internet.pdf

²⁶⁹ Nicolas VERMEYS, préc., note 265

Si on applique cette disposition au contrat intelligent, et que le juge venait à poser la même question en cas de litige, qui en aurait le contrôle ? Rappelons qu'une transaction réalisée via un contrat intelligent est validée par des milliers d'utilisateurs sur le réseau²⁷⁰. Comment pourrait-on alors identifier celui ou celle qui en aurait le contrôle ? Au sein d'une chaîne de blocs privée, il est possible d'envisager que la personne en capacité de garder le contrôle soit la personne qui ait initié la chaîne de blocs privée. Dans ce type de chaîne de blocs, cette personne est identifiable, ce qui nous permettrait de mettre un nom sur la personne responsable en cas de dommage subi par les parties dans le cas où le réseau commettrait une erreur ou subirait une attaque. Cependant, dans une chaîne de blocs publique, c'est l'anonymat qui prime via le système distribué.

Comme le mentionnent les auteurs Zetzche, Buckley et Arner²⁷¹, le grand livre distribué pourrait être considéré comme une coentreprise. Ainsi les nœuds du réseau seraient de simples entrepreneurs qui s'engagent à respecter un processus de traitement et à maintenir un niveau de sécurité des données. Dans ce cas, selon les auteurs les cocontractants pourraient compter sur une responsabilité contractuelle. Il y aurait selon eux une responsabilité du réseau interne, à savoir entre les nœuds du réseau, et une responsabilité du réseau externe c'est-à-dire vis-à-vis des tierces parties. Un nœud a envers les autres nœuds un devoir de loyauté (par exemple mettre à jour son matériel); il ne doit pas nuire au bon fonctionnement de la validation des transactions et serait directement responsable de la perte économique en cas de faille dans le réseau ou de piratage réussi. Si c'est un tiers qui est directement affecté par un stockage de données non sécurisé alors il pourrait engager une responsabilité délictuelle de tous les nœuds du réseau.

²⁷⁰ Se référer à la partie I du mémoire concernant les « nœuds du réseau ».

²⁷¹ ZETZSCHE, Dirk A., BUCKLEY, Ross P., et ARNER, Douglas W. "The distributed liability of distributed ledgers: Legal risks of blockchain". *U. Ill. L. Rev.*, 2018, p. 1361.

b. La responsabilité des cocontractants du contrat intelligent

Au Québec, le régime de responsabilité civile, qu'il soit contractuel ou extracontractuel, est basé sur la notion de faute²⁷². Alors, pour engager la responsabilité civile d'un individu en lien avec un contrat intelligent, comme le droit commun l'expose, il serait nécessaire d'invoquer une faute, un dommage et un lien de causalité.²⁷³ Selon les auteurs Jean-Louis Baudouin, Patrice Deslauriers et Benoît Moore, la faute se définirait au regard de deux éléments constitutifs : « un manquement à un devoir préexistant et la violation d'une norme de conduite »²⁷⁴. Les tribunaux vont en ce sens et adoptent la même qualification de la faute, à savoir une conduite qui s'écarte de la norme de comportement qu'adopterait une personne prudente et diligente²⁷⁵. À ce propos, en matière extracontractuelle, l'article 1457 du *Code Civil du Québec*²⁷⁶ se réfère à la personne « douée de raison » :

« Toute personne a le devoir de respecter les règles de conduite qui, suivant les circonstances, les usages ou la loi, s'imposent à elle, de manière à ne pas causer de préjudice à autrui. Elle est, lorsqu'elle est douée de raison et qu'elle manque à ce devoir, responsable du préjudice qu'elle cause par cette faute à autrui et tenue de réparer ce préjudice, qu'il soit corporel, moral ou matériel. »

²⁷² Jean-Louis BAUDOUIN, Patrice DESLAURIERS, *La responsabilité civile*, 8e Éd., Éditions Yvon Blais, Cowansville, 2014,

²⁷³ Article 1457 C.c.Q : « Toute personne a le devoir de respecter les règles de conduite qui, suivant les circonstances, les usages ou la loi, s'imposent à elle, de manière à ne pas causer de préjudice à autrui. Elle est, lorsqu'elle est douée de raison et qu'elle manque à ce devoir, responsable du préjudice qu'elle cause par cette faute à autrui et tenue de réparer ce préjudice, qu'il soit corporel, moral ou matériel. Elle est aussi tenue, en certains cas, de réparer le préjudice causé à autrui par le fait ou la faute d'une autre personne ou par le fait des biens qu'elle a sous sa garde. »

²⁷⁴ Jean-Louis BAUDOUIN, Patrice DESLAURIERS, préc., note 272 par. 1-162. Voir aussi Pierre TRUDEL, France ABRAN, Karim BENYekhlef et Sophie HEIN *Droit du cyberspace*, Montréal, Éditions Thémis, 1997, 1296 p., c. 5

²⁷⁵ *Affaire Ciment du Saint-Laurent inc. c. Barrette*, 2008 CSC 64, [2008] 3 R.C.S. 392, par. 21. Voir aussi J.-L. BAUDOUIN et P. DESLAURIERS, *La responsabilité civile* (7e éd. 2007), vol. I, p. 171

²⁷⁶ Préc., note 273

Dans le cas où une partie manquerait à son devoir et tenterait de nuire lors de l'élaboration du contrat intelligent (par exemple en omettant intentionnellement d'inclure une clause dans le contrat), sa responsabilité civile pourrait être engagée. Lorsque l'une des parties omet de transmettre une information ou fait une erreur dans la transmission de ses intentions envers le programmeur, la réparation du préjudice subi se fera sur la base de la responsabilité civile contractuelle²⁷⁷. S'ajoute à cette disposition les obligations qui résultent de l'article 1375 du *Code civil du Québec*²⁷⁸, à savoir la notion de bonne foi et les obligations annexes qu'elle engendre. L'une de ses obligations connexes est l'obligation d'information que les auteurs Baudouin et Jodoin déterminent ainsi :

« Lorsque l'un des futurs contractants occupe une position privilégiée par rapport à l'autre, soit en raison de la connaissance qu'il a de certaines informations, soit en raison de la possibilité d'y avoir accès, il doit parfois, pour ne pas tromper la confiance légitime de l'autre, prendre l'initiative de fournir à ce dernier certains renseignements cruciaux. L'obligation précontractuelle d'information se fonde donc, soit sur les articles 6 et 1375, soit, plus précisément, sur l'article 1401 C.c. »²⁷⁹

Dans l'exemple d'une mauvaise transmission des intentions d'une partie, il est possible d'envisager une faute d'omission²⁸⁰ dans le sens où l'individu en cause n'a pas agi et a omis de transmettre des informations essentielles à la bonne conception du contrat intelligent. Les parties sont dans l'obligation de communiquer de manière exacte leurs intentions au programmeur.

²⁷⁷ Art. 1434 C.c.Q: "Le contrat valablement formé oblige ceux qui l'ont conclu non seulement pour ce qu'ils y ont exprimé, mais aussi pour tout ce qui en découle d'après sa nature et suivant les usages, l'équité ou la loi."

²⁷⁸ Art 1375 C.c.Q: « La bonne foi doit gouverner la conduite des parties, tant au moment de la naissance de l'obligation qu'à celui de son exécution ou de son extinction. »

²⁷⁹ Jean-Louis BAUDOUIN et Pierre-Gabriel JOBIN, *Les Obligations*, 5e éd., Cowansville, Éditions Yvon Blais, 1998, no 306 p. 265.

²⁸⁰ *Bolduc c. Lévis (Ville de)*, (C.A., 2015-09-11), 2015 QCCA 1428 ; Dans cette affaire le juge retient la faute d'omission pour établir la responsabilité de l'intimée : [26] « Toutefois, le juge a estimé que la Ville a commis une faute à l'égard de l'appelant. Il précise que l'inspecteur municipal n'a pas fait respecter le règlement, n'a pas informé l'appelant de son existence et n'a procédé à aucune inscription relative à la zone sur le permis ».

Dans l'affaire *Distributeur MDR inc. c. Blanchette*²⁸¹, deux parties conviennent de la vente d'une route de machines distributrices. Après quelques temps, l'acheteur réalise que les machines sont souvent défectueuses, et que les revenus générés par les machines ne sont pas à la hauteur des prévisions que lui avait fourni son cocontractant. La victime plaide alors un dol de la part de son cocontractant, ce qui constitue un vice de consentement au sens de l'article 1401 du *Code civil du Québec*²⁸². Les juges considèrent qu'il y a eu dol par réticence concernant les revenus estimés, dans le sens où son cocontractant est resté réticent pour prononcer les ventes réelles alors que l'acheteur lui avait clairement demandé ces informations avant l'achat de la route. Le dol renvoie à un manquement à l'obligation d'agir de bonne foi prévue à l'article 1375 du *Code civil du Québec*²⁸³.

Cette affaire démontre bien les obligations annexes que l'obligation de bonne foi engendre, et que la faute commise par une partie peut être intentionnelle ou non, et découler d'un manquement de la part d'un individu à ses obligations contractuelles²⁸⁴. Une faute commise par les parties dans le contrat intelligent pourra découler d'un acte (c'est le cas d'un utilisateur du contrat qui corrompt la chaîne de blocs et prive alors les parties de « l'exécution automatique de leurs obligations »²⁸⁵), ou bien d'une omission d'agir par un manquement à leur obligation d'information.

Si les parties ne sont pas à l'abri de se voir invoquer une responsabilité pour faute, qu'en est-il du programmeur chargé de traduire l'intention des parties en langage informatique, ou de l'auditeur chargé d'en valider la conformité ?

²⁸¹ *Distributeur MDR inc. c. Blanchette* (C.S., 2014-05-26), 2014 QCCS 2204, SOQUIJ AZ-51076150, 2014EXP-1865

²⁸² Art. 1401 C.c.Q : « L'erreur d'une partie, provoquée par le dol de l'autre partie ou à la connaissance de celle-ci, vicie le consentement dans tous les cas où, sans cela, la partie n'aurait pas contracté ou aurait contracté à des conditions différentes. Le dol peut résulter du silence ou d'une réticence. »

²⁸³ Préc. note 278

²⁸⁴ *Provigo Distribution Inc. v. Supermarché A.R.G. Inc.*, 1997 CanLII 10209 (QC CA); « A civil fault exists as soon as there is an established breach of a contractual obligation, whether explicitly defined by the parties to the contract or implicit and arising from the nature of the contract or equity. »

²⁸⁵ Catherine BARREAU, préc., note 193

2. L'engagement de la responsabilité du programmeur ou de l'auditeur

Le programmeur ainsi que l'auditeur sont des acteurs qui interviennent lors de l'élaboration du contrat intelligent, avant que celui-ci entre en phase d'exécution. Il est donc opportun d'envisager les hypothèses dans lesquelles ces deux acteurs pourraient engager leur responsabilité. Le programmeur ayant pour rôle de traduire une partie des clauses communiquées par les parties en code informatique, sa responsabilité peut être engagée si les dommages causés par le contrat intelligent proviennent d'une erreur de codage par exemple. Quant à l'auditeur qui peut intervenir afin de valider la corrélation entre l'intention des parties dans la relation d'affaire et le codage mis en place par le programmeur, sa responsabilité pourrait aussi être engagée en cas d'erreur de validation.

a. L'engagement de la responsabilité du programmeur dans le contrat intelligent

Outre un manquement de la part des cocontractants à leur obligation d'information envers le programmeur, il est possible d'envisager le cas inverse c'est-à-dire un manquement du programmeur dans son obligation de traduire l'intention des parties sous forme de code pour créer le contrat intelligent. Dans cette partie, nous envisageons l'hypothèse où le contrat intelligent serait assimilé à un logiciel pour répondre aux questions d'engagement de responsabilité du programmeur.

i- Dans le cas d'une mauvaise traduction de l'intention des parties par le programmeur

Par le terme de contrat « intelligent », il serait possible de vouloir faire l'analogie avec l'intelligence artificielle et donc lui appliquer le régime juridique applicable aux robots²⁸⁶.

²⁸⁶ Art. 1468, al.1 C.c.Q : « Le fabricant d'un bien meuble, même si ce bien est incorporé à un immeuble ou y est placé pour le service ou l'exploitation de celui-ci, est tenu de réparer le préjudice causé à un tiers par le défaut de sécurité du bien ».

Cependant cette analogie ne serait pas exacte aujourd'hui. La seule hypothèse où nous pourrions considérer le contrat intelligent comme un robot, serait dans le cas où la technologie évoluerait et l'oracle serait en capacité d'aller chercher l'information là où celle-ci lui semblerait la plus exacte pour enclencher le contrat intelligent ; aucun intermédiaire n'aurait à pré-programmer l'oracle et celui-ci serait complètement autonome dans la recherche de l'information recherchée. Mais la technologie du contrat intelligent et des oracles n'en est pas là.

Dans l'hypothèse où la technologie évoluerait et rendrait l'oracle entièrement autonome, alors la question du respect de la volonté des parties serait remise en cause. En effet, celles-ci n'auraient aucune emprise sur le choix de la source d'information qui enclencherait le contrat intelligent. Les parties ne pouvant s'accorder sur ce point lors de la conclusion du contrat, est-ce que leur consentement serait alors valide ? Rappelons que le « le contrat se forme par le seul échange de consentement entre des personnes capables de contracter »²⁸⁷

Par conséquent, tout l'aspect contractuel qui gravite autour du concept du contrat intelligent car sans le consentement des parties à l'étape de la conclusion du contrat, celui-ci n'est pas valide. Le contrat intelligent n'est donc pas un robot et son régime juridique n'est pas assimilable en tant que tel aux dispositions existantes relatives à ce sujet²⁸⁸.

A défaut de pouvoir assimiler le contrat intelligent au robot, il existe une technologie qui s'en rapproche et dont il peut emprunter les fondements juridiques ; le logiciel²⁸⁹. L'office québécois de la langue française le définit comme un « ensemble des programmes destinés à effectuer un traitement particulier sur un ordinateur ». ²⁹⁰ Le contrat intelligent est une traduction, sous forme de programme informatique, d'un contrat traditionnel initialement formé. Il répond aux

²⁸⁷ Art 1386 C.c.Q

²⁸⁸ Par exemple le Conseil Européen a mis en place certaines dispositions relatives au régime juridique des robot, notamment la directive 85/374/CEE qui couvre les dommages causés par les défauts de fabrication d'un robot à condition également que la victime puisse apporter des preuves des dommages, du défaut du produit et de la relation de cause à effet entre les dommages et le défaut.

²⁸⁹ La Loi sur le droit d'auteur entend par l'expression « logiciel fixé sur un support », n'importe quel support (fichier informatique, code source... etc) tant que le logiciel en question ne reste pas dans l'esprit de son concepteur. Voir aussi Pierre Paul LEMYRE et Richard WILLEMANT, « Logiciels libres et ouverts : impacts juridiques sur les utilisateurs québécois »; vol 17, n°3, 2005; dans l'affaire *Apple Computer Inc. c. Mackintosh Computers Ltd.*, [1990] 2 R.C.S. 209, la Cour suprême reconnaît que le droit d'auteur protège le code source et le code objet d'un logiciel.

²⁹⁰ Office québécois de la langue française, 2005

exigences d'un « programme d'ordinateur » en tant qu'un « ensemble d'instructions ou d'énoncés destiné, quelle que soit la façon dont ils sont exprimés, fixés, incorporés ou emmagasinés, à être utilisé directement ou indirectement dans un ordinateur en vue d'un résultat particulier »²⁹¹ et peut ainsi être qualifié de logiciel²⁹².

Outre la *Loi Canadienne sur le droit d'auteur* qui encadre le régime de protection relatif aux logiciels²⁹³ en tant qu'œuvre littéraire, le régime de responsabilité du fait des biens pourrait aussi lui être appliqué. En droit québécois, c'est traditionnellement à la victime qui réclame des dommages et intérêts de prouver les trois éléments de la responsabilité civile, à savoir la faute, le préjudice et le lien de causalité. En revanche, le *Code civil du Québec* prévoit, entre autres²⁹⁴, une exception dans le cas de la responsabilité du fait des biens. Dans cette situation, c'est la personne à qui la victime demande des dommages et intérêts, en l'occurrence le programmeur, qui est présumée responsable et doit alors apporter la preuve nécessaire pour réfuter cette présomption.

Le régime de responsabilité du fait des biens est posé à l'article 1465 du *Code civil du Québec* :

« Le gardien d'un bien est tenu de réparer le préjudice causé par le fait autonome de celui-ci, à moins qu'il prouve n'avoir commis aucune faute ».

Cet article mentionne trois critères à savoir le bien, l'autonomie et la garde, sur lesquels nous porterons notre attention pour connaître l'applicabilité du régime de responsabilité du fait des biens aux cas de dommages causés par la programmation d'un contrat intelligent. A propos de la notion de bien, le *Code civil du Québec* l'évoque de manière très succincte à l'article 899 :

²⁹¹ Loi sur le droit d'auteur (S.R., ch. C-30), art. 2

²⁹² CLACK, Christopher D., BAKSHI, Vikram A., et BRAINE, Lee. "Smart contract templates: foundations, design landscape and research directions", 2016.

²⁹³ A condition que le logiciel ait été créé de façon indépendante. La Cour Suprême pose cette condition dans l'arrêt *CCH Canadienne Ltée c. Barreau du Haut-Canada*, 2004 CSC 13, par. 24; TAMARO, Normand, *La Loi sur le droit d'auteur: texte annoté*, 3e éd., Toronto, Carswell, 1995, 737 p. SOQUIJ AZ-95101203

²⁹⁴ Cette exception vaut aussi pour les cas de responsabilité du fait d'autrui.

« Les biens, tant corporels qu'incorporels, se divisent en immeubles et en meubles ». La jurisprudence et la doctrine apportent des précisions sur cette notion²⁹⁵.

En effet, la Cour considère comme « gardien » du bien, la personne qui, au moment du dommage, possédait le pouvoir, la direction et la surveillance du bien²⁹⁶. Quant au caractère autonome du bien, il est apprécié au regard de son activité propre, il ne doit pas être passif. Ainsi, le logiciel ne doit pas avoir été manipulé par son gardien ou une tierce personne, et doit avoir un rôle actif et indépendant dans la création du dommage.

Au regard de l'article 1465 du *Code civil du Québec* cité ci-dessus, se pose la question de savoir qui serait considéré comme « gardien » dans le contrat intelligent. En effet, les parties au contrat ne font que rédiger et manifester leur consentement ; elles ne sont pas, au moment du dommage, en possession du pouvoir, de la direction, ni de la surveillance du bien (le contrat intelligent). À défaut de pouvoir considérer les parties en tant que gardien, la chaîne de blocs, liée au contrat intelligent, pourrait en revanche endosser ce rôle. En effet, sur la chaîne de blocs, ce sont les nœuds du réseau qui détiennent un certain pouvoir de contrôle en hébergeant les données et en validant les transactions ; la qualité de « gardien » pourrait éventuellement leur revenir.

À ce propos, la LCCJTI prévoit les règles de responsabilité des prestataires agissant en tant qu'intermédiaires dans l'hébergement, l'archivage et la transmission de documents²⁹⁷. L'article 22 de la LCCJTI²⁹⁸ exonère l'hébergeur de toute responsabilité quant aux activités accomplies par une personne utilisant ce service au moyen des documents hébergés. Cette exonération prend fin si l'hébergeur avait connaissance de leur caractère illicite et n'a pas mis en œuvre les moyens pour rendre impossible l'accès aux documents²⁹⁹. Toutefois, sur une chaîne de blocs publique,

²⁹⁵ Jean-Louis BAUDOIN, Patrice DESLAURIERS, *La responsabilité civile*, 8e Éd., Éditions Yvon Blais, Cowansville, 2014 ; Maurice TANCELIN, *Des obligations en droit mixte du Québec*, 7e éd., Montréal, Wilson & Lafleur, 2009, no 621, p. 446

²⁹⁶ Sur ce point, consulter les affaires *Hydro-Québec c. Bell Canada** (C.Q., 2019-01-29), 2019 QCCQ 263, SOQUIJ AZ-51565116, 2019EXP-673 ; *Canada (Procureur général) c. CNIM Canada inc. ** (C.S., 2015-10-20), 2015 QCCS 5094, SOQUIJ AZ-51227648, 2015EXP-3332, J.E. 2015-1840

²⁹⁷ Art 22 L.C.C.J.T.I ; Art 36 L.C.C.J.T.I ; Art 37 L.C.C.J.T.I ; Voir l'écrit de Pierre TRUDEL, « La responsabilité sur internet en droit civil québécois ». online:< <http://www.chairelrwilson.ca/documents>

²⁹⁸ Préc. note 266

²⁹⁹ Voir Pierre TRUDEL, préc., note 297

il est difficile d'identifier les hébergeurs puisqu'ils sont multiples. Cette multiplicité des agents intermédiaires (en l'occurrence les nœuds du réseau) sur la chaîne de blocs rend impossible l'imputabilité d'une responsabilité envers une personne. De par leur caractère décentralisé, multiple et anonyme, les nœuds du réseau, sur la chaînes de blocs publique, ne peuvent donc être considérés comme « gardiens » au sens de l'article 1465 du *Code civil du Québec*³⁰⁰. La question de savoir à qui reviendrait la qualité de « gardien » dans un logiciel tel que le contrat intelligent reste donc une question sans réponse de la part des tribunaux et du législateur.

À la lumière de ce qui précède, il nous semble que l'interprétation la plus juste en cas de litige serait de considérer l'article 1457 du *Code civil du Québec*³⁰¹ relatif à la faute puisque les tribunaux n'ont pas encore donné de réponse à la question de savoir si la condition de « gardien » énoncée à l'article 1465 du *Code civil du Québec* est à prendre en compte dans le contrat intelligent ou non. Il semble alors opportun de revenir au fondement de l'article 1457 du *Code civil du Québec* qui repose sur la notion de faute pour évaluer la responsabilité en cas de préjudice causé. Dans ce cas, il faudrait réfléchir à qui reviendrait la faute en cas de litige : celle-ci ne pourrait pas être imputée aux utilisateurs de la chaîne de blocs puisqu'ils sont nombreux et non identifiables uns à uns. En revanche on peut imputer cette faute aux intermédiaires participants à l'élaboration du contrat intelligent, à savoir les cocontractants ou le programmeur qui met en place le logiciel, s'il est établi qu'ils n'ont pas agi comme une personne « douée de raison » l'aurait fait dans la même situation.

ii- Responsabilité et développement de logiciels par les programmeurs

Dans une étude relative aux *Réflexions sur l'application des garanties aux logiciels en droit civil québécois*³⁰² deux avocats relèvent trois types de problèmes informatiques dont l'un

³⁰⁰ Art. 1465 C.c.Q

³⁰¹ Préc. note 273

³⁰² SOLIS, Michel A. et LAPOINTE, Sébastien, « Réflexions sur l'application des garanties aux logiciels en droit civil québécois », (1999) 59 R. du B. 393-444

« connu notamment sous le nom de « bogue », se produit lorsqu'une erreur s'est glissée dans la programmation d'un logiciel ou d'un programme, et que l'utilisation du logiciel ou du programme interrompt le fonctionnement d'un logiciel ou de l'ordinateur, ou encore fausse les résultats que génère le programme. »³⁰³

Transposée à notre étude, cette définition est applicable au contrat intelligent en tant que logiciel imbriqué dans un contrat traditionnel dont certaines clauses sont transposées sous forme de code par le programmeur.

Dans l'affaire *Fondation des sourds du Québec Inc c. Oralys Inc*³⁰⁴, la demanderesse paie les services de la défenderesse afin de concevoir un logiciel qui puisse être capable de favoriser la communication en langage des signes québécois (LSQ) au bénéfice des personnes atteintes de surdité. Plus tard, la demanderesse résilie le contrat et demande une restitution de la somme virée car selon elle le logiciel ne répond pas aux attentes initialement convenues à la création du contrat. Sur la détermination de l'obligation de moyens ou de résultats, le juge Ivan Godin analyse les termes du contrat et rappelle que

« dans le préambule de l'entente contractuelle intervenue entre les parties, il est expressément stipulé que : "La défenderesse accepte de développer une application spécialement conçue pour les personnes sourdes, selon des paramètres qui lui permettent de le faire" ».

Le juge s'appuie sur la doctrine des auteurs Didier Lluelles et Benoît Moore³⁰⁵ pour conclure :

³⁰³ Préc. Note 246, p.403

³⁰⁴ *Fondation des Sourds du Québec inc. c. Oralys inc. (C.S., 2008-07-17)*, 2008 QCCS 6733, SOQUIJ AZ-50549537, J.E. 2009-899

³⁰⁵ LLUELLES, Didier et MOORE, Benoît, *Droit des obligations*, Montréal, Les Éditions Thémis, 2006, 2 324 p., p. 43, 44, 45, SOQUIJ AZ-40002314 ; Art.108, « À notre avis, un des critères de distinction les plus fonctionnels consiste à se demander si l'exécution de la prestation requérait ou non une expertise professionnelle particulière : dans la négative, la conclusion d'obligation de résultat serait vraisemblable ; elle ne le serait pas, dans l'affirmative."

« qu'il ressort donc de l'ensemble des clauses du contrat que la défenderesse assume une obligation de moyens et s'engage à prendre tous les moyens pour parvenir à un résultat sans toutefois garantir le résultat lui-même. »

Le *Code civil du Québec* ne propose pas de dispositions relatives aux logiciels et à la programmation. La doctrine rappelle que « l'obligation essentielle d'un prestataire est la délivrance de l'objet du contrat »³⁰⁶; le programmeur d'un logiciel a alors une obligation de délivrance, accompagnée d'une obligation d'information et de garantie.

Par obligation de délivrance, on entend la mise à disposition du logiciel par le programmeur aux cocontractants. Concernant l'obligation d'information, la jurisprudence relative aux logiciels³⁰⁷ les assimile à la vente d'un bien « traditionnel » qui peut être entaché d'un vice caché et donc engager la responsabilité du programmeur. Ainsi, ces dispositions s'appliquent au contrat intelligent dans le cas où on considère la vente par le programmeur du logiciel contenant le code du contrat intelligent destiné aux parties. Le *Code civil du Québec* prévoit en son article 1726 alinéa 1³⁰⁸, que le vendeur se doit de garantir l'absence de vice caché lors de la vente d'un bien³⁰⁹. En effet cette obligation de moyen vise celui qui rend le logiciel impropre à son usage ou diminue tellement cet usage que la personne n'aurait pas accepté les termes de la licence, ou aurait payé un prix moindre. La responsabilité du programmeur sera engagée dans ce cas, à la condition que le vice caché existait à la conclusion du contrat³¹⁰.

Les parties à l'origine de la demande de la mise en place du contrat intelligent ne sont pas les seules pouvant être lésées par le logiciel qu'est le contrat intelligent. En effet, un tiers peut subir

³⁰⁶ Michel VIVANT et al., *Lamy droit de l'informatique et des réseaux* (Lamy, Paris, 2001, no 840), p. 522.

³⁰⁷ *Mensys Business Solution Centre Ltd. c. Drummond (Municipalité régionale de comté de)*, (C.S., 2002-01-30) ; *Technologies Trellisys inc. c. Rousseau Métal inc.* (C.Q., 2009-02-05) ; *Programmation Gagnon inc. c. Lemay* (C.S., 2000-01-06).

³⁰⁸ Art. 1726 al.1 C.c.Q : « Le vendeur est tenu de garantir à l'acheteur que le bien et ses accessoires sont, lors de la vente, exempts de vices cachés qui le rendent impropre à l'usage auquel on le destine ou qui diminuent tellement son utilité que l'acheteur ne l'aurait pas acheté, ou n'aurait pas donné si haut prix, s'il les avait connus. » Sur l'appréciation du vice caché, voir l'affaire *Sincennes c. Lavigne*, 2010 QCCS 54 ainsi que *Royer c. Mazda Canada inc.*, 2015 QCCQ 1576.

³⁰⁹ Michel A. SOLIS, et Sébastien LAPOINTE, « Réflexions sur l'application des garanties aux logiciels en droit civil québécois », (1999) 59 R. du B. p.418

³¹⁰ Frédérique TOUBOL, *Le logiciel: Analyse Juridique*, Paris, Feduci - L.G.D.J., 1986, p. 128

un dommage via un contrat intelligent. Ce serait par exemple le cas d'une anomalie dans les instructions de codage qui ferait que, dans une transaction de vente, les fonds soient accidentellement débités du compte d'un tiers n'ayant jamais contracté. À ce propos, le droit de la responsabilité civile extracontractuelle établit trois conditions devant être remplies pour que la personne doive réparer le préjudice subi à autrui : une faute ou un manque de diligence³¹¹, un dommage, et un lien de causalité entre les deux.

Concernant la faute, comme en matière contractuelle, celle-ci implique le manquement à un devoir ou la violation d'une norme de conduite de la part du programmeur³¹². Ces manquements sont traditionnellement appréciés au regard du comportement d'une personne raisonnable, placée dans les mêmes circonstances et ayant le même niveau de connaissances. Il s'agira d'un comportement défailant au regard d'une norme connue à un moment donné. N'ayant pas de normes connues tels que des standards, des règles d'éthiques, ni d'ordre professionnel en matière de programmation, il est difficile de déterminer des critères régissant la responsabilité des programmeurs. C'est le caractère raisonnable des décisions prises par les développeurs qui prime, car il est impossible de leur demander de créer un logiciel exempt d'imperfections; ce dernier n'étant pas vérifiable intégralement³¹³. Puisqu'il n'existe pas de standards sur lesquels se référer afin d'apprécier le comportement négligent ou non du programmeur, il appartient au juge de le faire et ainsi de le comparer à un autre programmeur agissant de manière prudente et diligente³¹⁴. Le juge appréciera alors la méthodologie utilisée pour tester le programme ou encore la prise en compte des commentaires des utilisateurs par le programmeur.

³¹¹ L'affaire *Anns v. Merton London Borough Council* pose le principe général de l'obligation de diligence en common law qui doit être indépendant du contrat dans le sens où elle résulte de l'existence de rapports suffisamment étroits entre les intéressés. La nature et la portée de l'obligation de diligence invoquée comme fondement de la responsabilité délictuelle ne doivent pas dépendre d'obligations ou de devoirs précis créés expressément par le contrat.

³¹² Jean-Louis BAUDOUIN, Patrice DESLAURIERS, préc., note 295 p. 96 ; voir l'affaire *Mensys Business Solution Centre Ltd. c. Drummond (Municipalité régionale de comté de)*, (C.S., 2002-01-30), SOQUIJ AZ-50111904, J.E. 2002-591, [2002] R.J.Q. 765

³¹³ Thomas G. WOLPERT, «Product Liability and Software Implicated in Personal Injury », (1993) 60 De Couns. J. 519, 532.

³¹⁴ Jean-Louis BAUDOUIN, Patrice DESLAURIERS, préc. note 312

En revanche, il deviendra plus difficile pour le juge de déterminer la négligence du programmeur si celui-ci intègre une forme d'intelligence artificielle à son programme car une part d'imprévu entre en jeu. Cela soulève la question de savoir si l'on pourrait invoquer l'article 1470 du *Code civil du Québec*³¹⁵ et prétendre que dès lors que l'algorithme a évolué de par lui-même, on peut prétendre qu'il y a eu force majeure. Or, peut-on réellement prétendre que l'incertitude propre à certaines formes d'intelligence artificielle constitue une force majeure ? En effet, si les parties ne pouvaient y penser et qu'il y a une part d'imprévu, cela relève de la force majeure. L'algorithme qui évolue est alors une forme de force majeure puisqu'il est imprévisible. Cependant, à notre avis cette analyse ne serait pas valide car il semblerait un peu facile de pouvoir invoquer la force majeure quand on sait pertinemment qu'un algorithme va évoluer.

Pour l'instant les contrats intelligents ne contiennent pas d'éléments d'intelligence artificielle³¹⁶, mais le jour où ils en intégreront (par exemple si on imagine contrat intelligent composé d'un oracle doté d'intelligence artificielle qui jugera de lui-même quelle est la meilleure information à aller chercher pour déclencher l'exécution du contrat), le programmeur ne pourra plus être tenu responsable du dommage causé ; on en revient aux problématiques actuelles posées en termes de responsabilité et d'apprentissage automatique (*machine learning*)³¹⁷, notamment la question de savoir s'il est possible d'invoquer la responsabilité des biens défectueux³¹⁸ à un programmeur qui utilise des algorithmes capables d'évoluer et d'apprendre par eux-mêmes. Or est-ce qu'on peut parler de biens défectueux pour parler d'un algorithme qui ne fonctionne pas comme on l'aurait souhaité ? Selon nous ce fondement n'est pas applicable dans la mesure où le bien est supposé apprendre par lui-même. Donc si la responsabilité des biens défectueux ne

³¹⁵ Art 1470 C.c.Q : « Toute personne peut se dégager de sa responsabilité pour le préjudice causé à autrui si elle prouve que le préjudice résulte d'une force majeure, à moins qu'elle ne se soit engagée à le réparer. La force majeure est un événement imprévisible et irrésistible ; y est assimilée la cause étrangère qui présente ces mêmes caractères »

³¹⁶ Notons ici que cela dépendra notamment de la définition employée pour qualifier la notion d'intelligence artificielle. En effet, si on se réfère à la définition de Marvin Lee Minsky (en 1956), scientifique américain, l'intelligence artificielle est « la construction de programmes informatiques qui s'adonnent à des tâches qui sont, pour l'instant, accomplies de façon plus satisfaisante par des êtres humains ». La définition initiale est donc si vague qu'elle pourrait inclure certaines chaînes de blocs.

³¹⁷ Préc. note 171

³¹⁸ Art. 1468 C.c.Q : « Le fabricant d'un bien meuble, même si ce bien est incorporé à un immeuble ou y est placé pour le service ou l'exploitation de celui-ci, est tenu de réparer le préjudice causé à un tiers par le défaut de sécurité du bien. »

s'applique pas, à notre avis il est nécessaire de revenir, comme pour la question de l'applicabilité de la notion de « gardien », à l'application de la responsabilité pour faute sur le fondement de l'article 1457 du *Code civil du Québec*.

b. Le cas d'un contrat intelligent validé par un auditeur

Les parties peuvent faire appel à un audit afin de s'assurer que leurs intentions aient été correctement transposées en code par le programmeur. Comme dans tout contrat traditionnel, l'audit sera considéré responsable si le contrat intelligent ne s'exécute pas comme la relation d'affaire avait été envisagée par les parties. En effet, son rôle étant de valider que le code développé par le programmeur pour certaines clauses est en conformité avec la logique d'affaire souhaitée par les parties, en cas de dommage causé suite à un manquement de la part de l'auditeur, sa responsabilité contractuelle pourra être engagée. Qu'en est-il de sa responsabilité délictuelle ?

Sur le sujet de la responsabilité professionnelle, l'affaire *Central Trust Co. c. Rafuse*³¹⁹ pose la question de savoir si un avocat a une responsabilité délictuelle ou contractuelle envers son client ayant subi un dommage en raison d'un manque de diligence dans la prestation desdits services. Les juges considèrent que « si les avocats intimés ont fait preuve de négligence dans la prestation de leurs services professionnels, leur responsabilité envers l'appelante est non seulement contractuelle mais aussi délictuelle, sous réserve des autres moyens de défense qu'ils ont soulevés. »³²⁰ Ainsi, la responsabilité délictuelle de l'avocat, comme tout autre professionnel et notamment l'auditeur, peut être engagée sur le fondement d'une négligence basée sur un

³¹⁹ *Central Trust Co. c. Rafuse* (C.S. Can., 1988-06-30), SOQUIJ AZ-50072852, [1988] 1 R.C.S. 1206

³²⁰ *Ibid.*

manquement à une obligation de diligence qui découle de rapports suffisamment étroits entre les intéressés³²¹.

Si les parties peuvent demander l'intervention d'un auditeur pour vérifier la validité de leur contrat intelligent, il est aussi possible pour elles de trouver le contrat intelligent qui répond à leurs attentes, directement sur la chaîne de blocs, et intègre une procédure d'audit en cas de violation d'une règle prévue dans le contrat intelligent. C'est l'hypothèse envisagée schématiquement ci-dessous.

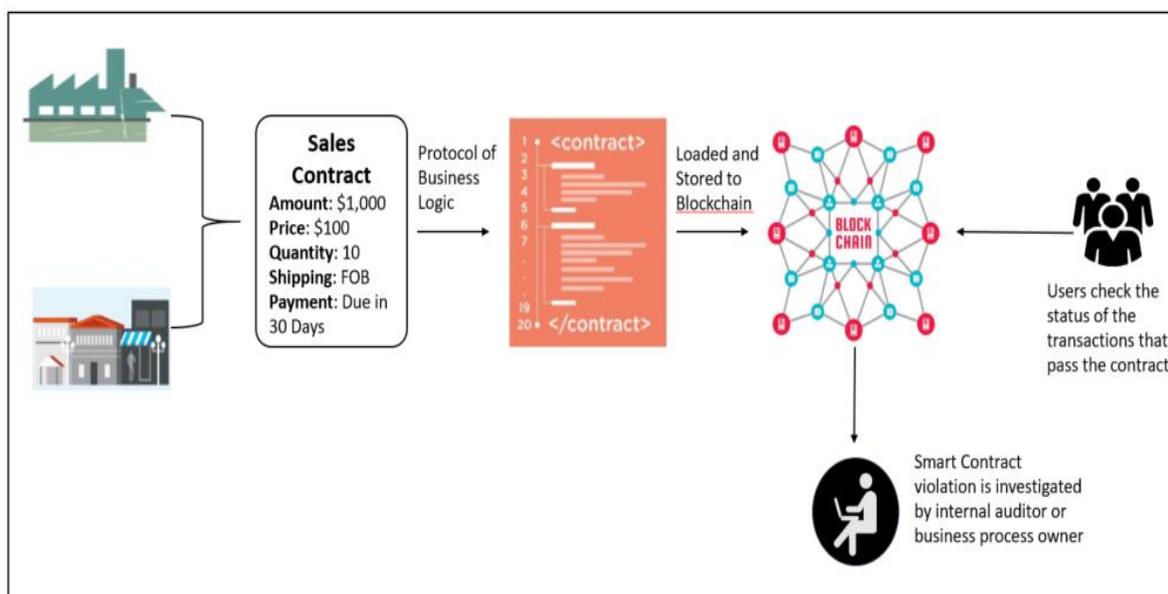


Figure 8. Exemple d'une procédure d'audit intégrée au contrat intelligent³²²

³²¹ *Roberge c. Bolduc* (C.S. Can., 1991-02-28), SOQUIJ AZ-91111033, J.E. 91-412, [1991] 1 R.C.S. 374, [1991] R.D.I. 239, [1991] R.R.A. 314 (rés.) ; *Mathieu c. Fonds d'assurance responsabilité professionnelle du Barreau du Québec** (C.S., 2008-07-10), 2008 QCCS 3021, SOQUIJ AZ-50501445, J.E. 2008-1521, [2008] R.R.A. 671

³²² ROZARIO et VASARHELYI, "Auditing with smart contracts", *The International Journal of Digital Accounting Research*, Vol 18, p.10

Ainsi, en cas de violation d'une règle intégrée au contrat intelligent choisi, un message d'erreur s'enclencherait pour que la transaction n'ait pas lieu. Dans ce cas précis, Rozario et Vasarhelyi envisagent alors trois possibilités :

« This violation would have to be addressed by a human user, presumably an internal auditor or business process owner, to verify the legitimacy of the transaction. Alternatively, the violation could be addressed by an automated procedure that handles smart contract violations. Otherwise, if there are no violations, the contract self-settles once the goods reach their destination and payment is satisfied. »³²³

Pour exercer ses fonctions, il va se soit que l'audit doit se prévaloir de compétences en compréhension du langage de programmation et des fonctions de la chaîne de blocs. A l'avenir, les sociétés pourraient utiliser des contrats intelligents, créés par d'autres sociétés, déjà présents sur une chaîne de blocs, ceci éviterait de vérifier nécessairement la validité et le bon fonctionnement des instructions de code du contrat intelligent, et limiterait les erreurs « humaines » dans l'élaboration du contrat intelligent. Une autre solution évoquée par Rozario et Thomas serait de mettre en place un contrat intelligent intégrant lui-même une procédure d'audit « intelligente » contenant une procédure d'audit automatisée prédéfinie. Leur idée serait que « these predefined procedures would be decomposed into 'IF- THEN' rules by the audit firm, for example, and embedded into a smart analytical procedure that is loaded to the external auditor blockchain and pre-approved by both the audit firm and the inspector »³²⁴. Cette méthode limiterait d'autant plus la possibilité d'erreurs dans l'audit du contrat intelligent.

Nous pouvons donc constater que la LCCJTI répond en partie aux problématiques que soulève le contrat intelligent, notamment en ce qui concerne les dispositions relatives au contrat technologique et à la jurisprudence existante concernant la programmation de logiciels, puisque,

³²³ Ibid.

³²⁴ ROZARIO, A.; THOMAS, C. (2017): "Reshaping the Audit with Blockchain and Artificial Intelligence: An External Auditor Blockchain for Close to Real-Time Audit Reporting", Rutgers University Working Paper.

rappelons-le, le contrat intelligent est une forme de logiciel. Ainsi, en cas de litige impliquant un contrat intelligent, nous avons vu que les tribunaux pourraient tout à fait utiliser l'article 22 de la LCCJTI quant à la responsabilité des intermédiaires techniques. D'autre part, que ce soit en matière contractuelle ou extracontractuelle, les dispositions du *Code civil du Québec*³²⁵ s'appliquent aux différents intermédiaires du contrat intelligent. En revanche, dans le cadre de l'application de l'article 1465 du *Code civil du Québec*³²⁶, nous remarquons que la notion de « gardien » est difficilement envisageable pour les contrats intelligents liés à une chaîne de blocs, dans le sens où la notion de décentralisation et la multitude des nœuds du réseau sur la chaîne de blocs ne permettent pas d'identifier un « gardien » ; il semble donc difficile d'appliquer cette disposition aux cas de dommages causés par un contrat intelligent. Au regard de l'analyse effectuée dans la section ci-dessus, il semble que la responsabilité des intermédiaires dans le contrat intelligent serait basée essentiellement sur le fondement de l'article 1457 du *Code civil du Québec*, à savoir la détermination de la faute commise.

B. Dans le cas d'un dommage causé par une erreur d'exécution du contrat intelligent

Le mariage entre le droit et la technologie a toujours été un débat épineux³²⁷. Le droit positif ne prend pas en compte les évolutions technologiques principalement pour deux raisons : il est impossible de changer de lois à chaque nouveauté technologique, et quand bien même ce serait possible, trop encadrer ces nouvelles technologies reviendrait à leurs nuire car les réglementations empêcheraient leur évolution. C'est pourquoi il est nécessaire pour le droit de s'adapter aux nouvelles technologies, en associant les principes généraux du droit présents dans le *Code civil du Québec*, à de nouvelles normes telles que les normes ISO ou la *Loi concernant*

³²⁵ Notamment l'Art. 1457 C.c.Q qui réfère à la personne « douée de raison » en matière extracontractuelle, ou encore l'article 1375 C.c.Q relatif au principe de bonne foi en matière contractuelle.

³²⁶ Art 1465 C.c.Q : «Le gardien d'un bien est tenu de réparer le préjudice causé par le fait autonome de celui-ci, à moins qu'il prouve n'avoir commis aucune faute. »

³²⁷ POLLAK Michael. « La régulation technologique : le difficile mariage entre le droit et la technologie », *Revue française de science politique*, 32^e année, n°2, 1982. pp. 165-184.

*le cadre juridique des technologies de l'information*³²⁸. Ces nouvelles normes ne sont cependant pas accueillies de la même manière par tous, et divisent la doctrine.

Nous avons vu précédemment que le dommage causé par un contrat intelligent peut être dû à la faute commise par l'une des parties au contrat, le programmeur ou encore l'auditeur lorsque le contrat est en phase de formation. Lors de son exécution, c'est l'oracle qui entre en jeu et, dans le cadre d'un contrat intelligent intégré à une chaîne de blocs, va donner l'information nécessaire au déclenchement du contrat intelligent. Si le contrat ne s'exécute pas comme prévu, est-il possible d'engager la responsabilité de l'oracle par exemple ?

1. L'engagement de la responsabilité de l'oracle dans le contrat intelligent

L'information recherchée qui déclenchera le contrat intelligent peut être apportée par des oracles lorsqu'elle est disponible en ligne. Ces données peuvent être issues de sources fiables sur Internet, tel que le site d'une compagnie aérienne, le site officiel météorologique, ou encore toutes informations issues d'un institut officiel de statistiques économiques et sociales par exemple³²⁹.

Nous mentionnerons dans cette partie deux hypothèses, non exclusives, dans le cas où c'est l'oracle qui fournit une mauvaise information et fausse la bonne exécution du contrat intelligent : soit l'oracle a été mal choisi et donne une information erronée, soit l'oracle donne une mauvaise information mais un contrat lie les parties à ce dernier.

³²⁸ Par exemple l'adoption de la Loi concernant le cadre juridique des technologies de l'information est venue modifier le droit de la preuve prévu dans le Code civil du Québec. Lire à ce sujet l'ouvrage de GAUTRAIS, Vincent. *La preuve technologique*. LexisNexis, 2013.

³²⁹ RABESANDRATANA, V. et BACCA, N. (2017). « L'Oracle hardware : la couche de confiance entre les blockchains et le monde physique ». *Annales des Mines - Réalités industrielles*, août 2017(3), 91-93

Comme tout logiciel ou base de données sur Internet, l'oracle n'est pas à l'abri de fournir une information erronée. Qu'en est-il si la source sur laquelle se base l'oracle est erronée ou piratée? Quel type de responsabilité pourra être engagé ? Nous verrons aussi que pour pallier à cette éventualité, certains auteurs envisagent la solution d'une entente entre les parties et ce dernier afin de s'assurer de sa fiabilité et de pouvoir reporter la faute sur celui-ci en cas de dommage causé par une fausse information fournie et ainsi pouvoir engager une responsabilité contractuelle de l'oracle.

a. Dans le cas où l'oracle donne une information erronée

Premièrement nous émettrons l'hypothèse où l'oracle fournit une fausse information en raison d'un piratage de la base de données sur laquelle il s'appuie, puis nous aborderons l'hypothèse dans laquelle l'oracle fournit une fausse information pour cause d'une erreur dans le choix de celui-ci de la part des parties au contrat.

i- Hypothèse d'un oracle piraté

Qui serait responsable si la source d'information à l'origine de l'exécution du contrat intelligent était piratée ? Nous avons vu en amont l'engagement de la responsabilité pour faute du cocontractant qui corrompt la chaîne de blocs et empêche ainsi le contrat intelligent d'exécuter les obligations de chacun. Imaginons désormais que le piratage ne provienne pas de l'une ou l'autre parties, mais d'un tiers inconnu qui corromprait la source de l'information à l'origine du déclenchement du contrat intelligent, à savoir l'oracle. Dans ce cas, peut-on alors envisager une faute de l'oracle ou un piratage informatique, ou bien peut-on parler de force majeure ?

Concernant la force majeure dans le contrat, l'article 1693 du *Code civil du Québec*³³⁰ stipule que :

« Lorsqu'une obligation ne peut plus être exécutée par le débiteur, en raison d'une force majeure (...), il est libéré de cette obligation; il en est également libéré, (...) lorsque le créancier n'aurait pu, de toute façon, bénéficier de l'exécution de l'obligation en raison de cette force majeure (...) ».

En application de cette disposition, la force majeure dans le contrat intelligent permettrait de remettre en cause le consentement des parties et de les exonérer de leurs obligations une fois que le contrat se serait exécuté. Finalement, la force majeure donnerait la possibilité du retour en arrière que le contrat intelligent ne permet pas³³¹. En effet l'article 1470 du *Code civil du Québec* énonce que « toute personne peut se dégager de sa responsabilité pour le préjudice causé à autrui si elle prouve que le préjudice résulte d'une force majeure »³³².

ii- Hypothèse d'une erreur dans le choix de l'oracle

Le fait qu'un oracle puisse ne pas fournir une bonne information fait penser à la problématique des « fausses nouvelles », souvent appelées « fake news » dans leur traduction anglaise. Celles-ci sont des informations ou des données, présentées par des individus comme étant vraies au grand public, le plus souvent via internet et les réseaux sociaux, mais qui sont totalement fausses en réalité. En France, une loi mise en place en 2018 intitulée « loi relative à la lutte contre la manipulation de l'information »³³³ propose une définition de ces « fake news » comme « toute allégation ou imputation d'un fait dépourvue d'éléments vérifiables de nature à la rendre

³³⁰ Art. 1693 C.c.Q.

³³¹ Rappelons que comme mentionné en première partie, le contrat intelligent une fois inscrit sur une chaîne de blocs ne peut être modifié ou supprimé.

³³² Art 1470 C.c.Q

³³³ Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information. Consultation en ligne sur le site <https://www.legifrance.gouv.fr/>

vraisemblable »³³⁴. Dans le contrat intelligent, un oracle préalablement choisi par les parties pourrait ainsi se retrouver « victime » d'une fausse information diffusée sur un site à priori fiable. Dans ce cas, à qui revient la faute ; l'oracle ou les parties ?

Le fait de se fier à un « mauvais » site n'est en soit pas une faute des parties. Toute personne « douée de raison », comme invoqué à l'article 1457 du *Code civil du Québec*, pourrait être victime de ce type d'erreur. Dans l'exemple d'un contrat intelligent dont l'exécution est conditionnée selon les informations que donne le site officiel « météo média », si une personne prudente et diligente se fie à un site tel que « météo média » qui se présente comme un site fiable et qu'il ne l'est pas en réalité, est-ce qu'on peut considérer que cette personne a commis une faute ? Est-ce qu'on peut considérer que la personne aurait agi de façon déraisonnable si l'information s'avère fausse ? A priori la réponse est non, et la question qui en découle sera de savoir pourquoi l'information s'avère fausse. Est-ce parce que le site « météo média » s'est fait pirater, ou est-ce parce que « météo média » a manqué à son devoir de valider ses sources ? Ainsi, est-ce qu'on pourrait retenir la responsabilité du site dans un cas ou dans l'autre ? Pour répondre à cette question, il nous semble opportun de se référer dans un premier temps au droit applicable quant à la responsabilité des plateformes en lignes, puis à la question de la responsabilité d'un site qui fournit de lui-même un faux contenu ; on utilisera l'exemple d'un journaliste qui met en ligne un article contenant de fausses nouvelles.

Tout comme l'Oracle pourrait présenter des données comme vraies et ainsi fausser la bonne exécution du contrat intelligent, la question se pose de savoir s'il serait possible de reprocher une responsabilité à quiconque, par exemple à la plateforme en ligne qui a promulgué la fausse information. En ce qui concerne la responsabilité des plateformes en ligne, la LCCJTI prévoit en son article 27 alinéa 1 que :

³³⁴ Article L163-1 A de la Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre les fausses informations.

« Le prestataire de services qui agit à titre d'intermédiaire pour fournir des services sur un réseau de communication ou qui y conserve ou y transporte des documents technologiques n'est pas tenu d'en surveiller l'information, ni de rechercher des circonstances indiquant que les documents permettent la réalisation d'activités à caractère illicite. »³³⁵

Imaginons que la personne réalisant le choix de l'Oracle dans le contrat intelligent choisisse de s'appuyer sur un autre site que le site officiel de la compagnie aérienne et que ce site ne donne pas les mêmes informations que celui de la compagnie, sa responsabilité extracontractuelle peut-elle être engagée ? Sur quels critères la personne doit elle se baser pour considérer un site comme fiable et sécuritaire. Aucune source d'information sur internet n'est à l'abri d'être falsifiée, ni à l'abri d'un problème informatique qui rend les informations momentanément indisponibles³³⁶.

Si les rédacteurs du contrat sont en charge de choisir la source d'information qui apportera les informations dans la chaîne de blocs alors l'erreur intentionnelle ou non intentionnelle pourrait leur être imputée. Dans ce cas nous nous rapportons à l'engagement de la responsabilité pour faute d'une partie au contrat comme évoqué en amont dans ce papier³³⁷. Toujours est-il que si l'oracle est déficient pour quelque raison, et n'envoie aucune information dans la chaîne de blocs, les parties ont tout intérêt à avoir prévu ce cas de figure et inséré une clause permettant de restituer les sommes compromises si aucune information n'a été donnée par l'oracle à un instant précis³³⁸.

À la lumière de ce que nous avons vu, pour connaître la part de responsabilité imputable à chacun, il est nécessaire de savoir si un site peut être tenu responsable dans certains cas. Pour illustrer nos propos, reprenons l'exemple de la traçabilité des aliments mentionné en première

³³⁵ Art. 27 de la Loi concernant juridique des technologies de l'information, préc., note 142

³³⁶ Consulter à ce propos l'ouvrage de Nicolas VERMEYS, *Virus informatiques: responsables et responsabilité*, Montréal, Thémis, 2006

³³⁷ L'engagement de la responsabilité pour faute des parties au contrat est traité en partie II-A-1.

³³⁸ <https://www.ethereum-france.com/les-oracles-lien-entre-la-blockchain-et-le-monde/>

partie de ce mémoire, à savoir le site officiel d'un magasin de grande distribution : « Walmart »³³⁹. Certes, l'article 27 LCCJTI énonce que le site ne possède aucune obligation de surveillance de l'information, mais qu'en est-il du contenu qu'il génère lui-même, en d'autres termes qu'en est-il s'il diffuse de lui-même un faux contenu ? Dans ce cas, les articles 36 LCCJTI³⁴⁰ et 37 LCCJTI³⁴¹ s'appliqueront et permettront d'engager la responsabilité du site dans la mesure où ce dernier « est à l'origine de la transmission du document »³⁴². Puisque ces deux articles sont pris en compte, alors les articles 22 LCCJTI et 27 LCCJTI ne s'appliqueront pas.

Pour faire le parallèle avec une entreprise comme Walmart qui diffuse de fausses informations sur son site, plusieurs décisions relatives à la diffamation dans les médias³⁴³ ont montré que ce sont les principes de responsabilité civile classiques, à savoir l'article 1457 du *Code civil du Québec*, qui s'appliquent. Dans l'affaire *Néron*³⁴⁴, le juge rappelle que les règles régissant la diffamation au Québec doivent respecter les règles générales de la responsabilité civile. Il ajoute que :

³³⁹ Préc., note 29

³⁴⁰ Art 36 L.C.C.J.T.I : « « 36. Le prestataire de services qui agit à titre d'intermédiaire pour fournir les services d'un réseau de communication exclusivement pour la transmission de documents technologiques sur ce réseau n'est pas responsable des actions accomplies par autrui au moyen des documents qu'il transmet ou qu'il conserve durant le cours normal de la transmission et pendant le temps nécessaire pour en assurer l'efficacité. Il peut engager sa responsabilité, notamment s'il participe autrement à l'action d'autrui : 1° en étant à l'origine de la transmission du document ; 2° en sélectionnant ou en modifiant l'information du document ; 3° en sélectionnant la personne qui transmet le document, qui le reçoit ou qui y a accès; 4° en conservant le document plus longtemps que nécessaire pour sa transmission. »

³⁴¹ Art 37 L.C.C.J.T.I : « « 37. Le prestataire de services qui agit à titre d'intermédiaire pour conserver sur un réseau de communication les documents technologiques que lui fournit son client et qui ne les conserve qu'à la seule fin d'assurer l'efficacité de leur transmission ultérieure aux personnes qui ont droit d'accès à l'information n'est pas responsable des actions accomplies par autrui par le biais de ces documents. Il peut engager sa responsabilité, notamment s'il participe autrement à l'action d'autrui : 1° dans les cas visés au deuxième alinéa de l'article 36 ; 2° en ne respectant pas les conditions d'accès au document ; 3° en prenant des mesures pour empêcher la vérification de qui a eu accès au document ; 4° en ne retirant pas promptement du réseau ou en ne rendant pas l'accès au document impossible alors qu'il a de fait connaissance qu'un tel document a été retiré de là où il se trouvait initialement sur le réseau, du fait qu'il n'est pas possible aux personnes qui y ont droit d'y avoir accès ou du fait qu'une autorité compétente en a ordonné le retrait du réseau ou en a interdit l'accès. »

³⁴² Préc.note 337

³⁴³ Voir l'affaire *Prud'homme c. Prud'homme* [2002] 4 R.C.S. 663 où la Cour suprême définit la diffamation : elle « consiste dans la communication de propos ou d'écrits qui font perdre l'estime ou la considération de quelqu'un ou qui, encore, suscitent à son égard des sentiments défavorables ou désagréables ».

³⁴⁴ *Société Radio-Canada c. Néron*, [2004] 3 R.C.S. 95.

« Somme toute, l'existence d'une faute constitue l'exigence de base du droit de la responsabilité civile pour diffamation et cette faute doit être appréciée en fonction des normes journalistiques professionnelles. Les journalistes ne sont pas tenus à un critère de perfection absolue ; ils sont astreints à une obligation de moyens. (...) D'autre part, un journaliste ne sera pas nécessairement exonéré de toute responsabilité simplement parce que l'information diffusée est véridique et d'intérêt public. Si, pour d'autres raisons, le journaliste n'a pas respecté la norme journalistique raisonnable, les tribunaux pourront toujours conclure à l'existence d'une faute. Vue sous cet angle, la responsabilité civile pour diffamation continue de s'inscrire parfaitement dans le cadre général de l'article 1457 C.c.Q. »³⁴⁵

Que ce soit une personne qui diffuse de fausses informations, ou un site d'information qui divulgue de fausses informations, dans un cas comme dans l'autre un préjudice est causé à autrui. Ainsi, au regard de ces décisions, si les médias peuvent être jugés responsables pour cause de diffamation sur le fondement de l'article 1457 du *Code civil du Québec*, il semble que la faute puisse aussi être imputée au site qui publierait une fausse information.

b. Le cas d'une entente réalisée entre les parties et l'oracle

Afin de s'assurer que les parties se basent sur un oracle fiable, il est possible d'envisager que celles-ci s'accordent au préalable avec l'oracle dans un cadre contractuel. En cas de litige, il est alors possible que l'une puisse se reprocher à l'autre le choix de l'oracle. Sans lien contractuel entre l'oracle et parties, ces dernières pourront plus difficilement être considérées responsables

³⁴⁵ Ibid. par. 61. Consulter aussi les décisions *Bernèche c. Vaillancourt* (C.S., 2017-01-12), 2017 QCCS 359, SOQUIJ AZ-51363026 et *Prud'homme c. Prud'homme* (C.S. Can., 2002-12-20), 2002 CSC 85, SOQUIJ AZ-50156257 relatives aux propos diffamatoires publiés par un journaliste.

car sur le champ de la responsabilité extracontractuelle il serait nécessaire de prouver une faute de l'oracle.

i- L'hypothèse d'une conclusion d'un contrat avec l'oracle

Une solution envisageable par les parties afin qu'elles puissent s'assurer au mieux que l'oracle sera dans la capacité de fournir au contrat intelligent des informations fiables et ainsi éviter les dommages causés par un contrat intelligent qui ne s'exécute pas comme prévu, c'est la conclusion d'un contrat entre une tierce partie qui représenterait l'oracle, et les parties contractantes³⁴⁶. Cette méthode revient en quelques sorte à réintroduire le tiers de confiance que la chaîne de blocs et les contrats intelligents souhaitaient éliminer.

Une autre solution, basée quant à elle sur le même fonctionnement que la chaîne de blocs et les preuves de travail qui servent à valider les transactions,³⁴⁷ une société nommée « Oraclize » s'assure de la validité de la donnée entrée dans la chaîne de blocs à partir d'une technique de « preuve d'honnêteté » qui garantit que la donnée récupérée par Oraclize est conforme à celle qui se trouve sur la chaîne de blocs. Oraclize décrit dans son rapport son activité comme :

« The solution developed by Oraclize is instead to demonstrate that the data fetched from the original data-source is genuine and untampered. This is accomplished by accompanying the returned data together with a document called authenticity proof. »³⁴⁸

³⁴⁶ Hypothèse issue d'un article intitulé « Les oracles, lien entre la blockchain et le monde » rédigé par Simon Polrot, publié le 13 septembre 2016 sur la plateforme Ethereum France. Consultation en ligne : <https://www.ethereum-france.com/les-oracles-lien-entre-la-blockchain-et-le-monde/>

³⁴⁷ La technologie de la chaîne de blocs en relation avec les preuves de travail est développée en première partie du présent papier.

³⁴⁸ Extrait issu du site officiel d'Oraclize. Pour aller plus loin dans la description du fonctionnement de la société Oraclize : <https://provable.xyz/index.html>. Consulter le document en ligne sur <https://docs.oraclize.it/#background>

Ce type de société semble être une partie de la solution à la question de la responsabilité, puisque comme pour la chaîne de blocs, la fiabilité de l'information est issue d'un consensus. D'un autre côté, contrairement à la chaîne de blocs, l'intermédiaire (Oraclize) n'est pas anonyme. Cette particularité divise la doctrine car intégrer ce type de société dans la chaîne de bloc et le contrat intelligent, est une pratique qui va à l'encontre de l'objectif initial de ces technologies, à savoir la désintermédiation.

ii- L'applicabilité d'une responsabilité partagée

Dans le cas où le contrat intelligent s'inscrirait dans un contexte contractuel entre les parties elles-mêmes ainsi qu'entre les parties et un oracle, ou encore les parties et un auditeur, il serait possible de se questionner sur l'idée d'une responsabilité partagée entre les acteurs.

Initialement, en vertu de l'article 1480 du *Code civil du Québec*³⁴⁹, une personne fautive n'est responsable uniquement du dommage qu'elle a causé. Lors de la conception d'un produit et concernant la responsabilité du fabricant, du distributeur et du fournisseur, l'article 1468 du *Code civil du Québec*³⁵⁰ pose une présomption de la connaissance du défaut de sécurité du produit. Pour s'en exonérer, le défendeur peut obtenir une responsabilité partagée sur la base d'une faute de la victime, si cette faute a pu contribuer, avec le défaut de sécurité, à la réalisation du préjudice. En effet l'article 1478 du Code civil du Québec prévoit que : « Lorsque le préjudice est causé par plusieurs personnes, la responsabilité se partage entre elles en proportion de la gravité de leur faute respective. La faute de la victime, commune dans ses effets avec celle de l'auteur, entraîne également un tel partage ».³⁵¹

³⁴⁹ Art. 1480 C.c.Q : « Lorsque plusieurs personnes ont participé à un fait collectif fautif qui entraîne un préjudice ou qu'elles ont commis des fautes distinctes dont chacune est susceptible d'avoir causé le préjudice, sans qu'il soit possible, dans l'un ou l'autre cas, de déterminer laquelle l'a effectivement causé, elles sont tenues solidairement à la réparation du préjudice. »

³⁵⁰ Art. 1468 C.c.Q : « Le fabricant d'un bien meuble, même si ce bien est incorporé à un immeuble ou y est placé pour le service ou l'exploitation de celui-ci, est tenu de réparer le préjudice causé à un tiers par le défaut de sécurité du bien. Il en est de même pour la personne qui fait la distribution du bien sous son nom ou comme étant son bien et pour tout fournisseur du bien, qu'il soit grossiste ou détaillant, ou qu'il soit ou non l'importateur du bien ».

³⁵¹ Art. 1478 C.c.Q

Il serait possible d'imaginer l'application de cette exception aux fondements de la responsabilité civile aux cas de dommages causés par un contrat intelligent dans le sens où, solidairement, les intermédiaires ayant participé à la mise en place du contrat intelligent se verraient chacun dans l'obligation de réparer le préjudice subi par une partie au contrat. Cette solution permettrait de renforcer la protection des parties au contrat intelligent tout en utilisant les fondements de responsabilité civile déjà présents dans le droit positif. Cependant, son applicabilité ne reste que partielle car, pour appliquer la responsabilité pour défaut de sécurité, les juges considèrent que, selon la doctrine, le défaut de sécurité vise l'intégrité physique des personnes³⁵², or dans le cadre d'un défaut de sécurité au sein d'un contrat intelligent, il est difficile d'envisager qu'un défaut de conception du contrat intelligent en lui-même puisse engager un préjudice corporel.

2. Les solutions envisageables pour l'encadrement juridique du contrat intelligent

« Paradoxalement, il est même souvent plus facile d'appliquer une vieille loi à une situation neuve qu'une nouvelle loi à un nouveau contexte. »³⁵³

Les questionnements juridiques relatifs à la chaîne de blocs et au contrat intelligent trouvent certaines réponses dans le droit positif. C'est l'exemple de l'analogie faite en amont dans ce mémoire entre le contrat intelligent et le logiciel qui pourrait lui rendre applicable le régime de protection du droit d'auteur quant à la responsabilité du programmeur³⁵⁴. Cependant, concernant

³⁵² Voir la décision *Fortin c. Mazda Canada inc.* * (C.S., 2014-05-20), 2014 QCCS 2617, SOQUIJ AZ-51080807: dans ce recours collectif contre Mazda Canada Inc, pour écarter le défaut de sécurité, le juge considère que (125) « la doctrine souligne que le défaut de sécurité vise l'intégrité physique des personnes. Comme le rappelle Yves Martineau (Yves MARTINEAU, « Le recours collectif et la garantie contre les vices cachés », dans *Développements récents sur les recours collectifs*, 2005, page 13.), la responsabilité des biens non sécuritaires est conçue pour protéger l'intégrité physique de la personne. » Or, même si le dispositif de verrouillage comportait un vice de conception, ce mécanisme ne représente aucun risque de préjudice corporel pour quiconque utilise le véhicule.

³⁵³ Vincent GAUTRAIS et Pierre TRUDEL, *Circulation des renseignements personnels et Web 2.0*, Thémis, Montréal, 2010, p47.

³⁵⁴ Préc. note 291

d'autres aspects du contrat intelligent, tel que l'impossibilité de le modifier, il serait opportun que le législateur vienne à statuer sur ces questions.

a. Vers quel type de réglementation pour le contrat intelligent ?

Bien qu'elle soit entrée en vigueur en 2001, il n'y a que très peu de décisions qui ont été rendues par les juges³⁵⁵ sur le fondement de la *Loi concernant le cadre juridique des technologies de l'information*. Pourtant, ce type de loi répond exactement au besoin d'évolution du cadre juridique traditionnel face aux évolutions technologiques.

Chaque pays entend intégrer la technologie de la chaîne de blocs à sa manière. En Europe, le Sénat italien a introduit, en date du 22 janvier 2019, un amendement relatif aux « Technologies à base de registres distribués »³⁵⁶. Quant à la France, dans son rapport du 14 décembre 2018 « Mission d'information sur les chaînes de blocs », l'Assemblée Nationale énonce :

« Le droit français semble en mesure d'appréhender un certain nombre de situations créées par l'usage des « blockchains ». La loi ne paraît pas devoir faire obstacle pour l'essentiel au recours à cette technologie et, à l'inverse, ses grands principes directeurs paraissent applicables à son usage. »³⁵⁷

Partant du constat que certains auteurs³⁵⁸ considèrent que le contrat intelligent n'est pas un contrat au sens traditionnel du terme. Il serait envisageable d'adapter le cadre juridique du droit

³⁵⁵ Patrick GINGRAS, et François SENÉCAL, « *Benisty c. Kloda*: cinq enseignements de la Cour d'appel du Québec en droit des technologies de l'information », (2018) 77 *R. du B.* 273-294

³⁵⁶ Proposta di modifica n. 8.0.3 al DDL n. 989, article 8bis « Tecnologia basate su registri distribuiti e smart contract ». Consultation en ligne : <http://www.senato.it/>

³⁵⁷ (Extrait page 87), Assemblée nationale, *Rapport d'information déposé en application de l'article 145 du Règlement par la Mission d'information commune sur les chaînes de blocs*. Consultation en ligne : <http://www.assemblee-nationale.fr/15/pdf/rap-info/i1501.pdf>

³⁵⁸ Boris BARRAUD, « Les blockchains et le droit », *Revue Lamy Droit de l'immatériel*, n° 147 (2018): 48-62.

des obligations au contrat intelligent. En effet, nous pourrions considérer le contrat intelligent comme un contrat traditionnel au sein duquel une clause précisera que les parties auront recours à un contrat intelligent pour son exécution³⁵⁹. D'autant plus que, comme mentionné en première partie³⁶⁰, certaines conditions ne sont pas traductibles en algorithmes.

C'est pourquoi cette forme de contrat « hybride » pourrait résoudre le problème de la traduction des composantes variables du contrat en code informatique telle que la bonne foi ou encore la détermination de la capacité des parties par exemple. Ceci permettrait alors de conserver l'application des fondements du droit des obligations c'est-à-dire continuer de protéger les cocontractants en conservant les règles relatives à l'objet, la cause, le consentement, la signature ou encore la capacité des parties.

b. La solution de l'ajout de clauses contractuelles dans le contrat intelligent

La clause résolutoire³⁶¹ prévue à l'alinéa 2 de l'article 1507 du *Code civil du Québec* mentionne que « la condition résolutoire accomplie oblige chacune des parties à restituer à l'autre les prestations qu'elle a reçues en vertu de l'obligation, comme si celle-ci n'avait jamais existé. »³⁶² Il est préférable pour les parties d'insérer une clause qui permet de revenir en arrière dans le cas où l'oracle fournirait une mauvaise information, ou ne fournirait pas d'information car une fois inscrite dans la chaîne de blocs, l'information deviendra la base de données sur laquelle le contrat intelligent se basera pour son exécution. Ainsi, à défaut de pouvoir rompre le contrat intelligent en exécution³⁶³, l'insertion de ce type de clause permettrait de sanctionner la partie

³⁵⁹ Akiobe SONGOLO, M. P. Chronique – « Le droit à l'épreuve de la technologie de chaîne de blocs », Repères Février 2018 EYB2018REP2414 À propos de la chaîne de blocs, il ajoute que « le législateur pourrait également procéder à des aménagements législatifs qui incluront des sanctions pour les concepteurs et les utilisateurs de la chaîne de blocs en cas d'inexécution automatique de la transaction et également en cas de manipulation frauduleuse de données informatiques. »

³⁶⁰ Préc., note 250

³⁶¹ La clause résolutoire sanctionne l'inexécution par l'une des parties de ses obligations.

³⁶² Art. 1507 C.c.Q.

³⁶³ Comme exposé en première partie de ce papier, il est impossible pour les parties de mettre fin au contrat intelligent lorsque son exécution est enclenchée.

qui ne respecterait pas ses obligations contractuelles durant l'exécution du contrat. Introduire au préalable dans le contrat une clause résolutoire semblerait être une bonne solution pour palier à cet inconvénient.

Outre la clause résolutoire, les parties pourraient aussi inclure une clause de résiliation unilatérale³⁶⁴ qui permettrait non pas de sanctionner une partie qui ne respecterait pas ses obligations, mais de pouvoir résilier le contrat unilatéralement dans le cas où une partie veuille rompre le contrat pour cause de changement des qualités de son cocontractant par exemple.³⁶⁵

A propos des exclusions de responsabilité, la théorie de l'acceptation des risques, très utilisée dans le domaine sportif et des communications, pourrait-elle être un fondement à envisager dans la détermination de la responsabilité en cas de litige qui implique un contrat intelligent ? En effet, l'acceptation des risques correspond au fait d'avoir volontairement pris le risque qu'un dommage survienne. A ce propos, en 2014 dans l'affaire *Provencher c. Janelle*³⁶⁶, le juge de la Cour Suprême se positionne sur l'applicabilité d'une clause d'acceptation des risques. En l'espèce, le demandeur est victime d'une chute de plusieurs mètres lors de l'exécution de travaux de peinture sur la toiture d'une résidence. Parmi plusieurs allégations pour sa défense, le défendeur invoque également une déclaration d'exonération de responsabilité signée par le demandeur en sa faveur.

Le juge Louis Crête reprend les termes de Baudoin et Deslauriers considérant que « la victime n'est tenue de supporter que les risques normaux et prévisibles inhérents à une activité, mais non l'aggravation de ces risques résultant d'un comportement fautif d'une autre personne »³⁶⁷.

³⁶⁴ Dans l'affaire *Gagnon c. Hydro-Québec* (C.S., 2005-08-10), le juge reconnaît la validité d'une clause de résiliation. Il énonce que « la clause de résiliation n'est pas abusive. Elle a été rédigée en termes clairs et non ambigus qui reprennent en substance l'article 1691 C.C. Il n'y a donc pas lieu de réduire les obligations du demandeur. »

³⁶⁵ Par exemple, une société X contracte avec la société B mais durant le contrat celle-ci fusionne avec une société A. La société X peut alors ne pas souhaiter continuer la relation d'affaire avec la société B ; LLUELLES, D. (2006). « La révision du contrat en droit québécois ». *Revue générale de droit*, 36 (1), 25–67.

³⁶⁶ *Provencher c. Janelle* (C.S., 2014-05-02), 2014 QCCS 1862, SOQUIJ AZ-51070204

³⁶⁷ Cité dans la décision *Provencher c. Janelle* (C.S., 2014-05-02), Jean-Louis BAUDOIN et Patrice DESLAURIERS, *La responsabilité civile*, 8^e éd., vol. 1, Cowansville, Éditions Yvon Blais, 2014, p. 646

Le juge ajoute que « l'acceptation des risques peut, dans certaines circonstances, constituer une négligence ou une imprudence de la part de la victime et permettre l'application d'un partage de la responsabilité. » Dans cette affaire, la construction de l'échelle fournie par le défendeur a augmenté le risque initialement accepté par la victime. Le juge a alors considéré que l'acceptation des risques constituait une imprudence de la victime et à la fois une part de responsabilité du défendeur pour la raison mentionnée ci-dessus, ce qui a permis au juge de fixer une responsabilité partagée dans l'accident en application de l'article 1478 du *Code civil du Québec*³⁶⁸. Transposé au contrat intelligent, il pourrait être possible que l'une des parties accepte le risque qu'un dommage survienne lors de l'exécution du contrat intelligent. Dans ce cas, si les conditions d'application³⁶⁹ sont réunies, l'utilisateur du contrat intelligent pourrait se voir assumer la pleine responsabilité d'un préjudice causé par l'exécution du contrat intelligent.

³⁶⁸ Art. 1478 C.c.Q : « Lorsque le préjudice est causé par plusieurs personnes, la responsabilité se partage entre elles en proportion de la gravité de leur faute respective. La faute de la victime, commune dans ses effets avec celle de l'auteur, entraîne également un tel partage. »

³⁶⁹ Dans le cas de l'acceptation des risques, les conditions d'application sont : une preuve claire que la victime a volontairement accepté de participer à l'activité comportant des risques / que la victime avait la connaissance du risque, et a reçu une information suffisante à cet égard / que l'acceptation porte sur le risque connu par la victime; voir l'affaire *Boisclair c. Nolet*, 2008 QCCA 2383.

Conclusion

Il ressort de plusieurs considérations légales et doctrinales que le terme de « contrat intelligent » ne semble pas approprié. Tout d'abord il n'est pas un contrat au sens juridique du terme, mais un programme informatique servant à la conclusion et l'exécution d'un véritable contrat traditionnel. On ne peut pas dire non plus qu'il soit intelligent, puisqu'il exécute simplement le programme mis en place par le développeur³⁷⁰.

Outre ce problème de qualification, nous avons vu que les contrats intelligents posent plusieurs autres difficultés comme l'intégration de données variables tel que le caractère raisonnable ou la bonne foi³⁷¹. Comment le contrat intelligent peut-il quantifier le caractère raisonnable d'un comportement en appliquant une approche algorithmique linéaire ?³⁷² C'est la raison pour laquelle, dans bien des cas, le contrat intelligent sera inévitablement accompagné d'un contrat « traditionnel » répertoriant les clauses non traductibles en algorithme.

Une autre difficulté tend à la question de la modification du contrat, une caractéristique commune à de nombreux accord commerciaux. Il manque encore un processus qui permettrait pour le contrat intelligent de contourner la nature immuable de la chaîne de blocs et cette nécessité de recourir à des professionnels expérimentés en programmation pour mettre en place un contrat intelligent fiable. Tous ces facteurs sont encore des freins à la démocratisation du contrat intelligent. C'est une technologie encore immature dont les applications restent très limitées. Son évolution nécessiterait d'approfondir tant son aspect technologique que juridique.

³⁷⁰ LUU, Loi, CHU, Duc-Hiep, OLICKEL, Hrishi, et al. « Making smart contracts smarter », Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. ACM, 2016. p. 254

³⁷¹ GIANCASPRO, Mark. « Is a smart contract really a smart idea? Insights from a legal perspective », Computer law & security review, 2017, vol. 33, no 6, p. 825-835.

³⁷² Un ordinateur manipule exclusivement des informations binaires. Lire à ce propos l'ouvrage de Pierre-Alain GOUPILLE, *Technologie des ordinateurs et des réseaux*, 9^e édition, Dunod, 2015.

En droit québécois, les régimes de responsabilité (autre que la responsabilité personnelle) se réfèrent principalement aux actes produits par autrui et le *Code civil du Québec* évoque les « choses qu'on a sous sa garde », comme la faute causée par un mineur³⁷³, ou le préjudice causé par l'animal³⁷⁴, ou encore le fait autonome d'un bien³⁷⁵. En ce qui concerne la chaîne de blocs, personne ne peut être personnellement visé comme détenant la gouvernance de celle-ci puisque c'est une gouvernance par consensus qui plus est anonyme, ce qui complique la question de la responsabilité en cas de dommage causé. Quant au contrat intelligent, sa bonne exécution est déterminée par la bonne exécution des algorithmes qui le composent et non pas par la bonne volonté des parties. Nous avons donc constaté qu'il n'est pas assimilable à un contrat traditionnel (qui se veut être une rencontre de volonté entre une ou plusieurs parties) mais plutôt à un logiciel. Par conséquent, le régime juridique du contrat intelligent peut tout à fait être assimilé à la protection du droit d'auteur qui régit les logiciels dans le droit positif.

Aussi, au regard des différentes hypothèses envisagées dans ce mémoire, nous avons pu constater que le droit positif semble applicable aux évolutions technologiques telles que le contrat intelligent, mais ces technologies n'étant certainement pas infaillibles, la mise en place de dispositions spécifiques seraient les bienvenues afin de pouvoir anticiper la protection des intermédiaires en cas de préjudice subi. Par exemple, on pourrait implémenter sur la chaîne de blocs les informations portées par des décisions de justice³⁷⁶. Mais si un contrat intelligent prévoit qu'une opération qu'il contient peut-être annulée par une décision de justice, il faudrait d'abord pouvoir s'assurer que la décision ait bel et bien ordonné l'annulation de l'opération avant d'intégrer cette information dans le réseau. Pour l'instant aucun oracle ne le fait. C'est

³⁷³ Art. 1459 CcQ : « Le titulaire de l'autorité parentale est tenu de réparer le préjudice causé à autrui par le fait ou la faute du mineur à l'égard de qui il exerce cette autorité, à moins de prouver qu'il n'a lui-même commis aucune faute dans la garde, la surveillance ou l'éducation du mineur. »

³⁷⁴ Art. 1466 CcQ : « Le propriétaire d'un animal est tenu de réparer le préjudice que l'animal a causé, soit qu'il fût sous sa garde ou sous celle d'un tiers, soit qu'il fût égaré ou échappé. »

³⁷⁵ Art. 1465 CcQ : « Le gardien d'un bien est tenu de réparer le préjudice causé par le fait autonome de celui-ci, à moins qu'il prouve n'avoir commis aucune faute. »

³⁷⁶ Jeremy M. SKLAROFF, "Smart contracts and the cost of inflexibility". U. Pa. L. Rev., 2017, vol. 166, p. 263.

l'exemple même du type d'outil qui pourrait être mis en place dans le futur si un marché du contentieux des contrats intelligents émergeait³⁷⁷.

Certes le fait de pouvoir intégrer les contrats intelligents à des registres distribués comme les chaînes de blocs a pour intérêt de rendre plus fiable les données numériques qui y sont intégrées et de s'assurer de la bonne exécution des engagements contractuels de chaque partie. Mais ceci n'est pas absolu et les chaînes de blocs, comme tout système informatique, sont vulnérables et ont notamment fait l'objet de plusieurs attaques réussies au cours de ces dernières années³⁷⁸; on parle « d'attaque 51% », c'est-à-dire lorsqu'un acteur (ou un groupe d'acteurs) dispose de plus de 50% de la puissance de minage de la chaîne de blocs visée³⁷⁹.

Pour pallier ses éventuelles attaques technologiques, les gouvernements commencent à entreprendre quelques avancées réglementaires sur le sujet. Au Québec et au Canada, en addition aux dispositions du *Code civil du Québec*, la *Loi concernant le cadre juridique des technologies de l'information* a apporté de nombreuses précisions quant au cadre juridique des technologies de l'information et semblent s'appliquer aussi au contrat intelligent. Aujourd'hui l'enjeu principal pour le législateur est de réussir à concevoir un cadre juridique adapté au développement des contrats intelligents, qui puisse à la fois réglementer le marché et protéger ses intervenants en cas de préjudice subi, sans pour autant devenir un frein à leur évolution sur le plan technologique.

De plus, l'organisation internationale de normalisation, connue sous l'acronyme « ISO », travaille sur l'élaboration d'une norme ISO³⁸⁰ à propos de la normalisation des technologies des

³⁷⁷ Ibid

³⁷⁸ Notamment l'attaque contre The DAO en 2016. Consulter le site <https://www.ethereum-france.com/the-dao-post-mortem/> pour plus de précisions.

³⁷⁹ En janvier 2019, des hackers ont réussi une attaque 51% contre Ethereum Classic (une alternative à la plateforme Ethereum) en prenant le contrôle de la chaîne de blocs et modifiant l'historique de toutes les transactions réalisées entre utilisateurs, afin de réaliser ce qu'on appelle des « doubles dépenses » en empêchant la réalisation de certaines dépenses. Pour aller plus loin sur le sujet, le site suivant démontre comment une attaque est envisageable sur Bitcoin et Ethereum : <https://blog.octo.com/attaque-des-51-sur-une-blockchain-demonstration-sur-ethereum/>

³⁸⁰ Comité d'étude national ISO/TC 307

chaines de blocs et des technologies de registres distribués. En France, le 12 décembre 2018, l'Assemblée nationale a présenté un rapport de la mission d'information commune sur les usages des chaines de blocs et autres technologies de certifications de registres³⁸¹, afin de proposer certaines réponses et plusieurs plans d'actions face aux problèmes que posent le développement des chaines de blocs, notamment sur la problématique de la consommation d'énergie excessive qu'entraîne ce genre de technologie, ou encore sur l'impact qu'elle a sur certaines professions juridiques règlementées telles que les notaires ou les avocats.

En effet, il peut sembler difficile pour les professions juridiques de s'affranchir de ce nouveau langage du code informatique, bien différent du langage juridique. Pourtant, le contrat intelligent le montre bien, la loi continue de se référer à un avocat, même dans un monde qui se veut sans tiers intermédiaire. Nick Szabo lui-même disait en 2016 qu'il n'était pas convaincu que le contrat intelligent puisse remplacer le contrat traditionnel³⁸². Le contrat intelligent ainsi que la chaîne de blocs sont des exemples concrets de l'évolution vers laquelle notre société souhaite tendre. Ces dispositifs court-circuitent les intermédiaires juridiques traditionnels dans le but de réduire les coûts transactionnels. Cependant, même s'il est certain que l'application du contrat intelligent continue de prendre de l'ampleur, les professions juridiques ne sont certainement pas amenées à disparaître, cependant il est fort probable que leurs compétences soient amenées à s'élargir ; on pense notamment aux services juridiques en ligne qui sont de plus en plus répandus.

Toujours est-il que, même si certains prônent l'avènement d'un système infallible grâce aux nouvelles technologies, le codage et la programmation d'un contrat intelligent, tout comme ceux d'un robot, nécessitent une intervention humaine qui est faillible. Pourtant, pour optimiser la rédaction du contrat intelligent, quoi de mieux qu'un avocat ayant lui-même des compétences en programmation pour traduire, le plus exactement possible et sans erreur d'interprétation, la

³⁸¹ Rapport d'information sur les chaines de blocs. En ligne version PDF : <http://www.assemblee-nationale.fr/15/pdf/rap-info/i1501.pdf>

³⁸² Michael del CASTILLO, « Relax Lawyers, Nick Szabo Says Smart Contracts Won't Kill Jobs ». En ligne : <https://www.coindesk.com/nick-szabo-lawyers-jobssafe-in-smart-contract-era/>.

volonté des parties ? Les auteurs Garapon et Lassègue³⁸³ conçoivent cependant que le public puisse aujourd'hui être plus rassuré par une vérité issue d'un algorithme que par une décision humaine. Selon eux,

« (...) pour comprendre l'utilisation du droit nouveau issu du numérique, (...) il faut à la fois replacer cette révolution graphique dans le temps long, sans quoi on se laisse fasciner par les seules innovations technologiques, mais aussi saisir le travail technique opéré par elle, qui en donne toute la mesure. (...) Pour nous tenir à distance du double péril consistant à tomber dans une fascination acritique pour une nouvelle technologie, ou dans un catastrophisme irrationnel qui redoute la fin du droit. »³⁸⁴

³⁸³ Antoine GARAPON, et Jean LASSÈGUE, *Justice digitale : révolution graphique et rupture anthropologique*. Presses universitaires de France, 2018.

³⁸⁴ *Ibid.* p20

Bibliographie

Monographies et recueils

- ANTONOPOULOS, A.-M. et WOOD, G. *Mastering ethereum: building smart contracts and dapps*. O'Reilly Media, 2018.
- BAUDOIN, J.-L., *La responsabilité civile délictuelle*, 3e éd., Cowansville, Éditions Yvon Blais, 1990, 838 p.
- BAUDOIN J.-L. et P. DESLAURIERS, *La responsabilité civile*, 6^e éd., Cowansville, Éditions Yvon Blais, 2003, 1953 p.
- BENSOUSSAN, A., et BENSOUSSAN, J., *Droit des robots*, Éditions Larcier, 2015.
- BORGIA, D., *La responsabilité professionnelle de l'avocat*. Service de la formation permanente du Barreau du Québec, *Développements récents en droit immobilier (1996)*, Cowansville, Éditions Yvon Blais, p.3
- BUSSAC, E. *Bitcoin, ether & Cie: Guide pratique pour comprendre, anticiper et investir 2019*. Dunod, 2018.
- CARBONNIER, J., *Droit civil*, Tome 4, « Les obligations », Paris, P.U.F., 1996, 610 p.
- DANNEN, C., *Introducing Ethereum and Solidity*. Berkeley : Apress, 2017.
- DE FILIPPI, Primavera De Filippi. *Blockchain and the law: The rule of code*. Harvard University Press, 2018.
- DRESCHER, D., *Blockchain basics: A Non-Technical Introduction in 25 Steps*. Berkeley, CA : Apress, 2017.
- DUMAS, J.-G., S. VARRETTE, P. LAFOURCADE, et A. TICHIT. *Les blockchains en 50 questions: Comprendre le fonctionnement et les enjeux de cette technologie*. Dunod, 2018.
- GARAPON, A. et LASSÈGUE, J. *Justice digitale: révolution graphique et rupture anthropologique*. Presses universitaires de France, 2018.

- GAUTRAIS, V., *Le contrat électronique international*, 2^e éd., Louvain-La-Neuve, Bruylant-Academia, 2002, 427 p.
- GAUTRAIS, V., et MACKAAY, E., *Les contrats informatiques*, dans Denys-Claude Lamontagne, *Droit spécialisé des contrats*, vol. 3, Cowansville, Éditions Yvon Blais, 2001, p. 279-315.
- GOUPILLE, P.-A., *Technologie des ordinateurs et des réseaux*, 9^e édition, Dunod, 2015.
- GRINGRAS, C., *The laws of the Internet*, Londres, Butterworths, 1997, 399 p.
- PINEAU, J. et M. OUELLETTE, *Théorie de la responsabilité civile*, 2^e éd., Montréal, Éditions Thémis, 1980
- LESSIG L., *Code and Other Laws of Cyberspace*, New York, Basic Books, 1999, 297 p.
- LEVESQUE, F., *Mise en perspective de la responsabilité civile*. Précis de droit québécois des obligations : contrat, responsabilité, exécution et extinction, 2014
- LLUELLES, D., & B., MOORE, *Droit des obligations*. Éditions Thémis, 2012.
- MOUGAYAR W., *Business Blockchain. Pratiques et applications professionnelles*, Dicoland, 2017.
- REID, H., *Dictionnaire de droit québécois et canadien*, 3^e édition, Montréal, Wilson & Lafleur, 2004, 828 p.
- ROYER, J., «La preuve civile » 2^e éd., Cowansville, Yvon Blais, 1995, 1290 p.
- SINGHAL, B., Gautam Dhameja, Priyansu Sekhar Panda 2018
- TANCELIN, M., *Des obligations en droit mixte du Québec*, 7^e éd., Montréal, Éditions Wilson & Lafleur, 2009, no 1107.
- TAPSCOTT, D., et A. TAPSCOTT., *Blockchain Revolution How the Technology behind Bitcoin Is Changing Money, Business and the World*, 2016.
- TRUDEL P., *Droit du cyberspace*, Montréal, Éditions Thémis, 1997

Articles

« Assemblée nationale ~ RELATIF À LA TRANSPARENCE, À LA LUTTE CONTRE LA CORRUPTION ET À LA MODERNISATION DE LA VIE ÉCONOMIQUE (no 3785) - Amendement no 227 ». Consulté le 20 janvier 2019. <http://www.assemblee-nationale.fr/14/amendements/3785/AN/227.asp>.

« Les blockchains et le droit ». *Revue Lamy Droit de l'immatériel*, n° 147 (2018): 48-62.

« The Law and Legality of Smart Contracts ». *Georgetown Law Technology Review* (blog), 17 avril 2017. <https://www.georgetownlawtechreview.org/the-law-and-legality-of-smart-contracts/GLTR-04-2017/>.

BARREAU, C. (2017). La régulation des smart contracts et les smart contracts des régulateurs. *Annales des Mines - Réalités industrielles*, Août 2017(3), 74-76.

BARRAUD, B., « Les blockchains et le droit ». *Revue Lamy Droit de l'immatériel*, n° 147 (2018): 48-62.

BARREAU, C., « La régulation des smart contracts et les smart contracts des régulateurs ». *Annales des Mines - Réalités industrielles* Août 2017, n° 3 (26 juillet 2017): 74-76.

BERGERON-DROLET, E., « Pourquoi les juristes doivent-ils s'intéresser à la blockchain? », SOQUIJ, L'Express, vol. 9, no 45, 16 novembre 2018

BERGERON-DROLET, E., et CAPOGROSSO, B. J., « Introduction au blockchain pour les avocats en propriété intellectuelle », dans Barreau du Québec, Service de la formation continue, *Développements récents en droit de la propriété intellectuelle* (2017), volume 437, Montréal, Éditions Yvon Blais, 2017

COHN, A., T. WEST, et C. PARKER., « Smart after all: blockchain, smart contracts, parametric insurance, and smart energy grids » 1 (2017): 32.

BERBAIN, C., « La blockchain : concept, technologies, acteurs et usages ». *Annales des Mines - Réalités industrielles* Août 2017, n° 3 (26 juillet 2017): 6-9.

- BLOCKCHAIN FRANCE (2016). *La Blockchain décryptée: les clefs d'une révolution*. Paris: Observatoire Netexplo.
- CASEAU, Y., and S. SOUDOPLATOFF., « La blockchain, ou la confiance distribuée. » Fondation pour l'innovation politique, 2016.
- DESPLEBIN, O., et G. LUX. « The evolution of accounting, control, audit and their practices through the prism of the Blockchain: a prospective reflection ». Dans *Transitions numériques et informations comptables*, cd-rom. 39ème Congrès de l'AFC. Nantes, France, 2018. Disponible sur le site <https://hal.archives-ouvertes.fr/hal-01907902>.
- EASTERBROOK, F. H., *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207.
- FAURE, P.-H., « Le bitcoin peut-il être assimilé à une monnaie ? Un examen à partir des différentes grilles de lecture de la science économique », 2016. Disponible en ligne sur le site <https://hal.archives-ouvertes.fr/hal-01337694>.
- FILIPPI, P. De., « Blockchain et cryptomonnaies ». *Que sais-je ?*, Presses Universitaires de France, 2018
- FILIPPI, P. De. « Chapitre III. Applications de la blockchain ». *Que sais-je?*, Consulté le 5 octobre 2018, 74-103.
- GIANCASPRO, M., *Is a 'smart contract' really a smart idea? Insights from a legal perspective*. *Computer law & security review*, 2017, vol. 33, no 6, p. 825-835.
- GRAMMOND, S., « La règle sur les clauses abusives sous l'éclairage du droit comparé », (2010) 51 C. de D. 83, 108.
- JEAN, B., et P. DE FILIPPI. « Les Smart Contracts, les nouveaux contrats augmentés ? » *Conseils et Entreprises*, décembre 2016. Disponible en ligne sur le site <https://hal.archives-ouvertes.fr/hal-01676878>.
- LECUN, Y., Y. BENGIO, et G. HINTON. « Deep Learning ». *Nature* 521, n° 7553 (mai 2015): 436-44. Disponible en ligne sur le site <https://doi.org/10.1038/nature14539>.
- LEMYRE, P.-P. et W., RICHARD, « Logiciels libres et ouverts: impacts juridiques sur les utilisateurs québécois », (2005) 17 C.P.I. 597-666

- LESSIG, L., *Code: And Other Laws of Cyberspace*. ReadHowYouWant.com, 2009.
- LESSIG, L., *The law of the horse: What cyber law might teach*. Harv. L. Rev., 1999, vol. 113, p. 501.
- LORE, P.-M., « Évolution ou révolution pour les contrats en France ? », s. d., 63.
- MASSE, C., « La responsabilité du fabricant, du distributeur et du fournisseur » dans *Collection de droit 2007-08, École du Barreau du Québec*, vol. 4, Responsabilité, Montréal, Éditions Yvon-Blais, 2007, p. 65
- MIGNOT, S., « Le bitcoin : nature et fonctionnement », 2015, 4.
- NAKAMOTO, S., et al. *Bitcoin: A peer-to-peer electronic cash system*. 2008.
- PLISSON, C., « La blockchain, un bouleversement économique, juridique voire sociétal ». *I2D Information, données documents* Volume 54, n° 3 (2 octobre 2017): 20-22.
- PONS, Par Jérôme. « La mise en œuvre de la blockchain et des smart contracts par les industries culturelles », s. d., 10.
- RABESANDRATANA, V., et N. BACCA. « L'Oracle hardware : la couche de confiance entre les blockchains et le monde physique ». *Annales des Mines - Réalités industrielles* Août 2017, n° 3 (26 juillet 2017): 91-93.
- SAVELYEV A., "Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law", *Information & Communications Technology Law*, 26:2, 116-134
- SHAPIRO, J., et DANIELS K., «Blockchain: An Unlikely Key to Improving Access to Justice?», *Le Blogue du CRL*, 26 mars 2019
- SILLABER, C., et WALTL, B., "Life cycle of smart contracts in blockchain ecosystems". *Datenschutz und Datensicherheit-DuD*, 2017, vol. 41, no 8, p. 497-500.
- SOLIS, M.-A. et S. LAPOINTE., « Réflexions sur l'application des garanties aux logiciels en droit civil québécois », (1999) 59 R. du B. 393-444
- SZABO, Nick. « Formalizing and Securing Relationships on Public Networks ». *First Monday* 2, n° 9 (1 septembre 1997). Disponible en ligne sur le site <https://doi.org/10.5210/fm.v2i9.548>.
- TRUDEL, P., "La responsabilité des acteurs du commerce électronique." (2002).

TRUDEL, P., La responsabilité sur internet en droit civil québécois, (2008) Consultation en ligne sur le site http://www.chairelrwilson.ca/documents/TRUDEL_resp_internet.pdf

TURING, A.-M. « Computing Machinery and Intelligence ». In *Parsing the Turing Test: Philosophical and Methodological Issues in the Quest for the Thinking Computer*, édité par Robert Epstein, Gary Roberts, et Grace Beber, 23-65. Dordrecht: Springer Netherlands, 2009. Disponible en ligne sur le site https://doi.org/10.1007/978-1-4020-6710-5_3.

VALENTA, M., et P. SANDNER. « Comparison of Ethereum, Hyperledger Fabric and Corda », s. d., 8. Automatic citation updates are disabled. To see the bibliography, click Refresh in the Zotero tab.

VERMEYS N., « C-11, la Loi concernant le cadre juridique des technologies de l'information et la responsabilité des intermédiaires techniques québécois : une dualité de régimes (in)utile(s)? », Cahiers de propriété intellectuelle, vol. 25, no 3, p. 1051, 2013

VERMEYS N., « La responsabilité civile du fait des agents autonomes », (2018) 30 Les Cahiers de propriété intellectuelle, 851-880.

Sites Internet

<https://blockchainfrance.net/?s=france>

<http://www.larousse.fr/dictionnaires/francais>

<https://lesconferences.openum.ca/files/sites/97/2018/05/Smart-contracts.pdf>.

<https://www.lccjti.ca/>.

<https://www.canlii.org/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

<https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf>.

Table de la jurisprudence

Textes canadiens

Apple Computer Inc. c. Mackintosh Computers Ltd., [1990] 2 R.C.S. 209

Bérubé c. Bois Rocam inc. SOQUIJ AZ-50286464,

Bolduc c. Lévis (Ville de), 2015 QCCA 1428

*Canada (Procureur général) c. CNIM Canada inc.**, 2015 QCCS 5094

CCH Canadienne Ltée c. Barreau du Haut-Canada, 2004 CSC 13

Central Trust Co. c. Rafuse (C.S. Can., 1988-06-30)

Ciment du Saint-Laurent inc. c. Barrette, 2008 CSC 64

Côté et Les entreprises générales Rimo c. Rancourt, Cour supérieure, St-François, 450-05-001065-966

Corriveau c. Canoe inc., 2010 QCCS 3396

Demers c. Roy, 2008 QCCQ 4708, par. 54 (CanLII)

Distributeur MDR inc. c. Blanchette (C.S., 2014-05-26), 2014 QCCS 2204

Fondation des Sourds du Québec inc. c. Oralys inc. (C.S., 2008-07-17), 2008 QCCS 6733

Gagnon c. Hydro-Québec (C.S., 2005-08-10)

Gordon v. Canada (Health), 2008 FC 258 (CanLII)

*Hydro-Québec c. Bell Canada** (C.Q., 2019-01-29), 2019 QCCQ 263

Labrie c. Tremblay, Cour d'appel, Québec, 200-09-001084-987, 7 décembre 1999.

*Mathieu c. Fonds d'assurance responsabilité professionnelle du Barreau du Québec** (C.S., 2008-07-10)

Mensys Business Solution Centre Ltd. c. Drummond (Municipalité régionale de comté de),
(C.S., 2002-01-30)

Provencher c. Janelle (C.S., 2014-05-02), 2014 QCCS 1862

Provigo Distribution Inc. v. Supermarché A.R.G. Inc., 1997 CanLII 10209 (QC CA)

Programmation Gagnon inc. c. Lemay (C.S., 2000-01-06)

Reichenbach c. Moto Internationale, 2010 QCCQ 4128, par. 28 et 29 (CanLII)

Roberge c. Bolduc (C.S. Can., 1991-02-28)

Royer c. Mazda Canada inc., 2015 QCCQ 1576

Samen Investments Inc. c. Monit Management Ltd. (2618 QCCS 17 juin 2010)

Syndicat des employées et employés professionnels et de bureau, section locale 571, CTC-FTQ
(SEPB) c. Barreau du Québec, 2007 QCCA 64, par. 30.

Sincennes c. Lavigne, 2010 QCCS 54

Technologies Trellisys inc. c. Rousseau Métal inc. (C.Q., 2009-02-05)

Union canadienne (L'), compagnie d'assurances c. Mini-entrepôt Longueuil inc., 2011 QCCQ
7058

Vaillancourt c. Lagacé, 2005 QCCS 29333

Warman c. Lemire, 2009 TCDP 26

Textes français

Cass. 1ère civ., 3 nov. 2016, n° 15.22-595

Table de la législation

Textes canadiens

Code civil du Québec, RLRQ c. CCQ-1991

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

Loi sur la protection du consommateur, L.R.O., 1990, c. C-31

Loi sur le droit d'auteur, L.R.C. (1985), c. C-42

Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000

Loi sur les sociétés par actions, RLRQ c S-31.1

Textes américains

Tennessee Code Ann. § 47-10-201

Textes français

Assemblée Nationale ~ Relatif à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (no 3785) - Amendement no 227

Avis 4/2007 sur le concept de données à caractère personnel. Groupe de travail « article 29 » sur la protection des données.

Ordonnance n° 2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers

Textes européens

Directive 85/374/CEE du Conseil du 25 juillet 1985 relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de responsabilité du fait des produits défectueux.

Directive 95/ 46/ CE - Règlement général sur la protection des données.

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