Lex Electronica

Lex Electronica

La gouvernance décentralisée des chaînes de blocs : mythe ou réalité du code

Rokhaya Diop

Volume 28, numéro 1, 2023

URI : https://id.erudit.org/iderudit/1108627ar
DOI : https://doi.org/10.7202/1108627ar

Aller au sommaire du numéro

Éditeur(s)

Centre de recherche en droit public Université de Montréal

ISSN

1480-1787 (numérique)

Découvrir la revue

Citer cet article

Diop, R. (2023). La gouvernance décentralisée des chaînes de blocs : mythe ou réalité du code. *Lex Electronica*, *28*(1), 200–227. https://doi.org/10.7202/1108627ar

Résumé de l'article

L'objectif de cet article est de s'interroger sur l'efficacité de la gouvernance décentralisée des chaînes de blocs qui renvoie au fonctionnement des chaînes de blocs publiques. Dans ce texte, l'auteure émet des critiques sur ces nouveaux paradigmes d'organisations, en déplorant le remplacement du droit par la gouvernance algorithmique et la régulation technique. L'analyse démontre que les chaînes de blocs publiques sont soumises à une gouvernance multiforme, qui, en réalité, est lacunaire. Les imperfections sont constatables, d'une part, dans le fonctionnement du code et, d'autre part, dans l'action de la communauté. Ensuite, les risques de comportements opportunistes susceptibles d'affecter le déroulement de l'activité dans les chaînes de blocs publiques sont mis en évidence. À cet égard, les fourches et le phénomène de concentration des pouvoirs sont illustrés comme des facteurs qui peuvent paralyser la gouvernance.

Pourtant, la technologie de la chaîne de blocs pourrait être indubitablement utilisée à bon escient. Pour ce faire, l'auteur propose la réintermédiation des professionnels du droit; ces spécialistes semblent incontournables dans le fonctionnement de cette technologie. Reconsidérer leur rôle devient alors nécessaire pour assurer la pérennisation de cette technologie.

LA GOUVERNANCE DÉCENTRALISÉE DES CHAÎNES DE BLOCS : MYTHE OU RÉALITÉ DU CODE[1]

Rokhaya DIOP[2]

1 Ce texte a été réalisé grâce à une bourse postdoctorale de la Chaire de recherche sur les contrats intelligents et la chaîne de blocs - Chambre des notaires du Québec.

2 Stagiaire postdoctorale, Chaire de recherche sur les contrats intelligents et la chaîne de blocs, Université Laval (Québec).

Table des matières

RÉSUMÉ

L'objectif de cet article est de s'interroger sur l'efficacité de la gouvernance décentralisée des chaînes de blocs qui renvoie au fonctionnement des chaînes de blocs publiques. Dans ce texte, l'auteure émet des critiques sur ces nouveaux paradigmes d'organisations, en déplorant le remplacement du droit par la gouvernance algorithmique et la régulation technique. L'analyse démontre que les chaînes de blocs publiques sont soumises à une gouvernance multiforme, qui, en réalité, est lacunaire. Les imperfections sont constatables, d'une part, dans le fonctionnement du code et, d'autre part, dans l'action de la communauté. Ensuite, les risques de comportements opportunistes susceptibles d'affecter le déroulement de l'activité dans les chaînes de blocs publiques sont mis en évidence. À cet égard, les fourches et le phénomène de concentration des pouvoirs sont illustrés comme des facteurs qui peuvent paralyser la gouvernance.

Pourtant, la technologie de la chaîne de blocs pourrait être indubitablement utilisée à bon escient. Pour ce faire, l'auteur propose la réintermédiation des professionnels du droit; ces spécialistes semblent incontournables dans le fonctionnement de cette technologie. Reconsidérer leur rôle devient alors nécessaire pour assurer la pérennisation de cette technologie.

Mots clés

Chaînes de blocs publiques, Gouvernance décentralisée, désintermédiation, réintermédiation, tiers de confiance, professionnels du droit.

INTRODUCTION

[1] La deuxième révolution numérique (Leloup, 2017, p. 240-258) est marquée par l'avènement de nouvelles technologies dont les chaînes de blocs[3], qui ont le vent en poupe. Survenue à la suite de la crise financière de 2008, la technologie de la chaîne de blocs s'est révélée comme une machine pouvant restaurer la confiance dans les relations d'affaires. Cette technologie est considérée comme un nouveau système qui entend remplacer la confiance aux humains par la confiance au Code (De Fillippi, Mannan & Reijers, 2020). Animés par une forte volonté de se départir de toutes institutions habilitées à exercer un pouvoir de contrôle sur la cité, les libertariens ont très vite adopter cette technologie. La chaîne de blocs, dans son sens originel, propose de nouveaux paradigmes d'organisations qui fonctionnent de manière autonome, sans l'immixtion d'une quelconque autorité centrale. Ces modèles reposent sur ce que l'on appelle la gouvernance décentralisée. Prônée par le mouvement des *cypherpunks* (De Fillipi, 2018, p. 7-14), la gouvernance décentralisée renvoie aux règles et procédures par lesquelles la gestion des chaînes de blocs publiques est assurée. Le recours aux chaîne de blocs publiques, voire décentralisées, a donc pour fondement cette méfiance manifeste que les libertariens ont à l'égard des institutions. En effet, ces registres fonctionnent de manière pseudonyme; tout individu peut participer au réseau sans qu'il soit nécessaire de demander l'approbation d'un quelconque individu.

[2] Bien qu'elle soit idéale pour ces initiateurs, cette forme de gouvernance semble imparfaite face aux *réalités* de la société. Notre analyse démontre que cette gouvernance est basée essentiellement sur la confiance à la technologie. Or, la technologie n'est pas sans faille. Les chaînes de blocs publiques présentent, dans leur fonctionnement, des défaillances tant au niveau du code[4] que de la communauté[5]. Cette gouvernance n'est pas, en outre, exempte de risques. Contrairement à l'idée de départ fondée sur la désintermédiation, l'immuabilité et la transparence, les chaînes de blocs publiques se heurtent à d'innombrables obstacles qui violent les trois principes susmentionnés. Ces entraves résultent des failles qui peuvent être constatées dans le fonctionnement des algorithmes, ce qui traduit les limites du code. Ces limites se manifestent à la suite de problèmes de coordination[6] qui affectent la communauté. Cette collectivité est composée essentiellement d'acteurs agissant au sein de l'infrastructure. Le caractère fermé de cette sphère met en péril la continuité du bon fonctionnement de cette technologie.

[3] La création de nouveaux modèles d'organisations basés sur la confiance au code ou aux chiffres n'est pas un phénomène nouveau. De nombreux juristes ont déploré, dans leur étude, ces nouveaux paradigmes où la gouvernance algorithmique et la régulation technique (Supiot, 2015 et 2020, Lehaire, 2022 & De Fillipi, 2017) se substituent au

3 La chaîne de blocs repose sur le système des registres distribués; ces registres sont dits décentralisés parce qu'ils fonctionnent sur un réseau pair-à-pair accessible à tous. Les chaînes de blocs sont des bases de données qui s'apparentent à des livres comptables dans lesquels sont enregistrés chronologiquement toutes les transactions.

4 Le fonctionnement du code renvoie à la gouvernance algorithmique. Ces infrastructures fonctionnent grâce à des protocoles de consensus et à des programmes informatiques nommés contrats intelligents.

5 Concernant la communauté, elle implique non seulement les acteurs qui agissent sur l'infrastructure, mais également les acteurs au service des applications décentralisées, à l'exemple des organisations autonomes décentralisées.

6 Les problèmes de coordination surviennent généralement en cas de fourches Voir section 1.2.1.

droit. Les travaux de ces auteurs constituent un départ intéressant pour appréhender les imperfections de la gouvernance décentralisée et réfléchir sur la manière dont ce modèle de gouvernance pourrait être amélioré.

[4] L'objectif de ce texte est donc de s'interroger sur l'efficacité de cette forme de gouvernance, en démontrant les carences du fonctionnement des chaînes de blocs publiques dites chaînes décentralisées ou sans autorisation. Cette conception critiquable, du point de vue technique, soulève également quelques observations juridiques. Dans le premier cas de figure, il faudrait démontrer, d'une part, que la gouvernance par le code est loin d'être parfaite. Certains mécanismes de consensus, utilisés par les membres de la chaîne dans le cadre du déroulement de l'activité de l'infrastructure, peuvent avoir un impact négatif sur l'environnement. Cela peut être constaté avec la preuve de travail, premier mécanisme de consensus exploité par les chaînes décentralisées, qui requiert une grande consommation d'énergie. Le caractère contraignant de l'exécution automatique des contrats intelligents démontre également qu'il est impossible d'arrêter le processus sans l'intervention d'un humain. Par conséquent, le contrôle des situations imprévisibles échappe au code, et ce, d'autant plus que l'action de la collectivité est limitée à l'infrastructure. D'autre part, les mesures d'incitation exposent l'infrastructure à des risques de comportements opportunistes. Ces agissements peuvent être à l'origine des fourches ou d'un phénomène de concentration des pouvoirs (économique et décisionnel) entre les mains d'un cercle restreint. Avec un tel fonctionnement, la gouvernance décentralisée ne saurait répondre aux besoins des communautés. Dans le second cas de figure, la réintroduction des tiers de confiance dans le fonctionnement de l'infrastructure est proposée pour une pérennisation de cette technologie innovante. Pour ce faire, de nouveaux modèles de chaînes de blocs sont adoptés; il s'agit des chaînes de blocs avec autorisation, c'est-à-dire les chaînes privées ou de consortium. Les chaînes de blocs privées fonctionnent sur des réseaux privés dont l'accès requiert une autorisation. Cette autorisation résulte soit de la présélection des participants, soit de la conformité aux règles d'accès fixées par les validateurs (Finney, 2018, p. 715), tandis que les chaînes de blocs de consortium sont des infrastructures hybrides accessibles avec autorisation. Dans ce type de chaîne, l'accès est généralement réservé à un groupe d'individus ou d'entreprises qui ont pour but la réalisation d'un projet commun sous la supervision d'une entité centrale (Bouchard, 2022, p. 22). Il est évident que la conception actuelle dominée par la gouvernance algorithmique écarte tout raisonnement juridique. Dans ce contexte, le juriste perdrait son rôle dans la normativité du droit. Or, il est essentiel que le droit accompagne la gouvernance algorithmique et la régulation technique. Avec les chaînes nécessitant une autorisation, les professionnels du droit deviendront des tiers de confiance qui participent à l'encadrement du fonctionnement de l'infrastructure.

[5] Dans cette perspective, notre analyse se présentera sous deux volets. La première partie consistera à démontrer que, dans leur conception actuelle, les chaînes publiques sont soumises à une gouvernance multiforme qui reste imparfaite (1). La gouvernance décentralisée ne favorise pas un essor fulgurant de la technologie de la chaîne de blocs. La deuxième partie portera sur la nécessité de mettre en place un modèle de gouvernance perpétuelle (2). Dans cette section, un nouveau modèle de gouvernance reposant sur deux idées sera exposé. La première idée est que l'intervention humaine est nécessaire pour la pérennisation de cette technologie, d'où le recours aux chaînes

de blocs privées ou de consortium. La seconde idée mettra en exergue le rôle essentiel des professionnels du droit dans le fonctionnement de cette technologie. Il sera question de leur réintroduction comme tiers de confiance; une réintroduction qui permettrait une gestion efficace et sécuritaire de l'infrastructure.

1. LES CHAÎNES DE BLOCS PUBLIQUES, DES REGISTRES SOUMIS À UNE GOUVERNANCE MULTIFORME MAIS IMPARFAITE

[6] Les chaînes de blocs publiques se présentent sous forme de registres partagés. Leur fonctionnement repose à la fois sur le code et la communauté qui joue un rôle important dans l'exécution du code. En d'autres termes, ces registres décentralisés sont soumis à une gouvernance hybride, voire multiforme, fondée essentiellement sur des algorithmes. Cette forme de gouvernance n'est pas nouvelle; elle marque tout simplement une évolution de la *gouvernance par les nombres* (Supiot, 2015 et 2020). La gouvernance décentralisée reprend ainsi l'idée d'une société où les algorithmes remplacent la loi. Dans les chaînes décentralisées, le code est la source de normativité qui détermine le fonctionnement de l'infrastructure. Au regard de la conception actuelle de ces chaînes, il peut être avancé que la gouvernance est basée essentiellement sur la confiance à la technologie; or celle-ci comporte des failles. Il convient d'analyser les lacunes qui peuvent être décelées dans le mode de gouvernance adopté par les chaînes publiques (1.1), avant de voir les risques qui peuvent affecter ces chaînes au cours de leur fonctionnement (1.2).

1.1 LES LACUNES DE LA CONCEPTION ACTUELLE DE LA GOUVERNANCE DES CHAÎNES DE BLOCS PUBLIQUES

[7] La gouvernance des chaînes décentralisées est très complexe; elle doit impérativement suivre les règles préétablies par le code. Celle-ci implique également un certain nombre d'acteurs dont le rôle est incontournable dans le fonctionnement des registres décentralisés. Les lacunes pouvant paralyser le fonctionnement des chaînes décentralisées se présentent à deux niveaux : elles sont constatables, d'une part, dans la gouvernance par le code (1.1.1). D'autre part, elles se matérialisent par l'action limitée des parties prenantes qui sont toutes appelées à intervenir exclusivement à l'interne, voire uniquement dans la gouvernance de l'infrastructure (1.1.2).

1.1.1 LES DÉFAILLANCES CONCERNANT LA GOUVERNANCE PAR LE CODE

[8] Bien qu'elle semble efficace, l'organisation par le code des activités menées par la communauté implique des insuffisances. Ces carences découlent des protocoles de consensus généralement choisis pour le fonctionnement des chaînes de blocs publiques (1.1.1.1) et des contrats intelligents chargés de l'exécution automatique de certaines tâches prédéterminées (1.1.1.2).

1.1.1.1 AU NIVEAU DES PROTOCOLES DE CONSENSUS

[9] Les protocoles de consensus dits algorithmes de consensus constituent l'élément fondamental qui garantit le fonctionnement des chaînes de blocs. Ces protocoles renvoient à un ensemble de règles dont les nœuds se servent pour déterminer si une

transaction est valide (Alzahrani, Bulusu, 2018, p. 465-485). Par consensus, il faut donc attendre le processus par lequel tous les membres du réseau s'accordent sur une valeur ou une transaction. De nouveaux blocs ne peuvent être validés par les mineurs que s'ils sont conformes au protocole de consensus sur lequel repose la gestion de la chaîne de blocs. Le fonctionnement dudit protocole consiste, d'une part, à analyser les propositions de nouveaux de blocs et, d'autre part, à prendre des décisions. Il existe plusieurs algorithmes de consensus. Dans cette présente section, les carences des deux protocoles les plus adoptés par les chaînes décentralisées, à savoir la preuve de travail et la preuve d'enjeu, seront mises en exergue.

[10] Le caractère énergivore de la preuve de travail. La preuve de travail, un protocole basé sur la preuve (Oyinloye, Teh, Jamil & Alawida, 2021, p. 1363), est la première méthode de consensus utilisée par les réseaux Bitcoin et Ethereum pour valider les transactions de cryptomonnaies. Le travail requis relève d'un calcul complexe dont la résolution nécessite beaucoup de temps et d'énergie[7]. Ce mécanisme s'appuie sur une puissance de calcul qui nécessite le recours à du matériel sophistiqué, c'est-à-dire d'ordinateurs quantiques suffisamment puissants pour faire du minage (Harri & Dupasquier, 2018, p. 426). Ce protocole serait à l'origine d'innombrables dommages climatiques, ce qui est néfaste pour l'environnement. L'importante consommation d'énergie qu'il requiert a conduit les régulateurs américains à interdire et à considérer la preuve de travail comme un mécanisme trop énergivore. En témoigne le rapport de la maison blanche relatif à l'impact environnemental des cryptomonnaies; ce rapport préconise le Congrès américain à prendre une loi qui interdit les mécanismes de minage jugés très énergivores[8] . C'est dans ce sens que des universitaires soucieux de l'environnement ont également reproché à la chaîne Bitcoin d'être extrêmement énergivore en considération de l'efficacité énergétique dont a besoin chaque nœud participant (Bogart, 2021, p.10296). Le caractère énergivore de ce protocole a des répercussions sur le plan économique. La preuve de travail s'avère également inopérante (Chaserant, Duchez & Harnay, 2021, p. 46) en ce qu'elle met en compétition plusieurs individus ou groupes de personnes dont un seul arrivera finalement à trouver le puzzle mathématique (Sénéchal, 2020, p.60-61). Pourtant, l'activité de minage requiert des investissements colossaux du fait du matériel et de l'électricité utilisés. Générer une preuve de travail est, en outre, un processus aléatoire; il nécessite plusieurs essais avant de trouver le hachage valide qui correspond à la puissance de calcul (Dimitropoulos, 2020, p. 1128). Le hachage est un moyen de sceller des données sous une forme mathématique, à un sens unique par le biais de la cryptographie (Van der linden, 2017, p. 57).

[11] Les failles de sécurité dans la preuve d'enjeu. À la recherche d'une méthode de consensus moins énergivore et peu couteuse, les développeurs ont trouvé comme alternative la preuve d'enjeu, un protocole établi selon un système de vote (Oyinloye, Teh, Jamil & Alawida, 2021, p. 6) Ce sont pour ces raisons principales que le réseau Ethereum, la deuxième plus grande plateforme de cryptomonnaies, a effectué sa

7 Samuel MASSEPORT, *Consensus blockchain : incitation des utilisateurs d'un réseau à la participation et à la loyauté*, Thèse, Université Montpellier, France. NNT2021MONTS058, p. 29. HAL. Id: tel-03583009, en ligne : <https://theses.hal.science/tel-03583009>.

8 OFFICE OF SCIENCE AND TECHNOLOGY POLICY, Climate and Implications of Crypto assets in the United States, The White House Washington, September 2022, en ligne : <https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Crypto-Assets-and-Climate-Report.pdf> (consulté le 14 mars 2023).

transition de la preuve de travail à la preuve d'enjeu au cours de l'année 2022[9]. Dans le protocole dénommé preuve d'enjeu ou de participation, le fonctionnement ne dépend pas de la résolution d'un puzzle. La preuve de participation nécessite plutôt un investissement des utilisateurs qui permet de témoigner de leur intérêt pour le bon fonctionnement de la chaîne de blocs. Plus la taille de la mise de l'utilisateur est grande, plus il augmente ses chances de gagner (Kaliat, 2020, p. 390). Les plateformes décentralisées comme Tezos et Dash reposent, depuis leur conception, sur la preuve de participation. Cette participation se fait par le biais de jetons détenus par chaque utilisateur. Les individus ayant plus de réserve ont plus de chance d'être sélectionnés pour participer à la validation des nouveaux blocs ajoutés à la chaîne. Tandis que pour la preuve de travail, la récompense résulte de la participation au mécanisme de consensus. La désignation des validateurs repose sur un modèle qui s'apparente au système capitaliste. C'est la richesse qui permet de déterminer les chances de participation (Knight, 2019, p. 531). Ce système favorise les grands détenteurs de jetons au détriment des petits investisseurs; il est aux antipodes de l'idéologie derrière la technologie de la chaîne de blocs, celle-ci se veut être un registre au service de la communauté. Compte tenu de son fonctionnement, ce système est confronté à des problèmes de sécurité. Les chaînes de blocs qui l'utilisent sont plus vulnérables aux attaques; le capitalisme est privilégié au détriment de la gouvernance démocratique. Le système peut ainsi être fragilisé à tout moment.

[12] Il ressort de cette présente section qu'aucun des protocoles de consensus utilisés pour le fonctionnement des chaînes de blocs publiques n'est parfait. La preuve de travail tout comme la preuve d'enjeu présentent des inconvénients. La confiance, la sécurité et la réduction des coûts prônées par les adeptes de cette technologie sont loin d'être atteintes. Au-delà des protocoles de consensus, les carences peuvent être constatées à travers les contrats intelligents.

1.1.1.2 AU NIVEAU DES CONTRATS INTELLIGENTS

[13] Dans un premier article publié en 1996, l'informaticien Nick Szabo définit l'expression « contrats intelligents » comme « un ensemble de promesses spécifiées sous formes numériques, y compris les protocoles dans lesquels les parties exécutent ses promesses[10] ». Pour Jerry Hsiao, les contrats intelligents sont des programmes informatiques capables d'exécuter automatiquement les termes d'un contrat sans intervention humaine (Hsiao, 2017, p. 686).

[14] L'idée d'une nouvelle catégorie de contrats numériques ne saurait donc être avancée. À ce propos, Jérémy Torres-Ceyte, dans le cadre de la conférence « Smart contracts : renouveau pour l'exécution des contrats ? », a affirmé que les contrats intelligents ne sont aucunement des contrats au sens juridique du terme. En effet, aux termes des dispositions de l'article 1378 du *Code civil du Québec* (ci-après le « C.c.Q. »)[11] : « le contrat est un accord de volonté, par lequel un ou plusieurs

9 « The Merge » ou la fusion a été exécutée le 15 septembre 2022. Cette transition a permis à la chaîne de blocs Ethereum de réduire une consommation d'énergie d'environs 99,95 %, en ligne : <https://ethereum.org/en/upgrades/merge/> (consulté le 28 mars 2023).

10 Nick SZABO, « Smart Contrats : Building Blocks for Digital Market », 1996, en ligne : <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html>. (consulté le 17 mars 2023).

11 Code civil dui Québec, L.Q. 1991, C.64.

personnes s'obligent envers une ou plusieurs autres à exécuter une prestation ». Or, les contrats intelligents sont plutôt des programmes informatiques, voire des logiciels qui exécutent des règles prédéfinies dès lors que les conditions fixées ont été remplies. Ces logiciels renvoient à des instruments chargés d'exécuter les engagements pris par les participants à la chaîne de blocs, et ce, sans possibilité de retourner à l'état ultérieur ou de mettre fin à son fonctionnement. Les contrats intelligents, à l'instar des chaînes de blocs, sont nés de l'idéologie libertaire. Ces protocoles informatiques fonctionnent de manière automatique dans une collectivité où les prétendues relations ne sont régies par aucun régulateur, tandis que le contrat au sens juridique est un accord de volonté générateur d'obligations régies par les lois étatiques.

[15] D'un point de vue juridique, les contrats intelligents jouent un rôle instrumental qui pourrait servir le droit des contrats. Ce sont des outils capables d'automatiser l'exécution d'un contrat légal. Contrairement aux contrats légaux, rédigés en langage humain, qui créent des obligations exécutoires, les contrats intelligents sont des automates, basés sur le langage informatique, qui se limitent à exécuter les obligations (Luesley, 2019, p. 156). Ces programmes informatiques pourraient être, à l'avenir, un instrument complémentaire du droit des contrats afin d'assurer l'efficacité des contrats légaux. Comme alliés du droit des contrats, ces logiciels assureront aux participants de la chaîne de blocs l'exécution des transactions et les protègeront également des dommages liés à l'inexécution du contrat. Chaque partie conservera ses fonds tant que les règles prévues dans le code ne sont pas exécutées.

[16] Pris de manière individuelle sur une chaîne de blocs, les contrats intelligents peuvent servir à plusieurs usages : faire du commerce, transférer des valeurs (jetons fongibles et non fongibles), ou encore extérioriser son consentement dans le cadre d'un accord juridique.

[17] Malgré tous les avantages qu'ils présentent, les contrats intelligents ne peuvent remplacer les contrats classiques prévus par le droit des contrats[12]. Comme l'a souligné Mustapha Mekki, les contrats intelligents ne prennent pas en compte les aléas et suscitent à cet effet de nouvelles questions juridiques (Mekki, 2017, p. 2160). Ces problématiques méritent d'être approfondies au regard du droit civil québécois.

[18] Le caractère irrémédiable de l'erreur dans le code. Rappelons que le contrat intelligent s'exécute de manière automatique sans l'intervention d'un tiers. Une fois que le programme est mis en exécution, il devient impossible d'arrêter le processus ou de l'annuler. Certes, dans le contexte d'une erreur commune si les parties s'en aperçoivent avant l'exécution, il serait possible d'annuler le contrat. L'exécution du contrat intelligent ne pourrait être déclenchée sans que l'une des parties y procède. Qu'en serait-il maintenant si l'exécution a déjà eu lieu ?

[19] Aux termes de l'article 1699 C.c.Q.[13] :

12 C.c.Q., *op.cit.*, note 11, art. 1379-1384.

13 C.c.Q., *op.cit.*, note 11.

> La restitution des prestations a lieu chaque fois qu'une personne est, en vertu de la loi, tenue de rendre à un 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.

[20] Au regard de cette disposition, tous les fonds constitués de cryptomonnaies devraient être restitués s'il y a eu un transfert à la suite d'une erreur. Les cryptomonnaies sont des biens fongibles déterminés et déterminables par leur nombre et interchangeables dans une transaction. Cependant, il demeure impossible, conformément au droit des contrats, d'opérer une rescision en raison du fonctionnement du code. L'erreur dans le code est, en principe, irrémédiable. Dans l'exemple de la DAO du réseau Ethereum, les pirates avaient transféré le tiers des fonds vers un compte subsidiaire qui échappait au contrôle des membres fondateurs de la DAO. Après examen de la situation, les membres de la communauté ont dû recourir à l'intervention humaine pour récupérer les fonds (Daniels, 2018, p. 429).

[21] L'inefficacité des contrats intelligents en cas de situations imprévues. Les contrats intelligents ne sont pas en mesure de régir les situations imprévues[14]. Ces programmes informatiques ignorent les faits découlant du monde extérieur; ils pourraient devenir inopérants dans ce contexte. Ceci permet de démontrer le caractère rudimentaire des contrats intelligents. Juridiquement, il est pourtant possible de résoudre ces problèmes dans deux cas de figure :

- premièrement, au regard de l'article1470 C.c.Q., les parties peuvent prévoir des clauses contractuelles qui pourraient les exonérer de leurs obligations lorsqu'un évènement imprévisible et irrésistible survient. Pour être appliquées dans le cas des contrats intelligents, ces clauses dites de force majeure doivent figurer au préalable dans le contrat préexistant. À défaut, les parties resteront dans une situation figée si un évènement indépendant paralyse l'exécution du contrat intelligent;

- deuxièmement, les parties peuvent prévoir des clauses de renégociation en cas d'imprévision bien que la notion d'imprévision ne figure pas dans le livre cinquième du *Code civil du Québec* intitulé « des obligations » (Bédard, 1997). Ce type de clauses permet aux parties d'adapter le contrat aux nouvelles circonstances qui pourraient bouleverser l'équilibre contractuel[15] .

[22] Sous forme groupée, les contrats intelligents permettent la création d'une nouvelle catégorie d'organisation communément appelée « organisation autonome décentralisée » et connue sous l'acronyme de DAO. Ces organisations sontentièrement intégrées dans des contrats intelligents qui, une fois déployés, fonctionnent selon la programmation (Allen, 2020, p. 53). Les relations entre les membres de la communauté

14 Dans notre analyse, deux situations seront mises en évidence : le cas de force majeure et l'imprévision.

15 Mustapha MEKKI, « Blockchain : l'exemple des smarts contracts. Entre innovation et précaution », en ligne : <https://lesconferences.openum.ca/files/sites/97/2018/05/Smart-contracts.pdf> (consulté le 21 mai 2023).

sont régies par le code. Aux termes de la *Loi type sur les organisations autonomes décentralisées* (DAO) rédigée par le groupe de travail international *Coalition of Automated Legal Applications* (COALA) :

[23] Une DAO renvoie aux contrats intelligents déployés sur une chaîne de blocs publique, voire sans autorisation, qui mettent en œuvre des règles spécifiques de prise de décision ou de gouvernance permettant à plusieurs acteurs de coopérer de manière décentralisée. Ces règles de gouvernance doivent être techniquement, mais pas nécessairement, d'un point de vue opérationnel, décentralisées[16].

[24] Timothy Nielsen les définit comme « une organisation basée sur un code informatique dans lequel la gouvernance est automatisée grâce à des contrats intelligents qui fonctionnent sur un réseau immuable et décentralisé » (Nielsen, 2019, p. 1105).

[25] Dans cette présente étude, ces deux définitions qui nous paraissent complémentaires seront retenues. Les DAO sont des entités numériques déployées par des contrats intelligents de façon automatique. Ce travail s'effectue sur la chaîne de blocs qui, par essence, est immuable et décentralisée; mais au cours de son fonctionnement des mises à jour peuvent être effectuées sur le plan technique. Dans ces entités, la confiance humaine est remplacée par la confiance au code. Pour Aaron Wright, l'objectif des initiateurs est de faire évoluer la coordination sociale en passant des entités bureaucratiques vers les entités algorithmiques (Wright, 2021, p. 3).

[26] Cette conception semble irréaliste. En cas de dysfonctionnement du code, la survie de l'entité et de ses membres demeure problématique; cela constitue une véritable insécurité pour la pérennisation d'une telle entité. Même si les membres d'une DAO collaborent sur un réseau pair-à-pair, leur activité peut s'étendre au monde extérieur. Celle-ci pourrait impliquer plusieurs ordres juridiques selon la situation géographique des membres de la DAO. Par conséquent, ces entités numériques ne pourraient échapper aux règles étatiques qui régissent la société[17]. La *Loi type sur les DAO* intervient dans ce contexte pour définir le cadre juridique applicable à ces entités autonomes décentralisées. L'objectif est de favoriser leur continuité et d'offrir une certaine sécurité juridique aux acteurs de cette collectivité[18].

[27] Il peut être ainsi avancé que les contrats intelligents ne sont pas des contrats au sens juridique du terme; par conséquent, ils ne peuvent se substituer au contrat. Le caractère contraignant de l'exécution automatique de ces programmes informatiques constitue un avantage mais également un inconvénient. Ces insuffisances montrent que, contrairement à l'idéologie véhiculée par les adeptes de la chaîne de blocs,

16 La loi type sur les DAO intitulée *Model Law for Decentralized Autonomous Organizations (DAOs* est rédigée par le groupe de travail *Coalition of Automated Legal Applications* (COALA) avec la contribution de Constance CHOI, Primavera DE FILIPPI, Rick DUDLEY, Silke Noa ELRIFAI, Fatemeh FANNIZADEH, Florence GUILLAUME, Andrea LEITER, Morshed MANNAN, Greg MCMULLEN, Sven RIVA, Ori SHIMONY, COALA 2021, en ligne : <https://www.lextechinstitute.ch/loi-type-sur-les-daos-un-regime-juridique-adapte-aux-nouvelles-formes-de-societes-numeriques/>.

17 Florence GUILLAUME, Sven RIVA, « DAO, code et loi : le régime technologique et juridique de la Decentralized Autonomous Organization », (2021) 4-4 *Revue de droit international d'Assas (RDIA),* p. 217, en ligne : <https://ssrn.com/abstract=4013798>.

18 Voir la loi type sur les DAO, *op.cit.*, note 16.

l'immixtion de l'être humain dans le fonctionnement du code reste le plus grand défi de cette technologie.

1.1.2 L'ACTION LIMITÉE DE LA COMMUNAUTÉ DANS DES CHAÎNES DE BLOCS PUBLIQUES

[28] Malgré que la chaîne de blocs soit un registre décentralisé qui fonctionne sur un réseau pair-à-pair, la gouvernance de cette technologie ne repose pas uniquement sur le code. Au-delà des algorithmes, il existe une communauté qui peut avoir un impact conséquent sur le fonctionnement de l'infrastructure. Dans les systèmes décentralisés, la gouvernance peut impliquer plusieurs parties prenantes. Les individus appelés à intervenir dans la gouvernance peuvent être classés en deux catégories. Certains d'entre eux interviennent directement au niveau de l'infrastructure, tandis que d'autres agissent à travers les applications décentralisées, il s'agit en général d'individus chargés d'intervenir sur la couche applicative qui peut être illustrée par les DAO (De Fillipi & Mcmullen, 2018, p. 36). L'ensemble des acteurs interviennent au sein des chaînes décentralisées; leur action est limitée. Autrement dit, parmi les membres de la communauté intrinsèque à la chaîne de blocs, aucun acteur n'effectue un rôle d'interface entre le monde virtuel et le monde physique. En cas de dysfonctionnement faisant échec à la gouvernance par le code, ces acteurs ne pourront créer une interconnexion entre les chaînes sans autorisation et le monde réel.

[29] Pour s'en convaincre, il faudrait examiner le rôle des acteurs agissant au sein de l'infrastructure ainsi que la manière dont les acteurs au service des DAO interviennent au niveau de la couche applicative.

[30] Le rôle des acteurs au service de l'infrastructure. Trois types d'acteurs interviennent directement dans la gouvernance de l'infrastructure : les développeurs, les mineurs et les utilisateurs. Ces intervenants peuvent influencer directement les opérations prévues par le code.

[31] Considérés comme des gestionnaires du réseau principal de la technologie, les développeurs constituent une collectivité dont le travail consiste à élaborer les règles techniques nécessaires à la création et au développement des projets de logiciels de chaîne de blocs (De Fillipi & Mcmullen, 2018, p.34). Leur rôle consiste ainsi à fournir aux nœuds la version officielle du logiciel. Les développeurs participent aux propositions d'amélioration du protocole de la chaîne de blocs ainsi qu'à leur approbation. Sur Bitcoin, les développeurs ont créé un mécanisme connu sous le nom de BIP qui permet de faire des propositions d'amélioration du protocole (Werbach, 2018, p. 548). Tout membre peut proposer des idées pour l'amélioration dudit protocole, mais ces propositions sont souvent de l'initiative des développeurs; ceux-ci envoient leurs idées à la communauté (Lacity, 2020, p. 372). L'adoption des propositions dépend de la communauté (Werbach, 2018, p. 548). Les membres de ce groupe peuvent soit les accepter après avoir trouvé un consensus, soit les reporter s'ils estiment que les changements ne sont pas conformes aux règles de l'infrastructure. Un système similaire dénommé « EIP » est également utilisé par la communauté d'Ethereum pour décrire les normes de la plateforme et améliorer la gouvernance du protocole (Haque, Silva-Herzog, Plummer& Rosario, 2019, p. 166).

[32] À ce stade, les mineurs jouent un rôle important dans la gestion et l'amélioration du réseau par le biais d'un système de vote. Ce système permet de déterminer si les propositions acceptées seront adoptées ou non. Les propositions acceptées ne peuvent être finalisées que si les mineurs les soutiennent à 95 % (Del Wright, 2019, p. 484). L'approbation des mineurs permet de renforcer l'immuabilité du protocole. Cela garantit qu'aucune personne ne puisse modifier le protocole, et ce, dès lors que les opérateurs de nœuds valident le passage à la nouvelle version incluant les propositions acceptées. Les mineurs évaluent ainsi la pertinence des propositions et sont récompensés par les utilisateurs pour leur participation à la sécurité et à la stabilité du réseau.

[33] Dans les systèmes de vote gérés par les mineurs, les utilisateurs sont considérés comme des électeurs (Del Wright, 2019, p. 488). En tant qu'acteurs, les utilisateurs ont la faculté d'accepter ou de rejeter les propositions, ce qui leur donne une liberté d'entrée et de sortie du réseau. Dans tous les cas, leur décision peut exercer une influence déterminante sur la pérennité et le succès des règles adoptées en vue du fonctionnement de la chaîne de blocs.

[34] La fonction des acteurs au service des organisations autonomes décentralisées. À l'instar des participants à l'infrastructure, les acteurs des applications décentralisées telles que les DAO sont également impliqués dans la gouvernance par le code. Ces personnes doivent détenir des jetons. Jonathan Rohr et Aaron Wright ont établi une classification de ces jetons. Pour ces auteurs, les « tokens », dénommés en français jetons, peuvent être divisés en deux catégories, à savoir les jetons d'utilité et les jetons d'investissement (Rohr & Wright, 2019, p. 475-476). Les jetons d'utilité confèrent à leurs titulaires le droit d'accéder et de profiter des produits ou services proposés par l'organisation; ils permettent également de reconnaître auxdits titulaires des droits de gouvernance tels que le droit de voter.

[35] Pour Primavera De Fillipi, les jetons d'utilité pourraient être scindés en deux catégories, soit les jetons applicatifs et les jetons participatifs (De Fillipi, 2020, p. 66). Selon le nombre de jetons applicatifs détenus, des membres peuvent avoir le droit d'accéder ou non aux produits proposés par l'organisation sans pour autant détenir le droit de vote. Les jetons participatifs ou jetons de gouvernance confèrent à leurs détenteurs le droit de participer aux décisions de gouvernance proposées à l'organisation. L'acquisition des jetons de gouvernance résulte soit d'un achat, soit d'un programme de fidélisation consistant à récompenser certains acteurs pour leur utilisation des services de la DAO (Bersani, 2022, p. 1317). Ce type de programme a pour objet d'exhorter les membres de la DAO à participer au fonctionnement de l'application décentralisée. À l'instar des membres d'un conseil d'administration d'une société[19], les titulaires des jetons participatifs sont appelés à donner leur avis et à participer à la gestion des activités de l'organisation.

[36] Par opposition aux jetons d'utilité, les jetons d'investissement donnent à un participant au service de l'organisation un droit économique relatif aux bénéfices générés par les projets d'investissement de la DAO (Bersani, 2022, p.1316). Ce sont des actifs numériques dont la valeur est évaluée au prorata de la part d'investissement

19 Loi canadienne sur les sociétés par actions, L.R.C. (1985), c. C-44, art. 102; Loi sur les sociétés par actions, RLRQ, c.S-31.1, art. 112.

initial. Les jetons d'investissement sont, aujourd'hui, considérés par les investisseurs comme le nouveau mécanisme de financement des organisations autonomes décentralisées à travers les ICO (première émission de jetons ou *Initial Coin Offering*) (Bouchard & Godbout, 2020, p. 85-114). Cette catégorie de jetons est qualifiée de titre par les autorités au Canada lorsque les critères inhérents à la qualification du contrat d'investissement sont constatés[20]. Au Québec, les jetons d'investissement pourraient ainsi être assujettis à la *Loi sur les valeurs mobilières*[21]. Les Autorités canadiennes en valeurs mobilières (ACVM) considèrent que la plupart d'émissions de cryptomonnaies constituent des titres au regard du mécanisme[22].

[37] Par l'émission de jetons, les acteurs peuvent financer leur projet, coordonner leurs activités et encourager l'ensemble des membres à participer à la gouvernance de l'organisation autonome décentralisée. Ce modèle de gouvernance a été adopté par « The DAO », une organisation autonome décentralisée créée par Ethereum. Cette organisation virtuelle de la chaîne de blocs Ethereum fonctionnait sur la base de contrats intelligents chargés d'automatiser et d'appliquer les règles de gouvernance (Minn, 2019, p. 149). En échange de l'Ether[23] des investisseurs, la DAO distribuait des jetons à ses membres. Les jetons conféraient à leurs détenteurs à la fois des droits d'accès aux services de la technologie, des droits de participation au vote, et enfin des droits aux bénéfices générés par les investissements de la DAO (Minn, 2019, p. 149). Les prises de décision au sein d'une DAO reposent donc sur un système de gouvernance où la richesse est l'élément déterminant du pouvoir. Plus le nombre de jetons détenus est élevé, plus l'influence sur les activités de la DAO est grande.

[38] À la suite de notre analyse concernant le rôle des acteurs au service des chaînes décentralisées, il nous paraît judicieux de reconnaître que les chaînes de blocs publiques reposent sur une gouvernance algorithmique au sein de laquelle l'humain a peu d'emprise. Les défaillances constatées, tant dans le fonctionnement du code que dans l'action limitée de l'ensemble des acteurs, démontrent les limites des chaînes de blocs publiques. Force est de constater que la volonté de remplacer l'humain par le code demeure un véritable enjeu pour les chaînes de blocs décentralisées. Les problèmes de sécurité technologique, le rôle normatif voué aux contrats intelligents ainsi que le détachement de la communauté des *réalités* du monde physique réduisent les chances de succès de la technologie de la chaîne de blocs. L'intervention humaine devient alors indiscutable pour encadrer la technologie. Certes, le droit semble être en retard face à l'innovation technologique, mais ce ralentissement est qualifié de retard méthodique (Lehaire 2022, p. 233). La finalité est de prévoir des mécanismes susceptibles de remédier non seulement les insuffisances actuelles de la technologie, mais également les risques pouvant paralyser, à l'avenir, son fonctionnement.

20 *Autorité des marchés financiers* c. *Longpré* 2021 QCTMF 62. Dans cette affaire rendue le 18 novembre 2021, le tribunal administratif énumère les critères inhérents à la qualification du contrat d'investissement en précisant que chacune des caractéristiques du contrat devrait être analysée à la lumière des preuves présentées. Cinq éléments ont été retenus : 1) l'engagement de l'investisseur; 2) l'espoir de bénéfice; 3) la participation au risque d'une affaire par la voie d'un apport ou d'un prêt; 4-5) l'absence d'expertise ou la non-participation aux prises de décisions concernant l'investissement.

21 Loi sur les valeurs mobilières, RLRQ, c.V-1.1.

22 AUTORITÉS CANADIENNES EN VALEURS MOBILIÉRES, *Les émissions de cryptomonnaie*, Avis 46-307du personnel des ACVM 24 août 2017, en ligne : < https://www.autorites-valeurs-mobilieres.ca/uploadedFiles/Industry_Resources/2017aout24-46-307-avis-acvm-fr.pdf >, (consulté le 21 février 2023).

23 L'Ether est la cryptomonnaie de la chaîne de blocs Ethereum.

1.2 LES RISQUES PESANT SUR LE FONCTIONNEMENT DES CHAÎNES DE BLOC PUBLIQUES

[39] Les risques susceptibles d'affecter la gouvernance décentralisée doivent être analysés à la lumière des aspirations des fondateurs de la chaîne de blocs, c'est-à-dire l'idéologie qui sous-entend cette technologie. Les chaînes de blocs publiques sont, par essence, caractérisées par la décentralisation, la transparence et l'immuabilité. Contrairement aux idées véhiculées par les fondateurs, une étude empirique permettra de démontrer que l'immuabilité de la technologie peut être remise en cause par les « bifurcations » dites fourches. Ces fourches peuvent se produire lors d'une modification du protocole ou d'une mise à jour des règles de fonctionnement des chaînes (1.2.1). À la suite de cela, notre analyse sera accentuée sur d'autres risques de comportements opportunistes qui favorisent l'évolution du registre vers la centralisation, ce qui marque un phénomène de concentration du pouvoir (1.2.2).

1.2.1 LES FOURCHES, UNE REMISE EN CAUSE DE L'IMMUABILITÉ DU REGISTRE

[40] À l'image de toute technologie émergente[24], les chaînes de blocs ne semblent pas encore matures, ce qui les expose à de multiples risques. Ces risques peuvent être constatés dans le cadre de la gouvernance. La modification du protocole ainsi que la mise à jour des règles de fonctionnement des chaînes de blocs posent souvent des divergences au sein de la communauté. Ces désaccords traduisent les limites du code par des fourches qui peuvent résulter soit d'une modification substantielle des règles de gouvernance dénommée en anglais « hard fork », soit d'une modification non substantielle desdites règles appelée en anglais « soft work ».

[41] Un « hard fork » est un changement majeur qui permet de modifier les règles de gouvernance prévues dans le code et le fonctionnement de la chaîne de blocs de sorte que toute nouvelle opération devra être validée conformément aux nouvelles règles. Le protocole modifié réécrit les informations de validation contenues dans l'infrastructure (Daniels, 2018 p. 406). Le « hard fork » produira à cet effet une chaîne continue qui intègre la nouvelle règle, mais une deuxième branche de cette chaîne peut également continuer à fonctionner. Tel est le cas si certains opérateurs de nœuds décident de se conformer aux anciennes règles du logiciel.

[42] Les « soft work » créent, en revanche, une mise à niveau de protocole rétrocompatible (Kaal 2020, p. 16). Les nouvelles règles respectent les anciennes prescriptions; les blocs produits après la mise à jour du logiciel sont également valides, selon les règles du précédent protocole.

[43] Que cela soit pour remédier à des problèmes techniques ou une mise à jour, les fourches dites « hard fork » engendrent souvent des problèmes de gouvernance, des pertes économiques et surtout une division de la communauté.

---

24 Aux termes de *l'Office québécois de la langue française*, les technologies émergentes sont des technologies qui se trouvent au stade de la recherche et des premières applications expérimentales et qui sont susceptibles de modifier les conditions de concurrence dans une activité donnée, en ligne : https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/26500743/technologie-emergente (consulté le 17 mars 2023).

[44] La scission de la communauté pourrait être à l'origine de l'existence de deux chaînes concurrentes. La remarque a été faite avec les « hard forks », les plus importants, survenus dans les protocoles respectifs du Bitcoin et d'Ethereum. C'est ainsi qu'à la suite d'une proposition de modification du protocole acceptée par certains acteurs et refusée par d'autres, portant sur l'augmentation des tailles de blocs, le Bitcoin a connu une révolution. Cette mutation a entraîné l'existence de deux versions différentes du code. Ces fourches ont été à l'origine de la création de cryptomonnaies apparentées, mais différentes telles que le *Bitcoin Cash* et le *Bitcoin Gold* (Chanson, 2018 p. 139). De manière similaire, Ethereum a connu une scission ayant donné naissance à deux plateformes (Ethereum et Ethereum classique) en raison de l'échec du projet DAO (Daniels, 2018, p. 429).

[45] Au regard des caractéristiques de la chaîne de blocs, ces fourches violent le principe qu'est l'immuabilité et même la transparence. Le caractère immuable de l'infrastructure renvoie à l'idée selon laquelle les informations inscrites sur la chaîne de blocs ne peuvent être supprimées, modifiées ou falsifiées. En principe, nul ne peut, de sa seule volonté, procéder à des modifications sur la chaîne de blocs sans qu'elles ne soient décelées par les autres membres de la communauté. Pourtant, les « hard fork » constituent un changement majeur des règles qui régissent le fonctionnement de la chaîne. Les crises ayant frappé l'organisation autonome décentralisée « The DAO » d'Ethereum et le Bitcoin ont montré que la gouvernance par le code ne permettait pas de résoudre les situations imprévues. Par ailleurs, les limites des règles techniques démontrent que la communauté exerce une influence considérable sur les décisions de mise à jour ou de modification du protocole. Selon leur décision, la gouvernance de la chaîne pourrait devenir plus efficace ou infructueuse. Or, tous les acteurs opérant dans les chaînes sans autorisation se trouvent au sein de l'infrastructure. Les fourches peuvent entraîner aussi une concurrence entre l'ancienne chaîne et la nouvelle chaîne. Cela pourrait conduire à la dépréciation de la valeur de la cryptomonnaie initiale, et ce, à cause des autres cryptomonnaies générées par la nouvelle chaîne. À partir de là, des pertes économiques peuvent en résulter; la réorganisation du fonctionnement de la chaîne de blocs s'imposerait alors (Kaal, 2020, p.17). Les « bifurcations » exposent également la chaîne de blocs à un risque de troubles sociaux. La mésentente des membres de la communauté engendrerait une perte d'une partie des acteurs qui participent à la gouvernance. Tous les mineurs n'accepteront pas évidemment de passer à la nouvelle version du protocole; certains vont vouloir conserver les blocs qu'ils ont déjà validés.

[46] D'un point de vue juridique, les crises survenues dans les réseaux Bitcoin et Ethereum appellent à deux observations à la lumière des législations canadienne et québécoise :

[47] Les implications de l'absence de mécanismes de coordination et de contrôle à la lumière du droit des sociétés. S'agissant de Bitcoin, la fourche survenue en 2017 était due à l'augmentation de la taille des blocs. L'objectif était d'accroître la capacité transactionnelle de la chaîne. Les troubles sociaux ont exposé les problèmes de coordination existant entre les acteurs chargés de la gestion du réseau. Pourtant, les chaînes décentralisées se présentent sous la forme d'un bien commun qui, par essence, n'est pas appropriable.

[48] À la différence des associés d'une société qui sont liés par des intérêts communs, les parties prenantes d'une chaîne de blocs peuvent avoir des finalités différentes. En droit des sociétés[25], le modèle de la gouvernance est conçu sous une forme hiérarchique. L'organisation et la gestion de la société sont confiées à un individu ou groupe d'individus désignés à cet effet; ceux-ci ont pour rôle de défendre les intérêts de la société. Selon la forme sociale choisie par les associés ou actionnaires, il peut s'agir d'un conseil d'administration[26] ou d'un ou de plusieurs gérants (Bouchard, 2021, p. 528). Dans les réseaux décentralisés, par exemple sur Bitcoin, si les développeurs initiaux sont motivés par des raisons philosophiques s'inspirant du mouvement *Cypherpunk,* la participation des mineurs à la gouvernance est, en revanche, déterminée par les incitations économiques (Del Wright, 2019, p. 484-485). Quant aux nœuds, leur rôle consiste à assurer la fiabilité de la chaîne. Plus le niveau de décentralisation est élevé, plus il sera difficile de compromettre la sécurité de la chaîne de blocs (Del Wright, 2019, p. 484-485). Chaque partie prenante peut accepter ou refuser les nouvelles règles de fonctionnement du protocole selon ses propres intérêts. Cette situation augmente les risques de fourches. À l'opposé du droit des sociétés, aucun mécanisme de contrôle n'est prévu dans l'univers des chaînes de blocs publiques. Se voulant démocratique, la gouvernance des chaînes décentralisées devrait nécessairement impliquer des mesures concernant les problèmes de coordination. En l'absence d'organes habilités à cet effet, il deviendrait difficile de dénouer l'impasse en cas de fourches.

[49] Les incertitudes concernant la réparation du dommage au regard du droit de la responsabilité civile. En vertu des dispositions de l'article 1474 C.c.Q. :

> Une personne ne peut exclure ou limiter sa responsabilité pour le préjudice matériel causé à autrui par une faute intentionnelle ou une faute lourde; la faute lourde est celle qui dénote une insouciance, une imprudence ou une négligence grossières.

[50] Dans l'hypothèse où les fourches sont intentionnelles, chose fréquente dans les chaînes de blocs publiques, l'application de cet article devrait être possible. Mais les fourches soulèvent, dans la pratique, de multiples questions quant à la détermination de la responsabilité. Dans les chaînes décentralisées, les transactions s'exécutent de manière autonome; il pourrait être difficile d'identifier une personne responsable du dommage causé à un ou plusieurs membres de la communauté. Mais cela ne s'avère pas impossible, si l'on distingue les chaînes qui fonctionnent sous le pseudonymat et celles reposant sur l'anonymat. Pour la première catégorie qui caractérise la plupart des chaînes de blocs décentralisées (Bitcoin, Ethereum), l'identification de la personne responsable est possible. Leur fonctionnement s'appuie sur des signatures numériques et la cryptographie asymétrique. Le chiffrement permet à une personne d'effectuer une transaction sans que son identité ne puisse être déterminée (Narayanan, Bonneau, Fellten, Miller, Goldfeder, 2016). Toutefois, il existe des experts en analyse de transactions qui peuvent, grâce à des techniques informatiques détectant les fluctuations monétaires, identifier les personnes qui font des transactions sur une

25 Voir, la Loi canadienne sur les sociétés par actions, L.R.C. (1985), c. C-44, art. 102 ; la Loi sur les sociétés par actions, RLRQ, c.S-31.1, art. 112.

26 Dans les sociétés en nom collectif, les associés ont le choix de nommer un associé ou de désigner un tiers comme gérant pour administrer les affaires de la société. C.c.Q., *op.cit.,* note 11, art. 2213, al.1.

plateforme[27]. Ces spécialistes pourront identifier les personnes responsables, si l'on fait appel à leur service.

[51] Pour la seconde catégorie qui se présente comme plus rare (Monéro, Dash), il serait difficile, voire complexe, de retracer les transactions.

[52] Il convient de relever que les cas de fourches illustrés exposent les risques qui peuvent paralyser le fonctionnement des chaînes décentralisées. Ces incidents montrent que l'intervention humaine provenant du monde réel est incontournable dans certaines circonstances. Chaque fois qu'il faudra mettre à jour le protocole ou résoudre des situations imprévues, des personnes agissant hors de l'infrastructure devront intervenir certainement.

1.2.2 LA TENDANCE VERS UN PHÉNOMÈNE DE CENTRALISATION DES POUVOIRS

[53] Le modèle de gouvernance adopté par les chaînes de blocs publiques repose sur des systèmes de récompenses financières. Ces récompenses sont instaurées pour exhorter la communauté à participer au fonctionnement de l'infrastructure. Contrairement à l'objectif initial qui est de favoriser une gouvernance décentralisée efficace, ces récompenses amènent les parties prenantes à adopter des comportements opportunistes. Cela se matérialise par un phénomène de concentration du pouvoir économique qui place le pouvoir décisionnel entre les mains de quelques acteurs de la collectivité.

[54] Cette pratique a déjà été relevée dans le modèle de gouvernance des institutions rationnelles. À ce propos, Kaal précise que toutes les fois où des actifs fongibles ont été considérés comme modèle d'incitation, des participants ont tenté de corrompre le système (Kaal, 2020 p. 14). Le modèle de la gouvernance des chaînes décentralisées reproduit les mêmes effets délétères qui affectent l'efficacité de la technologie en question. Ces comportements opportunistes, qui sont en déphasage avec l'idéologie soutenue par Satoshi Nakamoto[28], conduisent ainsi à une centralisation des pouvoirs. Cela est perceptible tant dans les chaînes de blocs utilisant la preuve de travail (l'exemple des groupes de mineurs), que dans celles fonctionnant sur la base de la preuve d'enjeu (le cas des détenteurs de jetons).

[55] La centralisation des pouvoirs par la constitution de groupes de mineurs. Les coûts considérables qu'implique l'activité de minage sont aujourd'hui à l'origine d'un phénomène de concentration des mineurs, et ce, dans des zones bien déterminées. La forte dépense en électricité, la complexité de la résolution de la puissance de calcul ainsi que la stricte réglementation de ladite activité[29] sont autant de facteurs qui justifient la création des groupes de mineurs, dénommés pools miniers. Ce genre de collaboration leur permet d'avoir la possibilité de valider la majorité ou la moitié des

27 Par exemple, il est possible de consulter sur la chaîne de blocs d'Ethereum l'ensemble des informations relatives aux transactions telles que les envois, les messages en attente, les blocs, les adresses publiques sur <https://etherscan.io>.

28 Satoshi Nakamoto est l'initiateur de la chaîne de blocs de Bitcoin, la plus célèbre des chaînes de blocs publiques qui a permis de développer la cryptomonnaie *bitcoin*. En ce sens, Satoshi NAKAMATO, « Bitcoin : A Peer-To-Peer Electronic Cash System », 2008, en ligne : <https://bitcoin.org/bitcoin.pdf>.

29 À ce propos voire la partie sur « Le caractère énergivore de la preuve de travail ».

blocs de transactions et, par conséquent, de bénéficier d'un grand nombre de récompenses (Hermstruwer, 2020, p. 459). Les récompenses gagnées sont réparties au prorata de leur puissance de calcul entre les membres du pool (Andhov, 2020, p. 13). Ces alliances formées par les mineurs pour augmenter les récompenses de blocs constituent un frein à la décentralisation, le *mythe* véhiculé par Satoshi Nakamoto. L'organisation des mineurs sous forme de groupe a pour principale conséquence la centralisation du pouvoir économique qui a des répercussions sur le pouvoir décisionnel. La gouvernance du réseau est contrôlée, d'une part, par un nombre restreint de personnes qui se partagent le pouvoir décisionnel. Autrement dit, la décision de valider ou non des blocs de transactions dépendra de quelques groupes de mineurs. D'autre part, ces groupes de mineurs auront plus de chance de résoudre le puzzle mathématique sur un temps record et de faire croître davantage leur pouvoir économique. Cette tendance de centralisation du pouvoir n'est pas seulement perceptible dans l'activité de minage, elle est également présente dans les modèles d'organisations impliquant l'usage de la preuve d'enjeu.

[56] La détention de pouvoirs, un monopole de la majorité des détenteurs de jetons. Dans les chaînes de blocs ayant recours à la preuve d'enjeu, la participation à la gouvernance requiert la détention d'un nombre assez conséquent de jetons participatifs. Cela est également constatable dans les organisations autonomes décentralisées. Par exemple, au sein de la DAO du réseau d'Ethereum, le système de vote reposait sur la quantité de jetons détenus. Il convient de souligner qu'un nombre important de jetons entre les mains d'un seul ou de quelques participants pourraient impacter sur le système de vote qui est pourtant réputé être décentralisé et transparent (Tse, 2020, p. 355). Ces individus pourront, selon leur bon vouloir, changer les règles de gouvernance ou du protocole. La concentration du pouvoir décisionnel entre les mains de quelques détenteurs de jetons entraînerait une centralisation de la gouvernance. Dans ce contexte, le pouvoir décisionnel est directement lié à la puissance économique des acteurs.

[57] Somme toute, tant dans les chaînes de blocs publiques utilisant la preuve de travail que dans celles ayant recours à la preuve d'enjeu, la gouvernance s'appuie sur des systèmes de récompenses financières. Ces récompenses pourraient être à l'origine de comportements opportunistes qui empêcheront le bon fonctionnement des chaînes décentralisées.

[58] Il ressort de cela que le fonctionnement des chaînes de blocs sans autorisation semble, dans la pratique, contraire à l'esprit d'origine qui gouverne la technologie de la chaîne de blocs. Les lacunes constatées dans la conception de la gouvernance des chaînes décentralisées ainsi que les risques pouvant affecter leur bon fonctionnement démontrent que le modèle de gouvernance adopté par ces chaînes est imparfait. Reconsidérer le modèle de gouvernance devient alors un impératif pour assurer la pérennisation de la technologie de la chaîne de blocs.

2. DE LA NÉCESSITÉ D'UNE GOUVERNANCE EFFICACE POUR UNE PÉRENNISATION DE LA TECHNOLOGIE DE LA CHAÎNE DE BLOCS

[59] L'objectif des libertariens est de remplacer les systèmes inopérants, dont la gestion et le contrôle sont centralisés entre les mains de quelques individus, par les chaînes décentralisées. Selon les libertariens, ces nouveaux modèles d'organisations basés sur le code permettraient de faciliter les interactions humaines. Pour ce faire, toute volonté tendant à contrôler l'infrastructure devrait être éradiquée. Les chaînes de blocs publiques sont à cet effet caractérisées par la décentralisation, la transparence et l'immuabilité. La plus grande innovation réside ainsi dans le fait que les chaînes de blocs publiques fonctionnent sur un réseau pair-pair, c'est-à-dire de manière désintermédiée. Mais la *réalité* semble montrer que le recours à un tiers de confiance est, dans certaines circonstances, indéniable. Malgré que la gouvernance algorithmique présente un certain nombre d'avantages en matière de célérité et d'automatisation, il va sans dire que la technologie n'est pas exempte de vice. Au-delà des failles techniques, les situations juridiques exposées ci-dessus ont démontré que l'intervention d'un tiers de confiance est nécessaire. L'idée d'une désintermédiation totale dans les chaînes de blocs publiques se présente dès lors comme une illusion (2.1). La technologie ne peut pas produire les mêmes effets que le droit. La réintroduction des professionnels du droit dans le maillon de la chaîne demeure alors obligatoire pour assurer les fonctions régulatrices du droit (2.2).

2.1 LA DÉSINTERMÉDIATION TOTALE, UNE ILLUSION TROP IDÉALISTE

[60] L'Office québécoise de la langue française définit la technologie de la chaîne de blocs comme « une base de données distribuée et sécurisée, dans laquelle sont stockées chronologiquement sous forme de blocs liés les uns aux autres, les transactions successives effectuées par les utilisateurs depuis sa création[30] » Il ne s'agit pas d'une base de données, mais de plusieurs bases de données. Les chaînes de blocs pourraient être très utiles à la société en cette ère de nouvelle économie, mais la vulnérabilité du modèle décentralisé réduit les chances de succès de cette technologie.

[61] Dans le rapport intitulé « La technologie des chaînes de blocs : les cryptomonnaies et bien plus encore » du Comité permanent de l'industrie et de la technologie, Me Charlaine Bouchard a révélé que la technologie de la chaîne de blocs peut être utilisée de façon inappropriée[31]. La spécialiste de la chaîne de blocs et des contrats intelligents confirme l'idée selon laquelle l'intervention humaine est nécessaire pour contourner les faiblesses des chaînes de blocs publiques. Pour une pérennisation de cette technologie, un nouveau mode de gouvernance a été proposé, un mode qui s'applique aux chaînes de blocs avec autorisation.

30 Voir la définition de l'Office québécois de la langue française, en ligne : <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/26531717/chaine-de-blocs> (consulté le 10 août).

31 CHAMBRE DES COMMUNES DU CANADA, *La technologie des chaînes de blocs : les cryptomonnaies et bien plus encore*, Rapport du Comité permanent de l'industrie et de la technologie, 44e législature, 1ère session, juin 2023, p. 32-33, en ligne : <https://www.ourcommons.ca/DocumentViewer/fr/44-1/INDU/rapport-15/> (consulté le 19 juin 2023).

[62] Les chaînes de blocs avec autorisation. Cette catégorie renvoie aux chaînes de blocs privées et de consortium. Dans les chaînes de blocs privées ou centralisées, l'accès à la plateforme est réglementé; il résulte de l'autorisation d'une autorité ou d'une entité centrale. Sa mission consiste à approuver l'accès des utilisateurs au réseau et à veiller au respect des règles de fonctionnement fixées préalablement. Au sein des chaînes de blocs de consortium, l'accès est réservé à un nombre de participants limité (Mekki, 2017, p. 2160) qui, généralement, appartiennent à une organisation ou entité. Dans ce type de chaînes, les modalités d'accès au contenu diffèrent selon que l'on est utilisateurs ou validateurs. Les premiers auront un accès limité au service offert par l'entité tandis que les validateurs disposeront d'un accès total sur l'ensemble du contenu.

[63] Atouts des chaînes de blocs avec autorisation. Les chaînes de blocs privées ou de consortium semblent plus avantageuses que les chaînes de blocs publiques. Dans un premier temps, la présélection des participants permet d'identifier les acteurs qui utilisent le réseau. En cas de préjudice causé à autrui, il serait facile de déterminer la responsabilité de l'individu fautif et de prévoir en conséquence la réparation du dommage. Dans un second temps, le concours de l'être humain dans le contrôle du fonctionnement des réseaux lui confère la possibilité de corriger les anomalies et de mettre à jour les protocoles à chaque fois que cela est nécessaire. Les réseaux privés fonctionnent souvent sur la base d'un protocole de consensus dit preuve d'autorité, une méthode jugée très efficace en raison des avantages qu'elle présente. Ce protocole offre une très grande célérité en ce qu'il permet de valider les transactions sans recourir à l'activité de minage; la vérification de l'identité des utilisateurs suffit largement pour valider les blocs (Dumas, Lafourcade, Tichit, Varette, 2022, p. 23). Dans le cadre de la preuve d'autorité, les validateurs sont choisis parmi les individus autorisés à participer au réseau, ceux-ci seront les seules personnes habilitées à déterminer le consensus (Dumas, Lafourcade & al, 2022, p. 23).

[64] Il peut être observé que les tiers de confiance restent toujours présents dans le fonctionnement des chaînes de blocs; la désintermédiation ne peut donc être absolue. Les chaînes de blocs avec autorisation permettent ainsi de réintégrer l'humain dans la gouvernance. À cela, il faut ajouter que la technologie de la chaîne de blocs est faite par les hommes et pour les hommes; elle ne peut être une innovation hors-la-loi. Les rapports sociaux sont régis par les règles de droit. Réintroduire les professionnels du droit dans l'écosystème des chaînes de blocs devient un impératif pour assurer non seulement la pérennisation de cette technologie, mais également son utilisation à bon escient.

2.2 POUR UNE RÉINTRODUCTION DES TIERS DE CONFIANCE INCONTOURNABLES DANS LE FONCTIONNEMENT DES CHAÎNES DE BLOCS : L'EXEMPLE DES PROFESSIONNELS DU DROIT

[67] Le fonctionnement des chaînes de blocs publiques englobe deux idées : d'une part, la gouvernance par le code qui résulte d'une programmation d'un ensemble de tâches que la machine doit accomplir selon les données qui y sont incorporées, d'autre part, la régulation technique qui sous-entend un ensemble de règles techniques contraignantes qui s'appliquent à la communauté (De Fillipi, 2017, p. 63et ss.).

L'organisation du fonctionnement des chaînes et l'automatisation des applications décentralisées en sont la preuve.

[68] Comme l'a souligné Primavera De Fillipi, la régulation technique pourrait être un instrument très utile pour le droit en ce qu'elle permet de réguler de manière courante l'environnement numérique, un espace en pleine mutation. Mais la régulation technique ne doit pas remplacer le droit. Pour Primavera, il est nécessaire de dissocier leurs différentes finalités; la technique a tendance à régir des faits dont la réalisation est prévisible, alors que le droit s'applique postérieurement (De Fillipi, 2017, p. 71 et 72).

[69] Jacques Chevallier, pour démontrer l'impact de la régulation juridique sur les systèmes, affirme que « tout système organisé, formé d'un ensemble d'éléments interdépendants et interagissant, serait en effet en permanence confronté aux facteurs de déséquilibre et d'instabilité provenant de son environnement; la régulation recouvre l'ensemble des processus par lesquels les systèmes cherchent à maintenir leur « état stationnaire », en annulant l'effet des perturbations extérieures » (Chevallier, 2001, p. 828). Pour Alain Supiot « en l'absence d'une instance hétéronome, les rapports sociaux seront totalement soumis à la logique binaire ami/ennemi » (Supiot, 2020, p. 409).

[70] Face aux limites de la technique, l'intervention du droit est indispensable dans certaines situations ignorées par la technologie. Cette intervention permettrait surtout d'éviter une dénaturation des règles juridiques qui sont, contrairement aux règles techniques, malléables (Moradinejad, 2020 p.131). Appréhender le rôle du juriste à l'ère de l'innovation technologique devient ainsi crucial pour situer leur place dans le fonctionnement de la technologie de la chaîne de blocs. Fort de ce constat, il faudrait tout simplement admettre la fonction sociale du droit; une fonction assurée par le juriste à l'ère numérique, comme l'a énoncé Benjamin Lehaire (Lehaire 2022, p. 137).

[71] Le rôle du juriste dans l'univers des chaînes de blocs. L'évolution du rôle du juriste est nécessaire pour appréhender les nouvelles situations techniques. Le passage du rôle contraignant consistant à imposer les règles à la fonction de garant du respect de la cohésion sociale est un des éléments essentiels sur lesquels les professionnels du droit devront travailler. À présent, la fonction du juriste serait de veiller à ce que les actes accomplis par la communauté des chaînes de blocs soient conformes aux règles prévues par la société. En tant que garant de la cohésion sociale, le professionnel du droit aura également l'opportunité d'agir auprès de la communauté. Son action consistera à apporter des solutions pour encadrer les défaillances techniques.

[72] Dans le cadre du fonctionnement des chaînes de blocs publiques, les adeptes de la gouvernance décentralisée ont mis en place ce que l'on appelle la gouvernance *Off-Chain* pour résoudre les problèmes techniques. Les règles *Off-Chain* renvoient aux décisions pouvant influencer la gouvernance *On-Chain*, c'est-à-dire les règles techniques automatisées et encodées sur la chaîne. Ces décisions peuvent se présenter sous forme de forces extérieures existant en dehors de l'infrastructure (De Fillipi & Mcmullen, 2018, p. 18); elles ont pour but de participer à l'amélioration et à l'adaptation des mécanismes *On-Chain*. Nous estimons que ces forces extérieures devraient inclure des entités ou individus ayant une expertise dans le domaine juridique.

Les personnes auxquelles ont fait référence seront dénommées « Oracles ». Les Oracles ont pour rôle d'enregistrer ou d'introduire des informations émanant du monde physique au monde numérique de la chaîne de blocs (Dimitropoulos, 2020, p. 1169). Dans les chaînes de blocs publiques, ces Oracles, qui sont des tiers, pourraient être des professionnels du droit. Leur rôle consistera à fournir et à vérifier les informations nécessaires au fonctionnement des contrats intelligents (Verheye, Verslype & Danneels, 2019, p. 72). Dans la pratique, ces professionnels du droit ont tendance à créer leur propre chaîne de blocs en adoptant des modèles de chaînes avec autorisation sous la direction de leur entité (Chaserant, Duchez & Harnay, 2021, p. 49). Identifier ces spécialistes du droit, par exemple les notaires et avocats, permettrait de mieux comprendre leur importance dans le fonctionnement de la chaîne de blocs de même que l'utilité de ladite technologie.

[73] Le notaire, garant de la sécurité et de la fiabilité des actes authentiques. À l'aune de la désintermédiation, une des caractéristiques principales des chaînes décentralisées, les libertariens avaient annoncé la fin du temps des notaires. L'idée selon laquelle la technologie de la chaîne de blocs offre les mêmes services que les notaires fait partie des arguments qui ont, pendant longtemps, nourrit le *mythe* derrière cette technologie. Pourtant, la *réalité* est tout autre. Cette technologie reste un instrument; elle ne pourrait se substituer au notaire (Chalati & Bouchard, 2020, p. 284).

[74] Aux termes de l'article 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 ». Pour plus de précisions, le législateur québécois prévoit à l'article 2819 C.c.Q. que : « l'acte notarié, pour être authentique, doit être signé par toutes les parties; il fait alors preuve, à l'égard de tous, de l'acte juridique qu'il renferme et des déclarations des parties qui s'y rapportent directement ».

[75] Suivant ces dispositions, il est clair que l'acte notarié n'est opposable à tous que si l'officier public y appose son cachet, et ce, après que les parties l'ont signé. Cet officier public n'est autre que le notaire. Le caractère authentique de l'acte ne peut résulter de la technologie de la chaîne de blocs. Comme l'a souligné Mustapha Mekki, cette technologie est un outil de conservation très utile (Mekki, 2017, p. 2160); elle permet d'enregistrer et de certifier les documents numériques. Mais seuls les actes établis par les notaires peuvent revêtir un caractère authentique; l'intervention du notaire est ainsi essentielle. Au regard des dispositions de l'article 440 C.c.Q., un contrat de mariage, par exemple, ne saurait être valable s'il a été fait et enregistré sur une chaîne de blocs sans la signature d'un notaire.

[76] Dans le cadre de l'immobilier virtuel[32], par exemple, les notaires pourraient bien s'établir en qualité d'oracles pour vérifier et authentifier les actes. Dans ce contexte, ces professionnels auront un rôle considérable à jouer dans le fonctionnement de la chaîne. Leur intervention permettrait d'assurer la véracité des informations fournies à l'infrastructure. À ce propos, des auteurs proposent que le notaire soit la personne par laquelle il faut passer pour avoir accès à la chaîne de blocs (Verheye, Verslype & Danneels, 2019, p. 56-57). Pour ce faire, la plupart des organismes chargés de

32 L'immobilier virtuel ou numérique peut être défini comme l'achat, la vente ou encore l'exploitation d'un bien immeuble, voire d'un terrain dans un monde virtuel.

réglementer la profession notariale ont décidé de s'approprier de cette technologie. Ces institutions privilégient le plus souvent les chaînes de blocs de consortium ou privées.

[77] Par exemple, la Chambre des notaires du Québec, en collaboration avec des chercheurs universitaires, a créé une institution de recherche pour promouvoir les contrats intelligents et la chaîne de blocs. Sous la houlette de Me Charlaine Bouchard, pionnière dans ce domaine au Québec, une chaîne de blocs notariale sera créée (Bouchard, 2022, p. 55); celle-ci aura pour but d'automatiser les contrats notariés[33] Cette infrastructure permettra d'alléger le travail des notaires. Une chaîne de blocs notariale présente beaucoup d'avantages en ce qu'elle garantit aux acteurs la sécurité, la traçabilité et l'immuabilité des actes notariés intégrés à la chaîne de blocs. Par ailleurs, l'infrastructure leur assure une certaine transparence et célérité dans la gestion desdits actes grâce à l'interaction des notaires. Au-delà de ces officiers public, garants des actes authentiques, la technologie de la chaîne de blocs pourrait être utile à d'autres professionnels du droit comme les avocats.

[78] L'avocat, le nouvel allié des investisseurs en cryptomonnaies. La démocratisation du secteur financier promise par les cryptomonnaies a créé un grand engouement auprès des investisseurs pour cette catégorie de cryptoactifs (Bouillet -Cordonnier, Gasser, Moulin & Quinou, 2021 p. 55). Les cryptomonnaies sont des actifs numériques utilisés dans les transactions qui s'effectuent sur des réseaux pair-à pair, c'est-à-dire de manière décentralisée sur la technologie des chaîne de blocs. Ce type d'investissement présente beaucoup de risques. À cet égard, tout individu désirant investir dans ces actifs numériques devrait se renseigner sur leur fonctionnement. À l'instar de la France (Thierry, 2022), l'avocat serait l'allié idéal des potentiels investisseurs en cryptomonnaies au Québec; en sa qualité de conseil juridique, il a une obligation d'information vis-à-vis des investisseurs. Ces informations peuvent porter sur le fonctionnement de la technologie de la chaîne de blocs et les plateformes de négociation de cryptoactifs enregistrées auprès des Autorités canadienne en valeurs mobilières (ACVM)[34]. Par ailleurs, son rôle consistera à les prévenir des risques de volatilité, de fraude et de liquidité. L'avocat devra également faire part à ses clients des règles mises en place par les ACVM pour encadrer l'usage de ces actifs[35].

CONCLUSION

[79] En définitive, le fonctionnement des chaînes de blocs publiques basé sur une désintermédiation totale n'est seulement qu'un *mythe*; il ne reflète aucunement la *réalité*. En l'état actuel, la gouvernance décentralisée des chaînes de blocs comporte beaucoup d'insuffisances (défaillance du code, détachement de la communauté du monde extérieur à la technologie, fourches, concentration des pouvoirs), mais, d'un

33 CHAMBRE DES COMMUNES DU CANADA, *La Technologie des chaînes de blocs : les cryptomonnaies et bien plus encore*, Rapport du Comité permanent de l'industrie et de la technologie, 44e législature, 1e session, juin 2023, p.17, en ligne : https://www.ourcommons.ca/DocumentViewer/fr/44-1/INDU/rapport-15/ (consulté le 19 juin 2023).

34 À propos des plateformes de négociation de cryptoactifs enregistrées auprès des Autorités canadiennes en valeurs mobilières, en ligne : <https://lautorite.qc.ca/grand-public/registres/plateformes-de-negociation-de-cryptoactifs> (consulté le 20 juillet 2023).

35 AUTORITÉS CANADIENNES EN VALEURS MOBILIÈRES, *Le Guide de l'investisseur : les cryptomonnaies,* Alberta Securites Commission, p. 12, en ligne : <https://www.autorites-valeurs-mobilieres.ca/investisseur/soyez-un-investisseur-avise/quest-ce-quune-cryptomonnaie> (consulté le 9 mars 2023).

point de vue juridique, celles-ci ne sont pas irrémédiables. Les nouveaux paradigmes impliquant la réintroduction des professionnels du droit comme tiers de confiance semblent efficaces. Les modèles de chaînes de blocs privées ou de consortium permettent de faire face aux failles de la technologie et aux risques de comportements opportunistes. La réintermédiation des spécialistes du droit dans la gouvernance demeure ainsi incontournable pour assurer la pérennisation de la technologie de la chaîne de blocs.

BIBLIOGRAPHIQUE SÉLECTIVE

Législations

Loi canadienne sur les sociétés par actions, L.R.C. (1985), c. C-44

Code civil du Québec, L.Q. 1991, C.64.

Loi sur les valeurs mobilières, RLRQ, c.V-1.1.

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

Monographies

BOUCHARD, C., *Droit et pratique de l'entreprise*, tome I, 4e éd., Entrepreneurs et sociétés de personnes, Éditions Yvon Blais, 2021.

BOUILLET-CORDONNIER, G., A. GASSER, J.-M. MOULIN, M. QUINOU, *La finance numérique : aspects juridiques et fiscaux du crowdfunding et des cryptoactifs*, EFE, 2021.

DE FILLIPI, P., *Blockchain et cryptomonnaies*, Presses universitaires de France, 2018.

DUMAS, J-G., P. LAFOURCADE, A. TICHIT, S. VARETTE, *Les blockchains en 50 questions : comprendre le fonctionnement et les enjeux de cette technologie*, Dunod, Hors collection, 2022.

LEHAIRE, B., *L'innovation-hors-la loi : les origines de la techno-normativité*, Bruylant, 2022.

LELOUP, L., *Blockhain : La deuxième révolution numérique*, édito Québec, mai 2017.

SUPIOT, A., *La gouvernance par les nombres*, cours au Collège de France (2012-2-14), Paris, Fayard, 2015 et 2020.

VERHEYE, B., K. VERSLYPE, P. DANNEELS, *Blockchain et contrats intelligents : quel impact sur le notaire en tant qu'intermédiaire de confiance?* Larcier 2019.

Ouvrages collectifs

BOUCHARD, C. (dir), Comment la chaîne de blocs va transformer le droit? Montréal, Éditions Yvon Blais, 2020.

Articles

ALLEN, J.G., « Bodies without Organs : Law, Economics, Decentralised Governance », (2020) 4(1) *Standford Journal of Blockchain Law & Policy*, p. 53-78.

ANDHOV, A., « Corporations on Blockchain: Opportunities & Challenges », (2020) 53(1) *Cornell International Law Journal*, p. 1-40.

BERSANI, K., « Separating governance tokens from securities: How the Utility Token May Fall Short of the Investment Contract », (2022) 43(3) *Cardozo Law Review*, p. 1305-1342.

BOGART, G., « Using blockchain to address the IPCC's Climate change mitigation strategies », (2021) 51(4) *Environmental Law Reporter*, p. 10296-10309.

DIMITROPOULOS, G., « The Law of Blockchain », (2020) 95 (3) *Washington Law Review*, p.1117-1192.

CHANSON, E.D., « How Bitcoin Functions as Property Law », (2018) 49(1) *Seton Hall Law Review*, p.129-172.

CHEVALLIER, J., « La régulation juridique en question », (2001) 49(3) *Droit et société*, p. 827-846.

DANIELS, A., « Blockchain & Shareholder Voting : A Hard Fork for 21st Century Corporate Governance », (2018) 21(2) *University of Pennsylvania Journal of Business Law*, p.405-441.

DE FILLIPI, P., M. MANNAN, W. REIJERS, « Blockchain as a Confidence Machine : The Problem of Trust & Challenges of Governance », (2020) 62 *Technology in Society*, 101284, en ligne : <https://doi.org/10.1016/j.techsoc.2020.101284>.

FINNEY, B. « Blockchain and Antitrust: New Tech Meets Old Regs. Transactions », (2018) 19 (2)*The Tennessee Journal of Business Law*. p.709-736

HAQUE, R.S., R.S. SILVA-HERZOG, B.A. PLUMMER et N.M. ROSARIO, « Blockchain Development and Fiduciary Duty », (2019) 2(2) *Standford Journal of Blockchain Law & Policy*, p. 139-187.

HARI, O. et U. DUPASQUIER, « Blockchain and Distributed Ledger Technology (DLT) : Academic Overview of the Technical and Legal Framework and Challenges for Lawyers », (2018) 5 *International Business Law Journal*, p. 423-448.

HERMSTRUWER, Y., « The Limits of Blockchain Democracy », (2020) 4(2) *New York University Journal of Law and Liberty*, p.402-492.

HSIAO, J., I-H., « Smart Contract on the Blockchain - Paradigm Shift for Contract Law ? » (2017) 14(10) *US-China Law Review*, p. 685-694.

KAAL, W.A., « Blockchain-Based Corporate Governance », (2020) 4(1) *Standford Journal of Blockchain Law & Policy*, p.3-28.

KALIAT, D., « Demystifying Blockchain and Cryptocurrencies », (2020) 3(6) *The Journal of Robotics, Artificial Intelligence & Law*, p. 377-396.

KNIGHT, E., « Blockchain Jenga : The Challenges of Blockchain Discovery and Admissibility under the Federal Rules », (2019) 48(2) *Hofstra Law Review*, p. 519-562.

LACITY, M., « Crypto and Blockchain Fundamental », (2020) 73(2) *Arkansas Law Review*, p. 363-396.

LUESLEY, A., « Unravelling Smart Contracts: Smart Contracts and the Law of Rescission in Canada », (2019) 19 *Asper Review of International Business and Trade Law,* p.155-174.

MEKKI, M., « Les mystères de la blockchain », *Recueil Dalloz*, 2017, p. 2160.

MINN, K.T., « Towards Enhanced Oversight of “Self-Governing” Decentralized Autonomous Organizations : Case Study of the DAO and its Shortcomings », (2019) 9(1) *Journal of Intellectual Property &Entertainment Law* (JIPEL), New York University, p.139-178.

NAKAMATO, S., « Bitcoin : A Peer-To-Peer Electronic Cash System », 2008, en ligne : <https://bitcoin.org/bitcoin.pdf>.

NIELSEN, T., « Cryptocorporations : A Proposal for Legitimizing Decentralized Autonomous Organizations », (2019) 5 *Utah Law Review*, p.1105-1130.

OYINLOYE, D.P., J. SEN TEH, N. JAMIL et M. ALAWIDA, « Blockchain Consensus : An Overview of Alternative Protocols », (2021) 13(8) *Symmetry Journal*, p. 1363.

ROHR, J. et A. WRIGHT, « Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets », (2019) 70(2) *Hastings Law Journal*, p. 463-524.

SKLAROFF, J.M., « Smart Contracts and the Cost Inflexibility », (2017) 166(1) *University of Pennsylvania Law Review*, p. 263-303.

SZABO, N., « Smart Contracts : Building Blocks for Digital Market », 1996, en ligne : <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/

LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html> (consulté le 17 mars 2023).

TSE, N., « Decentralised Autonomous Organisations and the Corporate Form », (2020) 51(2) *Victoria University of Wellington Law Review*, p. 313-356.

THIERRY, G., « Comment les avocats français investissent le droit des cryptoactifs », *Dalloz actualité*, 30 mai, 2022.

VAN DER LINDEN, T., « ODR and Blockchain », (2017) 4(18) *International Journal of Online Dispute Resolution*, p. 57-58.

WERBACH, K., « Trust, but Verify : Why the Blockchain Needs the Law », (2018) 33(2) *Berkeley Technology Law Journal*, p. 487-550.

WRIGHT, A., « The Rise of Decentralized Autonomous Organizations : Opportunities and Challenges », (2021) 4(2) *Standford Journal of Blockchain & Policy*, p.1-32.

WRIGHT, D. JR., « Quadratic Voting and Blockchain Governance », (2019) 88(2) *UMKC Law Review*, p. 475-496.

Chapitres d'ouvrages collectifs

ALZAHRANI, N. et N. BULUSU, « Towards True Decentralization : A Blockchain Consensus Protocol Based on Games Theory and Randomness », dans L. BUSHNELL, R. POOVENDRAN, T. BASAR, (eds), *Decision and Game Theory for Security*, GameSec. Lecture Notes in Computer Science, vol. 11199, Springer 2018, ISBN 78-3-030-01553-4.

BOUCHARD, C. et A.S. GODBOUT, « Les premières émissions de jetons en droit québécois », dans C. BOUCHARD, (dir.), *Comment la chaîne de blocs va transformer le droit ?*, Montréal, Éditions Yvon Blais, 2020 p. 85-114.

CHALATI, D. et C. BOUCHARD, « Le droit notarial », dans C. BOUCHARD, (dir), *Comment la chaîne de blocs va transformer le droit*, Éditions Yvon Blais, 2020, p.267-294.

DE FILLIPI, P., « Repenser le droit à l'ère numérique : entre régulation technique et la gouvernance algorithmique », dans P.-E. MOYSE et V. GAUTRAIS, (dir.), *Droit+Machine*, Éditions Thémis, 2017, p.53-95.

MORADINEJAD, R., « Le droit des contrats », dans C. BOUCHARD, (dir.), *Comment la chaîne de blocs va transformer le droit ?*, Montréal, Éditions Yvon Blais, 2020, p. 115-133

SÉNÉCHAL, J., « "Blockchains publiques" smart contracts organisations autonomes décentralisées et gouvernance », dans H. JACQUEMIN, A. COTIGA et Y. POULLET,

(dir.), *Les blockchains et les smart contracts à l'épreuve du droit*, Collection du CIRDS, Faculté de droit l'Unamur, Bruxelles, Édition Larcier, 2020. p. 51-96

Documents administratifs, Rapports, et autres

AUTORITÉS CANADIENNES EN VALEURS MOBILIÈRES, *Le Guide de l'investisseur : les cryptomonnaies*, Alberta Securites Commission, 2023, en ligne : <https://www.autorites-valeurs-mobilieres.ca/investisseur/soyez-un-investisseur-avise/quest-ce-quune-cryptomonnaie/>.

BOUCHARD.C., *Le virage numérique : le notaire du 21e siècle, un notaire numérique*, Rapport de la Chaire de recherche sur les contrats intelligents et la chaîne de blocs-chambre des notaires du Québec, mars 2022, en ligne : <https://www.chainedeblocs.chaire.ulaval.ca/rapports>.

CHAMBRE DES COMMUNES DU CANADA, *La technologie des chaînes de blocs : les cryptomonnaies et bien plus encore*, Rapport du Comité permanent de l'industrie et de la technologie, 44e législature, 1ère session, juin 2023, p.17, en ligne : <https://www.ourcommons.ca/DocumentViewer/fr/44-1/INDU/rapport-15/>.

DE FILLIPI, P., *La blockchain : entre régulation et gouvernance*, mémoire d'HDR soutenu le 18 septembre 2020, Université Paris-Panthéon-Assas.

DE FILLIPI., P. et G. MCMULLEN, *Goverance of Blockchain Systems : Governance of Land by Distributes Infrastructure*, Coalition of Automed Legal Applications (COALA), Blockchain Research Institute, June 2018.