



Institut
de gouvernance
numérique

Livre blanc

CFP - 011M

C.P. - PL 3

Loi sur les renseignements
de santé et de services sociaux



REGISTRES DISTRIBUÉS, L'ÉVOLUTION DE LA CHAÎNE DE BLOCS

Impacts, enjeux et potentiels pour le Québec

Novembre 2019

Comité directeur

Gouvernement et institutions

M^e Charline Bouchard, Université Laval
Lise-Estelle Brault, Autorité des marchés financiers
Christian Dejean, Hydro-Québec
Mylène Laroche, Autorité des marchés financiers
Rémi Quirion, Scientifique en chef
Marie-Hélène Savard, ministère de l'Économie et de l'Innovation
Dominique Tremblay, ministère de l'Économie et de l'Innovation
David Vincent, Hydro-Québec

Entreprises privées et regroupements

Mario Albert, La Capitale
Michel Besner, Catallaxy
Stéphane Bertrand, Bitfarm
M^e Jean-François DeRico, Langlois avocats
Sébastien Harvey, Québec Blockchain
Louis Lévesque, Finance Montréal
Patrick Moisan, Hub Saguenay-Lac-Saint-Jean
Florian Roule, Finance Montréal
Louis Roy, Raymond Chabot Grant Thornton

Équipe de réalisation

Coordinateur, **Jean-François Gauthier**, Institut de gouvernance numérique
Directeur de projet, **Carl Cloutier**, IGN
Rédacteur, **Patrice Servant**
Conseillers au contenu, **Mario Perron**, **Sébastien Harvey**, **Schallum Pierre**,
Yan Crevier, **Marc-Olivier Lebel** et **Guillaume Déziel**
Conseillère au contenu et chercheuse, **Camille Savard**
Graphiste, **Viva Design**

Mise à disposition



Les auteurs de ce livre blanc (ci-après «l'Œuvre») ont choisi collectivement de le rendre disponible au public sous une licence Creative Commons de type [CC] BY-SA.

Vous êtes donc autorisé à :

- **Partager** — copier, distribuer et communiquer l'Œuvre par tous moyens et sous tous formats.
- **Adapter** — remixer, transformer et créer à partir du matériel de l'Œuvre pour toute utilisation, y compris commerciale.

Selon les conditions disponibles à cette adresse : <https://creativecommons.org/licenses/by-sa/4.0/deed.fr>

Une initiative de :



Avec le soutien financier de :



PRÉAMBULE

Historiquement, les humains ont stocké des informations dans des lieux protégés. Évidemment, la forme de ces entrepôts a changé. Du bâtiment gardé au serveur géant hypersécurisé, l'approche n'en est pas moins demeurée la même; ce sont essentiellement des variations sur le thème du coffre-fort. La chaîne de blocs, soit le *blockchain*, vient bouleverser une pratique ancienne. Le concept né en 2008 est simple. Plutôt que de bâtir à grands frais des forteresses protégées contre les intrusions, on choisira de répliquer les renseignements sur une multitude de serveurs qui seront chacun cryptés. Lors des opérations ou transactions, l'information est validée sur chaque composante et ensuite insérée dans la chaîne par un algorithme de consensus. La chaîne de blocs représente une révolution en termes de stockage d'information, mais aussi en termes de sécurité des données, car la reconstitution de la chaîne par piratage et l'altération des informations de blocs existants à des fins malveillantes sont pratiquement impossibles. De plus, la chaîne de blocs est complètement transparente, son fonctionnement et ses limites étant connus par tous ses utilisateurs.

L'étanchéité de ce processus a constitué l'assise du Bitcoin et d'autres cryptomonnaies. Mais le concept émerge maintenant au grand jour avec une multitude d'applications. On parle alors de façon plus générale de « registres distribués » en référence à tout type de base de données ou de masses d'informations pouvant être ainsi décentralisées, que ce soit par des entreprises privées ou des organisations gouvernementales. Ces registres distribués peuvent fonctionner de façon autonome à l'aide de *contrats intelligents*, des programmes vérifiés publiquement qui sont exécutés de manière fiable par les serveurs qui maintiennent la chaîne de blocs.

À l'heure où les délits de vol de données sont un nouveau fléau à travers le monde, à la veille de l'arrivée de la connectivité 5G qui décuplera les données en circulation, au moment où s'amorce la révolution de l'intelligence artificielle, la technologie des registres distribués apparaît comme un élément incontournable. Elle devient un nouveau symbole de cette ère numérique qui fait des données une ressource, et de la sécurité des renseignements personnels, une condition de succès.

À travers le monde, les gouvernements se positionnent pour encadrer certaines applications de cette technologie, y recourir eux-mêmes, stimuler la recherche, constituer des écosystèmes entrepreneuriaux favorisant son essor et solutionner les défis qu'elle pose, notamment sur les plans technique, légal et fiscal ainsi qu'en matière d'utilisation d'énergie.

Au Québec, l'écosystème se développe. On compte des dizaines d'entreprises en démarrage. De plus grandes firmes s'y intéressent. La recherche universitaire s'anime. Des investisseurs sont à l'affût. L'objectif de ce livre blanc est de faire un tour d'horizon de ce phénomène transformateur afin de contribuer à la réflexion gouvernementale et de favoriser l'adoption de politiques publiques sur les chaînes de blocs adaptées à la réalité québécoise.

L'enjeu est éminemment stratégique. Le Québec se présente aujourd'hui comme un leader de la recherche en intelligence artificielle. Ce filon porteur s'appuie sur une maîtrise dans le domaine connexe des données massives : les données de masse ou le *big data*. En maîtrisant aussi la technologie des registres distribués, dont les chaînes de blocs, le Québec rassemblerait trois piliers de la nouvelle ère numérique et renforcerait son positionnement de pôle technologique.

Pr. Kaiwen Zhang

Département de génie logiciel
École de technologie supérieure

Mario Albert

Vice-président exécutif Assurance collective
La Capitale Groupe financier

TABLE DES MATIÈRES

COMITÉ DIRECTEUR	2	3. LES REGISTRES DISTRIBUÉS ET LES CHÂÎNES DE BLOCS AU CANADA ET AU QUÉBEC	25
ÉQUIPE DE RÉALISATION	2	3.1 Aperçu de l'écosystème canadien	25
PRÉAMBULE	4	Le gouvernement du Canada se positionne	26
LISTE DES FIGURES ET TABLEAUX	5	La Banque du Canada expérimente le concept	26
DÉFINITIONS	6	3.2 Québec et les registres distribués	27
INTRODUCTION	7	Portrait de l'écosystème québécois	27
1. TECHNOLOGIE	8	Organisations québécoises et leurs projets	29
1.1 Chaîne de blocs et registres distribués, qu'est-ce que c'est?	8	Catégories et joueurs clés	31
1.2 Comment ça marche?	9	Forces, faiblesses, menaces et opportunités de l'écosystème québécois	35
1.3 Quels sont les différents types de chaînes de blocs?	9	4. GOUVERNANCE – CHANTIERS STRATÉGIQUES	37
1.4 Qu'est-ce qui distingue les registres distribués des autres modes de stockage d'information?	10	4.1 Deux portes d'entrée principales à court terme	37
1.5 Quelle est l'importance du phénomène?	11	4.2 Des outils pour améliorer l'administration publique	37
1.6 Comment se positionnent les pays?	13	Applications gouvernementales	38
1.7 Chaîne de blocs, bitcoins et controverse	14	Applications organisationnelles	39
2. POTENTIEL ET APPLICATIONS	15	La nécessité d'une vision globale des données au sein de l'État québécois	39
2.1 Fonctions pouvant être accomplies par les registres distribués	15	CONCLUSION	40
2.2 Exemples d'applications potentielles	17	RECOMMANDATION	41
2.3 Démarche d'implantation de la technologie des registres distribués dans une organisation	19	BIBLIOGRAPHIE	42
2.4 Défis posés par les registres distribués	21	ANNEXE I : MESURES ET INITIATIVES À TRAVERS LE MONDE	45
Défis d'ordre technologique	21		
Défis d'ordre légal – Entrevue avec M ^e Charlaïne Bouchard	21		
Défis d'ordre opérationnel	23		
L'enjeu énergétique	24		

LISTE DES FIGURES ET TABLEAUX

FIGURE 1 – Schéma, registre centralisé, registre distribué	8
FIGURE 2 – Processus d’une transaction sur une chaîne de blocs	9
FIGURE 3 - Comparaison entre trois modes de stockage des données	11
FIGURE 4 – Revenus mondiaux tirés de la technologie des chaînes de blocs	12
FIGURE 5 – Dépenses mondiales en solutions de type chaînes de blocs	12
FIGURE 6 – Financement et investissement en démarrage de sociétés de type chaînes de blocs dans le monde	12
FIGURE 7 – Pays leaders dans la technologie des chaînes de blocs	12
FIGURE 8 – Stade d’adoption de la technologie des chaînes de blocs dans le monde	13
FIGURE 9 – Processus d’une transaction en bitcoins	14
FIGURE 10 – Tableau synthèse des fonctions types des registres distribués	16
FIGURE 11 – Perception perturbatrice des chaînes de blocs selon les secteurs d’activité	18
FIGURE 12 - Cas d’utilisation envisagés de la technologie des chaînes de blocs dans des organisations	18
FIGURE 13 – Faisabilité du recours à la technologie des chaînes de blocs par industrie	21
FIGURE 14 – Principaux obstacles à l’utilisation des chaînes de blocs	24
FIGURE 15 – L’écosystème canadien de la chaîne de blocs, répartition par province	25
FIGURE 16 – Représentation de l’écosystème québécois des registres distribués	29
FIGURE 17 – Tableau synthèse des forces et faiblesses de l’écosystème québécois	35
FIGURE 18 – Tableau synthèse des menaces et opportunités de l’écosystème québécois	36

DÉFINITIONS

Ces définitions sont tirées de l'Office québécois de la langue française et ont été élaborées avec la collaboration de l'Autorité des marchés financiers, de l'École de technologie supérieure ainsi que de l'Académie Bitcoin¹.

Bloc : Ensemble de données liées à des transactions, dont la validité doit être confirmée au moyen d'un mécanisme de validation pour qu'il puisse être intégré à une chaîne de blocs.

Chaîne de blocs : Base de données distribuée et sécurisée, dans laquelle sont stockées chronologiquement, sous forme de blocs liés les uns aux autres, les transactions successives effectuées entre ses utilisateurs depuis sa création.

Contrat intelligent : Programme dont le code est inscrit dans une chaîne de blocs et dans lequel est défini un ensemble d'instructions qui s'exécutent de manière automatique lorsque certaines conditions sont réunies.

Cryptomonnaie : Monnaie virtuelle utilisée pour des échanges de biens ou de services, de pair à pair, généralement de manière indépendante du système bancaire ou de toute politique monétaire, et dont l'émission et les transactions reposent sur la technologie des chaînes de blocs.

En-tête de bloc : Ensemble de métadonnées situé au début d'un bloc de données, qui fournit de l'information sur la nature de son contenu.

Jeton : Unité de valeur fondamentale d'une cryptomonnaie, généralement utilisée pour les paiements ou pour accéder aux services des applications décentralisées.

Mécanisme de validation : Mécanisme qui vise à assurer la validité des blocs ajoutés sur une chaîne de blocs ainsi que les transactions qu'ils contiennent.

Minage : Opération qui repose sur un mécanisme de validation et qui permet l'ajout de blocs à un réseau de cryptomonnaie, en échange d'une prime de minage.

Nœud : Appareil informatique relié au réseau qui héberge une chaîne de blocs, destiné à relayer les transactions effectuées et à maintenir une copie complète ou partielle du registre distribué sur lequel ces transactions sont enregistrées. Chaque nœud (ou appareil informatique) au réseau est défini au regard de ses fonctions particulières. Il existe ainsi différents types de nœuds.

Première émission de jetons (ICO) : Campagne de financement par laquelle un organisme vend une part des jetons de sa cryptomonnaie durant la phase de démarrage de son projet (*Initial coin offering*).

Preuve de travail : Mécanisme de validation de transactions qui repose sur la résolution d'un problème cryptographique complexe.

Prime de minage : Montant d'une cryptomonnaie remis à un mineur ou à un groupe de mineurs afin de le récompenser pour la création d'un nouveau bloc et d'encourager la participation au sein du réseau.

Registre distribué : Registre simultanément enregistré et synchronisé sur un réseau d'ordinateurs, qui évolue par l'addition de nouvelles informations préalablement validées par l'entière du réseau et destinées à ne jamais être modifiées ou supprimées.

¹ Office la langue française, *Vocabulaire de la cryptomonnaie*, 2018 [www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/vocabulaire-cryptomonnaie.aspx].

INTRODUCTION

Les registres distribués, dont la chaîne de blocs, ont toutes les caractéristiques de ces technologies qu'on dit « disruptives ». Comme les systèmes info nuagiques, l'impression 3D, l'Internet des objets, l'intelligence artificielle ou la réalité virtuelle, les registres distribués viennent bouleverser un ordre établi en faisant surgir des possibilités nouvelles et des défis nouveaux avec un impact transversal. Dans le cas des registres distribués, c'est tout l'enjeu de l'archivage, de la sécurité, de la confidentialité, de *l'auditabilité* et du flux des données qui est repensé. À brève échéance, les registres distribués pourraient devenir l'ossature technologique des transactions numériques à l'échelle mondiale avec un champ d'application illimité s'étendant de l'entreprise aux services publics au vote électronique. Devant ce phénomène transformateur et incontournable, plusieurs gouvernements du monde cherchent à se positionner, tandis que d'autres (Estonie, Chine, États-Unis, Suisse, Australie) sont déjà passés de la réflexion à l'action avec des politiques sur l'encadrement et le développement des registres distribués.

Ce livre blanc se veut un premier pas afin d'aider le Québec à se positionner. Il a ainsi pour objectifs :

- de présenter cette technologie de manière simple;
- d'aider à la compréhension du potentiel transformateur et parfois perturbateur des outils qui en découlent;
- de cerner certains enjeux plus spécifiques au Québec en regard du développement et de l'utilisation des registres distribués;
- de décrire les forces et les faiblesses de l'écosystème québécois en la matière;
- de définir des pistes d'action adaptées à la réalité québécoise pour le développement de cet écosystème.

L'élaboration de ce livre blanc a été pilotée par l'Institut de gouvernance numérique, un organisme à but non lucratif qui a pour raison d'être d'accompagner les institutions publiques et privées dans leur transition vers une gouvernance plus ouverte avec, entre autres, les nouveaux outils numériques.

Les travaux ont été menés par un comité directeur composé d'universitaires, d'entrepreneurs, d'avocats et d'administrateurs publics. L'Autorité des marchés financiers, Québec Blockchain, Catalaxy (une filiale de Raymond Chabot Grant Thornton), Bitfarms, l'Université Laval, l'École de technologie supérieure ainsi que La Capitale ont aussi contribué à l'exercice. L'information contenue dans ce livre blanc est le fruit d'entrevues réalisées avec des experts, des entrepreneurs, des chercheurs et une revue de documentation constituée d'études, de sondages et de documents d'institutions tant publiques que gouvernementales, du Canada comme de l'étranger.

Le Scientifique en chef du Québec, Hydro-Québec, le ministère de l'Économie et de l'Innovation du Québec, le ministère des Finances du Québec, Finance Montréal et le Hub Saguenay-Lac-Saint-Jean ont rendu possible la préparation de ce livre blanc par leurs contributions financières respectives.

1. TECHNOLOGIE

1.1 Chaîne de blocs et registres distribués, qu'est-ce que c'est?

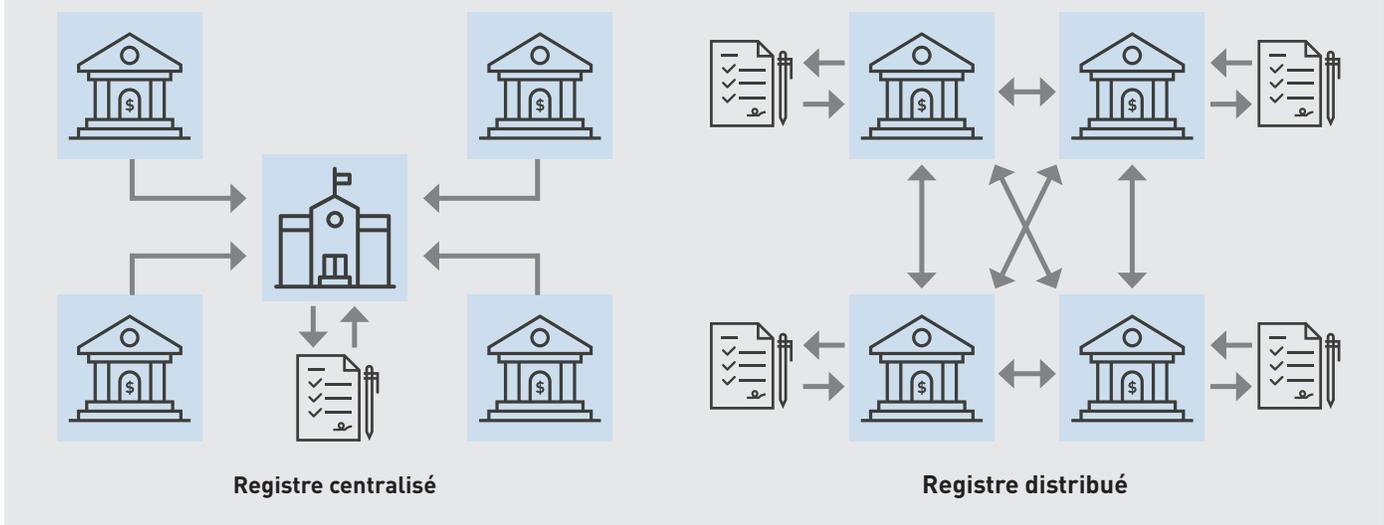
La chaîne de blocs, selon l'OQLF, est une base de données distribuée et sécurisée, dans laquelle sont stockées chronologiquement, sous forme de blocs liés les uns aux autres qui contiennent des transactions successives effectuées entre ses utilisateurs depuis sa création.

Le registre distribué est une évolution à usage plus général du concept des chaînes de blocs du système original de Bitcoin (2008-2009). Il s'agit, toujours selon l'OQLF, d'un registre simultanément enregistré et synchronisé sur un réseau d'ordinateurs, qui évolue par l'addition de nouvelles informations préalablement validées par l'entière du réseau et destinées à ne jamais être modifiées ou supprimées. Un registre distribué pourrait servir à archiver de manière sécurisée des cadastres, des transactions bancaires, des dossiers patients, des identités numériques, etc.

La chaîne de blocs est le type le plus connu de registre distribué. Un registre distribué se compare à un livre de compte dans lequel sont consignées les informations sur l'historique d'une transaction. C'est donc à la base une technologie de stockage et de sécurisation des données. Le registre distribué, comme son nom le dit, est une masse d'informations distribuées sur plusieurs ordinateurs.

Le changement conceptuel est fondamental. De tout temps, nous avons évolué avec des registres centralisés : toute l'information est stockée sur un serveur sécurisé qui fournit cette information à des clients et qui contient l'historique des transactions ou opérations. Dans un registre distribué, l'information est décentralisée et les transactions sont inscrites partout à la fois. Le schéma suivant illustre le concept.

Figure 1 - Schéma, registre centralisé, registre distribué



1.2 Comment ça marche?

Les registres distribués fonctionnent à peu près tous sur le même principe. Ici, nous allons détailler le fonctionnement de la chaîne de blocs en prenant l'application la plus connue, soit le concept. Dans une chaîne de blocs, chaque « **bloc** » est une petite unité d'information d'au plus un mégaoctet. Chaque bloc enregistre l'heure et les informations relatives à plusieurs transactions (environ 1 500 par bloc pour la version originale de Bitcoin). Une information stockée dans un bloc génère un identifiant en son pied-de-page. Cet identifiant sera par la suite recopié dans l'en-tête du prochain bloc. L'enchaînement des pieds-de-page et des en-têtes cryptographiés contribue à rendre le registre immuable.

Chaque serveur comportant des blocs est appelé un **nœud complet**. Et chaque nœud complet contient la totalité de la base de données, si bien que même si un nœud était compromis, l'information subsisterait sur tous les autres. (Dans certains types de registres distribués, l'information peut être scindée sur plus d'un nœud.) Toute cette information décentralisée forme ainsi un réseau. Ce réseau est dit « **pair-à-pair** ». Cela signifie que contrairement au registre centralisé, qui comporte un serveur et des clients, chaque nœud peut agir à la fois comme client et serveur selon la circonstance. Le nom le dit : pair-à-pair, égal à égal.

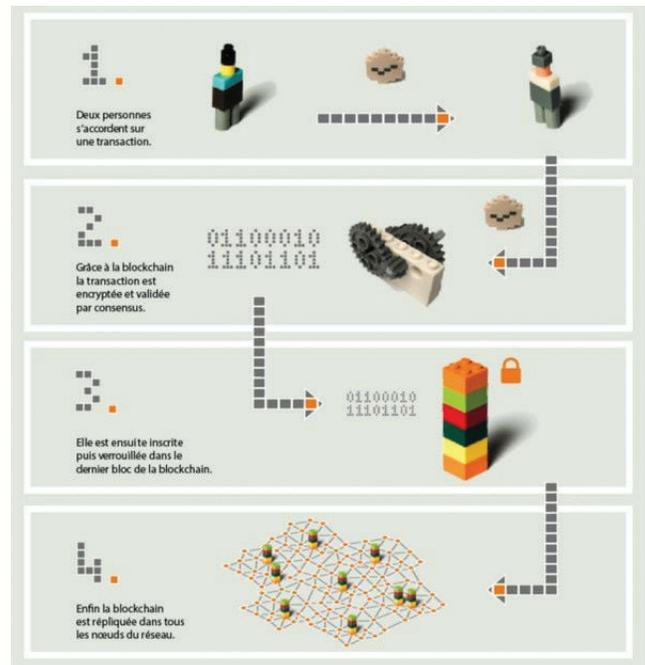
Un nouveau bloc est créé périodiquement, regroupant des transactions récentes. Mais pour que la transaction soit réalisée, ce nouveau bloc devra être intégré et approuvé. Ainsi, aucun ajout de bloc à un nœud n'est possible sans qu'il se duplique sur tous les nœuds. Et aucune transaction n'est possible sans être validée par chacun des nœuds. Ce processus de validation de la transaction est ce qu'on appelle le « **minage** » dans les cas de Bitcoin et de Ethereum, mais le minage n'est pas caractéristique de tous les types de registres distribués.

1.3 Quels sont les différents types de chaînes de blocs?

Les chaînes de blocs peuvent être **privées** ou **publiques**.

- Une chaîne de bloc **privée** peut être mise sur pied par un nombre restreint d'organisations pour permettre des échanges d'information sécurisés avec des clients, des citoyens ou des membres selon les termes qu'elles conviennent. Les organisations à l'origine de la chaîne ont alors l'autorité pour autoriser ou refuser la création de nouveaux blocs et de nouveaux nœuds. Le système est contrôlé. Par exemple, IBM et Maersk Line, la plus grande société de transport maritime au monde, sont en train de créer une plateforme de commerce en chaîne de blocs. L'objectif est de fournir aux utilisateurs et aux acteurs impliqués dans les transactions maritimes mondiales

Figure 2 - Processus d'une transaction sur une chaîne de blocs



Source : *Comprendre la blockchain*, Uchange.co, janvier 2016, p. 10 [iatranshumanisme.com/wp-content/uploads/2018/01/comprendre-la-blockchain-uchange.co_01.pdf].

Chaque chaîne de blocs comporte ses propres mécanismes de validation qui déterminent les critères à remplir pour qu'une transaction ou une opération soit considérée comme valide, autorisée par chaque nœud et inscrite sur chacun d'eux comme nouvel élément dans un historique réputé immuable et infalsifiable. En outre, des mécanismes de récompenses accordées par bloc et par transaction renforcent le respect des règles du protocole par tous les nœuds, dans certaines chaînes de blocs.

un échange sécurisé et en temps réel de données et de documents sur la chaîne logistique.

- Dans le cas d'une chaîne de blocs **publique**, il n'y a généralement pas d'autorité qui gouverne. Quiconque peut créer un bloc et faire croître la chaîne pour autant qu'il satisfasse au protocole de consensus du réseau, qui est donc ouvert (code ouvert ou *open source*). Le **Bitcoin** et **Ethereum** sont les plus connues des chaînes de blocs publiques.

1.4 Qu'est-ce qui distingue les registres distribués des autres modes de stockage d'information?

La force des registres distribués tient à ses caractéristiques principales. Cette combinaison transparence-traçabilité-immuabilité-désintermédiation n'a pas d'équivalent et associe les registres distribués à un engouement à l'échelle mondiale. Il faut toutefois noter que ces caractéristiques ne sont pas binaires et peuvent être mises en œuvre à des degrés divers selon les besoins.

Transparence

- Les registres distribués peuvent être des livres ouverts. Chaque participant peut avoir un accès égal aux registres complets des transactions incluant les codes des contrats intelligents.

Traçabilité

- Dans un registre distribué, les transactions sont inscrites dans un ordre logique ou chronologique inaltérable. Au sein d'un registre distribué, par exemple, des consommateurs pourraient suivre le parcours d'un produit agroalimentaire, de la semence à l'assiette.

Immuabilité et inviolabilité

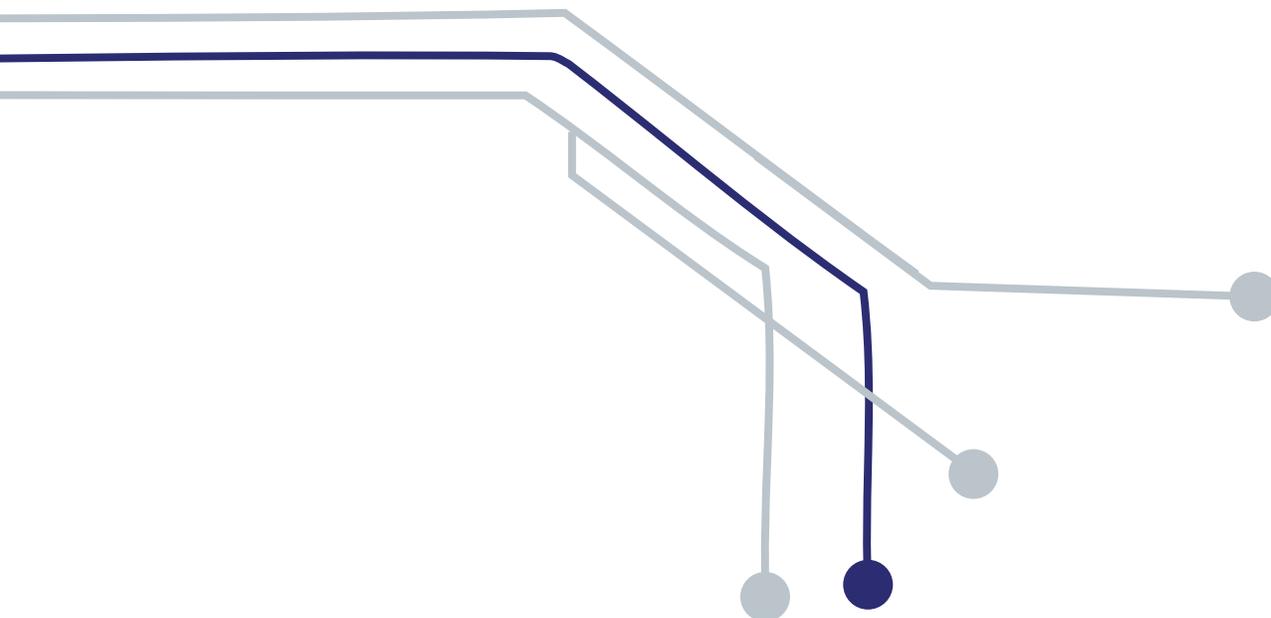
- Une donnée enregistrée sur un registre distribué ne peut s'effacer. Elle est permanente. Tous les ajouts sont comptabilisés et auditables par les participants du réseau. Le réseau est réputé inviolable et imperméable à toute forme de contrefaçon ou de corruption, puisque les données ne sont pas stockées sur un serveur unique,

mais dupliquées sur plusieurs serveurs. Cette duplication renforce la robustesse du réseau et le rend disponible en tout temps.

Désintermédiation et autonomisation (*empowerment*) des participants/citoyens/consommateurs

- Au sein d'un registre distribué, les échanges peuvent s'effectuer directement, de personne à personne ou d'organisation à organisation; c'est le réseau pair-à-pair. Les participants n'ont pas à placer leur confiance dans une autorité centrale. C'est la possibilité d'une désintermédiation, de la disparition des intermédiaires, qui laisse la place à des participants égaux entre eux, qui partagent le contrôle sur l'ensemble des données. La gouvernance décentralisée alliée à la cryptographie² favorise le respect de la vie privée et le contrôle des données.

Les registres distribués représentent une innovation importante dont on commence à mesurer la portée, mais c'est une technologie qui comporte aussi ses défis et ses contraintes. Le tableau suivant propose une comparaison sommaire entre les différents modes d'archivage des informations : l'approche conventionnelle d'un réseau centralisé, l'approche maintenant largement utilisée de l'infonuagique et les registres distribués.



² Ensemble des techniques de chiffrement qui assurent l'invulnérabilité de textes et, en informatique, de données. (Larousse).

Figure 3 - Comparaison entre trois modes de stockage des données

	FORCES	FAIBLESSES
Bases de données centralisées	<ul style="list-style-type: none"> • Personnalisation et convivialité pour les utilisateurs (ex. : adaptation en fonction des besoins, large distribution, regroupement des informations) • Vitesse de traitement et capacité de traiter un gros volume • Gestion des mises à jour et de la sécurité par l'administrateur 	<ul style="list-style-type: none"> • Défaillance unique (ex. : serveur de base de données, utilisation des données, piratage) • Dépendance envers l'administrateur de la base de données • Sécurité et vulnérabilité (ex. : piratage, modifications, extractions) • Partage limité d'information en raison de synchronisation partielle de données
Infonuagique « cloud »	<ul style="list-style-type: none"> • Déploiement facile et rapide • Gestion des services déchargée au fournisseur • Modèle de plus en plus répandu et technologies éprouvées • Gains d'efficacité démontrés • Multiplicité des modèles et des acteurs • Étendue des solutions prêtes à l'emploi 	<ul style="list-style-type: none"> • Différenciation des fournisseurs difficile à établir • Adaptation difficile si contrainte de localisation territoriale, de normes de sécurité... • Domination de quelques acteurs (GAFA) • Risques de sécurité des données • Dépendance à l'écosystème du fournisseur
Chaîne de blocs « Blockchain »	<ul style="list-style-type: none"> • Décentralisation des données (copies des nœuds sur un réseau distribué) • Immuabilité des informations • Transparence des transactions • Environnement sécurisé (cryptographie avancée, réseau distribué) • Solutions opérationnelles éprouvées (cryptomonnaies) • Haute tolérance aux pannes • Logiciels ouvert et open-source • Transparence et compréhensibilité du système • Réduction potentielle des coûts 	<ul style="list-style-type: none"> • Consommation d'énergie (pour certains systèmes seulement) • Performance limitée de la blockchain • Frais de transaction (pour certains systèmes seulement) • Manque de normes et interopérabilité entre les chaînes de blocs • Maturité de la technologie • Cadres réglementaire et juridique en développement • Complexité des mécanismes de modification des règles de protocole

1.5 Quelle est l'importance du phénomène ?

Nous sommes devant une technologie très jeune, ayant seulement une dizaine d'années d'existence. Cette technologie n'a pas encore atteint sa maturité, n'est pas encore utilisée à grande échelle, et n'a pas encore généré de modèles d'affaires éprouvés. Pourtant, même si beaucoup reste à faire, le monde technologique est rangé derrière une évidence : le phénomène des registres distribués est incontournable. Quelque 800 dirigeants et experts interrogés par le Forum Économique mondial³ ont estimé qu'en :

- 2027, **10 % du PIB mondial** pourrait être stocké dans les registres distribués;
- 2023, un premier gouvernement utiliserait une chaîne de blocs pour la perception de taxes ou d'impôts.

En outre, un sondage⁴ réalisé en février 2019 par la firme Deloitte auprès de 1 400 cadres dans une douzaine de pays est révélateur du niveau de conscientisation des décideurs d'entreprises face aux registres distribués. Ainsi :

- 82 % des répondants ont estimé que leurs fournisseurs, clients et/ou concurrents discutaient des solutions impliquant des registres distribués pour relever des défis touchant les chaînes de valeur ou travaillaient sur ces solutions;
- 77 % des répondants ont estimé qu'ils perdraient un avantage concurrentiel s'ils n'adoptaient pas la technologie des registres distribués;
- 56 % des répondants ont estimé que les registres distribués allaient perturber leur secteur d'activité.

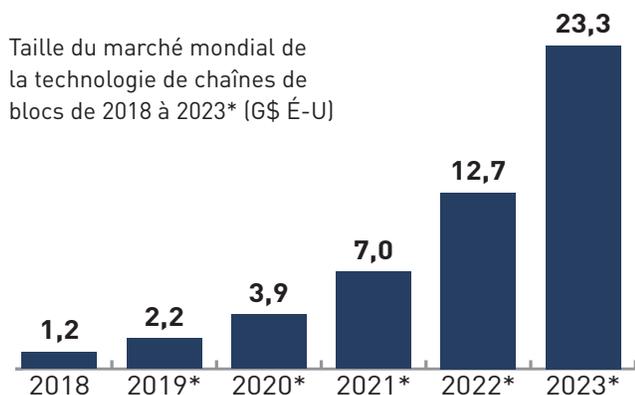
Les graphiques suivants permettent d'illustrer l'importance du phénomène des chaînes de blocs.

Les revenus mondiaux tirés de la technologie des chaînes de blocs connaîtront une croissance très dynamique au cours des prochaines années. Le marché devrait atteindre plus de 23,3 milliards de dollars américains d'ici 2023.

³ World Economic Forum, *Deep shift: Technology Tipping Points and Societal Impact*, September 2015, p. 24 et 26 [weforum.org]. [www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf].

⁴ Deloitte, *Deloitte's 2019 Global Blockchain Survey. Blockchain gets down to business*, 2019 [www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf].

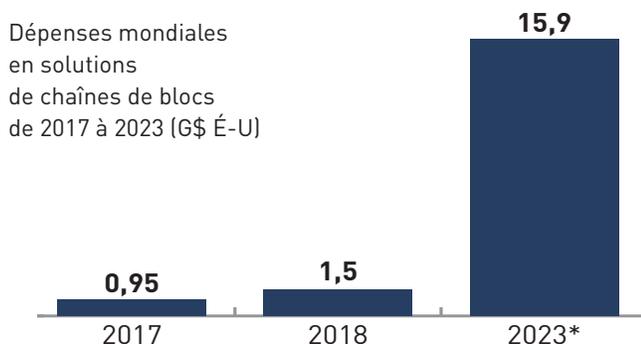
Figure 4 – Revenus mondiaux tirés de la technologie des chaînes de blocs



Source : MarketsandMarkets, décembre 2018
Extraction réalisée par l'Université McGill sur le site Statista

Les dépenses consacrées aux solutions de chaînes de blocs dans le monde de 2017 à 2023 connaîtront aussi une forte croissance. En 2019, les dépenses mondiales consacrées aux solutions de chaînes de blocs devraient atteindre environ 2,7 milliards de dollars américains.

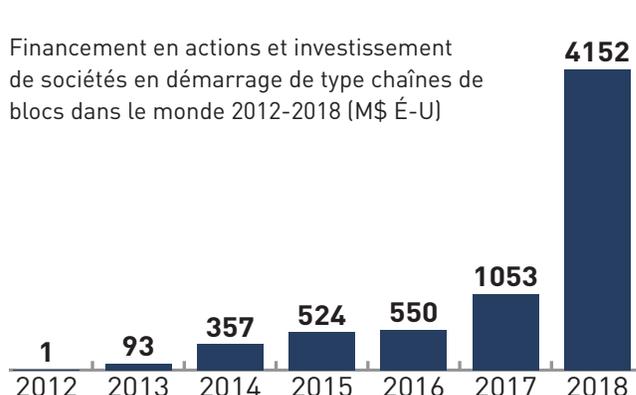
Figure 5 – Dépenses mondiales en solutions de type chaînes de blocs



Source : Idc.com, août 2019
Extraction réalisée par l'Université McGill sur le site Statista

Au premier semestre de 2019, les entreprises en démarrage de chaînes de blocs avaient amassé 783 millions de dollars américains en financement dans le monde. Le marché a connu une croissance spectaculaire depuis son introduction vers 2012, le financement total passant d'un million de dollars à plus de 4,15 milliards de dollars en 2018.

Figure 6 – Financement et investissement en démarrage de sociétés de type chaînes de blocs dans le monde

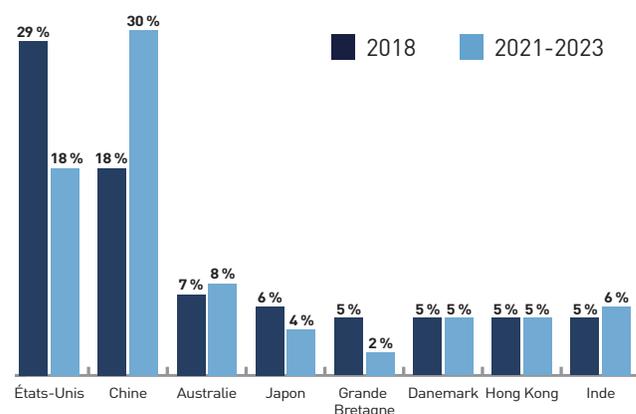


Source : CB Insights, juillet 2019
Extraction réalisée par l'Université McGill sur le site Statista

Les statistiques laissent entrevoir un mouvement, principalement une poussée de la Chine, dans les territoires considérés comme des leaders du développement technologique de la chaîne de blocs entre 2018 et la période 2021 à 2023, comme le montre la figure 7. Ainsi, en 2018, environ 18 % des personnes interrogées par PwC ont déclaré considérer la Chine comme le premier territoire en matière de développement technologique de la chaîne de blocs. Mais à la question *Quel territoire serait le chef de file du développement technologique blockchain de 2021 à 2023?*, 30 % des personnes interrogées ont répondu « Chine ».

Figure 7 – Pays leaders dans la technologie des chaînes de blocs

Les territoires considérés aujourd'hui et demain comme des leaders du développement technologique des chaînes de blocs dans le monde.



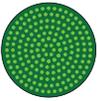
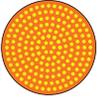
Source: PwC, août 2018
Extraction réalisée par l'Université McGill sur le site Statista

1.6 Comment se positionnent les pays?

Des sociétés et des experts se sont regroupés au sein de GovChain⁵ pour rassembler les meilleures pratiques en matière de mise en œuvre et de traitement réglementaire en regard des chaînes de blocs de plus de 30 États ou organisations intergouvernementales dans le monde. À l'aide d'un système d'évaluation de feux de signala-

tion, le rapport fournit un guide sur les différents niveaux d'adoption de la chaîne de blocs dans les juridictions ciblées, en identifiant les modèles et tendances émergents. Bien que ces catégories soient nécessairement subjectives dans une certaine mesure, l'objectif est de fournir un point de référence sur la situation des pays. Le stade d'adoption

Figure 8 – Stade d'adoption de la technologie des chaînes de blocs dans le monde

STADE	PAYS / ÉTATS / ORGANISATIONS INTERGOUVERNEMENTALES				
 <p>A appliqué la chaîne de blocs à divers cas d'utilisation et est susceptible de devenir un écosystème en plein essor.</p>	 Australie	 Union européenne	 Suède	 Singapour	 Gibraltar
	 Indonésie	 Nigéria	 Afrique du Sud	 Bahreïn	 Estonie
	 Émirats arabes unis	 Royaume-Uni	 États-Unis (fédéral)		
 <p>A pris des mesures pour encourager l'innovation, mais le travail reste préliminaire et pourrait ne concerner qu'un seul secteur.</p>	 France	 République dominicaine	 Haïti	 Ghana	 Illinois/Colorado/Ohio/Montana/Delaware
	 OCDE	 Financial Action Task Force	 Île de Man	 Kenya	 Thaïlande
 <p>A adopté une approche sceptique, n'est actuellement pas disposé à tester des initiatives basées sur la chaîne de blocs.</p>	 Brésil	 Chine	<p>Note : Bien que GovChain continue de classer la Chine dans les pays sceptiques, notamment à cause d'une grande méfiance des autorités chinoises envers Bitcoin, le pays est très actif dans le développement de la technologie et plusieurs sources rapportent que la Chine s'apprête à lancer sa propre cryptomonnaie⁶.</p>		

Source : Tableau composé à partir d'informations apparaissant sur la page d'accueil de www.govchain.world

⁵ [govchain.world].

⁶ Les enjeux sont de taille : la Chine s'apprête à lancer sa cryptomonnaie nationale; [<https://dailygeekshow.com/chine-cryptomonnaie-nationale/>]

de la technologie apparaît dans le tableau suivant.

1.7 Chaîne de blocs, bitcoins et controverse

Si le grand public a pu entendre parler de la chaîne de blocs au cours des dernières années, c'est probablement dans des reportages mêlant cryptomonnaies (principalement bitcoins) et activités illicites réalisées dans le cadre de ces applications particulières de la chaîne de blocs. Apportons quelques éclaircissements.

Bitcoin (avec un B majuscule) est le nom de la première chaîne de blocs qui est entrée en opération. Il s'agit d'une infrastructure d'échange décentralisée permettant des transactions dans une cryptomonnaie, appelée **bitcoin** (avec un b minuscule). L'idée a été présentée pour la première fois en novembre 2008 par une personne ou un groupe de personnes sous le pseudonyme mystérieux de Satoshi Nakamoto. Le code source permettant son envoi a été publié en janvier 2009. Le moment n'est pas anodin : le bitcoin et les autres cryptomonnaies sont en quelque sorte un produit de la grande crise financière de 2008 et d'une perte de confiance dans les institutions financières.

Bitcoin utilise des techniques de chiffrement pour sécuriser une transaction, de telle sorte qu'aucun organe central ne soit nécessaire. Dans cette chaîne de blocs, ceux qui valident les transactions, qui font donc le minage, sont eux-mêmes payés en bitcoins selon un protocole de rétribution. Ce système est à la fois le principal mode de gestion et de création des bitcoins. La rétribution est versée au premier qui parvient à générer un bloc valide, c'est-à-dire qui contient des transactions validées sur tous les nœuds. Cela crée une course à la performance, chaque détenteur d'un nœud voulant un ordinateur toujours plus puissant

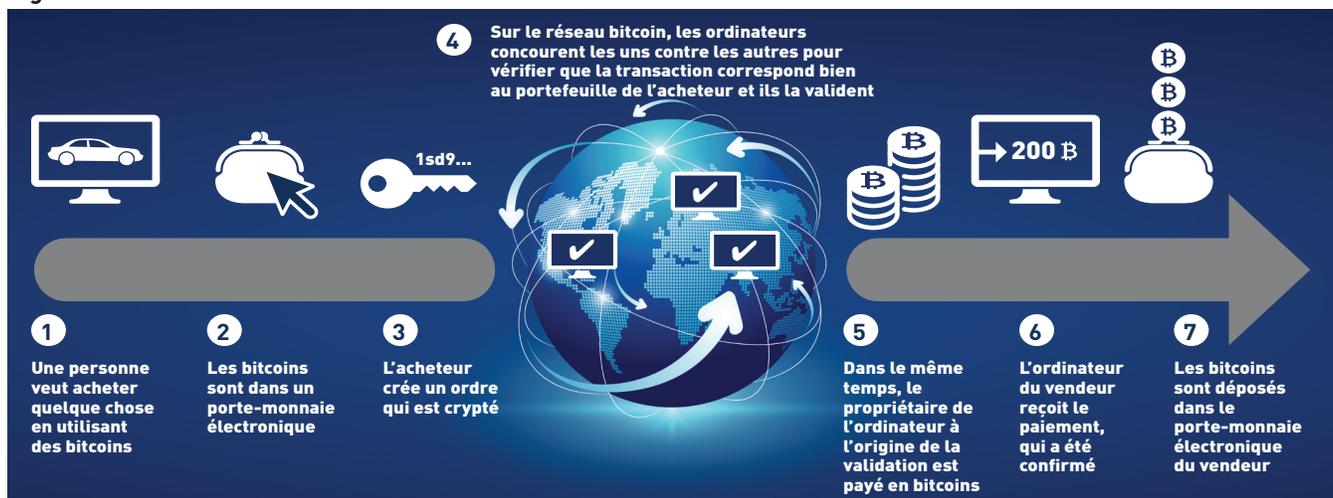
pour parvenir à réaliser le minage avant les autres et ainsi toucher sa récompense. C'est ce phénomène de ruée vers la puissance informatique qui fait du minage un processus énergivore. Nous y reviendrons plus loin.

Aujourd'hui, le système Bitcoin représenterait une capitalisation de plus de 140 milliards de dollars américains, tandis que l'ensemble des cryptomonnaies (on en compte aujourd'hui près de 2 400) représenterait une valeur comptable de plus de 220 milliards de dollars⁷.

Dès sa création, le bitcoin a été utilisé par des réseaux criminels et associé à des activités illicites sur le Web invisible (*darkweb*). Une intervention musclée de la police américaine contre le site de marché noir *SilkRoad* en 2013 et 2014 avait notamment fait grand bruit⁸. Plus récemment, un couple de Québécois qui a fait la promotion d'une cryptomonnaie jugée frauduleuse (le Plexcoin) a été condamné à payer près de 7 millions \$ US (plus de 9,3 M\$ CA) aux autorités boursières américaines⁹.

Néanmoins, les cryptomonnaies sont aujourd'hui associées à des activités parfaitement légitimes. Elles n'ont cependant pas cours légal et ne sont pas émises par des banques centrales. Elles peuvent toutefois être utilisées dans la plupart des pays et au Québec comme forme de paiement ou moyen d'échange à la suite d'une entente entre deux parties. Les cryptomonnaies sont liées à la naissance de la chaîne de blocs, mais la technologie a largement débordé de ce cadre originel pour devenir un phénomène transformateur puissant.

Figure 9 – Processus d'une transaction en bitcoins



Source : image tirée de www.coin24.fr/bitcoin

7 [www.coinmarketcap.com/all/views/all] Consulté le 18 octobre 2019.

8 *Silk Road : The dark side of cryptocurrency*, [https://news.law.fordham.edu/jcl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/]

9 « Un couple de Québécois qui a fait la promotion d'une cryptomonnaie jugée frauduleuse va devoir payer près de 7 millions \$ US (plus de 9,3 M\$ CA) aux autorités boursières américaines »; [https://www.tvanouvelles.ca/2019/10/04/un-couple-de-quebecois-accuse-de-fraude-force-de-payer-7-m-us]

2. POTENTIEL ET APPLICATIONS

En tant que moyen d'archivage des informations et de sécurisation des échanges, les registres distribués ont un champ d'application à peu près illimité, puisqu'en cette ère numérique, à peu près tous les domaines d'activité impliquent une gestion des données.

2.1 Fonctions pouvant être accomplies par les registres distribués

On pourrait associer les registres distribués à six fonctions types selon la firme d'analyse stratégique McKinsey¹⁰ :

1. La constitution de **registres sécurisés** tels des dossiers patients, des dossiers clients, des titres de propriété divers.
2. La **gestion des identités** par les listes de membres, de clients, de données personnelles ou par l'administration de systèmes de votation électronique.
3. Les **contrats intelligents** sont une des innovations apportées par les registres distribués. Ils permettent de déclencher automatiquement des opérations lorsqu'un certain nombre de conditions sont remplies. Par exemple, des contrats intelligents pourraient permettre l'automatisation de paiements pour des réclamations d'assurance.
4. La constitution de **registres dynamiques**. Pensons aux chaînes d'approvisionnement dans divers secteurs économiques, à la traçabilité des aliments, au suivi de la distribution des médicaments, soit autant de bases de données en constante mouvance qui nécessitent sécurité et fluidité.
5. Les **infrastructures de paiement**. Les registres distribués peuvent faciliter les paiements transfrontaliers, les règlements d'assurance, la gestion de dettes, la perception d'abonnements, de paiements entre particuliers...
6. Le **registre distribué adapté** (*blockchain as a service*). Déjà, des entreprises offrent des registres distribués sur mesure, adaptés aux besoins de toute organisation, association, compagnie désirant un mode de gestion performant et sécuritaire de ses informations.

¹⁰ « Blockchain beyond the hype: What is the strategic business value? », juin 2018

[www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value].

Figure 10 – Tableau synthèse des fonctions types des registres distribués

Tenue de registre : stockage d'informations statiques		
Registre statique	Identité	Contrats intelligents
Base de données distribuée pour le stockage de données de référence	Base de données distribuée avec des informations relatives à l'identité Cas particulier de registre statique traité comme un groupe distinct de cas d'utilisation en raison d'un ensemble étendu de cas d'utilisation propres à l'identité	Ensemble de conditions enregistrées sur une chaîne de blocs déclenchant des actions automatisées et auto-exécutantes lorsque ces conditions prédéfinies sont remplies
Exemples : • Brevets • Titres fonciers • Salubrité et origine des aliments	Exemples : • Usurpation d'identité • Registre d'état civil et registres d'identité • Vote	Exemples : • Prestation d'assurance • Négociation d'actions en espèces • Sortie de titres musicaux

Transactions : tenue de registre d'informations négociables		
Registre dynamique	Infrastructure de paiements	Autres
Base de données distribuée dynamique qui se met à jour au fur et à mesure que les actifs sont échangés sur la plateforme numérique	Base de données dynamique distribuée qui se met à jour au fur et à mesure que les paiements sont effectués entre les participants	Cas d'utilisation composé de plusieurs des groupes précédents Cas d'utilisation autonome ne correspondant à aucune des catégories précédentes
Exemples : • Fractionnement de placement • Chaîne d'approvisionnement en médicaments	Exemples : • Paiements internationaux • Demande d'indemnité	Exemples : • Émission de jetons numériques (ICO) • Blockchain en tant que service (BaaS)

Source : reproduit à partir de l'étude *Blockchain beyond the hype: What is the strategic business value?*, McKinsey, juin 2018

Dans tous ces cas types d'utilisation, les registres distribués présentent des avantages marqués par rapport aux modes d'archivage centralisés selon DZone¹¹, un forum de développeurs qui anticipe en outre l'arrimage entre les chaînes de blocs et les autres phénomènes transformateurs, comme les mégadonnées, l'Internet des objets et l'intelligence artificielle. Dans cette mouvance technologique, les registres distribués publics présentent les avantages opérationnels de :

- réduire les coûts de sécurité associés à la gestion d'un serveur central;
- réduire les délais par la disparition des intermédiaires;
- renforcer la sécurité par la cryptographie et la duplication des opérations;
- réduire les fraudes par l'immutabilité des inscriptions;
- limiter les risques de pannes par l'existence de multiples nœuds pouvant assurer le bon fonctionnement de la chaîne en cas de défaillance de l'un d'eux.

11 « How Blockchain Can Transform Artificial Intelligence », Dmitri Budko, DZone, 13 février 2018 [dzone.com/articles/how-blockchain-can-transform-artificial-intelligen].

2.2 Exemples d'applications potentielles

Les fonctions associées aux registres distribués peuvent trouver des applications très variées. La nomenclature qui suit est tirée d'un article paru en mars 2019 sur le site ScienceDirect.com¹² et réfère principalement à des chaînes de blocs privées.

Applications financières

- Déjà, la technologie des registres distribués est appliquée à une grande variété de domaines financiers, notamment les services aux entreprises, le règlement de paiements et des transactions diverses.

Applications commerciales et industrielles

- Les registres distribués ont le potentiel de devenir une source importante d'innovations en entreprises en améliorant, en optimisant et en automatisant une multitude de processus d'affaires. Les registres distribués seraient ainsi associés à des gains de productivité majeurs.

Chaîne d'approvisionnement

- Les chaînes d'approvisionnement pourraient être transformées par le recours aux registres distribués qui faciliteraient notamment l'identification des produits contrefaits, réduiraient les délais de traitement des opérations, standardiseraient la traçabilité des produits, simplifieraient les transactions sans intermédiaires entre vendeurs et acheteurs.

Vérification d'intégrité

- L'un des domaines émergents liés aux registres distribués serait la vérification d'intégrité et la gestion d'informations relatives à la création et à la durée de vie de produits ou de services. Les applications possibles toucheraient notamment :
 - les services d'assurance;
 - la gestion de la propriété intellectuelle.

Services publics

- Les applications de registres distribués pourraient renforcer l'administration des services publics, en sécurisant les données, en améliorant leur confidentialité, en automatisant certaines opérations.
- Les registres distribués pourraient simplifier et sécuriser l'enregistrement de documents légaux, l'attestation de contrats, l'administration des taxes.
- Les registres distribués pourraient aussi servir de plateforme de communication sécurisée pour l'intégration des infrastructures physiques, sociales et commerciales dans une ville intelligente.
- Le projet World Citizenship, par exemple, vise à offrir un service de passeport décentralisé permettant d'identifier les citoyens du monde entier.

Votation électronique

- Le vote électronique est considéré comme un développement prometteur qui pourrait accélérer et simplifier les consultations populaires.
- Les systèmes de vote électroniques existants reposent sur une gestion centralisée par une seule entité, ce qui nuit à la confiance dans le processus. Le registre distribué étant un réseau ouvert, décentralisé et pair-à-pair, il pourrait contourner ces difficultés et ainsi ouvrir la voie à des scrutins électroniques qui auraient la confiance des électeurs.

La gestion des soins de santé

- Les registres distribués pourraient être une solution pour la gestion d'informations sensibles comme les dossiers patients et le partage contrôlé des informations médicales tout en garantissant au patient concerné la sécurité et la confidentialité.

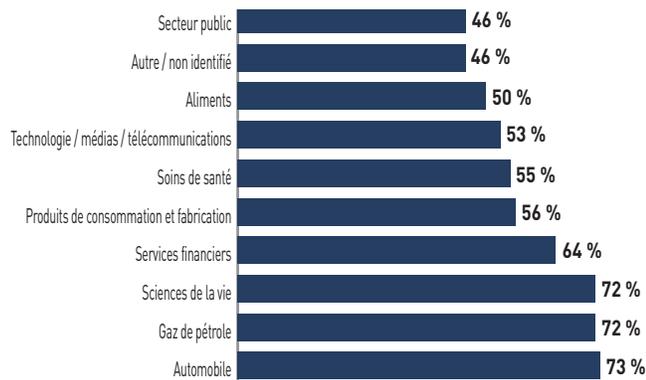
Éducation

- Les registres distribués pourraient résoudre des problèmes de vulnérabilité, de sécurité et de confidentialité dans l'archivage des dossiers pédagogiques. Les applications basées sur les registres distribués pourraient aussi améliorer l'accréditation numérique des apprentissages personnels et scolaires.

12 « A systematic literature review of blockchain-based applications: Current status, classification and open issues », Fran Casino, Thomas. K. Dasaklis, Constantino Patsakis, Telematics and Informatics, volume 36, mars 2019 [www.sciencedirect.com/science/article/pii/S0736585318306324].

Les registres distribués pourraient même être un élément de solution face à la crise des médias avec des modèles d'affaires novateurs. Un navigateur *open source* nommé *Brave* associé à la cryptomonnaie *Basic Attention Token* peut permettre à un utilisateur d'accepter (ou de refuser) de voir de la publicité, d'être rémunéré pour la regarder, et de partager les revenus générés par son attention avec les producteurs des contenus consultés. Par exemple, si un utilisateur passe 40 % de son temps de navigation mensuelle sur le site de son journal préféré, alors 40 % de ses *Basic Attention Token* récoltés en regardant de la publicité seraient attribués à ce site.

Figure 11 – Perception perturbatrice des chaînes de blocs selon les secteurs d'activité

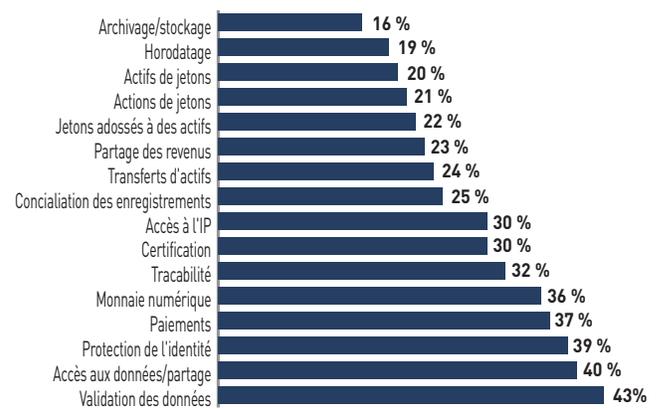


Source : *Breaking blockchain open*. Deloitte's 2018 global blockchain survey, p. 20
Extraction réalisée par l'Université McGill sur le site Statista

Cette variété d'applications se traduit dans de multiples secteurs d'activité par un sentiment de grands bouleversements à venir.

On note d'ailleurs déjà une grande variété d'intentions d'utilisation. Le graphique suivant présente le nombre de répondants au sondage Deloitte qui ont dit envisager le recours à la technologie des chaînes de blocs pour différents usages.

Figure 12 - Cas d'utilisation envisagés de la technologie des chaînes de blocs dans des organisations



Source : *Deloitte's 2019 Global Blockchain Survey. Blockchain gets down to business*, p. 34
Extraction réalisée par l'Université McGill sur le site Statista

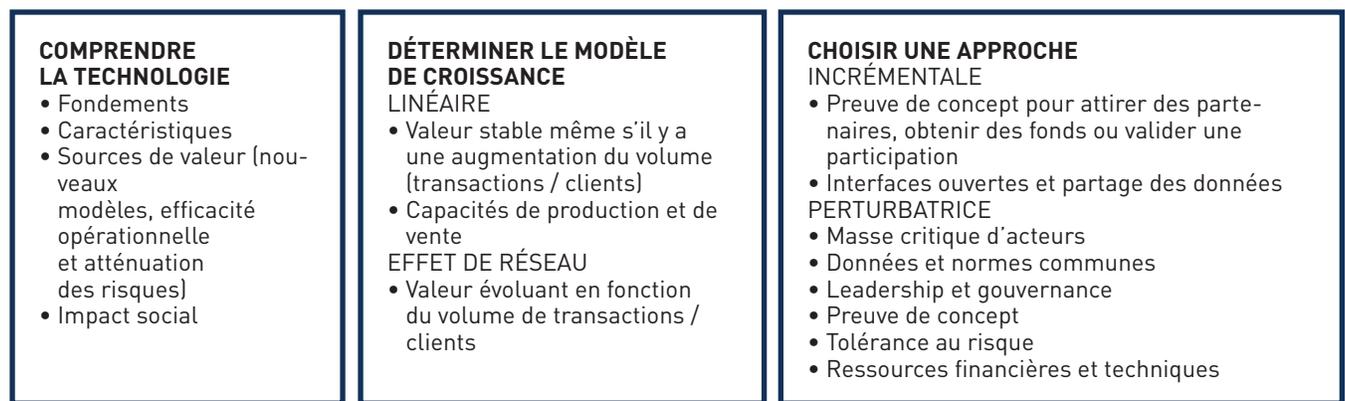
2.3 Démarche d'implantation de la technologie des registres distribués dans une organisation

La technologie des registres distribués pourrait avoir des effets déstabilisateurs sur diverses industries. Au cours des dernières années, des processus d'accompagnement se sont développés pour soutenir les industries et les organismes publics. Ces démarches peuvent se résumer par une série d'activités en quatre phases. Compte tenu des exigences de normalisation et du nombre de participants à fédérer, ces démarches d'implantation sont généralement réalisées sur plusieurs années.



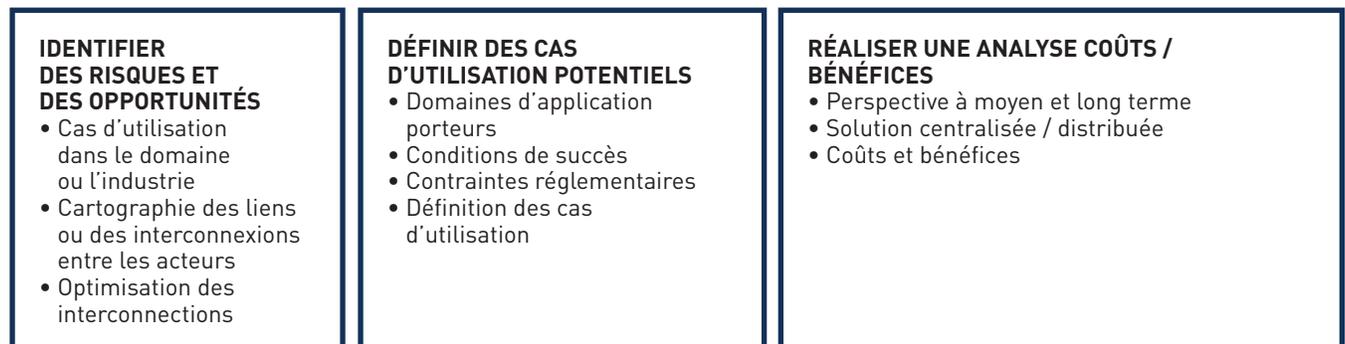
POSITIONNEMENT

La première de ces phases concerne le positionnement stratégique en regard de la technologie. Elle consiste à comprendre la technologie, à déterminer le modèle de croissance et à choisir une approche stratégique. L'ensemble de ces travaux oriente les réflexions pour les phases subséquentes.



IDÉATION

Après s'être livrées à cette réflexion stratégique, les organisations réalisent un exercice d'idéation dans le but d'identifier des risques et des opportunités, de définir des cas d'utilisation potentiels de la technologie et de procéder à une analyse coûts / bénéfices avant de passer à une phase de validation.



Dans le but de mettre les efforts sur les occasions d'application prometteuses, les industries et les organisations doivent privilégier une approche structurée. Dans un premier temps, elles doivent identifier les cas d'application où plusieurs parties sont impliquées et les cas qui présentent des coûts élevés pour le partenaire qui gère les données. Par la suite, il est recommandé de déterminer si le réseau devrait être public et s'il y a un enjeu de confiance. Ces étapes mèneront à se questionner sur les changements requis au processus, les relations entre les acteurs et les exigences.

Cet exercice devrait être complété par une réflexion sur la gouvernance à privilégier dans l'utilisation de cette technologie, c'est-à-dire le mécanisme par lequel les modifications aux règles du protocole seront apportées.

VALIDATION

Avant de se lancer dans l'implantation, les organisations doivent effectuer une ou des preuves de concept technique et procéder à une validation sur le plan commercial. Ces travaux sont critiques et demandent beaucoup de ressources et de temps.

EFFECTUER UNE PREUVE DE CONCEPT TECHNIQUE

- Processus et acteurs touchés
- Traitement des données
- Conception de la solution
- Audit

VALIDER LA PREUVE DE CONCEPT SUR LE PLAN COMMERCIAL

- Processus et acteurs touchés
- Leadership et gouvernance
- Traitement des données (normalisation)

IMPLANTATION

Dans la mesure où les preuves de concept sont probantes, les organisations peuvent finalement passer à l'implantation ou au déploiement de la solution.

PROCÉDER AU DÉPLOIEMENT

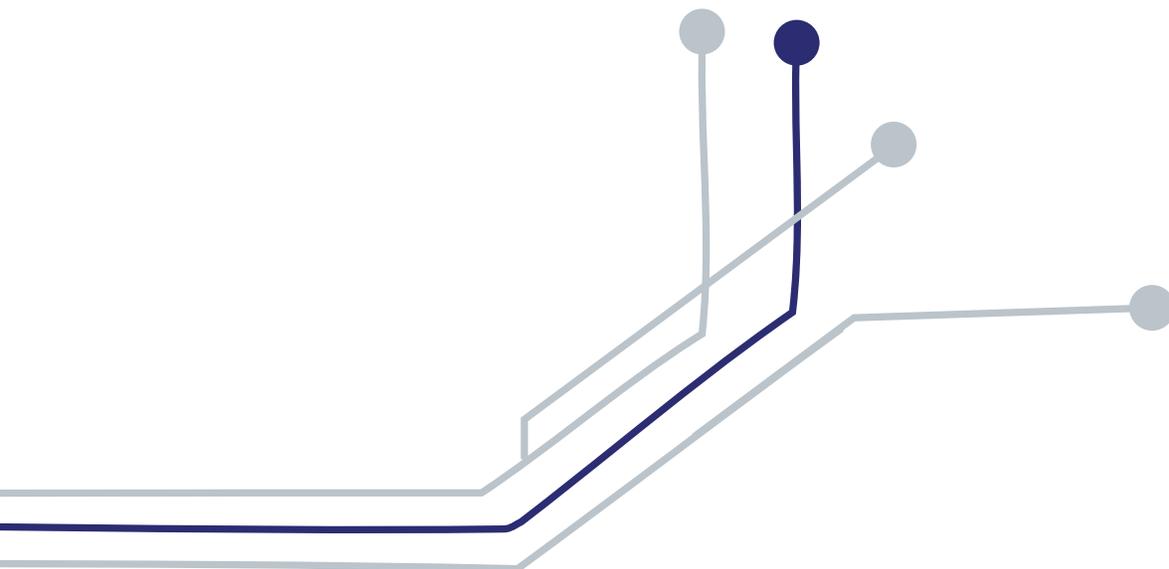
- Gouvernance / consortium
- Gestion du changement
- Communications

Pour assurer le succès de ces exercices, les industries et les organisations doivent réfléchir sur la gouvernance à privilégier pour aligner les intérêts et les ambitions des participants, ainsi que pour assurer la collaboration des principaux intervenants, dont les équipes informatiques et en gestion des données.

De plus, étant donné que les connaissances dans le domaine des registres distribués sont émergentes, il est nécessaire pour les organisations de maintenir et d'élargir leur bassin d'experts. Dans ce contexte, il pourrait être pertinent d'associer, à toutes les phases, les conseils d'experts soit par recrutement, par l'établissement de partenariats ou par l'intervention de consultants externes.

Également, même si les phases de positionnement et d'idéation peuvent se réaliser relativement rapidement, beaucoup de temps est à prévoir pour jeter les bases techniques et rassembler suffisamment de participants afin de générer une valeur réelle et évolutive.

Dans cette perspective, il s'avère important de garder à l'esprit que les industries ou des organisations doivent partager une vision ou des ambitions à long terme pour garder la mobilisation des participants et des acteurs tout au long des travaux.

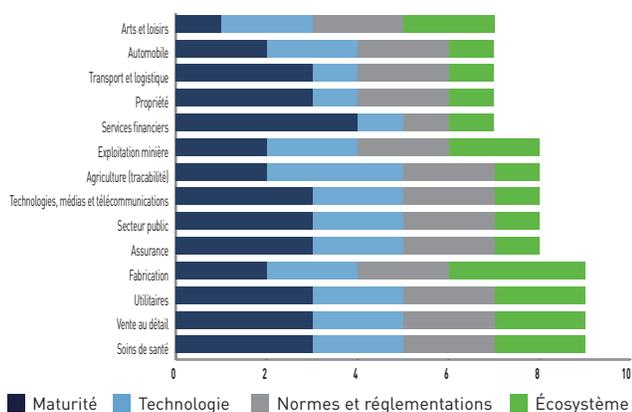


2.4 Défis posés par les registres distribués

Si la technologie des registres distribués suscite un intérêt planétaire, son utilisation massive et généralisée n'est pas encore chose faite et plusieurs défis devront être relevés avant son adoption. C'est pourquoi plusieurs experts sont d'avis qu'il faudra encore 5 à 10 ans avant que la technologie des registres distribués ait atteint une maturité permettant son déploiement à grande échelle.

Ainsi, selon les domaines d'activité, différents enjeux liés à la maturité de la technologie, à l'absence de normes d'utilisation et de réglementation et à la fragilité de l'écosystème naissant se manifestent.

Figure 13 – Faisabilité du recours à la technologie des chaînes de blocs par industrie



Graphique reproduit à partir de *Blockchain beyond the hype: What is the strategic business value?*, McKinsey, juin 2018

Défis d'ordre technologique

L'extensibilité ou l'évolutivité. Ces mots réfèrent à la possibilité pour une technologie de passer d'un stade à un autre et, dans le cas qui nous concerne, de passer d'un usage restreint à un usage de masse. Par exemple, à l'heure actuelle, Bitcoin permet un maximum de quatre à sept transactions par seconde, tandis que les systèmes de Visa traitent 65 000 transactions par seconde. Toutefois, certains registres distribués publics, comme EOS, atteignent 50 000 transactions par seconde. Ces écarts de performance s'expliquent par des différences importantes dans la conception des règles du protocole, notamment au niveau des mécanismes de validation.

La convivialité. Les registres distribués étant encore une technologie émergente, les applications permettant de les utiliser sont pour l'heure rébarbatives à une utilisation par le grand public. L'Internet a été popularisé par l'accès simple et facile aux contenus en ligne. Les registres distribués n'ont pas encore atteint ce stade.

La sécurité. Les registres distribués sont réputés immuables et inviolables. Ainsi, la plupart des enjeux de sécurité évoqués relativement aux registres distribués sont davantage liés à des éléments périphériques qu'à la technologie elle-même; ce sont des aspects telles les bonnes pratiques des utilisateurs et des entreprises et la bonne conception des applications qui sont alors en cause. Ainsi, certains cas de fraude qui ont été rapportés ont reposé sur l'exploitation malveillante de lacunes dans des contrats intelligents.

C'est ce qui s'est produit dans un cas notoire survenu en juin 2016. Un contrat intelligent dans Ethereum Classique, qui fournissait des fonctionnalités de financement participatif, a été attaqué par l'exploitation d'une faille dans le code de ce contrat intelligent. Le pirate a pu siphonner les fonds de cryptomonnaies de l'organisation virtuelle.

La numérisation des utilisateurs. Les registres distribués permettent de stocker des données numériques. Cela crée par la force des choses une barrière à l'entrée : posséder des données numérisées dans un mode permettant leur usage dans un registre distribué. Si l'immense majorité des entreprises d'aujourd'hui ont fait le passage à l'information numérisée, de nombreux organismes gouvernementaux et publics, chez nous et à travers le monde, ont encore des dossiers papier. La conversion se fera, inévitablement, mais demandera un certain temps.

Défis d'ordre légal – Entrevue avec M^e Charline Bouchard

Les défis d'ordre légal sont nombreux en regard des chaînes de blocs. La technologie entraîne une remise en question de concepts de base dans nos sociétés et notre économie : la monnaie, l'archivage, les intermédiaires de toutes sortes, la responsabilité des acteurs. Les innovations qui en découlent comportent des avantages majeurs pour les citoyens et les consommateurs qui se trouvent aussi exposés à des risques nouveaux. Pour aborder ces enjeux, nous présentons quelques extraits d'une entrevue avec M^e Charline Bouchard, membre du comité directeur de ce livre blanc. Elle est professeure à la Faculté de droit de l'Université Laval et l'une des rares spécialistes au Québec des enjeux légaux liés aux chaînes de blocs.

Entrevue avec M^e Charlaïne Bouchard

Quels sont les principaux domaines du droit qui sont touchés par les chaînes de blocs?

Les chaînes de blocs représentent un défi sans précédent sur le plan du droit avec des impacts nombreux et directs. Dans une perspective d'enjeux légaux, on peut voir trois grands domaines d'usages des chaînes de blocs : le transfert d'actifs, la conservation des données et les contrats intelligents.

Le transfert d'actifs, c'est toute la question financière, les cryptomonnaies, les titres, les actions, les obligations. Les chaînes de blocs permettent de soutenir et d'optimiser toutes les fonctions de paiement.

Quand on parle de la conservation des données, c'est tout ce qui est registre ou cadastre. Avec des avantages marqués en termes de transparence et d'intégrité, les chaînes de blocs vont constituer un support extraordinaire, entre autres pour la protection des données personnelles.

Et quand on parle de contrats intelligents, ce sont des applications qui s'exécutent de manière autonome pour déclencher, par exemple, des paiements d'assurances. Le concept est extrêmement intéressant, mais sur le plan légal, les conséquences sont nombreuses.

Est-ce qu'il y a aussi des avantages et des enjeux particuliers pour les consommateurs?

De façon générale, les chaînes de blocs vont permettre aux consommateurs de se réappropriier des droits. Actuellement, ce sont les grands groupes, les GAFAs qui contrôlent nos données. Les consommateurs sont tributaires des actions de ces grands groupes. Avec la chaîne de blocs, dans la mesure où on n'a plus besoin d'intermédiaires sans valeur ajoutée, les consommateurs vont pouvoir regagner le contrôle de leurs données et pourront être mieux protégés. Alors, il y a de nets avantages pour les consommateurs, mais aussi des enjeux délicats, particulièrement lorsqu'il sera question des contrats intelligents.

Parlons-en justement, de ces contrats intelligents, que viennent-ils changer?

C'est une innovation au potentiel extraordinaire. Les contrats intelligents émanent de la philosophie profonde des chaînes de blocs. L'objectif de cette technologie, à l'origine, c'est de se débarrasser de tout type d'intermédiaires, de l'État,

des banques et aussi des juristes. Selon cette philosophie, il suffit de s'entendre et de procéder. L'entente est scellée, immuable, infalsifiable. C'est l'idée maîtresse *code is law*. Le code informatique qui devient le droit. On voit actuellement émerger des documents de toute sorte sur chaîne de blocs : des testaments, des contrats de mariage, etc. Mais il faut être prudent! Pour être valables au Québec, ces documents doivent respecter la loi québécoise. Ça n'a aucune valeur en droit québécois. Plutôt que de parler de « contrats », il serait plus juste de parler de protocoles informatiques qui vont effectuer de façon autonome des procédures simples. On le voit déjà dans l'assurance. Vous achetez un billet d'avion avec une assurance annulation ou retard. Votre avion est en retard de deux heures, vous recevez une indemnisation automatiquement. En termes de simplicité d'opération, c'est formidable. Il y a des avantages évidents, mais il y a aussi des risques à contrôler. Comment être certain que le consommateur connaît l'étendue de l'offre qui lui est faite, comment être certain de son assentiment? Ce sont des protocoles immuables, alors que fait-on en cas d'imprévu ou de changements? Ce sont des questions très importantes en droit. On comprend la philosophie qui est derrière, mais les chaînes de blocs ne peuvent pas constituer un monde parallèle. Pour que leur usage se généralise, le droit devra s'appliquer, s'adapter, oui, mais s'appliquer, pour protéger les parties. C'est un peu comme le commerce électronique. Il a commencé dans l'ombre, mais à mesure qu'il s'est développé, le droit s'est appliqué.

Les défis sont nombreux, mais est-ce qu'il y a plus d'avantages que d'inconvénients?

C'est un progrès qui est certain. Il y a des avantages extrêmement importants dans la mesure où on comprend ce que c'est un contrat intelligent et qu'on l'utilise de la bonne façon. Les domaines d'application sont larges, pensons à la propriété intellectuelle. Avec Internet et les plateformes, c'est l'hémorragie en matière de violation de droits de propriété intellectuelle. Les chaînes de blocs se présentent comme un moyen de rétablir l'équilibre permettant aux auteurs de se réapproprier leurs droits, et avec des contrats intelligents, les acteurs pourraient toucher leurs revenus automatiquement. Ce sont des processus automatisés qui pourraient éviter des litiges ou permettre à des consommateurs ou des ayants droit d'obtenir des règlements rapidement sans recourir aux tribunaux. Il y a des avantages évidents. Mais ça ne remplace pas le contrat. Ce qu'on verra, ce sont des contrats dûment négociés qui prévoiront des clauses auto-exécutables.

Abordons la question des cryptomonnaies et du financement des entreprises. Quels sont les enjeux légaux?

Pour la première fois de l'histoire, avec les cryptomonnaies, l'argent circule instantanément sans intermédiaire, sans frontière, sans surveillance, sans régulation. C'est une rupture qui nous amène à repenser jusqu'à la nature de la monnaie. Les avantages sont extraordinaires en termes de facilité d'opération, de simplicité d'émission d'actions avec les ICO (Première émission de jetons : Campagne de financement par laquelle un organisme vend une part des jetons de sacryptomonnaie durant la phase de démarrage de son projet (*Initial coin offering*)).

Le phénomène est puissant et transformateur. Mais les enjeux sont majeurs. Les monnaies sont adossées à la crédibilité des États. La volatilité est contrée par les banques centrales. Avec les cryptomonnaies, ces remparts n'existent pas. Elles sont soumises entièrement aux humeurs du marché et ont des fluctuations très importantes. Une certaine forme d'encadrement est incontournable à moyen terme pour les stabiliser et légitimer les transactions en cryptomonnaies par la fiscalité. Il se fait actuellement des travaux intenses chez les autorités réglementaires partout dans le monde pour permettre l'innovation que représentent les cryptomonnaies dans un environnement qui va protéger les parties et les avoirs.

Quand vous regardez l'ampleur des défis légaux, êtes-vous en mesure de dire combien de temps il faudra pour encadrer ces technologies et voir leur usage se généraliser?

Le droit est toujours à la remorque des innovations et de la société, ce ne sera pas différent dans ce cas. Ce qui est particulier avec les chaînes de blocs toutefois, c'est l'ampleur des chantiers de législation qui devront être ouverts. Il faudra des années de travail. Mais à l'intérieur des balises actuelles, on peut déjà avancer, notamment à l'égard des contrats intelligents. On peut aussi penser qu'un certain encadrement des transactions en cryptomonnaies sera mis en place à brève échéance parce que ce domaine particulier est en pleine effervescence et que les sommes en jeu, sur le plan fiscal entre autres, sont importantes. Nous sommes devant une technologie nouvelle qui comporte des avantages certains pour les citoyens, les consommateurs, les entreprises. Le droit va s'adapter, mais le travail sera important.

À l'Annexe I, nous faisons état de certains pays et des initiatives qu'ils ont mises de l'avant pour encadrer, développer et utiliser les chaînes de blocs et les registres distribués, à partir du recensement apparaissant sur le site www.GovChain.world.

Défis d'ordre opérationnel

La généralisation de la technologie des registres distribués se heurte aussi à des défis de nature opérationnelle.

Coûts et rendement : La technologie des registres distribués est prometteuse, mais les défis financiers sont importants. Hormis tout l'aspect de l'encadrement des cryptomonnaies et des produits dérivés, il y a l'enjeu financier à proprement parler en espèces sonnantes. On réfère ici au coût initial de conversion d'un système centralisé déjà en place et fonctionnel à un système décentralisé. Et comme pour toute nouvelle technologie, le rendement ou « retour sur l'investissement » est encore incertain. Certaines étapes de maturation doivent donc être franchies pour déclencher des investissements massifs.

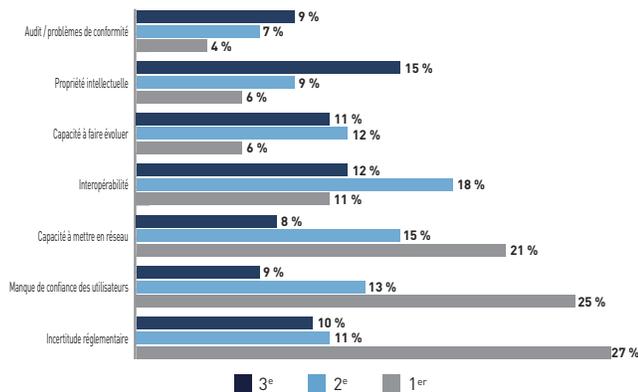
Standardisation et interopérabilité : Étant une technologie ayant des répercussions à l'échelle mondiale, les registres distribués retiennent l'attention des administrateurs des structures de régulation comme l'ISO. Les normes ISO/TC 307 pour les technologies de registres distribués sont en développement. Cependant, il y a plusieurs questions qui se posent au sujet des données qui doivent être enregistrées, telles leur provenance, leur nature, leur source. Afin de répondre à ces enjeux, une certaine standardisation des registres distribués devra être implantée de telle sorte que l'adoption de pratiques communes facilitera la participation à des chaînes de blocs, facilitera l'interopérabilité entre les registres distribués à travers le monde et stimulera le développement d'applications d'usage général.

Talents et connaissances : Les registres distribués sont en pleine effervescence, et cela, dans une ère de bouillonnement technologique où plusieurs filons en émergence, comme l'intelligence artificielle, aspirent les talents. La disponibilité de main-d'œuvre compétente dans les chaînes de blocs et l'existence, en amont, de programmes de formation adaptés aux besoins de cette nouvelle industrie, sont des enjeux opérationnels de première importance partout dans le monde.

Recherche : La technologie des chaînes de blocs n'a qu'une dizaine d'années. Si son potentiel transformateur est généralement admis, le développement de ce potentiel repose encore sur la recherche fondamentale, notamment en cryptographie, et la recherche appliquée, particulièrement en matière d'interopérabilité et d'efficacité. Parmi les aspects importants de la recherche universitaire figure aussi le développement de nouveaux algorithmes de consensus, réduisant grandement la demande énergétique qui devient alors comparable à ce qui est utilisé par des fournisseurs infonuagiques. Ces nouveaux systèmes seront donc mieux adaptés à des applications à grande échelle du secteur public.

Ces différents défis opérationnels sont d'ailleurs parmi les premiers facteurs évoqués lorsque les dirigeants d'entreprises sont appelés à s'exprimer sur les obstacles à l'adoption de la technologie des chaînes de blocs.

Figure 14 – Principaux obstacles à l'utilisation des chaînes de blocs



Source: PwC, septembre 2018
Extraction réalisée par l'Université McGill sur le site *Statistica*

L'enjeu énergétique

Les chaînes de blocs ont eu mauvaise presse à cause du caractère énergivore du processus de minage. Précisons ici qu'il existe d'autres règles de consensus qui nécessitent très peu d'énergie. Il est toutefois incontestable que, dans le cas de Bitcoin et des cryptomonnaies en général, les

exploitants de nœuds sont lancés dans une course perpétuelle à la puissance informatique afin de réaliser les opérations de minage le plus vite possible et de toucher la rétribution associée à la validation d'une transaction.

En 2014, un chercheur réputé dans le domaine de l'énergie, David Malone, a publié une étude-choc intitulée *Bitcoin Mining and its Energy Footprint*. Cette étude concluait de manière spectaculaire que le minage de Bitcoin consommait autant d'énergie que toute l'Irlande.

Cette affirmation peut être nuancée. Ce ne sont pas toutes les chaînes de blocs qui impliquent un processus de minage. Il existe d'autres règles de consensus. En outre, si le processus de minage commande une consommation d'énergie significative, des ordinateurs de nouvelle génération consomment 35 % moins d'énergie que les appareils précédents. Et comme toute nouvelle industrie, l'efficacité des processus est appelée à progresser rapidement.

Pour l'heure, le Québec, qui a l'atout stratégique d'une énergie renouvelable, manifeste un intérêt prudent. Après certains débats et décisions de la Régie de l'énergie, un bloc de 668 MW d'énergie a été alloué au domaine du minage des chaînes de blocs.

Extrait du communiqué¹³ de presse de la Régie de l'énergie sur sa décision du 29 avril 2019 :

« Hydro-Québec a déjà conclu des ententes avec des clients pour des abonnements pour usage cryptographique appliqué aux chaînes de blocs totalisant 158 MW, tandis que les réseaux municipaux ont conclu des ententes totalisant 210 MW. Avec le nouveau bloc de 300 MW, **c'est donc un total de 668 MW qui est réservé à cet usage**. Ce volume pourra être révisé à la hausse selon les besoins dans le cadre de l'examen des dossiers tarifaires. Pour le moment, la Régie juge qu'il est prudent de limiter l'énergie dédiée à cet usage, ce qui permet d'atteindre un équilibre entre les besoins individuels et collectifs, notamment en raison de l'importance de la demande, de la nécessité de procéder à de nouveaux achats en énergie et en puissance pour y répondre et de la nature incertaine de cette nouvelle industrie. »

13 « La Régie de l'énergie rend sa décision relative à la demande de fixation de tarifs et conditions de service pour l'usage cryptographique appliqué aux chaînes de blocs », communiqué de presse, 20 avril 2019 [www.newswire.ca/fr/news-releases/la-regie-de-l-energie-rend-sa-decision-relative-a-la-demande-de-fixation-de-tarifs-et-conditions-de-service-pour-l-usage-cryptographique-applique-aux-chaines-de-blocs-826345895.html].

3. LES REGISTRES DISTRIBUÉS ET LES CHÂÎNES DE BLOCS AU CANADA ET AU QUÉBEC

3.1 Aperçu de l'écosystème canadien

La Chamber of Digital Commerce of Canada a rendu public en octobre 2019 une enquête¹⁴ pancanadienne visant à mesurer l'écosystème des acteurs associés aux chaînes de blocs au Canada. L'enquête a été menée par des sondages en ligne effectués auprès d'institutions universitaires, de gouvernements, d'organismes de réglementation, d'entreprises privées, de sociétés de services professionnels et d'investisseurs.

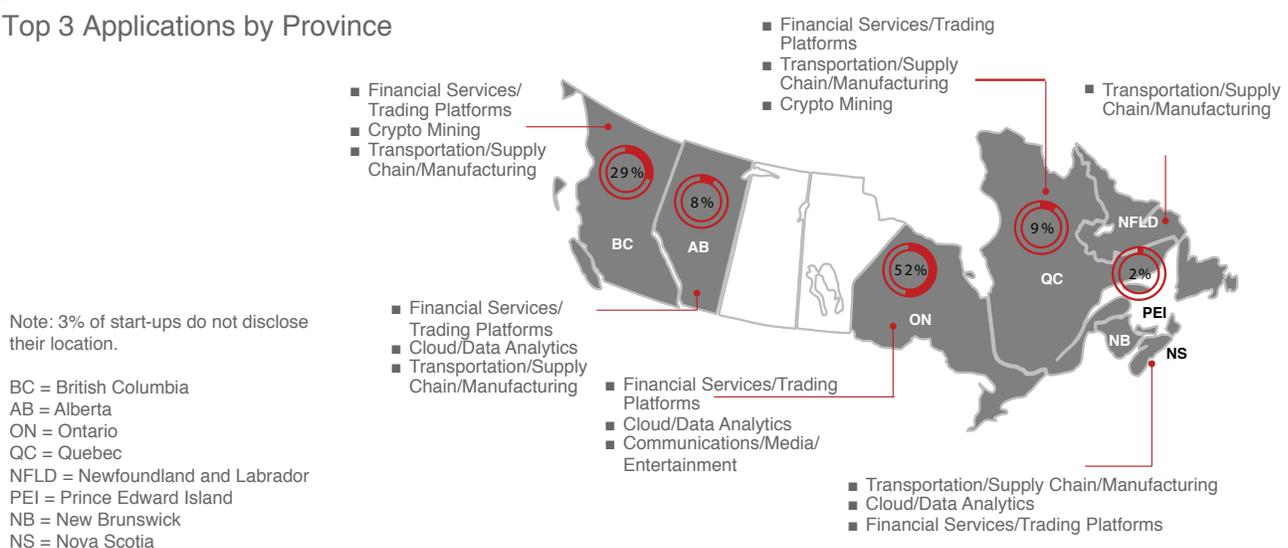
Il en ressort que l'industrie, bien que naissante, est présente à travers le Canada avec plus de 400 entreprises (excluant les entreprises en démarrage) qui utilisent déjà les technologies de chaînes de blocs pour développer des propositions de valeur. Pour l'heure, l'industrie canadienne concentre plus de 80 % de ses acteurs en Ontario et en Colombie-Britannique; le Québec et l'Alberta semblent encore loin derrière, mais seraient en progression rapide.

Toujours selon cette enquête de la Chamber of Digital Commerce, les dépenses au Canada en matière de chaînes de blocs devraient augmenter de façon exponentielle, passant de 72 millions US\$ en 2019 à 644 millions US\$ en 2023. Le domaine des chaînes de blocs offre un salaire moyen de 98 423 \$ au Canada, soit près du double de la moyenne des salaires versés au pays.

Les répondants à l'enquête ont estimé, dans une proportion de 60 %, que l'écosystème canadien de la chaîne de blocs avait besoin de soutien pour se développer; les questions juridiques et réglementaires (39 %) et les lacunes dans le financement (35 %) ont été citées comme les deux principaux défis.

Figure 15 – L'écosystème canadien de la chaîne de blocs, répartition par province

Top 3 Applications by Province



Source : *Canadian Blockchain Census 2019*, Chamber of Digital Commerce, octobre 2019, p. 11

¹⁴ *Canadian Blockchain Census 2019*, Chamber of Digital Commerce, octobre 2019, p. 11 [digitalchamber.org/wp-content/uploads/2019/10/Blockchain-Census_FINAL-Oct4-8.28.pdf].

Le gouvernement du Canada se positionne

Si plusieurs pays et États américains ont déjà amorcé un encadrement juridique de la technologie des registres distribués, le gouvernement canadien, sans aller jusqu'à la loi, a posé un premier geste visant à promouvoir l'expérimentation des chaînes de blocs.

Le 2 août 2019, le gouvernement fédéral a lancé sa nouvelle Politique sur les services et le numérique. Le communiqué¹⁵ de presse alors émis disait notamment ceci : « En modernisant les activités gouvernementales et en améliorant notre capacité d'innover et de mettre à l'essai de nouvelles technologies et solutions, comme l'intelligence artificielle et la chaîne de blocs, la politique permettra aux Canadiens d'avoir accès à des services gouvernementaux de qualité faciles à utiliser, sécurisés et, surtout, conçus pour les gens qui les utilisent. »

La Banque du Canada expérimente le concept

En outre, des institutions fédérales de premier plan sont déjà engagées dans des initiatives reposant sur la technologie des chaînes de blocs.

La Banque du Canada, par exemple, en est à la phase III de son projet appelé Jasper. Le projet est ainsi présenté sur le site Web de la Banque du Canada¹⁶ :

Jasper est un projet de recherche collaboratif mené par des acteurs des secteurs public et privé pour comprendre de quelle manière la technologie des registres distribués pourrait transformer le système de paiement de gros. Pendant les phases 1 et 2, le projet visait à étudier la compensation et le règlement des paiements interbancaires de grande valeur au moyen d'un grand livre partagé. La phase 3 portait sur les avantages qu'il pourrait y avoir à intégrer à ce « registre décentralisé avec espèces » d'autres actifs, par exemple des devises ou des titres.

De concert avec Paiements Canada et le Groupe TMX, la Banque étudie une solution qui repose sur la technologie du grand livre partagé pour créer un système de règlement de titres en monnaie de banque centrale.

La Banque et Paiements Canada se sont également associés à l'Autorité monétaire de Singapour et à la Banque d'Angleterre pour travailler à un système de règlement transfrontalier et multidevise. Cette collaboration, qui combine le projet Jasper et le projet Ubin de l'Autorité monétaire de Singapour, a pour but de se servir de la technologie du grand livre partagé pour accélérer les paiements transfrontières et en réduire le coût.

15 « La ministre Murray annonce la publication de la nouvelle Politique sur les services et le numérique, ce qui renforce notre engagement en matière de gouvernement numérique », communiqué de presse, 2 août 2019 [www.canada.ca/fr/secretariat-conseil-tresor/nouvelles/2019/08/la-ministre-murray-annonce-la-publication-de-la-nouvelle-politique-sur-les-services-et-le-numerique-ce-qui-renforce-notre-engagement-en-matiere-de-.html].

16 « Expériences et projets liés aux technologies financières », site Web de la Banque du Canada [www.banqueducanada.ca/recherches/monnaies-electroniques-et-technologies-financieres/experiences-et-projets-lies-aux-technologies-financieres].



3.2 Québec et les registres distribués

La communauté technologique et universitaire du Québec est déjà bien engagée dans la révolution des registres distribués. Des dizaines d'entreprises en démarrage reposant sur cette technologie fourmillent dans plusieurs régions. Les universités développent des programmes de recherche. Des investisseurs sont à l'affût des occasions favorables. Le mouvement est certes naissant, mais bien réel.

Portrait de l'écosystème québécois

Dans le cadre de ce livre blanc, l'Institut de gouvernance numérique a tenu à réaliser un premier portrait de l'écosystème québécois des acteurs oeuvrant dans des domaines liés aux registres distribués et aux chaînes de blocs en particulier. L'exercice a été effectué par l'entremise de recherches sur le Web, d'entrevues avec des experts et des entrepreneurs et de sondages ciblés sur les réseaux sociaux. L'ensemble des informations a par la suite été classé en s'inspirant d'exercices semblables menés dans d'autres pays, afin de faciliter des comparaisons. Ainsi, 14 catégories ont été retenues afin d'obtenir un portrait le plus juste possible et éventuellement de créer un répertoire.

Il faut voir ce portrait comme une image arrêtée tirée d'un film d'action. Le domaine évolue rapidement. Chose certaine, ce portrait d'une réalité en mouvement révèle la présence d'un nombre significatif de joueurs, d'une grande variété d'acteurs et de l'émergence d'un véritable filon économique allant de la recherche au capital de risque.

Le développement de l'écosystème est encore embryonnaire. Après quelques avancées précoces menées par des pionniers du Bitcoin, notamment, regroupés autour de l'Académie Bitcoin et de la compagnie Blockstream, ce sont surtout les firmes légales, les cryptomineurs et le domaine de la technologie financière (*fintech*) qui ont porté le développement depuis 2015.

Le Québec a très peu produit de financements à succès lors de la folle période des ICOs en 2017 et 2018. Depuis, se développe organiquement, un écosystème assez varié, gravitant autour du noyau des populaires rencontres d'intérêt (*meetups*) Ethereum. L'écosystème québécois compte ainsi plus de 150 organisations.

Figure 16 – Représentation de l'écosystème québécois des registres distribués



Organisations québécoises et leurs projets

Nous avons rassemblé quelques exemples d'organisations québécoises ou actives au Québec pour donner un aperçu du type de projets et une idée du nombre de secteurs d'activité où la technologie peut être utile.

SERVICES FINANCIERS	
Entreprise	Objet
Banque Nationale du Canada (BNC)	La BNC a testé la chaîne de blocs pour l'émission de la dette. À l'heure actuelle, Quorum-Ethereum de J.P. Morgan est utilisé comme réseau de base. Quorum est une version d'entreprise d'Ethereum avec des protocoles de sécurité supplémentaires pour parer toute forme de cyberattaque. L'entreprise travaille également sur d'autres projets comme un canal sécurisé pour les industries de la chaîne d'approvisionnement.
Aon	La division de réassurance d'Aon et celle de Guy Carpenter ont conclu un partenariat avec la firme technologique The Institutes RiskStream afin de numériser leurs transactions dans le but d'améliorer l'efficacité du processus de placement de risques en réassurance. En utilisant un système de registre distribué, les réassureurs pourront profiter d'un flux simplifié et d'une meilleure vérification des données, notamment, afin de réduire les coûts à travers le marché ¹⁷ .

ARTS ET LA CULTURE	
Entreprise	Objet
Office national du film du Canada (ONF)	L'ONF teste des solutions de type chaîne de blocs pour la distribution d'une dizaine de titres avec une formule de récompense des utilisateurs. Le concept pourrait permettre d'améliorer la diffusion de certaines œuvres ¹⁸ .
Copibec – Scenarex	Pour développer une solution automatisée dans la gestion du droit d'auteurs et de reproduction à destination des entreprises, Copibec signe un accord avec Scenarex. La société montréalaise fournira ainsi une solution basée sur les outils de chaîne de blocs qui protégera les droits des auteurs et facilitera l'encaissement de leurs revenus. La chaîne de blocs mise en œuvre a été rebaptisée Bookchain, et ne repose pas sur le recours à une cryptomonnaie ¹⁹ .
Smartsplit	Soutenu financièrement par le <i>Conseil des arts du Canada</i> et entouré d'une vingtaine d'acteurs clés du milieu québécois de la musique, ce projet développé en code source ouvert sur Ethereum (une blockchain publique) vise à explorer les possibilités des contrats intelligents, notamment dans le partage des droits et des revenus entre les ayants droit.

17 « Des réassureurs veulent numériser leurs transactions », portail-assurance.ca, 21 mai 2019

[journal-assurance.ca/article/des-reassureurs-veulent-numeriser-leurs-transactions]

18 « En Inde, l'accès au cinéma passe par la blockchain », Catherine Mathys, 13 juin 2019, trends.cmf-fmc.ca

[trends.cmf-fmc.ca/fr/en-inde-laces-au-cinema-passe-par-la-blockchain].

19 « Gestion collective : au Québec, Copibec opte pour la blockchain, avec Bookchain », Clément Solym, 26 février 2019, actualitte.com

[www.actualitte.com/article/monde-edition/gestion-collective-au-quebec-copibec-opte-pour-la-blockchain-avec-bookchain/93539].

GESTION DES IDENTITÉS	
Entreprise	Objet
Transport Canada et Accenture Canada	Blockchain Accenture teste une solution d'identification numérique et biométrique des passeports avec des voyageurs au Canada et aux Pays-Bas ayant les caractéristiques de la chaîne de blocs. Les Pays-Bas participeront activement au projet-pilote. De nombreux partenaires, comme le département de la Sécurité intérieure des États-Unis, l'Agence nationale de lutte contre la criminalité du Royaume-Uni, Interpol, Google et Visa, se sont également joints au projet. Le système permettra aux voyageurs de transmettre leurs renseignements aux gouvernements et aux fournisseurs de voyages à l'aide d'appareils mobiles personnels. En simplifiant et en accélérant les procédures aéroportuaires pour les voyageurs dignes de confiance, les autorités veulent concentrer davantage de temps et d'énergie à vérifier les informations des voyageurs qui présentent des risques. Ce projet devrait également aider les autorités à faire face à un flux de voyageurs en croissance constante ²⁰ .
DigiHub Shawinigan	Un projet-pilote de cryptopass, lancé par un consortium d'entreprises du DigiHub Shawinigan, est en discussion avec l'écosystème de Sophia Antipolis en France. La cryptopass en question fait office de contrat auto-exécutant et facilitera l'entrée au pays de travailleurs immigrants, en permettant de les diriger au bon endroit pour rendre leur parcours plus efficace ²¹ .

TRANSPORT ET LOGISTIQUE	
Entreprise	Objet
Port de Montréal	TradeLens est une solution chaîne de blocs développée conjointement par Maersk, société de transport maritime, et IBM. TradeLens devrait permettre au port de Montréal d'améliorer le niveau de précision des différentes opérations et du trafic. Le port de Montréal traite à lui seul plus de 38 tonnes métriques de marchandises chaque année ²² .
Eva (taxi)	Application pour le taxi à Montréal basée sur la chaîne de blocs. La coopérative Eva offre une application aussi rapide et conviviale qu'une application centralisée. L'application décentralisée offre la même expérience que toutes les applications de covoiturage traditionnelles, mais avec les coûts et les avantages de la décentralisation ²³ .
Choco4Peace	Choco4Peace, basé à Montréal et en Colombie, vise l'autonomisation des petits exploitants qui sont prêts à délaissier la production de cocaïne pour celle du cacao <i>fino de aroma</i> . Des contrats auto-exécutants de chaîne de blocs permettent de créer un réseau économique décentralisé et inclusif (REDI). Ce réseau agrège les agriculteurs de cacao avec les parties prenantes dans l'industrie, permettant aux entrepreneurs d'accéder aux marchés équitables, à de l'investissement, à l'assurance et à la technologie ²⁴ .

AGRICULTURE	
Entreprise	Objet
Agri-Traçabilité Québec et Epsilia	Agri-Traçabilité Québec travaille sur un projet faisant appel à la technologie des chaînes de blocs pour la traçabilité du bœuf. Le projet est développé en collaboration avec Bœuf du Québec et la société Epsilla ²⁵ .

20 « Identité numérique : une nouvelle technologie mise à l'essai dans les aéroports », Agence QMI, 28 janvier 2018, sur tvanouvelles.ca [www.tvanouvelles.ca/2018/01/28/identite-numerique-une-nouvelle-technologie-mise-a-lessai-dans-les-aeroports-1].

21 « Un autre allié pour DigiHub », L'Hebdo du St-Maurice, 31 mai 2019 [www.lhebdodustmaurice.com/un-autre-allie-pour-le-digihub].

22 « Le port de Montréal choisit une solution blockchain », David Nathan, 29 octobre 2018, cryptonews.fr [fr.cryptonews.com/news/le-port-de-montreal-choisit-une-solution-blockchain-2214.htm].

23 [eva.coop].

24 [choco4peace.org].

25 « L'intégration de la blockchain à la traçabilité : une technologie à l'épreuve complète des fraudes informatiques », Bernard Gauthier, agri-tracabilite.qc.ca, février-mars 2018

[www.agri-tracabilite.qc.ca/images/stories/Actualits/mci_magazine_-_L'integration_de_la_blockchain_à_la_traçabilité_février-mars_2018.pdf].

DIVERTISSEMENT	
Entreprise	Objet
DigiHub-PicksVenture et Deloitte	La chaîne de blocs dans le jeu vidéo. Ce partenariat vise à créer un nouveau studio de jeux vidéo qui utilisera et intégrera la technologie de chaîne de blocs. L'entreprise sera basée dans le DigiHub de Shawinigan ²⁶ .

CHAÎNE DE BLOCS SUR MESURE (BLOCKCHAIN AS A SERVICE)	
Entreprise	Objet
Hydralab	Hydralab fournit son service Hydra Network afin d'offrir des solutions sur mesure en matière de chaîne de blocs aux entreprises le désirant. Ces projets portent notamment sur le vote électronique, les consentements numériques, les assurances ou la traçabilité des chaînes de production ²⁷ .

ÉMISSION DE JETONS (ICO)	
Entreprise	Objet
Cycle Montréal	Cycle Montréal est un projet visant à donner une seconde vie à des produits divers, en les échangeant contre des jetons de cryptomonnaie permettant de les échanger contre un autre bien ou une autre monnaie numérique ²⁸ .

Catégories et joueurs clés

Dans cette section, nous avons tenté de regrouper par catégorie les entreprises de l'écosystème québécois. C'est, modestement, le premier répertoire du genre au Québec.

1. Formation :

Il s'agit des intervenants qui offrent des services de formation à propos des registres distribués au sens large, ainsi que des domaines connexes à cette technologie (cryptomonnaies, gestion d'un portefeuille cryptographique, programmation d'une chaîne de blocs, etc.) Les intervenants de cette catégorie se divisent en deux groupes principaux : les institutions d'enseignement et certaines entreprises privées.

FORMATION – Environ 15 acteurs au Québec dont...

- L'École de technologie supérieure, les HEC Montréal, l'Université McGill, l'Université de Montréal, l'Université Concordia et l'Université Laval;
- Le Cégep du Vieux Montréal, le Collège régional Champlain à Saint-Lambert et le Collège Bois de Boulogne;
- Blockchain Guru, Communautique, Formations Sarobas, HydraLab, Nuvoola, QB Solutions et Québec Blockchain.

2. Recherche fondamentale et appliquée :

Cette catégorie regroupe les chercheurs associés à des universités tournés vers la progression de la science et les connaissances générales, ainsi que des intervenants du secteur privé plutôt présents dans des sphères plus économiques et entrepreneuriales.

RECHERCHE FONDAMENTALE ET ADAPTÉE – Environ 7 acteurs au Québec

- L'École de technologies supérieures (Laboratoire FUSÉE), l'Université Concordia (Chaire de recherche industrielle CRSNG / Raymond Chabot Grant Thornton / Catallaxy en technologies blockchain), l'Université de Montréal (CIRRELT, Network Research Lab), l'Université du Québec à Chicoutimi, l'Université du Québec à Rimouski (Fintech Lab), l'Université Laval et HydraLab.

²⁶ « La technologie blockchain au DigiHub, » Vincent Mongrain, *Le Nouvelliste*, 12 décembre 2017

[www.lenouvelliste.ca/affaires/la-technologie-blockchain-au-digihub-d67042e60040c3b41a1234d78ed13818]

²⁷ <http://www.hydralab.io/en>.

²⁸ « Une monnaie numérique montréalaise en attendant celle de Facebook », Alain McKenna, *lesaffaires.com*, 20 juin 2019

[www.lesaffaires.com/blogues/alain-mckenna/une-monnaie-numerique-montrealaise-en-attendant-celle-de-facebook/611073].

3. Services professionnels :

Il s'agit de consultants en services professionnels. La grande majorité d'entre eux ne sont pas spécialisés dans les registres distribués, mais comptent un ou des professionnels de leur équipe qui ont une expertise ou une connaissance générale dans ce domaine. Ils peuvent notamment offrir des conseils sur le plan de la comptabilité générale, des exigences réglementaires liées au démarrage d'entreprise ou encore de l'encadrement des « *Initial Coin Offerings* » (ICO).

SERVICES PROFESSIONNELS –

Environ 20 acteurs au Québec dont...

- Des cabinets d'avocats tels que Borden Ladner Gervais (BLG), BCF Avocats d'affaires, Canada Bitcoin Law, Fasken, Gowling WLG, Langlois Avocats, Lavery Avocats, McCarthy Tétrault, McMillan LLP, Miller Thomson LLP, MLS Legal, Dentons, Holmsted & Associés s.e.n.c.r.l, Stikeman Elliott LLP et ROBIC;
- Des cabinets comptables tels que Deloitte, EY, KPMG, PwC et Raymond Chabot Grant Thornton.

4. Consultation et développement de projets :

Il s'agit des intervenants qui ont la vocation d'assister et de faciliter l'implantation et le développement des entreprises et projets qui intègrent la technologie. Il s'agit d'intervenants qui agissent sur le plan du développement et de l'optimisation des modèles d'affaires des entreprises; certains de ces acteurs interviennent presque exclusivement dans le domaine de la chaîne de blocs.

DÉVELOPPEMENT DE PROJETS –

Environ 25 acteurs au Québec dont...

- Des entreprises en technologie de l'information telles que CGI, Cofomo, SAP, Levio, Novipro, Arche Innovation, Blockchain Guru, ChainDigit, HydraLab, Planaxis / Talan, Savoir-faire Linux et SIA Innovations;
- Des organismes régionaux tels que le Quartier de l'innovation Montréal, Québec Blockchain, Blockchain Hub, Cryptopôle Shawinigan, DigiHub Shawinigan et Hub Saguenay-Lac-Saint-Jean et Innopôle Sherbrooke;
- Des entreprises spécialisées dans divers domaines telles que Catallaxy (RCGT), Accuracy, Badel Media, IPtoki, Picks Ventures, Rokaboat.

5. Développement de solutions technologiques :

Ce sont les acteurs qui se concentrent dans la programmation, dans la conception et le développement de logiciels d'implantation, dans l'offre et la distribution d'interfaces de programmation (API), etc. Il s'agit du développement purement technologique des registres distribués.

DÉVELOPPEMENT DE SOLUTIONS TECHNOLOGIQUES –

Environ 20 acteurs au Québec dont...

- Blockchain Guru, Catallaxy, ChainDigit, HydraLab, IPtoki, Picks Ventures, Planaxis / Talan, SAP et SIA Innovations, Blockstream corporation, Copibec, dfuse, Inmind Technologies, Mantle Technology, Nebula AI, Nuvoola, Optik 360, OSEDEA, Projet Artigas, Scenarex, Smartsplit.

6. Technologies financières (*fintech*) :

Il s'agit d'une catégorie qui, de manière générale, est plus large que l'utilisation des registres distribués, étant donné qu'elle englobe toutes les innovations technologiques qui cherchent à transformer le domaine financier. Cependant, dans les dernières années, notamment en raison de l'émergence des cryptomonnaies, de plus en plus d'acteurs du domaine financier ont réalisé l'impact considérable des registres distribués dans la technologie financière et explorent les possibilités qui s'offrent à eux.

TECHNOLOGIE FINANCIÈRE –

Environ 6 acteurs Québec

- Banque Nationale du Canada, Brainfinance, Fintech Cadence, Impak finance, Transledger, XeoHive

7. Investissements :

Il s'agit des entreprises qui injectent des fonds capitaux dans les projets avec les registres distribués pour faciliter leur déploiement et leur succès, ainsi que les gestionnaires de portefeuilles. Ces intervenants ont confiance en l'émergence des registres distribués et cherchent à tirer profit de la croissance de cette industrie.

INVESTISSEMENT –

Environ 3 acteurs au Québec

- Fonds Rivemont Crypto, Inception Block Ventures, Real ventures.

8. Gouvernance et gestion des identités :

Il s'agit des intervenants liés au domaine de la sécurité des données et de la gestion identitaire. Cependant, il y a encore certaines contraintes techniques associées à ces concepts, ce qui explique qu'il y a, du moins pour l'instant, très peu d'intervenants dans cette catégorie au Québec.

SÉCURITÉ ET GESTION DES IDENTITÉS –

Environ 3 acteurs au Québec

- Artigas, Blockchain Citiz, Qohash.

9. Infrastructures :

Il s'agit des intervenants qui bénéficient des registres distribués en l'intégrant à leur infrastructure opérationnelle, ou encore qui en tirent profit pour optimiser et faciliter certains aspects de leurs affaires. Près de la moitié des intervenants de cette catégorie se servent de cette technologie pour faciliter la traçabilité de produits. Cette catégorie permet donc d'avoir un bon aperçu des applications potentielles des registres distribués, en dehors des créneaux plus connus comme les technologies financières et les cryptomonnaies.

INFRASTRUCTURES ET LOGISTIQUE –

Environ 8 acteurs au Québec

- A-Malgam, Canadian Blockchain Supply Chain Association (CBSCA), Choco4Peace, Cryptothermie, EVA Coop, Optel, Port de Montréal, Hydro Network.

10. Médias/communications :

Il s'agit des intervenants qui sont dans le monde des médias et des communications, et qui ont une relation avec les registres distribués et ses applications. Il peut s'agir de médias traditionnels ou d'intervenants spécialisés dans ce domaine qui diffusent de l'information à propos de la technologie et leurs applications.

MÉDIAS ET COMMUNICATIONS –

Environ 9 acteurs au Québec

- *Cryptofacile.ca*, *Cryptonews*, *Crypto.Québec*, *Journal Le Métro*, *Revue H*, *Mine de rien* (blogue) *Les Affaires*, *Pensez Blockchain*, *Blockchain Hub Québec*, *Un bloc à la fois* (blogue).

11. Audit et vérification sur la chaîne de blocs :

Il s'agit des intervenants qui offrent des services spécialisés en matière d'audit et de vérification d'actifs numériques, souvent associés aux registres distribués. Compte tenu de l'effervescence nouvelle associée au domaine numérique et aux registres distribués, de plus en plus d'entités ont des actifs numériques, notamment des cryptomonnaies.

AUDIT ET VÉRIFICATION –

Environ 6 acteurs au Québec

- Catallaxy, CoinLevy, Crypto Impôts, EZ Ledger, Raymond Chabot Grant Thornton, Waltio.

12. Cryptomonnaies :

Il y aurait actuellement plus de 2 400 cryptomonnaies dans le monde. Elles sont encore très présentes dans l'esprit collectif associé aux chaînes de blocs, ainsi que dans le développement entrepreneurial.

CRYPTOMONNAIES –

Environ 15 acteurs au Québec

- Académie Bitcoin, Bylls / Satoshi Portal, Bit-cluster, Blockstream corporation, Consensus, D-Central Tech, DigiBit Consulting, EOS Nation, Grin, Instacoin, Octonomics, Shakepay, Solutions technologiques MyWoom, Veriphi, Yap.

13. Cryptominage :

Intimement reliés à la catégorie des cryptomonnaies, ces intervenants valident les transactions dans la chaîne de blocs d'une cryptomonnaie, et par le fait même contribuent à l'émission de nouvelles unités de cette cryptomonnaie. Nous retrouvons dans cette catégorie les intervenants du domaine de l'énergie, responsables de gérer les enjeux associés à la consommation d'énergie inhérente aux opérations de cryptominage.

CRYPTOMINAGE –

Environ 10 acteurs au Québec

- Bitfarms, D-Central Tech, Dynamine, Floxis, Inominers, Mining Cave, Nuvoo mining, Picks Ventures, Québec mining corporation, Ubimust.

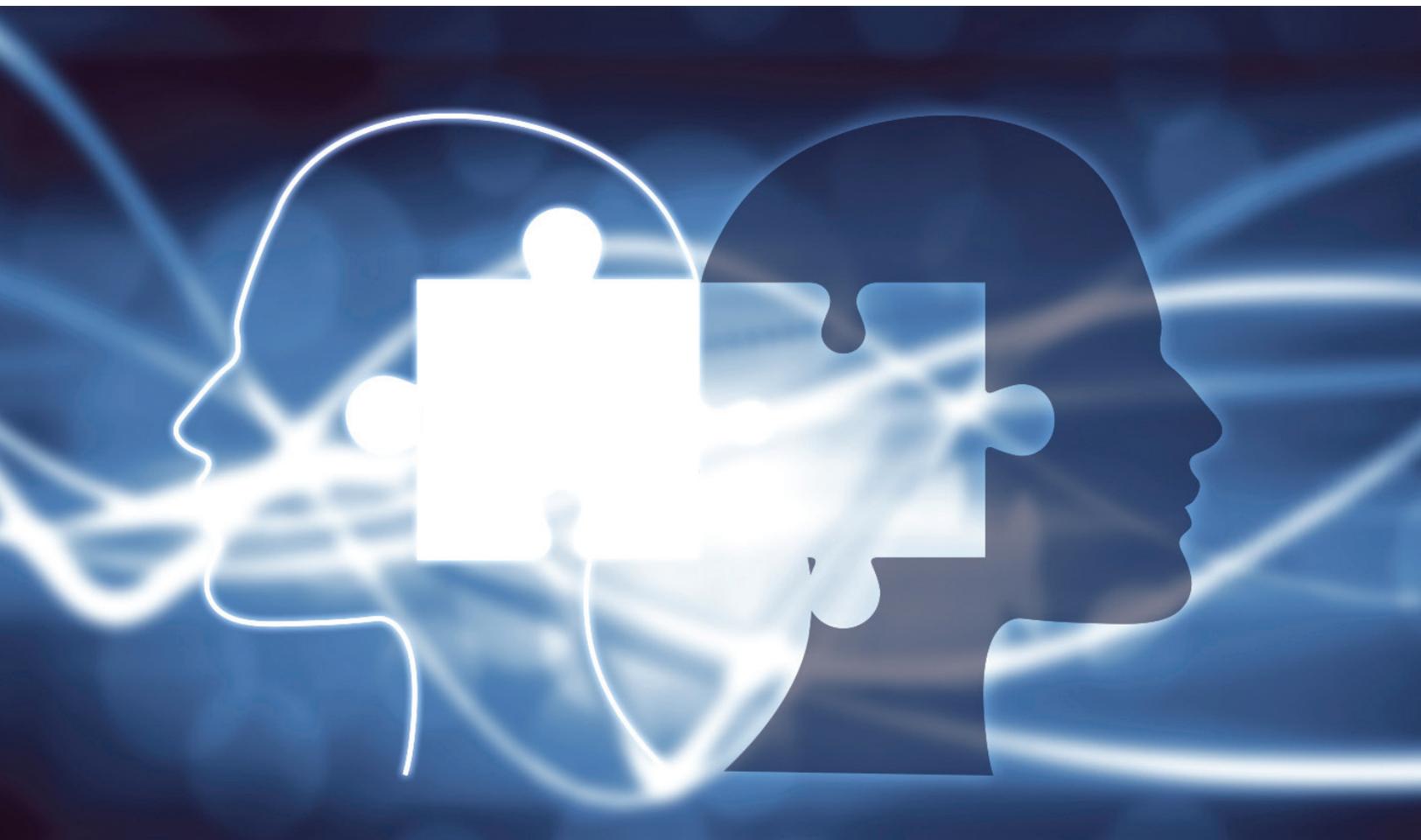
14. Autres :

Malgré nos efforts, ce ne sont pas tous les intervenants qui ont pu être intégrés dans l'une ou l'autre des catégories précédentes. Pour certains, c'est en raison de la nature hautement spécifique de leurs activités, qui ne cadre pas avec les paramètres généraux des autres catégories. Pour d'autres, il s'agit plutôt d'un manque d'information à propos de la nature de leurs activités.

AUTRES –

Environ 11 acteurs

- Blockchain Montréal, GPU.One, Indominus Inc, Kelvin Emtech, krypto.ai, Nash Agency, N-Gage Studio, Technologies Hashing & Beyond, VIA Science, Hydro Québec et Hydro-Sherbrooke.



Forces, faiblesses, menaces et opportunités de l'écosystème québécois

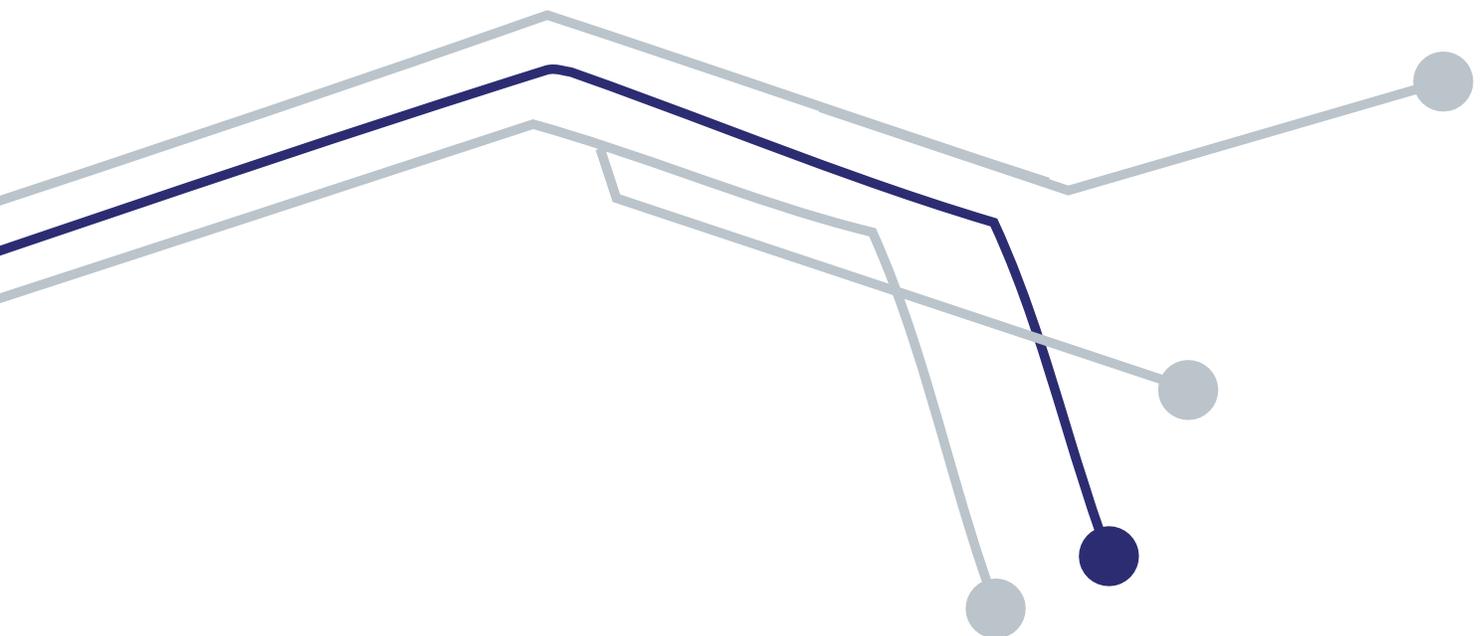
L'écosystème québécois est naissant, mais déjà bien diversifié avec des ramifications nombreuses qui favorisent un réel potentiel en maturation. Évidemment, il reste beaucoup à faire pour concrétiser ce potentiel, saisir les occasions et combler les lacunes. Les tableaux suivants proposent une vue qualitative de cet écosystème sous l'angle des forces, faiblesses, menaces et opportunités.

Figure 17 – Tableau synthèse des forces et faiblesses de l'écosystème québécois

Forces	Faiblesses
<p>Talents et connaissances</p> <ul style="list-style-type: none"> • Capacités de recherche fondamentale et appliquée dans plusieurs institutions d'enseignement supérieur • Bassin de talents dans les technologies de l'information et de l'intelligence artificielle 	<p>Talents et connaissances</p> <ul style="list-style-type: none"> • Absence de recherche prospective sur les risques de perturbations par secteur ou domaines d'activité • Manque de main-d'œuvre formée par rapport aux besoins des entreprises • Manque de formation de niveau universitaire ou menant à des certifications reconnues • Peu de projets de recherche sur les algorithmes de consensus et sur les autres implications, notamment juridiques, de la technologie • Peu de projets de collaboration interdisciplinaires dans les universités
<p>Structure / Capacités</p> <ul style="list-style-type: none"> • Grappes ou écosystèmes existants dans les domaines des technologies de l'information et en intelligence artificielle • Présence de plusieurs firmes dans le domaine des services juridiques • Émergence d'un tissu actif et innovant d'entreprises en démarrage • Intérêt émergent par différents groupes ou organisations envers la technologie • Surplus en énergie hydroélectrique verte et prix de l'énergie très compétitif • Plusieurs projets de collaboration entre les institutions d'enseignement supérieur et les entreprises dans divers domaines • Expertise de pointe en technologie financière à la bourse de Montréal 	<p>Structure / Capacités</p> <ul style="list-style-type: none"> • Peu d'acteurs offrant des services-conseils pour accompagner les organisations à toutes les phases (de bout en bout) au regard de la technologie Blockchain (c'est-à-dire positionnement stratégique, idéation, validation et implantation) • Faible présence d'acteurs spécialisés en sécurité, en gouvernance et en gestion des identités dans le domaine des registres distribués • Difficulté des acteurs à se positionner à l'échelle tant canadienne qu'internationale • Pas de référentiel sur la technologie ou de répertoire des acteurs • Peu de collaboration ou de mise en commun des expertises publiques et privées • Déficit de coopération entre les entreprises en démarrage et les grandes entreprises, par rapport à ce qui existe aux États-Unis
<p>Financement</p> <ul style="list-style-type: none"> • Présence et intérêt de quelques fonds d'investissement en capital de risque 	<p>Financement</p> <ul style="list-style-type: none"> • Peu de soutien financier à la réalisation de l'ensemble des phases de développement jusqu'à l'implantation ou au déploiement commercial • Peu de programmes ou de mesures pour les dépenses qui ne sont pas couvertes par les crédits d'impôt pour le développement des affaires électroniques et pour la recherche et développement telles que celles associées aux études de faisabilité, aux preuves de concepts, à l'expérimentation ainsi qu'aux frais juridiques et de coordination • Peu d'appels publics à l'investissement (ex. : ICO, IPO) • Peu de mesures permettant d'évaluer systématiquement le potentiel technologique des registres distribués dans le cadre du développement de solutions informatiques au gouvernement

Figure 18 – Tableau synthèse des menaces et opportunités de l'écosystème québécois

Menaces	Opportunités
<p>Talents et connaissances</p> <ul style="list-style-type: none"> • Exode des cerveaux dans les domaines de pointe telles la technologie financière et la chaîne de blocs (le recrutement est très actif à l'échelle internationale et les conditions sont alléchantes) • Expertises et talents provenant de l'extérieur du Québec et offrant leurs services en mode imparti (en provenance de nombreux pays ayant développé ces expertises : Inde, Pologne, Ukraine, etc.) 	<p>Talents et connaissances</p> <ul style="list-style-type: none"> • Gestion des identités et de la sécurité des informations personnelles tant dans le secteur public que dans le secteur privé • Vote électronique • Gouvernance décentralisée des organisations
<p>Structure / Capacités</p> <ul style="list-style-type: none"> • Risques de perturbations à la suite du déploiement de solutions développées à l'extérieur du Québec 	<p>Structure / Capacités</p> <ul style="list-style-type: none"> • Capacités de minage avec retombées économiques locales • Gestion des données en matière de santé • Intégration de la chaîne de blocs dans les jeux interactifs • Médias et propriété intellectuelle • Développement d'un réseau d'expertises croisées avec les grappes des technologies de l'information et de l'intelligence artificielle
<p>Financement</p> <ul style="list-style-type: none"> • Faible volume d'investissement au Québec 	<p>Financement</p> <ul style="list-style-type: none"> • Milieu favorable aux investissements en R et D pour les entreprises • Milieu favorable aux appels publics à l'investissement en R et D



4. GOUVERNANCE – CHANTIERS STRATÉGIQUES

Dans ce dernier chapitre, nous allons tenter de cerner comment le Québec peut contribuer par ses politiques publiques au développement de l'écosystème des registres distribués, et comment l'État québécois lui-même pourrait mettre à profit le potentiel de la technologie pour bonifier nos institutions démocratiques.

4.1 Deux portes d'entrée principales à court terme

De prime abord, l'État québécois peut s'appuyer sur deux bases pour contribuer au positionnement de l'écosystème.

- En premier lieu, la Stratégie de transformation numérique gouvernementale 2019-2023²⁹ devrait offrir l'occasion de tester l'usage de la technologie dans différents processus et structures de l'État et dans la relation avec les citoyens. Cette stratégie a pour orientation « une administration publique innovante, efficiente et transparente »; elle vise notamment à ce que « les données [soient] valorisées et redonnées aux citoyens ». Le Québec pourrait s'inspirer du gouvernement fédéral et de plusieurs États américains qui engagent leurs entités dans l'expérimentation de la technologie. Cette approche de projets pilotes permettrait de tester la technologie et de contribuer au renforcement de l'écosystème par l'établissement de partenariats porteurs entre l'État et des entreprises en démarrage de chez nous.
- En deuxième lieu, le gouvernement du Québec a lancé une réforme de la société Investissement Québec avec le Projet de loi 27³⁰ pour en faire le véritable maître d'œuvre des politiques économiques gouvernementales. Dans le cadre de cette transformation, Investissement Québec se verra accorder des moyens accrus et de nouvelles responsabilités, notamment en matière d'innovation, avec l'intégration projetée à ses activités du Centre de recherche industrielle du Québec (CRIQ). Cette priorité à l'innovation et aux nouvelles technologies devrait amener Investissement Québec à soutenir tant le développement de l'écosystème des entreprises liées aux registres distribués que des projets de transformation numérique provenant de différents horizons et faisant appel à cette technologie.

4.2 Des outils pour améliorer l'administration publique

Les registres distribués font partie des outils technologiques pouvant contribuer à la modernisation de l'État.

- Les registres distribués, rappelons-le, permettent de **certifier l'intégrité des informations** utilisées dans les processus décisionnels et de **valider l'identité des participants**, ce qui augmente la confiance dans les processus, optimise les opérations et contribue à minimiser les coûts de fonctionnement.
- L'immutabilité et l'auditabilité des données dans les registres distribués peuvent **réduire l'asymétrie de l'information**³¹ entre les parties prenantes.
- Les organisations sont en outre constituées d'un ensemble de contrats qui définissent les relations entre les parties prenantes et cristallisent les intérêts communs et les rapports de forces³². En cela, **l'utilisation de contrats** intelligents combinés aux registres distribués permet d'assurer une exécution automatique et conforme des contrats, ce qui contribue à maintenir la confiance entre les parties. Cela participe à réguler les interactions entre

²⁹ Stratégie de transformation numérique gouvernementale 2019-2023 [www.quebec.ca/gouv/politiques-orientations/transformation-numerique].

³⁰ Projet de loi n°27 : Loi concernant principalement l'organisation gouvernementale en matière d'économie et d'innovation [www.assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-27-42-1.html ?appelant=MC].

³¹ Collusion et information asymétrique, Jean-Jacques Laffont, erudit.org, diffusion numérique 9 février 2009 [www.erudit.org/fr/revues/ae/1997-v73-n4-ae2752/602242ar].

³² Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure, Michael C. Jensen, Harvard University Press, 1998, p. 9 [www.sfu.ca/~wainwrig/Econ400/jensen-meckling.pdf].

les parties tout en certifiant les processus transactionnels inhérents à des logiques contractuelles. En améliorant la transparence, le contrat intelligent peut devenir un nouveau vecteur de confiance dans les relations.

- En outre, dans une nouvelle économie dite « de l'attention », le temps de disponibilité des individus et des groupes pour s'impliquer dans des processus participatifs possède une grande valeur. Ce temps est sollicité sous tous les azimuts par des structures qui sont en concurrence pour la mobilisation de participants. L'utilisation de la technologie pourrait ici permettre de nouveaux modèles qui valorisent la participation et la relation entre les citoyens et les institutions, ou entre des clients et une entreprise³³.

Applications gouvernementales

La gouvernance numérique décentralisée repose sur trois grandes catégories d'utilisation de la technologie : l'identité numérique, les mécanismes décisionnels comme le vote numérique et les délibérations, ainsi que les dynamiques transactionnelles, qui regroupent autant l'inscription d'une information dans un registre qu'un échange de valeur ou un mécanisme d'incitatifs.

- Les **systèmes d'identités numériques**³⁴ permettent de valider l'identité des parties prenantes et de confirmer leur accès à des services gouvernementaux. Par extension, l'identité numérique reconnue par l'État permet de certifier des titres de propriété³⁵, de voter dans différents contextes, de procéder à l'approbation de l'ouverture de comptes bancaires et de répondre aux exigences administratives de différents intervenants. Les systèmes d'identité numérique utilisant la chaîne de blocs offrent aux individus des options de contrôle d'accès à leurs données³⁶ en passant par différents modèles de gestion.

✓ **Utilité : identité officielle pour tous les usages, comme un passeport numérique.**

- En tenant compte de multiples nuances³⁷ et de la nécessité d'assembler des systèmes hybrides³⁸, la chaîne de blocs ouvre la voie au **vote numérique**³⁹. Des expérimentations partielles ont eu lieu dans le cadre d'élections ou de consultations en Australie⁴⁰, en Estonie⁴¹, en Suisse⁴², en Inde⁴³, aux États-Unis⁴⁴ et en Nouvelle-Zélande⁴⁵.

✓ **Utilité : faciliter l'exercice du droit de vote, notamment pour les personnes à mobilité réduite, hausser le taux de participation électorale, réduire le coût de l'organisation des scrutins, évoluer vers une démocratie plus participative.**

33 *From Economization to Tokenization: New Forms of Economic Life On-Chain*, Francis Jervis, New York University, 28 février 2019 [papers.ssrn.com/sol3/papers.cfm?abstract_id=3344748].

34 *E-residency 2.0 White Paper, gouvernement de l'Estonie* [s3.eu-central-1.amazonaws.com/ereswhitepaper/e-Residency+2.0+white+paper+English.pdf].

35 IBM eyes Blockchain technology deal for Kenya's public records, *businessdailyafrica.com*, 15 décembre 2016 [www.businessdailyafrica.com/Corporate-News/IBM-eyes-Blockchain-technology-deal-for-Kenya-s-public-records/539550-3488120-1fk4q7z].

36 Ethereum identity system uPort working with Brazil's Ministry of Planning, Ian Allison, *ibtimes.co.uk*, 23 août 2017 [www.ibtimes.co.uk/ethereum-identity-system-uport-working-brazils-ministry-planning-1636253].

37 « Online Voting: A Path Forward for Federal Elections », site Web du gouvernement du Canada, janvier 2017 [www.canada.ca/en/democratic-institutions/services/reports/online-voting-path-forward-federal-elections.html].

38 Blockchains and Voting: Somewhere between hype and a panacea [A Position Paper], Yomna Nasser, Chidinma Okoye, Jeremy Clark, Peter Y A Ryan, users. encs.concordia.ca, [users. encs.concordia.ca/~clark/papers/draft_voting.pdf].

39 « A Study on Ways to Apply the Blockchain-based Online Voting System », Hye Ri Kim, Kyoungsik Min, Seng-phil Hong, *International Journal of Control and Automation*, 2017 [article.nadiapub.com/IJCA/vol10_no12/11.pdf].

40 « Final line-up for the new Minister's Recreational Fishing Advisory Council announced », gouvernement de South Australia, communiqué de presse, 25 mars 2019 [s3-ap-southeast-2.amazonaws.com/assets.yoursay.sa.gov.au/production/2019/03/25/03/46/57/ea46b888-1392-44ac-8069-73d0bb385f59/3-25_Whetstone_-_MRAFC_Final.pdf].

41 Estonian elections: 2014 -2015, *tivi.io*, 2015 [tivi.io/case/estonian-elections-2014-2015].

42 « "Crypto Valley" Zug to trial blockchain voting », Matthew Allen, *swissinfo.ch*, 8 juin 2018 [www.swissinfo.ch/eng/system-test_-crypto-valley--zug-to-trial-blockchain-voting/44177440].

43 « Horizon State and MiVote announce deal with Indian political party », *Micky News*, 24 août 2018 [micky.com.au/democracy-deal-horizon-state-breaks-into-india].

44 « Mobile Voting is Coming to Utah County Municipal Elections, Tusk Philanthropies », communiqué de presse, 23 juillet 2019 [www.prnewswire.com/news-releases/mobile-voting-is-coming-to-utah-county-municipal-elections-300889121.html].

45 « TOP runs NZ's first Blockchain political party election », *The Opportunities Party*, communiqué de presse, 6 novembre 2018 [www.scoop.co.nz/stories/PO1811/S00059/top-runs-nzs-first-blockchain-political-party-election.htm].

- La technologie permet des mécanismes nouveaux de consultation utilisant des systèmes de **délibération numérique** (propositions, argumentaires, amendements); une approche facilitant l'usage de données dans les prises de décisions (*data-driven decisions*) et impliquant davantage les parties civiles⁴⁶.

✓ **Utilité : amener des manières innovantes de consulter les citoyens, revitaliser la relation démocratique État-citoyen, renforcer les communautés.**

- Les registres distribués peuvent supporter la transformation des modes d'interaction entre les citoyens et l'État et la relation entre les électeurs et les élus. La certification de l'intégrité de l'information permet la traçabilité des actions gouvernementales et offre plusieurs options pour la **reddition de comptes publics**, le suivi des indicateurs de résultats, les audits, les registres publics de l'État, le suivi des affectations budgétaires, la surveillance de la chaîne d'approvisionnement et, pour améliorer **les processus d'approbation gouvernementale**, interne et externe, en évaluant l'apport des contrats intelligents dans ce domaine.

✓ **Utilité : plus grande transparence de l'État, renforcement de la confiance des citoyens dans les institutions, renforcement de la capacité de l'État d'agir pour faire respecter des normes au nom de l'intérêt public.**

Applications organisationnelles

Ces applications dans le domaine de l'État trouvent aussi leurs déclinaisons dans la vie des grandes entreprises et institutions.

1. Le vote numérique utilisant la chaîne de blocs peut servir aux membres d'une organisation, à **ses administrateurs et aux actionnaires d'une entreprise**.
2. Les systèmes de gouvernance numériques décentralisés ont le potentiel d'offrir des **mécanismes décisionnels adaptés à des partenariats multipartites**, augmentant la flexibilité organisationnelle tout en assurant une sécurité et une intégrité des informations utilisées.
3. **Les systèmes d'identité internes aux organisations**, dossiers d'employés, dossiers clients ou autres, peuvent améliorer le suivi de certaines informations, qualitatives ou quantitatives, sur l'apport d'une personne, la reconnaissance de son expertise⁴⁷, de ses compétences ou de ses formations continues.

La nécessité d'une vision globale des données au sein de l'État québécois

Les registres distribués se présentent ainsi comme de nouveaux outils technologiques qui pourront découler de la numérisation de l'État et être mis en œuvre afin de contribuer à moderniser nos institutions démocratiques.

La numérisation de l'État québécois est donc la clé de voûte permettant d'accéder au potentiel de nouvelles technologies numériques. Le mouvement est bien lancé, mais il reste encore beaucoup à faire. En ouverture de la Stratégie de transformation numérique gouvernementale 2019-2023, le ministre responsable de l'Administration gouvernementale et président du Conseil du trésor, Christian Dubé, affirme d'ailleurs : « Jusqu'à présent, trop peu d'initiatives numériques gouvernementales ont su être mises en œuvre et intégrées dans une vision commune et cohérente. La présente stratégie vise ainsi à mettre en marche l'ensemble des organisations publiques vers une seule et même véritable transformation numérique gouvernementale. »

Le défi n'est surtout pas propre au Québec. Tous les gouvernements du monde sont devant la nécessité d'effectuer une transformation qui est technologique, oui, mais qui est aussi conceptuelle, en passant d'une gestion de l'information par ministère, en silos, à une gestion horizontale et transversale. C'est cette conversion qui permet de profiter au maximum des possibilités des technologies numériques.

Il reste beaucoup à faire au Québec, mais la nomination d'un ministre responsable de la Transformation numérique révèle l'importance que le gouvernement du Québec accorde à ce dossier.

Qui plus est, même si la transformation numérique n'est pas achevée, plusieurs gestes peuvent déjà être posés pour expérimenter le potentiel de la technologie.

⁴⁶ Le processus législatif : de la politique gouvernementale à la promulgation, Parlement du Canada, 1^{er} septembre 2015 [lop.parl.ca/sites/PublicWebsite/default/fr_CA/ResearchPublications/201552E].

⁴⁷ « Melbourne University to pilot a distributed database for micro-credentials », University of Melbourne, communiqué de presse, 27 avril 2017 [about.unimelb.edu.au/newsroom/news/2017/april/melbourne-university-to-pilot-a-distributed-database-for-micro-credentials].



CONCLUSION

La technologie des registres distribués est un autre puissant phénomène transformateur de la révolution numérique. Comme l'intelligence artificielle, l'infonuagique, l'Internet des objets, cette technologie vient bouleverser un ordre établi.

Elle amène une rupture sans précédent dans la conception de l'archivage, du transit des données, des transactions électroniques. Elle redéfinit des notions aussi fondamentales que la monnaie, elle a le potentiel d'ébranler presque tous les domaines d'activité et peut même être associée à une modernisation de la relation démocratique État-citoyen.

À travers le monde, les États se positionnent face à cette technologie, élaborant des cadres réglementaires, adoptant des politiques de soutien à l'écosystème, mettant en place des initiatives favorisant l'expérimentation.

Le Québec, à travers sa communauté technologique, entrepreneuriale, universitaire et financière, est engagé dans la révolution des registres distribués avec un écosystème encore fragile, mais prometteur.

L'État québécois doit prendre position. Il doit reconnaître le potentiel de cette technologie; il doit reconnaître le rôle qu'elle joue dans la transformation numérique des organisations et des entreprises; il doit voir le levier que représente cette technologie pour améliorer la productivité des organisations et des entreprises, ce qui est précisément l'un des enjeux les plus stratégiques de l'économie québécoise. Enfin, l'État québécois doit voir le potentiel extrêmement novateur des registres distribués comme élément participant à la modernisation de l'État et des institutions démocratiques.

Pour le Québec, qui se présente au monde comme un leader dans plusieurs technologies d'avant-garde, la maîtrise de cette nouvelle technologie disruptive revêt une valeur stratégique et économique très élevée.



RECOMMANDATION

Le domaine des chaînes de blocs et des registres distribués compte parmi les technologies disruptives qui connaîtront un rapide essor au cours des prochaines années. Les implications sont très nombreuses; elles vont de la perturbation de plusieurs domaines d'activité, à l'émergence de nouveaux leaders dans une filière industrielle au grand potentiel, jusqu'à la modernisation des institutions démocratiques. Au terme de ce livre blanc, et face à ces multiples enjeux, nous formulons une seule recommandation qui comporte toutefois différents volets.

Nous recommandons que le gouvernement du Québec se mette en marche dans les meilleurs délais et reconnaisse la technologie des chaînes de blocs et des registres distribués comme un enjeu économique stratégique et incontournable.

Recommandation principale :

Que le Gouvernement du Québec reconnaisse la technologie des chaînes de blocs et des registres distribués comme un enjeu économique stratégique et incontournable.

Cette reconnaissance mettra le gouvernement en mode action.

D'abord, le gouvernement devrait se donner des moyens de compréhension et d'analyse. En s'inspirant du modèle mis sur pied par le Comité d'implantation de la grappe en intelligence artificielle, le gouvernement devrait soutenir un groupe réunissant des experts, des entrepreneurs, des universitaires, des investisseurs pour l'aider à déterminer les meilleurs gestes à poser. Ce groupe devrait avoir entre autres mandats de :

- créer un répertoire détaillé des acteurs;
- mettre en place une plateforme d'échange et de vigie;
- réaliser des analyses pour identifier les domaines les plus porteurs ou à risques élevés de perturbation;
- développer des formations pour sensibiliser les décideurs sur les fondements, les caractéristiques et les sources de valeur ;
- conseiller le gouvernement sur les initiatives porteuses;
- Secondier le gouvernement dans la mise en place des initiatives retenues.

Le gouvernement devrait également s'engager à stimuler l'innovation :

- En créant un espace d'expérimentation, le concept de bac à sable, où les entrepreneurs pourront tester des technologies à l'abri des contraintes que poserait une réglementation non encore adaptée;
- En s'inspirant du gouvernement fédéral et en invitant des constituantes – ministères, sociétés d'État, organismes publics – à mener des projets pilotes utilisant les registres distribués; en agissant de cette façon, l'État innove et contribue au renforcement de l'écosystème en associant à ses projets des entreprises en ascension.
- En instaurant des mesures de soutien financier adaptées à la réalité des registres distribués favorisant l'attraction des talents et touchant la réalisation de l'ensemble des phases de développement jusqu'à l'implantation et le déploiement.

Le gouvernement devrait également enclencher en son sein trois chantiers stratégiques :

- Sur l'encadrement légal et réglementaire de chaînes de blocs et des registres distribués;
- Sur le développement des compétences et des talents et le soutien à la recherche;
- Sur les possibilités nouvelles de votation électronique, de consultation, d'identité numérique, de modernisation de nos institutions démocratiques offertes par cette technologie.

BIBLIOGRAPHIE

« A Study on Ways to Apply the Blockchain-based Online Voting System », Hye Ri Kim, Kyoungsik Min, Seng-phil Hong, *International Journal of Control and Automation*, 2017
[article.nadiapub.com/IJCA/vol10_no12/11.pdf].

« A systematic literature review of blockchain-based applications: Current status, classification and open issues », Fran Casino, Thomas. K. Dasaklis, Constantino Patsakis, *Telematics and Informatics*, volume 36, mars 2019
[www.sciencedirect.com/science/article/pii/S0736585318306324].

Bitcoin et autres cryptomonnaies Ce que vous devez savoir, l'Autorité des marchés financiers
[[lautorite.qc.ca/grand-public/investissements/bitcoin-et-autres-cryptomonnaies](http://autorite.qc.ca/grand-public/investissements/bitcoin-et-autres-cryptomonnaies)].

« Blockchain beyond the hype: What is the strategic business value? », *McKinsey*, juin 2018
[www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value].

Blockchains and Voting: Somewhere between hype and a panacea (A Position Paper), Yomna Nasser, Chidinma Okoye, Jeremy Clark, Peter Y A Ryan
[users.encs.concordia.ca/~clark/papers/draft_voting.pdf].

Canadian Blockchain Census 2019, Chamber of digital commerce, Octobre 2019
[digitalchamber.org/wp-content/uploads/2019/10/Blockchain-Census_FINAL-Oct4-8.28.pdf].

Collusion et information asymétrique, Jean-Jacques Laffont, erudit.org, diffusion numérique 9 février 2009
[www.erudit.org/fr/revues/ae/1997-v73-n4-ae2752/602242ar].

Comprendre la blockchain, Uchange.co, janvier 2016,
[iatranshumanisme.com/wp-content/uploads/2018/01/comprendre-la-bookchain-uchange.co_01.pdf]

« “Crypto Valley” Zug to trial blockchain voting », Matthew Allen, swissinfo.ch, 8 juin 2018
[www.swissinfo.ch/eng/system-test_-cryptovalley--zug-to-trial-blockchain-voting/44177440]

Deep shift: Technology Tipping Points and Societal Impact, World Economic Forum, septembre 2015
http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

Deloitte's 2019 Global Blockchain Survey. Blockchain gets down to business, Deloitte, 2019
[www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf].

« Des réassureurs veulent numériser leurs transactions », portail-assurance.ca, 21 mai 2019
[journal-assurance.ca/article/des-reassureurs-veulent-numeriser-leurs-transactions].

« En Inde, l'accès au cinéma passe par la blockchain », Catherine Mathys, 13 juin 2019
[trends.cmf-fmc.ca/fr/en-inde-laces-au-cinema-passe-par-la-blockchain].

E-residency 2.0 White Paper, gouvernement de l'Estonie,
[s3.eu-central-1.amazonaws.com/ereswhitepaper/e-Residency+2.0+white+paper+English.pdf].

Estonian elections: 2014 -2015, tivi.io, 2015
[tivi.io/case/estonian-elections-2014-2015].

Ethereum identity system uPort working with Brazil's Ministry of Planning, Ian Allison, ibtimes.co.uk, 23 août 2017
[www.ibtimes.co.uk/ethereum-identity-system-uport-working-brazils-ministry-planning-1636253].

« Expériences et projets liés aux technologies financières », Banque du Canada
[www.banqueducanada.ca/recherches/monnaies-electroniques-et-technologies-financieres/experiences-et-projets-lies-aux-technologies-financieres].

« Final line-up for the new Minister's Recreational Fishing Advisory Council announced », gouvernement de South Australia, communiqué de presse, 25 mars 2019
[s3-ap-southeast-2.amazonaws.com/assets.yoursay.sa.gov.au/production/2019/03/25/03/46/57/ea46b888-1392-44ac-8069-73d0bb385f59/3-25_Whetstone_-_MRAFC_Final.pdf].

From Economization to Tokenization: New Forms of Economic Life On-Chain, Francis Jervis, New York University, 28 février 2019
[papers.ssrn.com/sol3/papers.cfm ?abstract_id=3344748].

« Gestion collective : au Québec, Copibec opte pour la blockchain, avec Bookchain », Clément Solym, 26 février 2019, actualitte.com
[www.actualitte.com/article/monde-edition/gestion-collective-au-quebec-copibec-opte-pour-la-blockchain-avec-book-chain/93539].

« Horizon State and MiVote announce deal with Indian political party », *Micky News*, 24 août 2018
[micky.com.au/democracy-deal-horizon-state-breaks-into-india].

« How Blockchain Can Transform Artificial Intelligence », Dmitri Budko, DZone, 13 février 2018
[dzone.com/articles/how-blockchain-can-transform-artificial-intelligen].

« IBM eyes Blockchain technology deal for Kenya's public records », businessdailyafrica.com, 15 décembre 2016
[www.businessdailyafrica.com/Corporate-News/IBM-eyes-Blockchain-technology-deal-for-Kenya-s-public-records/539550-3488120-1fk4q7z].

« Identité numérique : une nouvelle technologie mise à l'essai dans les aéroports », Agence QMI, 28 janvier 2018
[www.tvanouvelles.ca/2018/01/28/identite-numerique-une-nouvelle-technologie-mise-a-lessai-dans-les-aeroports-1].

« La ministre Murray annonce la publication de la nouvelle Politique sur les services et le numérique, ce qui renforce notre engagement en matière de gouvernement numérique », communiqué de presse, 2 août 2019
[www.canada.ca/fr/secretariat-conseil-tresor/nouvelles/2019/08/la-ministre-murray-annonce-la-publication-de-la-nouvelle-politique-sur-les-services-et-le-numerique-ce-qui-renforce-notre-engagement-en-matiere-de-.html].

« La Régie de l'énergie rend sa décision relative à la demande de fixation de tarifs et conditions de service pour l'usage cryptographique appliqué aux chaînes de blocs », communiqué de presse, 20 avril 2019
[www.newswire.ca/fr/news-releases/la-regie-de-l-energie-rend-sa-decision-relative-a-la-demande-de-fixation-de-tarifs-et-conditions-de-service-pour-l-usage-cryptographique-applique-aux-chaînes-de-blocs-826345895.html].

« La technologie blockchain au DigiHub », Vincent Mongrain, Le Nouvelliste, 12 décembre 2017
[www.lenouvelliste.ca/affaires/la-technologie-blockchain-au-digihub-d67042e60040c3b41a1234d78ed13818].

« Le port de Montréal choisit une solution blockchain », David Nathan, 29 octobre 2018
[fr.cryptonews.com/news/le-port-de-montreal-choisit-une-solution-blockchain-2214.htm].

Le processus législatif : de la politique gouvernementale à la promulgation, Parlement du Canada, 1^{er} septembre 2015
[lop.parl.ca/sites/PublicWebsite/default/fr_CA/ResearchPublications/201552E].

« Les enjeux sont de taille : la Chine s'apprête à lancer sa cryptomonnaie nationale », Daily Geek Show, 23 septembre 2019
[<https://dailygeekshow.com/chine-cryptomonnaie-nationale/>]

« L'intégration de la blockchain à la traçabilité : une technologie à l'épreuve complète des fraudes informatiques », Bernard Gauthier, agri-tracabilite.qc.ca, février-mars 2018
[www.agri-tracabilite.qc.ca/images/stories/Actualits/mci_magazine_-_Lintegration_de_la_blockchain_a_la_traçabilité_février-mars_2018.pdf].

« Melbourne University to pilot a distributed database for micro-credentials », University of Melbourne, communiqué de presse, 27 avril 2017
[about.unimelb.edu.au/newsroom/news/2017/april/melbourne-university-to-pilot-a-distributed-database-for-micro-credentials].

« Mobile Voting is Coming to Utah County Municipal Elections », Tusk Philanthropies, communiqué de presse, 23 juillet 2019
[www.prnewswire.com/news-releases/mobile-voting-is-coming-to-utah-county-municipal-elections-300889121.html].

« Online Voting: A Path Forward for Federal Elections », site Web du gouvernement du Canada, janvier 2017
[www.canada.ca/en/democratic-institutions/services/reports/online-voting-path-forward-federal-elections.html].

Projet de loi n°27 : Loi concernant principalement l'organisation gouvernementale en matière d'économie et d'innovation, Assemblée nationale du Québec
[www.assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-27-42-1.html?appelant=MC].

Stratégie de transformation numérique gouvernementale 2019-2023, gouvernement du Québec
[www.quebec.ca/gouv/politiques-orientations/transformation-numerique].

Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure, Michael C. Jensen, Harvard University Press, 1998
[www.sfu.ca/~wainwrig/Econ400/jensen-meckling.pdf].

« TOP runs NZ's first Blockchain political party election », The Opportunities Party, communiqué de presse, 6 novembre 2018
[www.scoop.co.nz/stories/PO1811/S00059/top-runs-nzs-first-blockchain-political-party-election.htm].

« Un autre allié pour DigiHub », *L'hebdo du St-Maurice*, 31 mai 2019
[www.lhebdodustmaurice.com/un-autre-allie-pour-le-digihub].

« Une monnaie numérique montréalaise en attendant celle de Facebook », Alain McKenna, lesaffaires.com, 20 juin 2019
[www.lesaffaires.com/blogues/alain-mckenna/une-monnaie-numerique-montrealaise-en-attendant-celle-de-facebook/611073].

« Vocabulaire de la cryptomonnaie », Office québécois de la langue française, 2018
[www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/vocabulaire-cryptomonnaie.aspx].

ANNEXE I : MESURES ET INITIATIVES À TRAVERS LE MONDE

Mesures et initiatives de gouvernements et d'organisations internationales à travers le monde visant l'adoption et l'encadrement de la technologie des chaînes de blocs et des registres distribués; informations tirées du site GovChain.world.



AUSTRALIE

Stratégie nationale de chaînes de blocs

- Le 18 mars 2019, le gouvernement australien a annoncé le lancement d'une stratégie nationale de chaînes de blocs.
- La stratégie comprend une feuille de route axée sur la réglementation, les compétences, l'innovation, les investissements ainsi que la compétitivité et la collaboration internationales.
- L'Australian Transaction Reports and Analysis Centre (Austrac), une agence gouvernementale d'intelligence financière, s'est associée à la Swinburne University of Technology de Melbourne pour tester l'utilisation de la technologie des chaînes de blocs et des contrats intelligents afin d'aider plusieurs acteurs à automatiser leurs instructions de transfert de fonds internationaux.

Technologie financière et cryptomonnaie

- Le gouvernement australien a récemment signé le UK – Australia FinTech Bridge entre le Royaume-Uni et l'Australie (mars 2018). L'accord vise à favoriser :
 - une collaboration entre les gouvernements pour identifier les tendances en matière de technologie financière et améliorer la réponse politique;
 - le partage de l'expertise entre régulateurs, facilitant l'entrée des entreprises en démarrage en technologie financière dans chaque juridiction et permettant un traitement plus rapide des licences;
 - .. les échanges bilatéraux et les flux d'investissement.
- En septembre 2017, la Commission australienne des valeurs mobilières et des investissements (ASIC) a publié les directives des ICO.
- L'Australian Taxation Office (ATO) a également fourni des indications sur le traitement fiscal des cryptomonnaies. Selon les indications, les transactions avec des cryptomonnaies s'apparentent à un « accord de troc, avec des conséquences fiscales similaires ».
- Des impôts sur les gains en capital peuvent s'appliquer chaque fois qu'un individu dispose de sa cryptomonnaie.



UNION EUROPÉENNE

- Création de l'EU Blockchain Observatory & Forum regroupant de nombreux groupes internationaux, dont le Blockchain Partnership et l'International Association for Trusted Blockchain Applications (INATBA).
- En matière de sécurité juridique, l'Union européenne a créé une réglementation spécifique définissant les monnaies virtuelles (5AMLD⁴⁸).

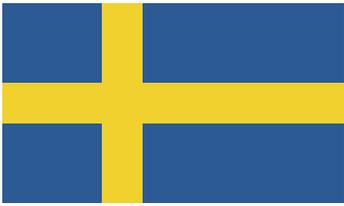
Infrastructure : beaucoup d'investissements d'ici 2020

- L'Union européenne (UE) a promulgué un certain nombre de mesures visant à promouvoir l'utilisation de la chaîne de blocs en Europe.
- La stratégie repose sur la mise en place de conditions propices à l'instauration d'un environnement transactionnel, ouvert, innovant, digne de confiance, transparent et conforme au droit de l'UE.
- Trois acteurs sont au cœur de cette mise en œuvre de la chaîne de blocs en Europe : le Parlement européen, la Commission européenne, l'Observatoire et le Forum européen sur la chaîne de blocs.
- L'UE se démarque en créant un espace réglementaire pour encourager l'adoption de la chaîne de blocs.
- Le Parlement européen a d'abord adopté une proposition de résolution sur les technologies de blocs de registres distribués et les chaînes de blocs (octobre 2018).
- S'appuyant sur cette motion, le Parlement a adopté le rapport sur la chaîne de blocs : une politique commerciale tournée vers l'avenir⁴⁹ (décembre 2018). Le rapport met en évidence les problèmes dans les chaînes d'approvisionnement, la politique commerciale et les procédures douanières. Il identifie les avantages plausibles découlant de la mise en œuvre généralisée de la chaîne de blocs.
- Bien que la cryptomonnaie ne soit pas l'objet principal de ce rapport, la cinquième directive anti-blanchiment (5AMLD)⁵⁰ (mai 2018) a élargi le champ d'application des règles de lutte contre le blanchiment d'argent de l'UE pour inclure les fournisseurs de services d'échange entre les monnaies virtuelles et la monnaie fiduciaire ainsi que les fournisseurs de portefeuilles dépositaires.

⁴⁸ Fifth Anti-Money Laundering Directive (5AMLD).

⁴⁹ Report on Blockchain: a forward-looking trade policy.

⁵⁰ Fifth Anti-Money Laundering Directive (5AMLD).



SUÈDE

- La Suède pourrait devenir la première société sans numéraires (à peine 1 % de la valeur de tous les paiements a été effectué en pièces ou en billets en 2018). Dans ce contexte, le gouvernement a adopté une approche ouverte et a testé l'utilisation de la technologie de chaîne de blocs dans de nombreux aspects de la société.

Cryptomonnaie

- Il n'y a pas de réglementation spécifique à la cryptomonnaie en Suède. Toutefois, le Finansinspektionen, l'autorité suédoise de surveillance financière, est d'avis que les bitcoins sont soumis à son autorité et à des exigences de déclaration obligatoires.
- La Riksbank, la banque centrale suédoise, a déclaré que « les bitcoins ne sont pas de l'argent ». La Suède ne considère pas les cryptomonnaies comme des monnaies.

Initiative gouvernementale

- La Finansinspektionen a lancé le Centre d'innovation (mars 2018). Il s'agit du premier point de contact pour les entreprises incertaines des règles et des principes qui régissent les innovations. Le centre sert également de catalyseur pour tester de nouvelles idées d'entreprise et leur intégration dans le cadre réglementaire.

e-Krona

- Bien que la cryptomonnaie ne soit pas considérée comme un moyen d'échange viable, la Riksbank envisage de lancer une monnaie électronique (e-Krona). L'objectif est que cette monnaie numérique de la banque centrale compense la baisse de l'utilisation des liquidités en Suède. Une monnaie électronique permettrait au grand public d'avoir toujours accès à des moyens de paiement garantis par l'État.

Application domestique de chaînes de blocs

- Lantmäteriet, l'autorité suédoise du registre foncier, travaille sur un projet explorant les possibilités de la chaîne de blocs en tant que solution technologique pour les transactions immobilières. Actuellement, le délai entre la signature d'un contrat et l'enregistrement d'une vente dans une transaction immobilière peut prendre des mois. L'espoir est de réduire ce temps de traitement à quelques heures.



ESTONIE

- L'Estonie est peut-être le premier pays à avoir adopté la technologie des registres distribués au niveau gouvernemental. Déjà en 2007, avant même la publication du livre blanc sur les bitcoins, le gouvernement estonien testait les applications basées sur la chaîne de blocs.
- e-Estonie, une politique gouvernementale visant à faciliter les interactions des citoyens avec l'État grâce à l'utilisation de solutions électroniques, teste et met en œuvre une chaîne de blocs en relation avec les services publics depuis plusieurs années.

X-Road et Infrastructure de signature sans clé (KSI⁵¹) Blockchain

- L'infrastructure numérique très sophistiquée de l'Estonie est basée, depuis 2001, sur la X-Road, une plateforme *open source*. La X-Road est complétée par le KSI, une technologie de chaîne de blocs conçue en Estonie en 2007, qui fournit une authentification à haute vitesse en temps réel pour tous les actifs numériques en réseau du monde.
- En Estonie, le KSI est utilisé pour la vérification indépendante de tous les processus gouvernementaux et la protection des services de gouvernance électronique offerts au public.

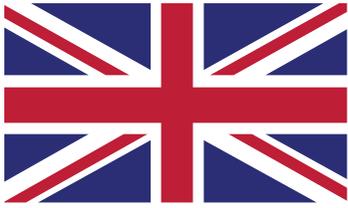
Dossier de santé électronique

- Le secteur de la santé estonien est un cas révolutionnaire d'utilisation nationale de la chaîne de blocs. Afin de sécuriser complètement les informations sur la santé tout en les rendant accessibles aux personnes autorisées, le système de carte d'identité électronique estonien utilise la technologie de la chaîne de blocs pour assurer l'intégrité des données et limiter les menaces internes.

Cryptomonnaie et ICO

- Bien qu'il n'y ait pas de réglementation spécifique aux bureaux de pays en Estonie, les jetons peuvent être considérés comme des valeurs mobilières, en fonction de leur conception et de leur portée.
- Les ICO peuvent également être régies par une loi sur les établissements de crédit si elles s'apparentent à des prêts.
- Par un arrêt de la Cour suprême estonienne, il a été établi que les cryptomonnaies correspondent à des modes alternatifs de paiement. Cela signifie qu'ils sont régis par une loi sur la lutte contre le blanchiment d'argent et une loi contre le financement du terrorisme.

⁵¹ Infrastructure de signature sans clé (KSI).



ROYAUME-UNI

- Le gouvernement britannique évalue les applications de la chaîne de blocs depuis quelques années. Le rapport *Distributed ledger technology: beyond Blockchain* (January 2016), préparé par le conseiller scientifique en chef du gouvernement, a comporté des recommandations visant notamment à assurer un leadership ministériel, à mettre en place un cadre réglementaire et à assurer un partenariat étroit entre les secteurs public et privé.
- Innovate UK, agence gouvernementale de promotion de l'innovation, a annoncé en janvier 2018 qu'elle investirait 19 millions de livres sterling dans des technologies basées sur la chaîne de blocs.
- L'agence a également offert 12 millions de livres sterling supplémentaires (16,8 millions de dollars US) aux entreprises qui tentent de recruter des diplômés pour les aider à développer leur projet.
- En juillet 2017, elle a notamment sollicité des groupes de spécialistes pouvant implémenter des outils chaîne de blocs dans les technologies émergentes de la santé.
- Le Royaume-Uni cherche également à créer et à promouvoir une coopération internationale pour la mise en œuvre de la technologie de la chaîne de blocs. Le pays est signataire, avec 21 autres pays, du Partenariat Blockchain (avril 2018).
- Le Parlement a créé, en janvier 2018, un groupe parlementaire multipartite sur la chaîne de blocs (APPG Blockchain⁵²) pour analyser les effets perturbateurs de la technologie et ses effets positifs sur l'économie britannique.
- En mars 2018, le gouvernement a annoncé la création d'un groupe de travail sur les actifs cryptographiques. Le groupe élaborera des normes industrielles pour les technologies financières et soutiendra l'innovation dans ce secteur. En octobre 2018, le groupe de travail a publié un rapport exposant l'approche du Royaume-Uni en matière de cryptoactifs et de la technologie de grand livre distribué dans les services financiers.
- Un rapport du Comité du Trésor de la Chambre des communes du Royaume-Uni sur les actifs cryptographiques (septembre 2018) recommande leur intégration dans le champ d'application de la FCA (Financial Conduct Authority).
- La FCA a également mis en œuvre des politiques visant à promouvoir l'innovation des chaînes de blocs au Royaume-Uni. L'organisme a aussi annoncé, avec 11 autres régulateurs financiers et organisations apparentées, la création, en août 2018, du réseau Global Financial Innovation Network (GFIN). Le réseau cherchera à fournir de meilleures façons pour les entreprises en technologie financière d'interagir avec les régulateurs.

Preuve de concept au ministère du Travail et des Pensions pour les prestations sociales (juin 2016)

- Le gouvernement a testé l'utilisation de la chaîne de blocs pour mettre en œuvre la distribution des paiements de protection sociale. Avec le système conçu par GovCoin Systems Limited, les demandeurs utilisaient une application sur leur téléphone pour recevoir et dépenser leurs paiements de prestations. Avec leur consentement, leurs transactions ont été enregistrées sur un grand livre distribué afin de faciliter leur gestion financière.

Preuve de concept au ministère de l'Environnement, de l'Alimentation et des Affaires rurales sur la traçabilité des aliments tout au long de la chaîne d'approvisionnement (mars 2018)

- Le ministère a examiné comment la technologie de la chaîne de blocs pourrait améliorer la transparence et l'efficacité des données pour les fournisseurs, les transformateurs et les consommateurs, et aussi améliorer le suivi du bien-être animal.

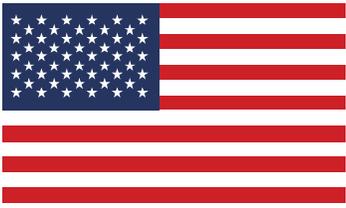
Preuve de concept au ministère du Revenu (septembre 2018)

- Le ministère du Revenu effectue des tests sur l'utilisation d'une chaîne privée à la frontière britannique afin d'aider les organisations à coordonner leurs activités et à échanger des informations lors des procédures douanières.

Preuve de concept sur le registre foncier pour le transfert numérique de propriété (mai 2019)

- Les autorités britanniques ont construit un prototype utilisant la plateforme Corda, qui permet le transfert numérique d'une propriété et met automatiquement à jour le registre foncier.

⁵² All-Party Parliamentary Group on Blockchain (APPG Blockchain).



ÉTATS-UNIS (FÉDÉRAL)

- Alors que certains États, tels que le Wyoming et le Delaware, mettent en place des réglementations relatives à la chaîne de blocs, l'État fédéral ne dispose toujours d'aucune loi ou réglementation régissant l'utilisation complète de la chaîne de blocs et d'autres registres distribués.
- Les agences fédérales explorent néanmoins activement la technologie, ses possibilités et ses risques, dans des domaines tels que la gestion de la chaîne logistique, l'identité numérique, la conformité douanière et la provenance des marchandises.

Le Intragovernmental Emerging Citizen Technology Office (ECTO)

- Ce bureau évalue, teste et met en œuvre des initiatives de modernisation informatique avec les technologies émergentes. Il mène des consultations sur les chaînes de blocs et sur les moyens de mieux comprendre les applications possibles de la technologie dans le secteur public fédéral.

Cryptomonnaie

- Afin de soutenir l'innovation dans l'industrie des chaînes de blocs, les législateurs ont présenté deux projets de loi : la *Loi sur la taxonomie des jetons* et la *Loi sur la taxonomie numérique*. Elles visent à exclure spécifiquement les jetons numériques de la définition de valeurs mobilières et à « apporter une certitude réglementaire aux entreprises, aux entrepreneurs et aux régulateurs de l'économie de la chaîne de blocs aux États-Unis ».
- Les régulateurs américains veulent définir rapidement ces nouveaux actifs afin de concurrencer des États tels Singapour et la Suisse qui ont pris un leadership en ces domaines. Ils estiment que le fait d'exclure les jetons numériques des exigences relatives aux valeurs mobilières peut favoriser l'innovation en évitant une surréglementation.

Hub stratégique pour l'innovation et la technologie financière (FinHub)

- La Securities and Exchange Commission (SEC) a une approche teintée de méfiance, mais a néanmoins lancé un pôle stratégique pour l'innovation et la technologie financière (FinHub) en octobre 2018.

Cadre d'analyse des « contrats d'investissement » des actifs numériques

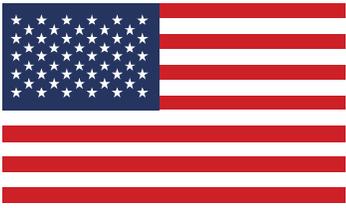
- Le 3 avril 2019, le FinHub de la SEC a publié un cadre d'analyse des contrats numériques destiné à aider les acteurs du marché à déterminer si les lois fédérales sur les valeurs mobilières s'appliquent à l'offre, à la vente ou à la revente d'un actif numérique particulier.

US Food and Drug Administration (FDA)

- La Food and Drug Administration (FDA) des États-Unis a lancé un projet pilote visant à tester des approches innovantes dans la chaîne d'approvisionnement en médicaments.

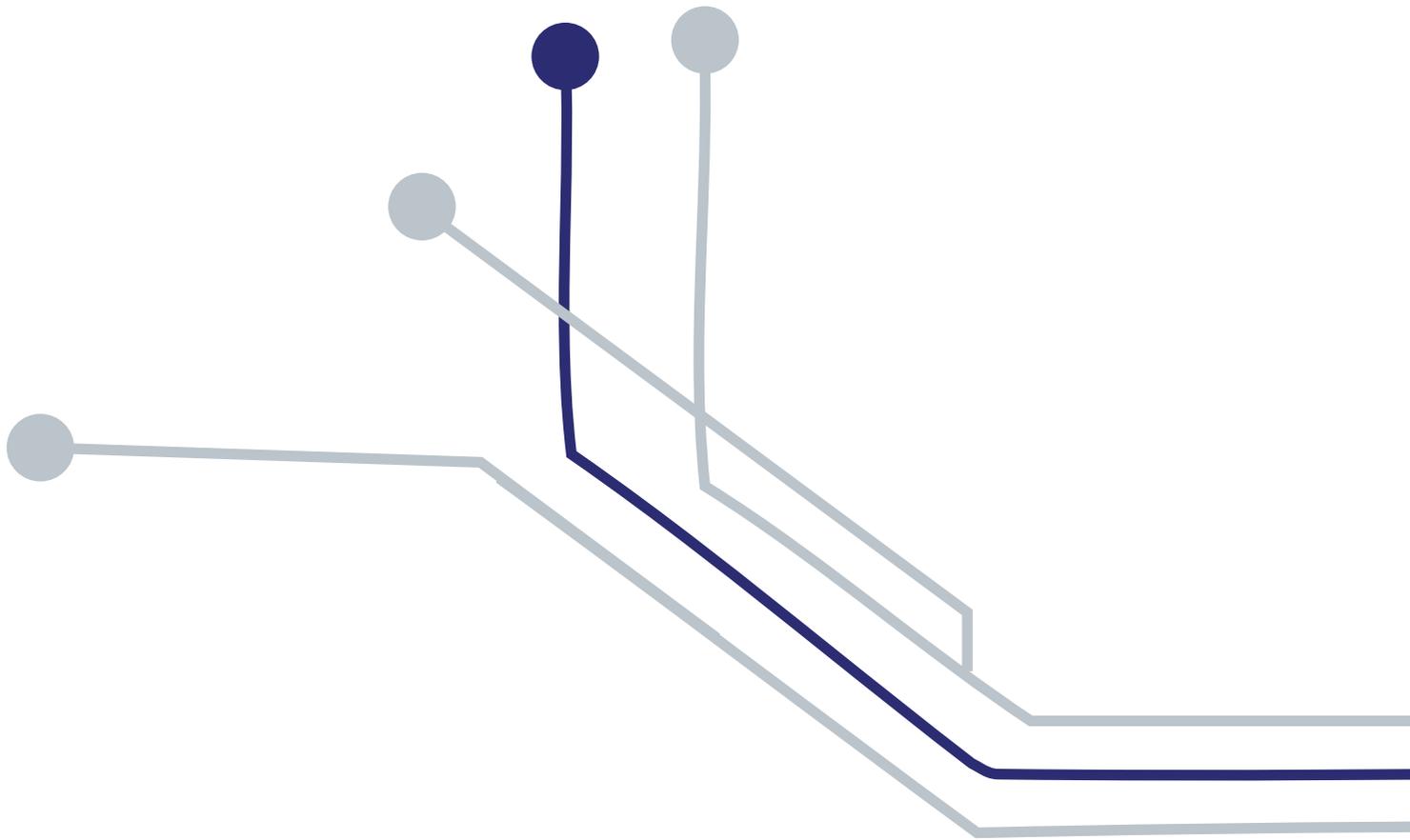
Facebook

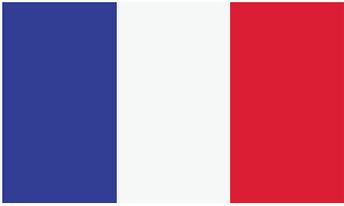
- Facebook est entré dans l'espace de la chaîne de blocs en annonçant la création du Libra, une monnaie numérique avec chaîne de blocs autorisée. La monnaie sera une cryptomonnaie stable (*stablecoin*), c'est-à-dire adossé à des actifs corporels afin d'éviter la volatilité des prix. La devise sera gouvernée par un groupe à but non lucratif basé en Suisse et composé de 28 membres fondateurs, comprenant l'unité Calibra de Facebook, Visa, Mastercard, Uber, PayPal, des investisseurs en capital de risque et autres.
- Les régulateurs et des politiciens américains ont exprimé leur inquiétude face à cette annonce. Le Comité de la Chambre des États-Unis sur les services financiers est allé jusqu'à exiger que Facebook arrête tout développement tant qu'un encadrement adéquat n'est pas en vigueur.



ÉTATS-UNIS (WYOMING)

- Le Wyoming est sans doute le plus avancé des États-Unis en ce qui concerne la mise en place d'un cadre juridique complet pour les entreprises basées sur la chaîne de blocs, ayant promulgué 13 lois en la matière.
- Les lois de l'État permettent ainsi de :
 - reconnaître les droits des propriétaires individuels d'actifs numériques de tous types;
 - mettre en place un bac à sable en technologie financière afin d'offrir un cadre d'expérimentation en dehors des lois existantes pendant trois ans au maximum;
 - consentir à un nouveau type d'institution de dépôt fournissant des services bancaires basés sur la chaîne de blocs;
 - soutenir le premier véritable « dépositaire qualifié » pour les actifs numériques qui est une banque.





FRANCE

Projet de loi PACTE

- Le 11 avril 2019, l'Assemblée nationale française a adopté le projet de loi PACTE (Plan d'action pour la croissance et la transformation de l'entreprise). La nouvelle loi établit un cadre pour la collecte de fonds par l'émission d'offres de pièces de monnaie initiales (ICO) et des fournisseurs de services numériques. Une fois adoptée, la loi fournira:
 - un régime de visas facultatif pour les ICO;
 - une licence facultative pour les fournisseurs de services;
 - un enregistrement obligatoire pour deux activités (fourniture de services de conservation d'actifs numériques à des tiers ou achat / vente d'actifs numériques en contrepartie d'un cours légal);
 - une possibilité pour certains fonds d'investir dans des actifs numériques;
 - des exigences de protection des investisseurs.

Possibilité pour certains fonds d'investir dans des actifs numériques

- Le PACTE prévoit que deux types de fonds peuvent désormais investir dans des actifs numériques, soit :
 - les fonds d'investissement professionnels spécialisés, à condition qu'ils respectent les règles de liquidité et de valorisation qui leur sont applicables;
 - les fonds d'investissement professionnels de capital-investissement, dans la limite de 20 % de leurs actifs.

Exigences de protection des investisseurs

- Le PACTE renforce également les pouvoirs de l'Autorité pour mieux protéger les investisseurs. L'Autorité aura le pouvoir de superviser les ICO; l'Autorité peut en outre publier une « liste noire » des ICO et des fournisseurs de services d'actifs numériques qui ne se conforment pas à la réglementation.

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (OCDE)

- L'Organisation de coopération et de développement économiques étudie actuellement les avantages potentiels de la chaîne de blocs pour accroître la transparence, la traçabilité et l'efficacité des transactions.
- L'un des objectifs essentiels de l'OCDE est de s'assurer que la technologie repose sur des politiques et des cadres réglementaires sains, afin de libérer ce potentiel tout en réduisant les risques d'utilisation abusive.
- Le Forum sur les politiques de la chaîne de blocs de l'OCDE (4-5 septembre 2018) a été la première grande conférence internationale à faire le point sur les impacts de la chaîne de blocs dans l'ensemble des activités gouvernementales et des priorités publiques. Les participants se sont concentrés sur :
 - l'impact économique global potentiel de la chaîne de blocs;
 - l'implication sur la vie privée et la cybersécurité;
 - l'utilisation de la chaîne de blocs pour améliorer l'inclusion;
 - l'utilisation de la chaîne de blocs pour promouvoir la croissance verte et la durabilité;
 - l'utilisation de la chaîne de blocs pour renforcer les pratiques de gouvernance et d'application.

Rapports

- L'OCDE a également publié un certain nombre de rapports sur les différentes utilisations de la chaîne de blocs. En juin 2018, elle a publié le guide *La technologie chaîne de blocs et son utilisation dans le secteur public*. Celui-ci visait à doter les fonctionnaires des connaissances nécessaires pour comprendre l'architecture de la chaîne de blocs, ses implications pour les services gouvernementaux, ainsi que les possibilités et les défis qui pourraient en résulter pour les gouvernements.

En janvier 2019, l'OCDE a publié un rapport sur les offres de pièces de monnaie initiales (ICO) pour le financement des PME, analysant l'émergence et le potentiel des OIC en tant que mécanisme de financement des jeunes entreprises et des PME.



CHINE

Bien que GovChain continue de classer la Chine dans les pays sceptiques, notamment à cause d'une grande méfiance des autorités chinoises envers Bitcoin, le pays est très actif dans le développement de la technologie et plusieurs sources rapportent que la Chine s'apprête à lancer sa propre cryptomonnaie.

Administration du cyberspace chinois (CAC) – Réglementation de la chaîne de blocs

- En février 2019, l'Administration chinoise du cyberspace (CAC) a introduit une nouvelle réglementation sur la technologie de la chaîne de blocs, imposant de nouvelles exigences aux fournisseurs de services de la chaîne de blocs, afin de les empêcher de contourner les règles de censure sur Internet.
- Le règlement relatif à la gestion du service d'information chaîne de blocs impose à ces entreprises non seulement d'enregistrer les utilisateurs avec leurs noms et identité nationale réels, mais également de supprimer toutes les données stockées que les autorités chinoises considèrent comme une violation des lois nationales existantes.

Banque populaire de Chine (PBoC) – Plateforme de financement du commerce basée sur la chaîne de blocs

- En septembre 2018, la Banque populaire de Chine (PBoC) a apporté son soutien à une plateforme de financement du commerce reposant sur une chaîne de blocs. La plateforme chaîne de blocs du financement du commerce dans les districts de Guangdong, Hong Kong et Macao Dawan vise à fournir un écosystème alimenté par la chaîne de blocs pour les échanges transfrontaliers.

Food and Drug Administration du District chinois de Chongqing Yuzhong

- La mise en œuvre de la chaîne de blocs en Chine s'est principalement déroulée au niveau des administrations locales, notamment dans les domaines de la gestion de la chaîne logistique et de la collecte des impôts, ainsi que de la sécurité des aliments et des médicaments. La Food and Drug Administration du district chinois de Chongqing Yuzhong a testé la technologie chaîne de blocs pour renforcer la supervision de l'assurance de la qualité des aliments et des médicaments avec une meilleure traçabilité du cycle de vie du produit et des mesures anti-contrefaçon.

Décision du tribunal Internet de Hangzhou

- Dans un geste qui semble indiquer que le gouvernement adoucit sa position sur le bitcoin, le tribunal Internet de Hangzhou a statué, le 17 juillet 2019, que le bitcoin, et le crypto en général, devait être considéré comme une « propriété Internet virtuelle » légale et qu'il mérite d'être traité comme d'autres actifs.

Hong Kong

- Contrairement au reste de la Chine, Hong Kong a adopté une approche conviviale à l'égard des cryptomonnaies. En novembre 2018, la Securities and Futures Commission (SFC) a publié une déclaration précisant les domaines d'application de la réglementation en vigueur aux actifs cryptographiques et indiquant qu'elle envisageait de réglementer formellement les échanges.



ign.quebec