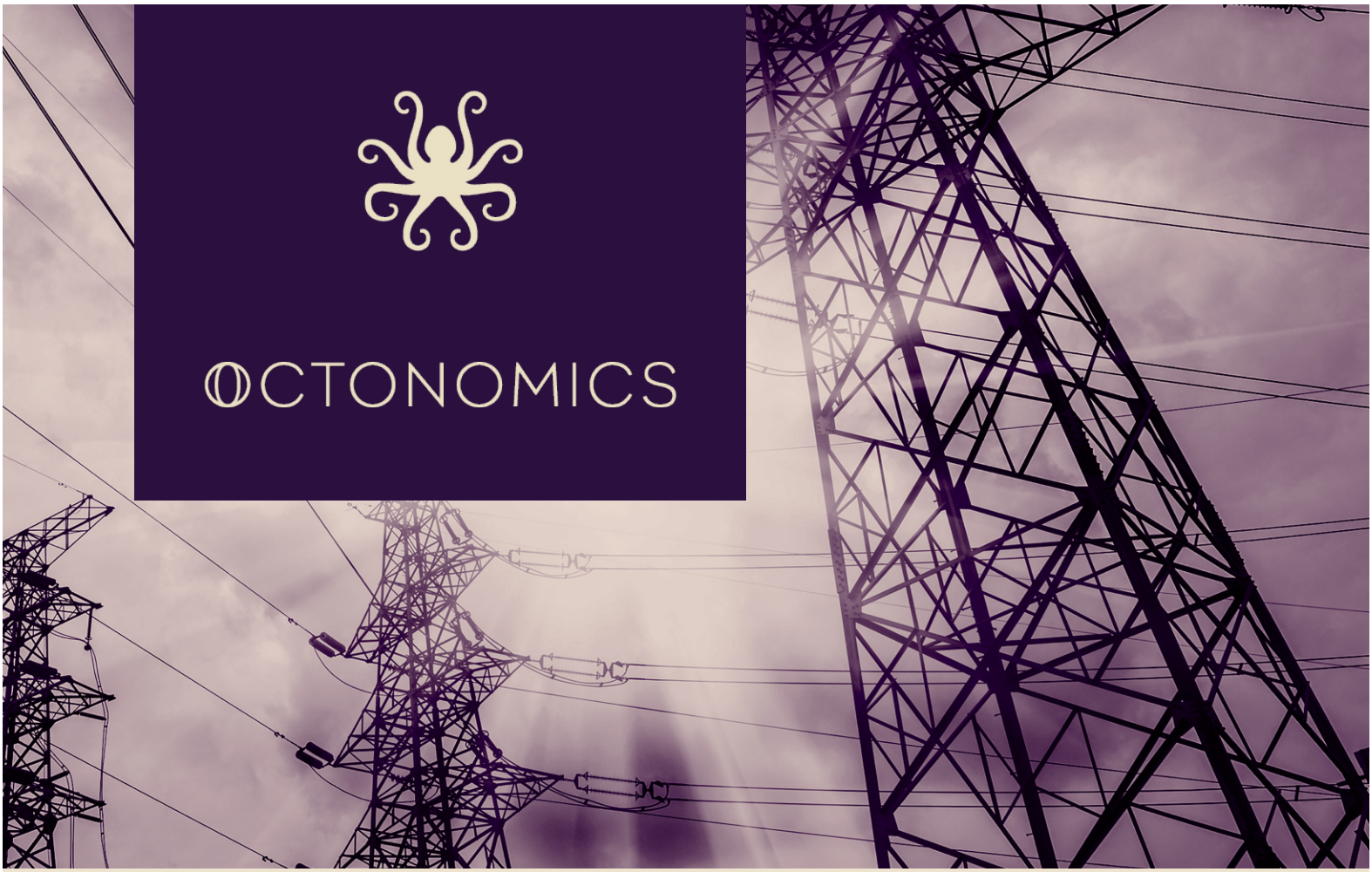


OCTONOMICS

DEMANDE DE FIXATION DE TARIFS ET CONDITIONS DE SERVICE POUR L'USAGE CRYPTOGRAPHIQUE APPLIQUÉ AUX CHAÎNES DE BLOCS

Rapport d'analyse

Présenté à la Régie de l'énergie R-4045-2018

Préparé pour Bitfarms

Elisabeth Préfontaine, MBA, CFA, CAIA, CBP

FONDATRICE DE OCTONOMICS

Description du mandat

Octonomics a été mandaté par Bitfarms pour produire un rapport d'analyse dans le but de renseigner la Régie de l'énergie du Québec sur l'industrie de l'usage cryptographique appliqué aux chaînes de blocs, le tout dans le cadre du dossier R-4045-2018. Ce rapport traitera des trois éléments du mandat qui a été confié par Bitfarms :

1. Quels sont les impacts économiques et technologiques pour le Québec associés au déploiement de l'industrie de la chaîne de blocs? Le rapport d'analyse illustrera le changement technologique profond qui se déroule et exposera une évaluation des perspectives d'emplois et des impacts économiques qui en découlent.

2. En quoi est-il important de conserver un environnement commercial compétitif, notamment à travers des tarifs d'électricité, afin que cette industrie émergente puisse se développer au Québec?

3. Quels sont les impacts que pourrait avoir la demande du Distributeur dans le dossier R-4045-2018 sur le développement de l'industrie de la chaîne de blocs, notamment sur la compétitivité des entreprises du Québec?

Avertissement

L'industrie liée à l'usage cryptographique appliqué à la chaîne de blocs est composée d'expériences technologiques. Les entrepreneurs dans ce domaine sont des pionniers, des explorateurs qui investissent leur capital et leur temps pour supporter la R et D de l'industrie et trouver des solutions novatrices aux problèmes rencontrés. Il n'y a toutefois pas de garantie de succès. Les cas, projets et cryptomonnaies cités ne représentent aucunement une recommandation d'achat, de vente, de viabilité ou un endossement. Leur présence dans ce rapport devrait plutôt être comprise à titre d'illustration des développements en cours. Les opinions et observations contenues dans ce rapport ne constituent pas un conseil en investissement et n'engagent aucunement la responsabilité ou quelconque obligation de l'auteur et de sa firme.

Précisions

L'exemple de Bitcoin est largement utilisé dans ce document pour les raisons citées ci-dessous. Il faut d'abord comprendre l'innovation qu'il représente et comment il y est arrivé avant d'extrapoler sur d'autres concepts. Le risque est d'omettre certaines informations essentielles au développement de sa pensée critique par rapport à ce que représente un « usage cryptographique appliqué aux chaînes de blocs ». Bitcoin est une catégorie en soi et référer aux cryptomonnaies dans le sens large ferait perdre des nuances essentielles à la compréhension du lecteur.

Bitcoin n'est pas que le nom d'une devise, c'est aussi le nom d'un réseau et aussi d'un protocole dont l'historique et le déploiement n'a pas de comparable. Pour faciliter la lecture et l'identification des différences dans le rapport, nous allons référer au « protocole Bitcoin » et au « réseau Bitcoin » pour

désigner la technologie et à « bitcoin » pour désigner la devise. « Bitcoin » (majuscule) sera aussi utilisé pour référer à l'ensemble que représentent le protocole, le réseau et la devise.

Le protocole Bitcoin est le principal client énergivore. C'est la raison principale de sa présence dominante dans le rapport. C'est aussi parce que sa chaîne de blocs opère de manière décentralisée, qu'un premier cas d'utilisation fonctionnel (monnaie) est déployé et qu'un schème clair de monétisation est proposé. Bitcoin aura dix ans le 3 janvier 2019.

D'autres cryptomonnaies sont aussi des clients énergivores (tel que défini par la preuve de travail). Il s'agit principalement de ethereum (ETH), bcash (BCC), litecoin (LTC) et monero (XMR).

Divulgation

L'auteure (et fondatrice de Octonomics), Elisabeth Préfontaine, déclare détenir de la cryptomonnaie à l'intérieur d'un portefeuille diversifié d'actifs traditionnels et alternatifs.

Sommaire exécutif

À la lumière de l'analyse du dossier R-4045-2018, deux problématiques générales ont fait surface.

La première problématique est que la quantité élevée de MW demandés en électricité combinée à la manière simultanée dont ces demandes ont été présentées n'a pas tenu compte de la dynamique économique du minage de cryptomonnaie. Même si ces MW avaient été octroyés, il est peu probable qu'ils aient pu être déployés par les centres de calcul de cryptomonnaie de manière économiquement viable. De plus, même si ces MW avaient été octroyés, il est peu probable que l'équipement informatique nécessaire à ce déploiement énergétique ait été disponible. La dynamique économique et le défi de l'approvisionnement en équipements informatiques pointent vers une demande simultanée de différents clients et non pas vers la matérialisation du déploiement d'une telle demande énergétique.

La deuxième problématique réside dans le manque de nuances importantes de cette nouvelle industrie qui est en émergence. Il appert que certaines définitions, perceptions et informations qui ont circulé ont besoin d'être nuancées et précisées. Ces informations sont à la base d'hypothèses qui ne permettront pas d'exécuter certaines mesures tarifaires et outils de surveillance envisagés. L'usage cryptographique appliqué aux chaînes de blocs n'a pas un profil de consommation énergétique similaire pour l'ensemble des clients et usages de la définition proposée. Il sera impraticable de cerner la consommation d'un bloc dédié compte tenu des définitions proposées. Si l'on vise à identifier un sous-groupe de cryptomonnaie (celles qui sont énergivores), il faut savoir qu'elles ne présenteront des variations de consommation perceptibles que si leur réseau a du succès et reçoit des investissements massifs. Autrement dit, tenter de les isoler, créerait une tarification différente pour un même usage selon le niveau de succès du réseau de la cryptomonnaie en question.

L'utilité de l'électricité dans le contexte d'un usage cryptographique appliqué aux chaînes de blocs doit d'abord être comprise. De plus, la définition de ce qu'est une chaîne de blocs, de son fonctionnement et des nuances qui existent est essentielle. Le manque de distinction entre les différents usages ou applications et le moment où la consommation énergétique devient élevée méritent d'être revisités. Advenant des conditions de marchés défavorables, comme par exemple lorsque le prix du bitcoin est à la baisse et que le taux de hachage à la hausse, les entreprises qui ont accès à un tarif d'électricité non compétitif auront à éteindre de l'équipement informatique avant d'autres. Lorsque l'équipement est éteint, les revenus qui y sont associés cessent. Donc, un tarif non compétitif nuirait à la compétitivité des entreprises.

De ces deux problématiques de haut niveau ont émergé un décret gouvernemental et des réponses sous forme de solutions tarifaires. Il serait impraticable d'englober les clients dans une catégorie distincte définie par l'usage, les outils de surveillance proposés ne seraient pas efficaces et un tarif non compétitif nuirait au développement économique de ces entreprises.

Table des matières

5. IMPACTS ECONOMIQUES

1. Consommation énergétique et dynamique économique

Selon la preuve du Distributeur, celui-ci aurait reçu des « demandes massives, soudaines et simultanées »[1] dont le compte initial s'élevait à 18,000 MW. Lors des audiences tenues les 26-27 juin 2018, ce total fut rectifié à 6500 MW[2]. Le Distributeur n'a pas la capacité d'accueillir l'ensemble des demandes reçues[3]. « À toutes fins pratiques, ces demandes ont été présentées en même temps.[4] »

Messages clés

Le fond du problème semble la manière simultanée avec laquelle les demandes ont présentées plutôt que l'octroi et le déploiement de celles-ci.

- Ce n'est pas la chaîne de blocs qui consomme de l'énergie, mais la preuve de travail.
- La dynamique économique du minage de cryptomonnaies est impactée par la variation de puissance déployée sur le réseau. La rentabilité est affectée.
- Il y a un seuil de rentabilité en deçà duquel il n'est pas économiquement rationnel d'ajouter de la puissance de calcul au réseau.
- Un tarif non compétitif aurait l'effet de diminuer la compétitivité des centres de calcul en sol québécois puisqu'ils pourraient devoir éteindre l'équipement avant d'autres.
- Toutes les cryptomonnaies ne sont pas de grandes consommatrices d'électricité.
- Toutes les utilisations cryptographiques appliquées à la chaîne de blocs ne sont pas énergivores.
- Les clients énergivores de cette industrie minent une commodité qui s'apparente à l'or sur plusieurs points donc ont un revenu confirmé pour s'acquitter de leur facture énergétique.

Bien que la comparaison soit imparfaite, on peut penser à un client énergétique tel que Bitcoin comme un hybride entre un centre de données et une mine de métaux.

Pour saisir cette nuance, il faut à la fois comprendre la raison de la consommation énergétique (volet centre de données/ protocole bitcoin) et sa dynamique économique (volet mine de métaux/ devise bitcoin).

1.1 Consommation énergétique

Le réseau Bitcoin a des règles mais n'a pas de dirigeants. Plutôt que d'avoir à faire confiance aux membres du réseau, le protocole Bitcoin vérifie tout ce qu'ils font. Ce processus de vérification (preuve de travail) engendre une dépense énergétique. Cette méthode de consensus est la seule solution connue à un problème ouvert en science informatique qui s'appelle « le problème des

[1] HQD-2 doc 1 (2.) p. 3
[2] HQD1 doc 6 p. 4
[3] HQD-2 doc 5 (2.2) p. 6
[4] HQD-2 doc1 en liasse Annexe B (57.) p. 10

Généraux byzantins [5]». En d'autres mots, c'est la solution trouvée pour éliminer le problème de la double dépense dans un contexte numérique sans organe de contrôle. Il n'y a actuellement pas d'autres alternatives.

Les transactions sont horodatées en les « hachant » dans une chaîne continue de « hash » basée sur la preuve de travail. La preuve de travail balaie (scan) pour des valeurs qui sont hachées avec un algorithme tel que SHA-256. Le nombre de tentatives à la seconde pour trouver ce « hash » est ce qui est appelé le taux de hachage.

La consommation de joules d'énergie fait donc partie intégrante du design de l'infrastructure de Bitcoin et de certaines autres cryptomonnaies qui utilisent la méthode de consensus distribué appelée la preuve de travail. La preuve de travail, telle qu'utilisée dans le contexte du protocole Bitcoin, implique que les membres du réseau soient en compétition pour résoudre un problème mathématique difficile et dont la solution est facile à confirmer. Une fois celle-ci trouvée, elle est diffusée au reste du réseau et un nouveau bloc est créé (comme une nouvelle page qui est ajoutée à un grand livre comptable). Ce travail est récompensé en devise bitcoin créant ainsi un incitatif financier à préserver l'intégrité du réseau.

Bitcoin peut être expliqué comme une technologie qui convertit de l'électricité en archives véridiques via la dépense de puissance de calcul.

Le coût financier de l'ajout d'un bloc est très élevé alors que le coût de vérification est très bas. Cette caractéristique élimine pratiquement l'incitatif de quiconque à créer des transactions invalides. La détection de fraude s'effectue à peu de frais tandis que le coût de la perpétrer est extrêmement élevé. Pour inscrire une transaction frauduleuse au registre, il faudrait avoir accès à, payer pour et maintenir la majorité (51%) de la puissance de calcul du réseau.

Les faits historiques du registre sont écrits avec une dépense énergétique.
Il n'y a pas de façon abordable de réécrire l'histoire.

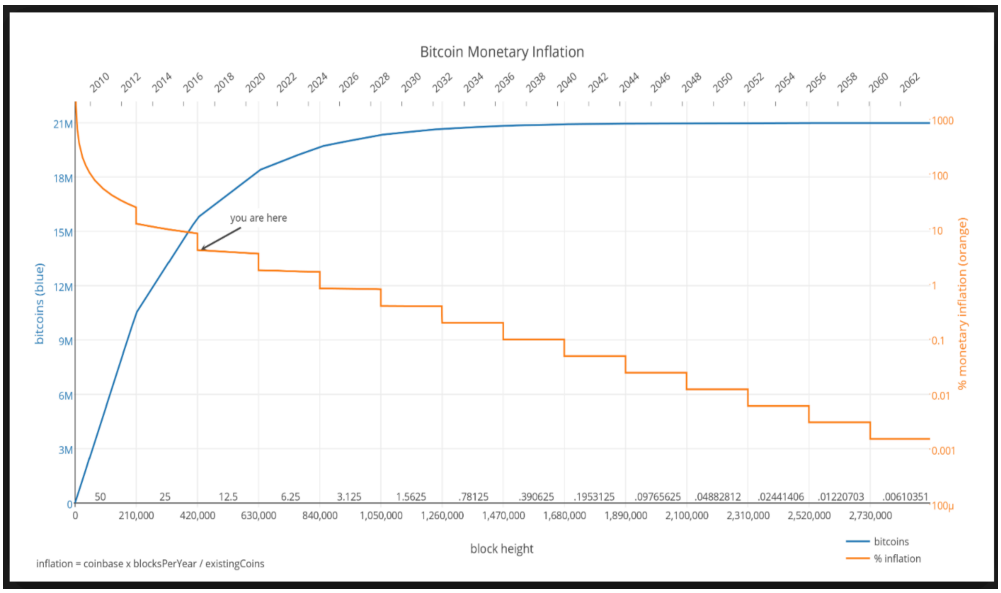
Le rapport de KPMG[6] n'a soit pas fourni suffisamment d'information ou a fourni de l'information qui mérite d'être précisée, complétée ou nuancée. La section 1 de l'annexe 1 se penche sur le volet preuve de travail. Cette annexe vise à nuancer, préciser ou apporter un complément d'information à l'étude de KMPG intitulée « Analyse économique des installations de minage d'actifs cryptographiques ».

[5] http://wcours.gel.ulaval.ca/2016/h/GIF3003/default/5notes/diapositives/pdf_H16/C12.pdf (Dernière consultation 03/10/18)

[6] Rapport de KPMG intitulé « Analyse économique des installations de minage d'actifs cryptographiques » et daté du 26 février 2018

1.2 Dynamique économique

La devise bitcoin est l'actif monétaire (et la première application) du protocole Bitcoin. Ils sont indissociables. La courbe d'émission de la devise bitcoin est transparente et pleinement prévisible[7].



Un élément qui est souvent mal compris est que même si l'on déploie plus de puissance de calcul (c'est-à-dire en augmentant la dépense énergétique pour trouver le hash), il n'y aura pas plus d'unités de la devise bitcoin qui seront créées.

L'effet obtenu sera d'augmenter temporairement la vitesse de validation des blocs (qui s'effectuent environ toutes les dix minutes). Cet effet est temporaire puisqu'à chaque 2016 blocs, la difficulté de calcul est ajustée à la hausse ou à la baisse (via le taux de hachage) en fonction de l'augmentation ou de la diminution de la puissance de calcul qui est fournie au réseau. Ce mécanisme permet de ramener la vitesse de validation d'un bloc à dix minutes.

Progression du taux de hachage du protocole Bitcoin au 28 septembre 2018[8] (52.163 Ehash/s)

[7] https://cointelegraph.com/news/worlds-best-performing-currency-bitcoin-inflation-rate-drops-to-4 (03/10/18)
[8] https://bitinfocharts.com/ (28-09-18)

Plus la difficulté de calcul est élevée, plus le centre de calcul de cryptomonnaie doit déployer de puissance de calcul ce qui a pour effet d'augmenter directement sa facture d'énergie. La profitabilité du centre de calcul s'évalue essentiellement en fonction du coût de la dépense énergétique, du prix de la devise bitcoin et de l'efficacité de l'équipement informatique utilisé pour miner. Il y a un seuil de rentabilité en deçà duquel il n'est pas économiquement rationnel d'ajouter de la puissance de calcul au réseau. Le prix de l'électricité est un facteur déterminant.

Il est possible de tracer un parallèle simplifié avec le marché de l'or. Plus il y a d'or d'extrait, plus l'offre d'or sur le marché est élevée et l'augmentation de l'offre crée une pression à la baisse sur les prix. Les mines d'or qui sont au seuil de la rentabilité ne pourront éventuellement plus continuer à opérer à ces conditions et cesseront ou diminueront leur production. Moins d'or sera ainsi extrait, ce qui diminuera l'offre, créant une pression à la hausse sur les prix, ce qui incitera les mineurs d'or à recommencer à extraire.

L'ajustement de difficulté dans le protocole sert à compenser le fait que la courbe d'émission est entièrement prévisible. Un apport supplémentaire en ressources énergétiques, financières ou matérielles ne changera pas la somme produite selon le protocole.

Un autre élément qui est souvent mal compris est que le cours de la monnaie bitcoin n'est pas un facteur à considérer en isolation pour déterminer la rentabilité des opérations. La puissance de calcul et le cours sont interdépendants. Par exemple, il est possible que le prix du bitcoin soit à la baisse et que la profitabilité soit à la hausse si le taux de hachage est en baisse. L'inverse est aussi vrai.

Dans le scénario où le taux de hachage est à la hausse et que le prix du bitcoin est en baisse, les centres de calcul qui étaient au seuil de rentabilité et qui sont maintenant à perte vont éteindre de l'équipement informatique, ce qui créera une pression à la baisse sur le taux de hachage. Il est important de comprendre ce mécanisme d'autorégulation pour saisir les fondements économiques de cette industrie. L'énergie étant la plus grande dépense au budget des centres de calcul, leur compétitivité est directement liée au prix de l'énergie auquel ils ont accès. Ceci est important pour le Distributeur car les clients qui sont les moins compétitifs sont ceux qui devront éteindre l'équipement en premier. Un tarif non compétitif aurait l'effet de diminuer la compétitivité des centres de calcul en sol québécois puisqu'ils devront éteindre les machines avant d'autres. Advenant la situation où une partie ou la totalité de l'équipement devait être débranchée, les ventes d'électricité et les revenus des entreprises diminueraient ou cesseraient.

L'estimation de la consommation énergétique mondiale du réseau Bitcoin dans son ensemble doit, outre le taux de hachage, prendre en compte l'efficacité de l'équipement informatique utilisé pour effectuer les calculs. En date du 24 mars 2018, la consommation totale d'électricité était estimée entre 2 187 et 5 809 MW. Veuillez vous référer à l'annexe 2 pour obtenir le cadre d'estimation.

En tenant compte de la dynamique économique entre le taux de hachage, la dépense monétaire associée à la dépense énergétique et l'actif monétaire produit, on peut démontrer qu'il n'était pas économiquement viable de déployer toute cette puissance énergétique sur le réseau. Ceci va à l'encontre des intérêts économiques des centres de calcul. On peut aussi se questionner sur la faisabilité et la disponibilité du matériel informatique permettant de répondre à une telle demande.

Donc, des demandes de l'ordre de plusieurs milliers de MW (18,000 MW ou 6500 MW) [9] [10] telles que formulées au Distributeur signalent une demande simultanée d'entrepreneurs désirant déployer de la puissance de calcul pour miner de la cryptomonnaie et non pas une capacité réelle d'absorption du déploiement de cette puissance sur le réseau.

Il est possible qu'une partie des demandes formulées au Distributeur provienne d'entreprises internationales voulant déplacer leurs opérations. Cette situation n'aurait pas pour effet d'augmenter la capacité du réseau Bitcoin mais plutôt de la déplacer. Ceci dit, les principes de la décentralisation sont un pilier de l'architecture Bitcoin. La diversification géographique des centres de calcul est une caractéristique non négligeable. Donc bien que le Québec soit un endroit propice pour les centres de calcul de cryptomonnaie, il n'est pas souhaitable que le réseau soit déployé en totalité au même endroit et ce, dans l'intérêt économique de tous les participants à l'écosystème. Par exemple, s'il y a une tempête de verglas comme en 1998 et que tous les centres de calcul du Québec sont interrompus, le réseau survit quand même. La diversification géographique des nœuds et des centres de calcul est une protection.

Pour estimer la vraie demande d'augmentation en puissance qui serait déployée sur le réseau Bitcoin, on doit tenir compte des déplacements d'équipements actuels par rapport au branchement de nouveaux équipements.

Par ailleurs, comme le coût de l'énergie est la plus grande dépense des centres de calcul, les fournisseurs tels que les fabricants de puces ont tout intérêt à poursuivre leur R et D afin d'offrir de l'équipement toujours plus performant. Par exemple, au cours des 4.5 dernières années, le taux de hachage a augmenté de 300% annuellement[11]. Mais au cours de la même période, l'efficacité des puces a augmenté en moyenne de 80% par année et le coût de la puce ($/TH/s) a diminué de 50% annuellement. Les centres de calcul ont intérêt à développer des procédés énergétiquement efficaces car l'impact de ces améliorations est directement lié à la profitabilité de leur entreprise.

L'évolution de l'équipement utilisé pour miner la devise bitcoin témoigne des progrès qui sont faits. Initialement, il était possible de miner avec des CPU (processeur standard d'ordinateur), puis avec des GPU (matériel informatique spécialisé disponible au détail). Il y a eu une brève période associée au FPGA après les GPU. Présentement ce sont les ASIC (Application-Specific Integration Circuit) qui sont utilisés. Cette évolution requiert de la R et D sur les procédés technologiques et n'est pas unique. Prenons l'exemple il y a 40 ans, du premier téléphone cellulaire[12]. Le poids de l'appareil (un kilogramme) était rébarbatif au transport, sa durée d'utilisation extrêmement limitée (35 minutes) et la durée de charge très longue (10 heures). La R et D fait qu'aujourd'hui les téléphones sont légers, ils permettent d'effectuer des appels vidéo et de rouler une multitude d'applications. Les moteurs technologiques deviennent plus efficaces avec le temps lorsqu'il y a un incitatif financier à les développer.

[9] HQD1 doc 6 p. 3-4

[10] https://www.lesoleil.com/affaires/cryptomonnaies-hydro-croule-sous-la-demande-978779cd0acb29f0823dc50922a73c26 (03/10/18)

[11] https://medium.com/coinshares/re-cost-of-mining-misconceptions-e3fcff1ce726 (03/10/18)

[12] https://ici.radio-canada.ca/nouvelle/607003/telephone-motorola-iphone (03/10/18)

1.3 Complément d'information

«Le Distributeur réitère le contexte prévalant au début de l'année 2018, alors qu'il faisait face à un nombre record de demandes de raccordement représentant plusieurs milliers de MW. Les capacités techniques d'Hydro-Québec pour planifier et réaliser les infrastructures nécessaires pour répondre à toutes ces demandes sont largement insuffisantes. Aussi, les délais de réalisation pour lancer des projets d'infrastructures d'une telle ampleur ne sont pas compatibles avec l'urgence exprimée par les demandeurs pour profiter d'un secteur en pleine effervescence.[13]*»*

« Le Distributeur prévoit, à court terme, une augmentation de la proportion des demandes pour l'usage cryptographique appliqué aux chaînes de blocs concernant l'intelligence artificielle et les cryptomonnaies autres que le bitcoin.[14]*»*

- Les principales cryptomonnaies qui utilisent actuellement la preuve de travail sont : bitcoin (BTC), ethereum (ETH), bcash (BCC), litecoin (LTC) et monero (XMR).
- Bitcoin représente de loin la plus grande puissance de calcul (voir annexe 3)
- D'autres cryptomonnaies utilisent des procédés différents qui ne sont pas aussi énergivore mais dont les propriétés, les modèles d'affaires et le déploiement commercial (cas d'utilisation) sont encore à l'étape du développement ou ne sont pas encore prouvés.
- Les projets en intelligence artificielle et chaînes de blocs semblent être développés avec du matériel informatique (GPU). La méthode de consensus utilisée, le type de chaînes de blocs (ouverte ou fermée), le niveau de sécurité nécessaire et l'utilisation dudit projet détermineront si la consommation énergétique sera élevée ou non.

Avec cette compréhension le Distributeur aurait pu atténuer ses craintes de ne pouvoir répondre à la demande en identifiant que les demandes étaient largement supérieures à la capacité économique des réseaux sur lesquels cette puissance aurait été déployée. Il aurait aussi pu s'apercevoir qu'il nuirait à la compétitivité de ses clients à l'échelle internationale en imposant un tarif non compétitif. Il aurait possiblement pu déterminer d'entrée de jeu que, l'enjeu est la manière simultanée dont les demandes ont été présentées et non le plein déploiement de ces demandes. Nous verrons à la section 2 d'importantes nuances relativement aux définitions de l'industrie car il est possible qu'une perception existe voulant que toutes les cryptomonnaies et usages cryptographiques appliqués aux chaînes de blocs soient de grands consommateurs d'énergie.

[13] HQD-2 doc 5 (2.1) p. 5

[14] HQD-2 doc 1 en liasse Annexe B (11.) p. 3

1.4 Conséquences : mesures protectrices

La situation des « demandes massives, soudaines et simultanées »[15] exposée préalablement et l'information sur l'industrie dont disposait le Distributeur ont donné lieu à certaines mesures protectrices.

- « Le Distributeur soutient que la fixation de tarifs et conditions de service provisoires pour une alimentation en électricité pour un usage cryptographique appliqué aux chaînes de blocs est nécessaire de façon urgente. [16]»
- « Ces tarifs et conditions de service provisoires permettront d'assurer la sécurité des approvisionnements du Québec dans ce contexte particulier et de demandes massives soudaines, inattendues et simultanées annoncées par des clients utilisant la technologie de la chaîne de blocs, y compris du minage de cryptomonnaie.[17] »
- « Les résultats du processus de sélection constitueront une base factuelle pertinente afin que la Régie puisse se prononcer sur les risques associés à cette industrie et sur le caractère juste et raisonnable des tarifs et conditions de services qui seront fixés pour l'usage cryptographique appliqué aux chaînes de blocs.[18]»
- « La quantité associée au Bloc dédié est de 500MW en service non ferme pour une durée minimale de 5 ans. Cette quantité est importante mais permet au Distributeur d'être en mesure de répondre aux demandes d'alimentation des autres industries au Québec.[19]»

Outre les mesures protectrices, la situation a été propice à l'expression de certaines préoccupations du Distributeur et du rapport KMPG relativement à la pérennité du réseau, du modèle d'affaires, des charges et de la volatilité du cours des actifs cryptographiques.

1.5 Préoccupation exprimée : pérennité

La situation des « demandes massives, soudaines et simultanées »[20] exposée préalablement et l'information sur l'industrie dont disposait le Distributeur a donné lieu à certaines mesures protectrices.

« ...afin que la Régie puisse se prononcer sur les risques associés à cette industrie et sur le caractère juste et raisonnable des tarifs...[21]»

---

[15] HQD-2 doc 1 (2.) p. 3
[16] HQD-2 doc 1 en liasse Annexe B (42.) p. 8
[17] HQD-2 doc 1 en liasse Annexe B (49.) p.9
[18] HQD-2 doc 1 en liasse Annexe B (72.) p. 11
[19] HQD-2 doc 1.2 (vi) p. 11
[20] HQD-2 doc 1 (2.) p. 3
[21] HQD-2 doc 5 (7 i) p. 13

Commentaire sur la pérennité du Réseau Bitcoin

« Les clients font partie d'un nouveau secteur d'activité peu connu, dont la demande est exceptionnelle, mais pour laquelle la pérennité est incertaine;[22]*»*

« Par ailleurs, le Distributeur n'a aucune assurance quant à la pérennité de la demande associée à l'usage cryptographique appliqué aux chaînes de blocs.[23] *»*

Retournons un instant au milieu des années 1990 alors que l'Internet en était à ses débuts. Certains ont douté de ce secteur d'activité nouveau et peu connu. À titre d'exemple, en 1998, M. Paul Krugman, lauréat du prix Nobel d'économie, a prédit que :

« The growth of the Internet will slow drastically, as the flaw in "Metcalfe's law" - which states that the number of potential connections in a network is proportional to the square of the number of participants - becomes apparent: most people have nothing to say to each other! By 2005 or so, it will become clear that the Internet's impact on the economy has been no greater than the fax machine's.[24]*»*

Vous trouverez à la section 3 du présent rapport une présentation sur les applications actuelles et potentielles de la technologie Bitcoin et de la monnaie bitcoin. L'objectif est d'y expliquer la nature de l'innovation afin de comprendre sa pérennité potentielle.

Commentaire sur la pérennité du modèle d'affaires

À sa plus simple expression, un centre de calcul convertit des joules d'énergie en actif monétaire.

Le rôle des centres de calcul n'est pas de créer des bitcoins, mais plutôt d'inscrire des entrées dans le registre de la cryptomonnaie, c'est-à-dire d'ajouter des blocs à la chaîne de blocs. Leur travail consiste à fournir de la sécurité en vérifiant la validité des transactions et des blocs selon les règles établies.

Le fait que le processus de vérification génère des bitcoins est un effet secondaire qui sert d'incitatif financier (théorie des jeux) pour assurer que les règles de consensus soient suivies adéquatement. Ce sont les centres de calcul qui prennent la décision d'entreprise d'encourir la dépense énergétique en échange de l'incitatif financier qu'est la devise bitcoin.

---

[22] HQD-2 doc 1 (3.2) p. 8

[23] HQD-2 doc 1 en liasse Annexe B (19) p. 4

[24] https://web.archive.org/web/19980610100009/http://www.redherring.com/mag/issue55/economics.html (03/10/18)

Lorsque tous les ''nouveaux'' bitcoins seront minés (un maximum de 21millions atteint en 2140), le rôle des centres de calcul ne cessera pas pour autant. Ils continueront d'inscrire les transactions bitcoins dans les blocs et leur incitatif financier continuera d'être les frais (libellés en bitcoin) associés aux transactions.

Le protocole Bitcoin est un logiciel à l'architecture ouverte qui se développe depuis près de dix ans. L'augmentation de la puissance de calcul associée à ce type de réseau est un excellent indicateur de la santé de celui-ci. Elle témoigne d'un nombre croissant d'investissements en infrastructure (équipement informatique, dépense énergétique) qui y est fait à l'échelle de la planète. Dit différemment, la puissance de calcul augmente justement parce que des entrepreneurs investissent dans l'infrastructure dans l'expectative de générer un retour sur investissement.

Le nombre croissant d'utilisateurs, la présence d'une communauté technique vibrante qui soutient le réseau et la participation de joueurs financiers traditionnels (voir annexe 4) développant des solutions pour ce nouveau marché sont aussi des indicateurs de santé du réseau.

Les demandes simultanées qu'a reçues le Distributeur témoignent que des entrepreneurs privés sont prêts à déployer des capitaux significatifs pour participer à cette industrie et indiquent un fort signal de marché. Les entrepreneurs y croient et veulent y investir.

Le minage de bitcoins est l'une des rares industries où la rentabilité peut-être prédite avec précision lorsque toutes les variables économiques sont connues. Il y a donc peu de hasard puisque ces variables (prix du bitcoin, coût et efficacité de l'équipement et puissance de calcul) sont transparentes, accessibles et connues. Le Distributeur a le potentiel de servir des clients qui effectuent leur calcul de rentabilité avec une précision élevée. La donnée manquante actuelle est le prix de l'électricité.

Commentaire sur la pérennité de la charge (consommation énergétique)

> *« En effet, les charges en provenance du secteur d'activité sont considérables et la nature de celui-ci font en sorte que plusieurs questions se posent quant à sa pérennité.*[25] *»*

Tel qu'expliqué précédemment, la preuve de travail est ce qui explique la consommation énergétique. Y trouver une alternative est un problème ouvert en science informatique et représenterait une percée technologique majeure. La dépense énergétique du protocole Bitcoin n'est pas un défaut, c'est une propriété. Elle est essentielle, assure la sécurité du réseau et fait partie des raisons pour lesquelles la chaîne de blocs de Bitcoin (p. 21) est considérée immuable.

[25] HQD-2 doc 1 (5.2) p. 14

Commentaire sur la pérennité des activités en sol québécois

> *« (…) ceux-ci demeuraient plus risqués que d'autres clients comme les centres de données et les mines du fait de l'importance de leur charge et la nature hautement volatile du cours des cryptomonnaies qui influence l'intensité de leurs activités et leur capacité à se relocaliser dans d'autres juridictions dans de brefs délais.*[26] *»*

La volatilité des cours n'a pas d'influence directe sur la relocalisation dans d'autres juridictions. L'influence de la variation des cours, tel qu'illustré à la section sur la dynamique économique qui doit tenir compte du taux de hachage, se fait sentir sur la profitabilité. Les machines sont allumées ou éteintes. Le choix d'emplacement inclut plusieurs facteurs dont le contexte politique, règlementaire, et le climat. Mais le principal facteur est l'accès et le coût de l'énergie.

Il est vrai que certaines entreprises sont possiblement plus mobiles que d'autres. Certaines entreprises déploient leur équipement informatique à l'intérieur de conteneurs. Ces conteneurs peuvent être localisés à différents endroits et être déplacés avec plus de facilité. D'autres entrepreneurs choisissent d'établir leur centre de calculs à l'aide d'installations fixes. Ces installations peuvent cibler des usines désaffectées et leur donner un second souffle. Elles ont la caractéristique d'être moins mobiles et diminuent la capacité à se relocaliser dans d'autres juridictions dans de brefs délais. Les préoccupations du Distributeur pourraient être allégées en prenant en considération cet aspect et en favorisant les installations fixes lors du choix de ses clients.

Commentaire sur la volatilité du cours des cryptomonnaies

> *« Dans l'hypothèse où le Distributeur serait en mesure d'obtenir les garanties financières nécessaires pour couvrir le risque à l'égard du coût de raccordement des clients pour un usage cryptographique, ceux-ci demeuraient plus risqués que d'autres clients comme les centres de données et les mines (…) de la nature hautement volatile du cours des cryptomonnaies qui influence l'intensité de leurs activités »* [27]

> *« On en peut donc éliminer le risque que les entreprises qui s'établiraient au Québec pour réaliser du minage de bitcoins, ou certaines d'entre elles, réduisent voire ferment leurs opérations si le contexte change.*[28]*»*

C'est vrai, et ce, au même titre que n'importe quelle autre industrie. Il s'agit d'une décision et d'un risque d'entreprise. Comme nous l'avons vu précédemment, à la section sur la dynamique économique, le cours du bitcoin n'est que l'une des variables à considérer pour évaluer la

[26] HQD-2 doc 1.2 (1 ii) p. 3 et HQD-2 doc 5 (7 ii) p. 4-5
[27] HQD-2 doc 1.2 (1 ii) p. 3 et HQD-2 doc 1.1 (4 ii) p. 10
[28] Rapport KPMG Section 1.3 p 4

profitabilité. À titre d'exemple, il est possible que le prix du bitcoin soit à la baisse et que la profitabilité soit à la hausse si le taux de hachage est à la baisse. Les centres de calcul de cryptomonnaie vivent actuellement une tempête parfaite : le prix du bitcoin est à la baisse et le taux de hachage est significativement à la hausse. Le fait que les demandes en électricité soient toujours présentes témoigne de la confiance que les entrepreneurs placent dans le futur de leurs activités commerciales qui justifie leur investissement.

Toutes les cryptomonnaies ne sont pas des clients dont la proposition est énergivore ou même fonctionnelle. Il est important de découpler le prix d'une cryptomonnaie en particulier du prix des cryptomonnaies dans leur ensemble. Le protocole Bitcoin a une dépense énergétique qui supporte la sécurité de son actif monétaire et a un schème de monétisation démontré. Cette phrase n'est pas applicable à l'ensemble des cryptomonnaies.

Veuillez au besoin vous référer au commentaire sur la pérennité du réseau, à la section sur la dynamique économique et au commentaire complet au sujet du rapport de KPMG à l'annexe1.

La cryptomonnaie et l'usage cryptographique appliqué aux chaînes de blocs sont traités différemment que d'autres types d'entreprises. À ce sujet, mentionnons deux réponses qu'a données le Distributeur et qui pointent vers ces différences.

« Le Distributeur gère les risques pour les autres secteurs par l'obtention de garanties ou lettres de crédit, comme il est prévu aux conditions de services.[29] *»*

« Veuillez préciser si le Distributeur considère le cours du minerai lorsqu'il reçoit une demande de raccordement de la part d'un client dans le secteur minier ? Rép : non[30] *»*

L'industrie de l'usage cryptographique appliqué aux chaînes de blocs est certes relativement nouvelle, mais comporte des risques similaires ou qui chevauche d'autres industries : changement de modèle d'affaires, changement technologique, baisse de la demande, volatilité des prix, amélioration de processus des compétiteurs, etc. Le Distributeur pourrait utiliser le même type d'outils de gestion de risque qu'il applique par exemple aux mines ou aux centres de données, mais dans le cadre des centres de calcul. Par ailleurs, le Distributeur reconnait qu'il n'est pas de son ressort d'évaluer le caractère réaliste d'un projet.

« Le Distributeur est d'avis que l'évaluation du caractère réaliste d'un projet particulier, quel que soit l'usage, n'est pas de son ressort[31] *» (contexte demande de 2000 MW).*

---

[29] HQD-2 doc 5 (7.1) p. 14
[30] HQD-2 doc 5 (7.2) p. 14

1.6 Sommaire de réflexion

Rappelons finalement que le minage de bitcoins produit un actif qui est une commodité ayant des propriétés apparentées à l'or et qui permet aux entreprises dans ce secteur d'activité de payer pour l'électricité, les impôts fonciers, les impôts d'entreprise, les salaires des employés et d'avoir la possibilité de générer un bénéfice net qui peut être redéployé vers de la R et D pour poursuivre l'exploration des usages cryptographiques appliqués aux chaînes de blocs.

À la lumière de ces précisions quant à la pérennité (du réseau, du modèle d'affaires, de la consommation) et à la volatilité du cours des cryptomonnaies, et afin que la Régie de l'énergie « puisse se prononcer sur les risques associés à cette industrie et sur le caractère juste et raisonnable des tarifs [32]», est-il toujours pertinent de considérer que :

> *« … Ceux-ci demeuraient plus risqués que d'autres clients comme les centres de données et les mines du fait de l'importance de leur charge, de la nature hautement volatile du cours des cryptomonnaies qui influence l'intensité de leurs activités et de leur capacité à se relocaliser dans d'autres juridictions dans de brefs délais.* [33] *»*

Avant de répondre à cette question, il est important d'aborder la deuxième problématique identifiée : la compréhension et les nuances de ce qui est actuellement appelé : « usage cryptographique appliqué à la chaîne de blocs ».

[31] HQD-2 doc 5 (10.5) p. 21
[32] HQD-2 doc 5 (7 i) p. 13
[33] HQD-2 doc 5 (7 ii) p. 4-5 et HQD-2 doc 1.2 (1 ii) p. 3

2. Nuances, définitions et compréhension de l'industrie

L'industrie est nouvelle et complexe, le jargon utilisé n'est pas familier, l'expertise est rare et d'importantes nuances sont essentielles afin de prendre des décisions informées.

Messages clés

Toutes les cryptomonnaies et les projets auxquels est associé le terme parapluie "chaînes de blocs" ne sont pas de grands consommateurs énergétiques.

- Ce qui consomme de l'énergie ce n'est pas la chaîne de blocs, mais la preuve de travail.
- La chaîne de blocs n'existe pas en isolation. C'est une résultante.
- Tous les projets nommés "chaînes de blocs" ne sont pas automatiquement immuables.
- Il y a une certaine convergence entre centres de données et centres de calcul.
- Il existe une nuance dans les cas d'utilisation. Les sections 3 et 4 y sont dédiées.
- Le « changement significatif du profil de consommation» ne permettra pas d'identifier tous les cas d'utilisations et donc la définition du bloc de 500MW est difficilement applicable.
- La facturation séparée ne pourra être appliquée.
- Les outils de surveillance ne seront pas efficaces.
- Isoler la preuve de travail créerait une injustice à l'intérieur d'une même catégorie d'utilisation.

Le manque de compréhension de ces éléments et des nuances importantes pourrait mener à des décisions injustes ou inapplicables.

2.1 Les définitions

Chaîne de blocs[34] : « signifie une base de données distribuée et sécurisée, dans laquelle sont stockées chronologiquement, sous forme de blocs liés les uns aux autres, les transactions successives effectuées entre ses utilisateurs depuis sa création, selon les variantes actuelles et futures. »

Usage cryptographique appliqué aux chaînes de blocs [35]: « signifie un usage de l'électricité pour l'exploitation d'équipements informatiques aux fins de calculs cryptographiques permettant notamment de valider les transactions successives effectuées entre utilisateurs de chaînes de blocs.

Ces définitions sont problématiques, car elles supposent que:

- La chaîne de blocs peut être considérée en isolation.
- Toutes les initiatives sont de grandes consommatrices d'énergie.
- Il n'y a pas de nuances entre les chaînes de blocs ouvertes, fermées ou à permission.

[34] HQD-2 doc 1 en liasse Annexe B (31.) p. 7 et HQD-2 doc 7 (1. iii) p. 3
[35] HQD-2 doc 1 en liasse Annexe B (31.) p. 7 et HQD-2 doc 7 (1. iii) p. 3

- Le même niveau de sécurité est nécessaire tant pour un actif monétaire (tel que le bitcoin) et des jetons de jeux vidéo, des fichiers de données, jetons de fidélisation, etc.

Technologies sous-jacentes

La chaîne de blocs est souvent présentée comme LA technologie sous-jacente à Bitcoin. C'est partiellement vrai. Bitcoin est basé sur quatre technologies sous-jacentes et interreliées dont fait partie la chaîne de blocs à titre de résultante:

1. **Réseau pair-à-pair :** une structure de réseau à l'intérieur de laquelle les membres qui y participent ont les mêmes privilèges et obligations les uns envers les autres. Il n'y a pas d'autorité centrale qui peut changer les règles du réseau.

2. **Système de validation:** comme utilisée dans Bitcoin, la preuve de travail offre une solution au problème informatique de la double-dépense sans intermédiaire de confiance. C'est la seule solution à grande échelle connue au « problème des Généraux byzantins». En d'autres mots, trouver une alternative à la preuve de travail est un problème non solutionné en science informatique.

3. **Cryptographie :** les mécanismes de hachage et de signature cryptographique permettent de générer des identités numériques uniques et de vérifier leur validité facilement et avec peu d'effort. Le cryptage ne sert pas seulement à rendre un message "secret" mais sert aussi à identifier de manière unique les expéditeurs et receveurs de messages numériques. Bitcoin s'apparente à un service de messagerie cryptée.

4. **Chaînes de blocs :** la chaîne de blocs est le registre qui contient de l'information objective de l'historique des transactions du réseau. Ce registre est maintenu de manière simultanée par des milliers d'ordinateurs sur la planète. D'où l'appellation « technologie de registre distribué ».

Il est important de mentionner que ces technologies ne sont pas nouvelles.

BitTorrent est un exemple de réseau pair-à-pair qui est utilisé par certaines compagnies pour distribuer leur logiciel. Le principe du système de validation de la preuve de travail sert à dissuader les attaques DDOS (attaque par déni de service) sur un réseau informatique (ex : dissuader le spam par courriel). Les standards cryptographiques utilisés dans le protocole Bitcoin sont largement utilisés en général sur Internet.

Ce qui est nouveau c'est l'assemblage qui a été fait. La chaîne de blocs est une résultante.

On peut comprendre Bitcoin comme un code informatique ouvert qui n'est contrôlé par personne et qui est adopté sur une base volontaire. Les décisions et le fonctionnement sont automatisés et préprogrammés. On peut le comparer au protocole TCP/IP (l'ensemble des protocoles utilisés pour transférer des données sur Internet comme le courriel). On peut aussi le comparer au système d'exploration ouvert Linux : initialement lancé par une seule personne, le logiciel compte aujourd'hui des centaines de milliers de contributeurs et représente la fondation de l'infrastructure serveur

Internet. En ce sens, Bitcoin est apparenté à Linux mais pour le transfert d'information (à qui le marché a attribué une valeur).

Bitcoin n'est pas une compagnie, n'a pas de structure organisationnelle corporative ou de conseil d'administration. Il n'y a pas de siège social, de numéro de téléphone ou même de site web. Bitcoin est une idée qui a été publiée de manière anonyme dans un livre blanc (''white paper'') en 2008. La technologie et le réseau se sont déployés organiquement et spontanément par la suite. L'annexe 5 démontre l'unicité du phénomène.

Pour que l'intégrité d'une chaîne de blocs soit sécurisée et qu'elle fonctionne de manière décentralisée (sans organe de contrôle), certains éléments doivent être présents. Ces propriétés sont rencontrées dans la chaîne de blocs de bitcoin.

La définition suivante est intéressante pour autant que l'on reconnaisse qu'une telle chaîne de blocs est la résultante d'interactions complexes entre plusieurs concepts qui se renforcent l'un et l'autre : cryptographie, incitatif financier (théorie des jeux) et informatique distribué. L'incitatif financier ne semble pas présent dans cette définition.

« Le protocole chaînes de blocs est une technologie de stockage et de transmission d'informations transparente, sécurisée et fonctionnant sans organe central de contrôle. Un réseau chaîne de blocs constitue une base de données qui contient l'historique de tous les échanges effectués entre tous ses utilisateurs depuis sa création. L'intégrité de ce registre (base de données) est garantie par l'utilisation d'algorithmes cryptographiques de signature et de vérification des transactions. Le registre est partagé par ses différents utilisateurs, sans intermédiaires, ce qui permet à chacun de vérifier la validité de la chaîne. Le cryptage des entrées d'information, le partage de l'historique des échanges, de même que cette capacité de validation par tous, expliquent que la base de données soit sécurisée et décentralisée [36]»

Cela est important, car tout ce qui est nommé « chaînes de blocs » n'est pas immuable.

Le fait que la chaîne de blocs ne puisse être altérée est l'une des propriétés qui suscitent un engouement marqué tel qu'en témoignent les nombreux projets qui seront couverts à la section 4. C'est cette propriété d'immuabilité qui permet d'ancrer des données dans le temps sans que personne ne puisse les retirer, les renverser ou en modifier la date.

Cette propriété est rencontrée sur la chaîne de blocs de bitcoin.

Comme expliqué précédemment, une chaîne de blocs n'existe pas en isolation. Afin de déterminer si une chaîne de blocs est véritablement inaltérable, sécurisée, sans intermédiaire et sans organe de contrôle, elle doit pouvoir présenter les qualités suivantes :

[36] HQD-2 document 1 en liasse Annexe B 10. p. 3 qui réfère au Rapport KPMG

- **Ouverte :** c'est-à-dire que les règles de consensus sont transparentes, accessibles sur une base volontaire et sont disponibles à tous via une architecture ouverte.

- **Sans frontière**: accessible à quiconque veut y participer, comme pour l'Internet.

- **Neutre** : les règles de consensus sont radicalement neutres et ne sont pas dirigées par une entité externe. Les transactions sont soit valides ou invalides.

- **Résistante à la censure** : pour que le système soit ouvert, sans frontière et neutre, il doit pouvoir démontrer sa résistance contre des entités qui voudraient par exemple restreindre l'utilisation ou renverser des transactions.

- **Décentralisée** : qui est distribuée, qui n'est pas contrôlée par quiconque.

La chaîne de blocs de bitcoin a acquis sa réputation d'immuabilité après de nombreuses années à résister aux attaques (voir la section 3.2 sur le concept novateur en sécurité informatique). Bien que cette technologie soit encore relativement jeune, cette chaîne se construit depuis près de dix ans et transporte actuellement des milliards de dollars en valeur. Ce qui confère à bitcoin son immuabilité, ce n'est pas sa chaîne de blocs. C'est plutôt l'assemblage de technologies qui le compose et la dépense énergétique colossale qui devrait être engagée pour réécrire l'histoire. Aucun acteur économique rationnel n'encourrait une telle dépense pour "tricher" une transaction.

Il faut donc comprendre que les chaînes de blocs à l'architecture fermée (centralisée) n'offrent pas l'immuabilité numérique et ne règlent pas le problème de la double-dépense sans intermédiaire de confiance. Ces environnements sont facilement identifiables puisqu'il est possible d'y renverser des transactions, de modifier unilatéralement les règles de consensus ou de censurer des utilisateurs. Ce type de projet s'apparente plus à une base de données dotée de signatures et permissions même si l'appellation "chaînes de blocs" est utilisée. De manière générale, ces projets utilisent une autre méthode de consensus (ou des permissions) et requièrent de l'équipement informatique différent et ont un profil énergétique est plus faible. Ils peuvent être utiles dans le cadre de projets dont les niveaux de sécurité ou de décentralisation sont de moindre importance.

Finalement, la force et la résilience d'une chaîne de blocs ouverte sont à leur plus fort quand tous se joignent à un même réseau. Il est donc possible que dans le futur nous référions à LA blockchain. C'est le même concept qui explique qu'il y a plusieurs Intranets (chaînes fermées) mais il n'y a qu'un seul Internet (chaîne ouverte). Par conséquent, il faut spécifier à *quelle* chaîne de blocs l'on fait référence. Comme illustré ci-après, le distributeur n'est pas en mesure de faire une telle distinction.

« Le Distributeur a-t-il envisagé un scénario où la sélection des projets ne s'effectuerait que sur la base des critères qualitatifs (ou non monétaires), excluant ainsi une distorsion au niveau des tarifs applicables à ce groupe de consommateurs » Réponse : Un tel scénario ne permettait pas de répondre aux préoccupations exprimées par le gouvernement dans son décret.[37] *»*

---

[37] HQD-2 doc 5 (8.2) p.16

2.2 Création d'une catégorie parapluie englobant tous les clients

La section précédente a illustré les problématiques des définitions proposées par le Distributeur. Tous les clients de la catégorie proposée ne sont pas de grands consommateurs énergétiques. Le Distributeur a admis ne pas être en mesure de ventiler entre le minage et les autres activités.

«Le Distributeur a présenté à l'engagement n° 2 à la pièce HQD-1, document 6 (B-0023) une ventilation entre le minage de cryptomonnaies et les autres utilisations. Il ne dispose pas de l'information pour départager les différents types de cryptomonnaie.[38] *»*

Illustrons avec l'exemple d'un jeton de fidélité du magasin X. Le développeur du jeton veut utiliser la cryptographie appliquée à la chaîne de blocs. Est-ce que la valeur monétaire du jeton de fidélité vaut la dépense énergétique qu'exige la preuve de travail sur le long terme? Probablement pas puisque c'est la rareté numérique dudit jeton qui crée la richesse.

Un autre exemple est celui du lancement de la chaîne du réseau EOS qui a eu lieu en juin 2018. Cette chaîne teste actuellement la méthode de consensus appelée « preuve d'enjeux délégués ». Le lancement de cette chaîne a certes été chaotique et la viabilité à long terme reste à déterminer mais sa demande énergétique est nettement inférieure à celle du protocole Bitcoin. Pourtant elle rencontre les définitions proposées précédemment bien qu'elle ne consomme pas une grande quantité d'énergie. Notons que « preuve d'enjeux délégués » n'est pas en compétition avec « preuve de travail ». Elles traitent des enjeux différents.

Ces exemples démontrent que des projets qui rencontrent la définition[39] d'usage cryptographique appliqué à la chaîne de blocs peuvent être testés ou développés et qu'ils peuvent avoir un profil de consommation énergétique différent de la preuve de travail. Pensez à Facebook, aux institutions financières, aux paliers de gouvernements et à toutes les industries qui testent des solutions à usage cryptographique appliqué aux chaînes de blocs. Ils devraient faire partir de la catégorie proposée. La section 4 présente une sélection de projets dans différentes industries qui selon la définition actuelle, devraient faire partie de la nouvelle catégorie de clients proposée.

La nouvelle catégorie de clients ne nuance pas la consommation énergétique de ceux qui en font partie. Pourtant cette hypothèse est à la base de nombreux éléments du dossier R-4045-2018 et vise à regrouper les clients sous la même catégorie.

Les hypothèses de départ sont que:

- *« …les clients sont énergivores*[40] *»*
- *« Les abonnements liés à un usage cryptographique appliqué aux chaînes de blocs ont comme caractéristiques particulières d'être énergivores et d'avoir un facteur d'utilisation élevé* [41]*»*

---

[38] HQD-2 doc 1 (1.3) p. 4

[39] HQD-2 doc 1 en liasse Annexe B (31.) p. 7 / HQD-2 doc 7 (1. iii) p. 3 / HQD-2 doc 1 en liasse Annexe B 10. p. 3 réf. Rapport KPMG

[40] HQD-2 doc 1.1 (4. i) p. 10

L'effet de ces hypothèses est de proposer le regroupement des clients sous une même catégorie.

- *« … le Distributeur demande à la Régie d'encadrer la distribution d'électricité pour l'usage cryptographique appliqué aux chaînes de blocs comme suit : a) de façon urgente, approuver la nouvelle catégorie de clients pour un usage cryptographique appliqué aux chaînes de blocs… [42]»*

- *« a) de façon urgente, approuver la nouvelle catégorie de clients pour un usage cryptographique appliqué aux chaînes de blocs. [43]»*

- *«Cependant, le Distributeur rappelle qu'il demande la création d'une nouvelle catégorie de consommateurs visant à regrouper tous les clients usant de la technologie chaînes de blocs.[44] »*

- *« C'est d'ailleurs cette nouvelle catégorie de consommateurs qui permettrait de circonscrire le plus adéquatement l'activité à l'origine de la demande. [45]»*

- *« La présente demande s'applique à tous les usages cryptographiques appliqués aux chaînes de blocs. Le Distributeur n'est pas en mesure de distinguer le minage de cryptomonnaie des autres usages de cette technologie. [46]»*

- *(…) « Cette catégorie comprend tous les consommateurs d'électricité qui sont responsables d'un abonnement au service d'électricité pour un usage de l'électricité pour l'exploitation d'équipements informatiques aux fins de calculs cryptographiques permettant de valider des transactions successives effectuées entre utilisateurs de chaînes de blocs.[47] »*

Les conséquences pratiques de nuancer s'expriment à travers les réponses du Distributeur:

- *« Veuillez indiquer si les consommations en énergie et en puissance sont différentes entre, par exemple, un usage cryptographique appliqué aux chaînes de blocs dans le domaine des « Fintech » et dans le domaine du minage de cryptomonnaie » - le Distributeur ne dispose pas de cette information[48].*

- *«Le cas échéant, les abonnements d'Hydro-Québec ou du gouvernement du Québec pour un usage cryptographique appliqué aux chaînes de blocs seraient assujettis aux tarifs et conditions de service approuvés par la Régie[49] »*

---

[41] HQD-2 doc 1 en liasse Annexe B (14) p. 4
[42] HQD-2 doc 1 (1) p. 3
[43] HQD-2 doc 1 (1a) p. 3
[44] HQD-2 doc 1.2 (6.4) p. 20
[45] HQD-2 doc 1.1 (4. i) p. 10
[46] HQD-2 doc 7 (1.1) p. 4
[47] HQD-2 doc 1 en liasse Annexe B (29) p. 6
[48] HQD-2 doc 7 (2.3) p. 6
[49] HQD-2 doc 7 (1.3) p. 4

2.3 Facturation séparée et outils de surveillance

Les sections précédentes ont illustré les problématiques associées aux définitions actuellement proposées par le Distributeur pour catégoriser les clients de cette industrie et ont expliqué en quoi le profil énergétique n'est pas similaire.

Le « changement significatif du profil de consommation» ne permettra pas d'identifier tous les cas d'utilisations et les applications de la catégorie de client. Ceci empêchera une facturation séparée pour l'ensemble de la catégorie.

Par conséquent, la catégorisation sans ces nuances importantes rendra impraticables plusieurs mesures proposées par le Distributeur. Par exemple :

- *« (…) la consommation d'électricité pour un usage cryptographique appliqué à la chaîne de blocs dans les réseaux municipaux sera isolée et facturée distinctement[50] »*
- *« En outre, et ce de façon générale, les distributeurs appliquent fréquemment des tarifs et options pour lesquels une partie de la facture est calculée au tarif régulier et une autre partie à un prix différent [51]»*
- *« Comme les conditions de service le prévoient, l'usage cryptographique sera considéré comme un abonnement distinct qui sera mesuré séparément. Les tarifs appropriés seront appliqués. [52]»*
- *« Le Distributeur rappelle également que l'usage associé aux centres de données n'est pas un usage équivalent à celui cryptographique appliqué aux chaînes de blocs et pour cette raison, ces deux usages sont facturés séparément[53] »*

Par conséquent, les outils de surveillance envisagés par le Distributeur ne seront pas applicables. Les réseaux municipaux sont également touchés par cette inapplicabilité. Les propositions suivantes ne pourront être implantées:

- *«Pour les autres clients, le Distributeur dispose d'outils informatiques qui lui permettent de déceler tout changement significatif au profil de consommation et à la facture.[54] »*
- *«La proposition du Distributeur au présent dossier est donc cohérente avec les dispositions que l'on trouve présentement aux tarifs qui permettent déjà au Distributeur de capter l'usage chez le client ultime. [55]» (Contexte réseaux municipaux)*
- *« À titre d'exemple, le Distributeur pourrait offrir de mesurer l'usage cryptographique au moyen d'un sous-mesurage au primaire avec l'utilisation de connexions de compteur en parallèle.[56]»*

[50] HQD-2 doc 1 (4) p. 10 et HQD-2 doc 1 8. (40.) p. 21
[51] HQD-2 doc 1 (4.2) p. 11
[52] HQD-2 doc 1.2 (1.3) p. 5
[53] HQD-2 doc 7 (3.3) p. 8
[54] HQD-2 doc 1 (7.1) p. 19
[55] HQD-2 doc 1 (8.1) p. 22
[56] HQD-2 doc 1.2 (1.6) p. 7

- *« Le Distributeur procèdera à des vérifications auprès de ses clients pour s'assurer de l'usage adéquat des charges.[57] »*

- *« Changement significatif » du profil de consommation signifie « il s'agit d'une augmentation de puissance appelée ou du facteur d'utilisation du profil saisonnier de consommation d'électricité ou de tout changement inattendu au profil de consommation pour l'usage habituel du client, le cas échéant.[58] »*

Précisons que le Distributeur sera cependant en mesure de distinguer les variations de consommation pour la preuve de travail, mais uniquement si le réseau qui la déploie a du succès. Par exemple, il est possible de copier le code du protocole Bitcoin et de lancer un nouveau réseau. Ce réseau débuterait avec quelques ordinateurs et la puissance de calcul ne sera pas élevée au début. La puissance de calcul augmente au fur et à mesure que le réseau grossit et parce que des entrepreneurs y font des investissements en infrastructure.

Donc même si on voulait isoler la preuve de travail, cela ne sera pas possible de manière équitable. Cela représenterait une forme de ségrégation à l'intérieur d'une catégorie mais aussi en fonction de la phase d'expansion du réseau. L'effet serait de favoriser financièrement les nouveaux réseaux (plus risqués) qui utilisent la preuve de travail (mais qui ne seraient pas détectables) et de pénaliser le succès des réseaux comme démontré par leur expansion.

Ceci dit, l'annexe 5 explique l'unicité de Bitcoin et pourquoi il sera difficile à répliquer.

2.4 Sommaire de réflexion

Les définitions proposées sont problématiques, car des nuances essentielles sont présentes à l'intérieur de la catégorie de clients proposés. L'hypothèse selon laquelle tous les clients de la catégorie sont énergivores est incorrecte. La facturation séparée et les outils de surveillance ne pourront être implantés comme envisagé.

Même s'ils l'étaient, ils créeraient des injustices basées sur l'utilisation et les applications. Rappelons que les technologies utilisées ne sont pas nouvelles, que la nouveauté réside dans l'assemblage qui en est fait.

Imaginez un centre de données qui fait de la R et D sur un usage cryptographique appliqué à la chaîne de blocs et qui n'utilise pas la preuve de travail. Son profil de consommation énergétique ne sera pas identifié. Pourquoi accepterait-il volontairement de payer un tarif supérieur à celui auquel il a accès dans le cours normal de ses activités?

Par ailleurs, un centre de données peut héberger un centre de calcul. Veuillez consulter l'annexe 6 qui traite de la convergence entre les centres de données et les centres de calcul.

Pour sa part, le centre de calcul est le consommateur énergivore qui génère un actif monétaire. C'est ce type de client qui a un schème de revenu confirmé lui permettant de s'acquitter de sa

[57] HQD-2 doc 5 (7.3) p. 15
[58] HQD-2 doc 7 (2.4) p. 6

facture d'électricité et qui peut réinvestir une partie de ses bénéfices en R et D. Un tarif non compétitif aura l'effet de diminuer sa compétitivité, de dissuader l'établissement local de ces entreprises (vente d'électricité, impôts corporatif et foncier, création d'emploi) et d'étouffer le réinvestissement local en R et D (effet multiplicateur pour le développement économique du Québec).

À la lumière des informations contenues dans les sections 1 et 2, il est peu probable que les principes tarifaires suivants puissent être appliqués dans le contexte proposé.

« La récupération des revenus requis, l'équité, le signal de prix, la simplicité, la stabilité et la continuité tarifaire sont les principes et critères fondamentaux pour porter un regard objectif sur la tarification.[59] *»*

« La fixation des tarifs doit se fonder principalement sur le reflet des coûts de services et non sur l'usage ou le secteur d'activité.[60] *»*

---

[59] HQD-2 doc 1 (3 i 1)
[60] HQD-2 doc 1 (3 i 2) p.7

3. Applications du protocole Bitcoin

« Nous assistons à une révolution technologique.
Peut-être que nous assistons à un miracle moderne.[61] *»*

Rostin Behnam, Commissaire U.S. Commodity Futures Trading Commission (CFTC), 06 2018

« Bitcoin est défini par les mathématiques, il n'y a qu'une certaine quantité de bitcoins, c'est un système distribué… et c'est pur et il n'y a pas d'humains, ni de compagnie qui l'exécute et ça continue à grandir et grandir et survivre, ça me dit qu'il y a quelque chose de naturel et la nature est plus importante que toutes les conventions humaines. [62] *»*

Steve Wozniak, Cofondateur d' Apple, 06 2018

« …Vous n'avez pas besoin de faire confiance au gouvernement ou à Twitter et Facebook ou d'autres personnes sur le réseau. Vous avez simplement à faire confiance aux mathématiques. Et ceci ouvre un monde très intéressant pour les développeurs parce qu'ils peuvent bâtir de nouvelles applications comme l'argent. Personne n'a jamais été capable de programmer de l'argent auparavant. Maintenant oui. Vous pouvez programmer la loi et des contrats sans vous préoccuper d'un avocat corrompu. Vous n'avez pas à faire confiance à un avocat. Vous n'avez pas à faire confiance à un juge. Vous pouvez programmer de la propriété numérique. Vous pouvez créer de l'art qu'une seule personne détient. Vous n'avez pas à faire confiance à un courtier ou à quelqu'un qui pourrait faire semblant… [63] *»*

Ben Horowitz Cofondateur de la firme de capital de risque Andreessen Horowitz, 09 2018

[61] https://www.cftc.gov/PressRoom/SpeechesTestimony/opabehnam7 (03/10/2018)
[62] https://www.cnbc.com/2018/06/04/apple-co-founder-steve-wozniak-hopes-bitcoin-will-become-global-currency.html?__source=facebook%257Ccrypto (03/10/2018)
[63] https://www.youtube.com/watch?v=I7QdIQVTly0 (03/10/2018)

3.1 Comprendre l'innovation : la rareté numérique

L'innovation de Bitcoin est d'avoir créé la rareté numérique sans intermédiaire de confiance. L'une des pièces maîtresses de Bitcoin est d'avoir proposé une solution innovante et fonctionnelle à un problème ouvert en science informatique, soit celui de la double-dépense. Pour expliquer simplement, lorsque vous envoyez une photo via un courriel, c'est une copie de cette photo qui est envoyée. Imaginez à présent que vous puissiez envoyer un fichier sans qu'une copie soit créée, et ce, sans qu'une tierce partie doive témoigner de son authenticité.

C'est le problème qu'a réglé Bitcoin, il y a près de dix ans. Il a été le premier à permettre qu'un actif numérique ne puisse être envoyé à plusieurs destinataires en même temps. À la base, bitcoin c'est de l'espace d'information. Le marché a attribué de la valeur à cet espace parce qu'il est disponible en quantité limitée. Le premier bloc de bitcoins (le bloc de la genèse) a été miné le 3 janvier 2009. Ce n'est pourtant qu'en octobre de la même année qu'une valeur monétaire lui a été attribuée pour la première fois. La monétisation du bitcoin s'est accrue à mesure que le marché a reconnu spontanément son utilité d'entrepôt de valeur numérique.

La prouesse de Bitcoin est de permettre la désintermédiation de la confiance à l'aide d'une infrastructure qui s'appuie sur une interaction complexe entre plusieurs concepts qui se renforcent l'un et l'autre : cryptographie, théorie des jeux, incitatif financier et informatique distribuée. Bitcoin repose à 100% sur la vérification et à 0% sur la confiance. Ce concept repose sur le consensus preuve de travail. Il s'agit de la seule méthode actuellement connue pour régler à grande échelle le problème de la double dépense. Cette compréhension est importante puisque c'est ce qui explique la demande énergétique des cryptomonnaies adoptant cette méthode.

3.2 Concept novateur en sécurité informatique

Les réseaux informatiques tels que nous les connaissons aujourd'hui assurent la sécurité en s'efforçant de rendre les ordinateurs et les serveurs impénétrables. Ce type de sécurité s'active autour d'utilisateurs et de codes d'accès et tente de protéger les données en érigeant des murs de protection. Dans ce type d'architecture centralisée, pour réussir la protection, il faut avoir une sécurité parfaite. Les exemples récents d'Equifax[64] et de British Airways[65] nous rappellent que des millions d'utilisateurs ont pourtant vu leurs données personnelles compromises.

Bitcoin approche la sécurité informatique de manière complètement différente. Bitcoin ne tente pas de sécuriser les ordinateurs individuellement et prends pour hypothèse que tous les nœuds sont potentiellement hostiles. Au lieu de chercher à protéger l'information à l'aide d'une forteresse, Bitcoin l'ouvre et l'étale en la distribuant sur des milliers d'ordinateurs. L'information est distribuée si finement qu'il n'y a pas de faille centrale à exploiter par les pirates informatiques.

---

[64] https://www.cnet.com/news/equifaxs-data-breach-by-the-numbers-the-full-breakdown/ (03/10/2018)
[65] https://thenextweb.com/security/2018/09/12/hackers-used-22-line-code-stole-british-airways data/?utm_source=TNW&utm_campaign=4ce7b44c38-EMAIL_CAMPAIGN_2018_06_07_01_28_COPY_01&utm_medium=email&utm_term=0_32f70ba9aa-4ce7b44c38-12941949&mc_cid=4ce7b44c38&mc_eid=d643670b08 (03/10/2018)

Un système fermé, isolé des forces extérieures a des bogues, mais ceux-ci ne sont pas nécessairement identifiés rapidement. Les vulnérabilités peuvent subsister plus longtemps et les solutions être décalées dans le temps.

Par opposition, un système ouvert est continuellement exposé aux attaques externes. Il a aussi des bogues, mais ceux-ci sont continuellement identifiés. Les vulnérabilités sont identifiées plus tôt et les processus pour les résoudre sont activés rapidement. Le système devient ainsi plus résistant grâce aux différentes attaques, et ce, potentiellement plus rapidement. Par contre, les défis sont différents. La concertation, la coordination et le déploiement des solutions aux bogues identifiés ne sont pas effectués de manière centralisée. La dynamique est différente.

La sécurité de Bitcoin est assurée par la simplicité de son design, par la grande puissance de calcul et par le fait que les différents nœuds doivent atteindre un consensus pour que quelconque changement soit effectué. D'où la notion de consensus distribué à grande échelle sans intermédiaire de confiance.

Bitcoin et la cryptographie en général sont des technologies défensives qui font en sorte que le coût lié à la défense est significativement inférieur au coût d'une attaque. Les tentatives de fraudes sont non seulement extrêmement coûteuses, mais leur chance de succès très mince.

Il est important de préciser que certaines fraudes informatiques ont été commises en périphérie et non dans Bitcoin directement. Ce sont plutôt, par exemple, des plateformes d'échanges telles que MtGox[66], des individus qui ont vendu de la marchandise en échange de bitcoins (sans livrer le produit) ou des pirates informatiques qui ont fait de l'hameçonnage et demandé des rançons en bitcoins. La nuance est importante puisque ce ne sont ni le protocole Bitcoin, ni la devise bitcoin qui ont été piratés.
Puisqu'il est basé sur des standards cryptographiques existants (entre autres SHA-256) et qui sont utilisés dans la plupart des applications Internet, l'impact d'une telle faille serait bien plus catastrophique pour l'ensemble des commerces (incluant les services financiers) et l'Internet en général que pour Bitcoin.

3.3 La première application du protocole Bitcoin

La première application d'Internet fut le courriel.
La première application de Bitcoin fut une monnaie.

Bitcoin est une transformation fondamentale de la technologie de l'argent. À priori, Bitcoin est un système monétaire indépendant, distribué, global, inclusif et qui est adopté sur une base volontaire. Les fonctions d'émission, d'exécution, de compensation et de règlement de la monnaie ont été combinées et sont maintenant possibles de personne à personne, et ce, à l'échelle planétaire. Bitcoin propose un système de paiement prévisible, inaltérable et une monnaie. Il y a 25 ans, le courriel a connecté la planète en termes de communications de personne à personne. Il y a près de dix ans, Bitcoin a connecté la planète au niveau de l'échange de valeur de personne à personne via une devise unique, neutre et mondiale.

[66] https://cointelegraph.com/news/the-mess-that-was-mt-gox-four-years-on (03/10/2018)

La devise bitcoin représente également pour plusieurs un actif rare et précieux. Il représente un entrepôt de valeur numérique basé sur les principes d'un système monétaire reposant sur l'équité et non sur la dette. Bien que volatile et n'ayant pas encore atteint le stade de maturité, le bitcoin est souvent comparé à de l'or numérique.[67] Les propriétés proposées par bitcoin incluent : rareté, divisibilité, durabilité, fongibilité, transportabilité et sans possibilité de contrefaçon. Son utilisation permet également les transferts internationaux de manière efficace, sécuritaire, abordable, rapide et transparente.

Comme pour le courriel, l'adoption est une progression qui s'opère sur plusieurs années. Initialement le courriel était peu répandu. Il était lent et limité dans sa capacité de transfert de fichiers. De nos jours, le courriel est largement répandu, rapide et peut servir à de nombreuses utilisations. L'impact du courriel a largement dépassé les communications de personne à personne et a notamment transformé profondément le commerce, le travail, la transmission de la connaissance, le divertissement et les interactions avec nos institutions financières.

L'innovation que représente la plateforme technologique proposée par Bitcoin pourrait être l'une des pièces déterminantes des interactions économiques dans la quatrième révolution industrielle. Nous sommes à l'ère du développement de l'Internet des objets et de l'intelligence artificielle. Ces objets intelligents et connectés globalement via internet auront besoin d'une devise native avec laquelle ils pourront interagir sans friction et à l'échelle de la planète. Les nouvelles technologies proposées par Bitcoin, par la chaîne de blocs et par la numérisation des actifs s'orchestrent naturellement à l'intersection de ces courants technologiques.

Plusieurs acteurs financiers traditionnels croient en l'avenir de ces nouvelles technologies (annexe 4). Ils créent des rampes d'accès ou de développent des produits afin de continuer à servir leurs clients dans l'écosystème de la cryptomonnaie. Ceci témoigne d'une étape supplémentaire dans la compréhension et l'adoption de ces nouvelles technologies.

3.4 Bitcoin la suite : une vague d'innovations à venir

D'une certaine façon, Bitcoin a résumé, voire simplifié, le système financier en une "application" en donnant naissance à une devise native d'internet. Cette première application a en soi beaucoup de potentiel.

La présente sous-section vise à présenter les autres applications qui sont en voie d'être développés sur Bitcoin. Ces applications sont celles qui ont à priori un besoin d'entrepôt numérique ou de transfert de valeur monétaire, de sécurité et d'immuabilité. Autrement dit, ces projets sont ceux qui ont besoin d'une chaîne ouverte et sans permission (pensez à Internet versus Intranet).
Voici dans un premier temps, quelques applications directes qui sont en progression et dont la concrétisation est à court, moyen terme ou à long terme. Notez également qu'il n'est pas possible de prévoir tous les développements possibles avec cette technologie. Par exemple, Facebook n'aurait pas pu être déployé en 1995 parce que la courbe d'adoption du courriel était au début de sa progression. Une décennie supplémentaire a été nécessaire à l'imagination, au lancement et au

[67] https://www.youtube.com/watch?v=q8R71WGO3qU (03/10/2018)

déploiement de cette entreprise. Voici donc une lecture actuelle et non exhaustive du potentiel applicatif de Bitcoin et de sa chaîne de blocs.

Court terme

- **Conformité** : au lieu d'écrire des règles et de nommer un régulateur pour surveiller les violations, ses règles sont écrites dans le code de Bitcoin et le réseau vérifie la conformité. Si une transaction enfreint les règles, elle est rejetée par le réseau. Les transactions sont valides ou invalides.

- **Virements internationaux** : en quelques minutes, il est possible d'échanger de la valeur avec un partenaire commercial ou d'envoyer de la valeur à un membre de sa famille à l'autre bout de la planète peu importe où il ou elle se trouve, peu importe l'heure qu'il est, et le tout moyennant de faibles frais. Un processus administratif simple et pleinement transparent est disponible avec Bitcoin. Par exemple, l'Unicef[68] en France accepte maintenant de recevoir des dons libellés dans 9 différentes cryptomonnaies.

- **Application de deuxième couche (**second layer application) : permet aux entreprises et aux particuliers de créer des produits et des services par-dessus l'application de base. Par exemple, le *Lightning Network (LN)* est une chaîne développée en parallèle (side chain) qui permettrait d'effectuer des micro-transactions (0.00000001 bitcoin) et de payer instantanément. Ci-dessous un exemple de ce type de micro transaction en développement[69]. Il s'agit d'un projet open source appelé donnercraft et qui utilise le LN pour permettre le paiement dans le jeu Minecraft. On y voit le téléphone interagir avec le QR code du jeu vidéo. (Le QR code est la clé publique du « wallet » de cryptomonnaie).

Les micropaiements instantanés ont le potentiel de bouleverser plusieurs modèles d'affaires. Outre l'industrie du jeu en ligne, pensons notamment aux producteurs de contenu journalistique et artistique et à l'impact sur les modèles d'affaires basées sur la publicité,

[68] https://news.bitcoin.com/unicef-france-accepts-donations-in-9-cryptocurrencies/ (03/10/2018)
[69] https://githb.com/donnerlab1/donnercraft (03/10/2018)

Moyen terme

- **Inclusion financière** : un tiers de l'humanité[70] [71] n'a pas accès au système financier que nous utilisons. Les femmes et les personnes défavorisées sont les plus susceptibles de ne pas avoir de compte bancaire. La combinaison de la progression des téléphones cellulaires, de l'accès à Internet et de l'adoption de la cryptomonnaie pourrait permettre à un grand nombre d'individus d'accéder à la liberté économique.

- **Argent programmable** : c'est-à-dire programmer d'avance des transactions financières à l'aide de HTLC (Hash Time-Locked Contract). L'expéditeur envoie des fonds (ex. : BTC/ETH) à condition que le destinataire exécute une tâche ou livre un produit ou un service à l'intérieur d'une période de temps qu'ils auront déterminée ensemble. Si le service, le produit ou la tâche n'est pas exécuté à l'intérieur de la limite de temps, les fonds seront automatiquement retournés à l'expéditeur. Ce processus pourrait révolutionner la manière dont les entreprises interagissent les unes avec les autres, ou avec leurs consommateurs et pourrait réduire considérablement le temps d'exécution et les frais des transactions commerciales.

Long terme

- **Immuabilité comme service** : utiliser la chaîne de bitcoin peut servir à ancrer des données comme un titre de propriété immobilière, un certificat de naissance ou toute autre information dont on veut préserver l'authenticité et la date historique de manière inaltérable. (Second layer)

- **"Streaming d'argent"** : imaginez louer une voiture pendant 12 minutes et 14 secondes et payer de l'assurance-collision pour 12 minutes et 14 secondes et que le paiement s'effectue en flux continu pendant que vous roulez. Pensez à la diffusion de musique (streaming) qui a remplacé les fichiers mp3 et appliquez ce concept à l'argent.

- **Numérisation d'actifs financiers** : métaux précieux, actions, obligations, autres actifs adossés à Bitcoin.

Voici à présent, quelques exemples de technologies connexes qui pourraient être développées indirectement grâce à l'écosystème:

- **Agritech** : récupération de la chaleur produite par les centres de calcul de cryptomonnaie pour chauffer des serres. Ce concept a été testé sur cinq acres et a permis de faire pousser des tomates (cryptomatoes)[72].

- **Biométrie** : Bitsy[73] développe un "wallet" qui propose d'utiliser la combinaison des marqueurs biométriques votre visage et votre empreinte digitale à titre de clé privée. L'objectif est de simplifier la gestion et la récupération de clés.
- **Énergie renouvelable** : le besoin de sources énergétiques renouvelables et à peu de frais pourrait propulser la R et D vers des solutions novatrices et à grande échelle.

[70] https://news.bitcoin.com/a-third-of-humanity-remains-financially-excluded/ (03/10/2018)
[71] https://globalfindex.worldbank.org/ (03/10/2018)
[72] https://cointelegraph.com/news/cryptomatoes-grows-5-acres-of-fruit-from-bitcoin-mining-heat (03/10/2018)
[73] https://news.bitcoin.com/overstock-to-offer-bitcoin-for-sale-after-acquiring-bitsy-com-biometric-wallet/ (03/10/2018)

- **Matériel informatique** : puces, surveillance automatisée de l'équipement des centres de calcul, autre.

Voici à présent une réflexion à plus long terme portant sur les grands thèmes de la 4e révolution industrielle. Contrairement aux marchés financiers traditionnels, il n'est pas nécessaire d'être un humain pour détenir de la cryptomonnaie. Un robot, un logiciel ou un objet pourrait avoir besoin, dans le contexte de la 4e révolution industrielle, d'être bancarisé.

Des technologies émergentes telles que l'Internet des objets et l'intelligence artificielle auront probablement des effets systémiques sur les générations à venir. Afin d'être pleinement autonomes, ces technologies auront besoin d'accéder à des plateformes de contrats intelligents pour programmer des interactions économiques et à un système monétaire compatible avec leur réalité.

La fragmentation, la lourdeur administrative, la non-disponibilité en temps continu, les coûts élevés et le risque de contrepartie du système financier actuel risquent fort de ne pas pouvoir répondre aux besoins d'agilité, de rapidité, de fluidité, de neutralité et de globalité 24/7 de ces entités économiques autonomes du futur.

Il est aussi possible que ces entités aient besoin d'horodater des actions, des informations ou des titres de propriété sans que ceux-ci soient réversibles. Bitcoin offre un monument d'immuabilité qui a été construit bloc par bloc et qui est disponible à l'échelle mondiale.

Le potentiel d'innovation technologique à l'intersection de l'intelligence artificielle, de l'Internet des objets, de la cryptomonnaie et des chaînes de blocs est riche, pertinent et façonnera probablement un futur très différent de ce que l'on peut imaginer aujourd'hui en fonction des technologies actuellement existantes.

Finalement, il est important de préciser que bitcoin n'est pas la seule chaîne de blocs ouverte. D'autres cryptomonnaies (ex : bcash, litecoin, monero, zcash) tentent de répondre à l'utilité de la monnaie mais Bitcoin est de loin le réseau le plus développé, résilient et ayant passé (en relatif) la plus grande épreuve du temps. Le taux de hachage en témoigne (annexe 3).

D'autres projets de chaînes de blocs ouvertes sont en progression. Notamment le réseau Ethereum et le réseau EOS. Ce ne sont pas des concurrents à bitcoin mais plutôt des plateformes en développement qui ont un modèle d'affaires, un déploiement et des visées commerciales différentes. L'objectif de leur mention est de préciser que le potentiel des chaînes de blocs ouvertes (qui requièrent leur propre cryptomonnaie) ne se limite pas à Bitcoin.

4. Chaînes de blocs et registres distribués

« Il est important de se rappeler que sans Bitcoin il n'y aurait pas technologie de registre distribué. »[74]

J. Christopher Giancarlo, Président U.S. Commodity Futures Trading Commission (CFTC) 02 2018

"...Un milliard de personnes seront dans l'écosystème crypto d'ici cinq ans."[75]

Brian Armstrong, PDG de Coinbase, 09 2018

4.1 La R et D en plein essor

Les modèles d'affaires évoluent, se mondialisent et les solutions technologiques accélèrent ces transformations. Prenons l'exemple de Airbnb qui est le plus grand fournisseur d'hébergement, et ce, sans détenir de propriété, l'exemple de Facebook qui est le fournisseur de contenu le plus populaire sans produire de contenu ou l'exemple de Uber qui domine l'industrie du taxi mondial sans détenir de voiture.

Les thèmes de l'Internet des objets, de l'intelligence artificielle et de la propriété et de la confidentialité des données sont des sujets hautement complémentaires au potentiel applicatif de la chaîne de blocs. Ce potentiel s'inscrit dans un contexte de globalisation, où l'interopérabilité et la gestion des données individuelles sont au cœur des préoccupations de plusieurs.

Rappelons que la chaîne de blocs ne tient pas toute seule, qu'un assemblage de technologies est nécessaire pour réaliser l'infrastructure lui permettant d'exister. Certains projets sont développés dans une architecture fermée (chaînes à permission), d'autres sont développées dans une architecture ouverte pouvant déployer des projets à permission (Ethereum, EOS, autre) et d'autres sont déployés en architecture ouverte et décentralisée et offrent l'immuabilité, comme Bitcoin. Le choix de l'architecture est déterminé par le modèle d'affaires, le produit à livrer et le marché cible.

[74] https://blockexplorer.com/news/cftc-regulator-won-hearts-bitcoin-faithful-us-senate-hearing/ (03/10/2018)
[75] https://techcrunch.com/2018/09/07/coinbase-plots-to-become-the-new-york-stock-exchange-of-crypto-securities/ (19/09/2018)

La section qui suit vise à présenter des exemples de projets en lien avec les chaînes de blocs qui sont en cours de recherche et développement à travers diverses industries. Étant à l'étape de preuve de concept et de R et D ces projets sont plus risqués. Il est possible qu'ils découvrent que ce dont ils ont besoin n'est pas une solution chaînes de blocs ou que le principe de décentralisation n'est pas pertinent à leur modèle d'affaires. Précisons que les projets présentés ne sont que des exemples et que leur inclusion dans le rapport n'indique d'aucune façon qu'ils seront viables, concluants ou commercialisés.

Cette revue internationale à haut niveau vise à illustrer la variété, le type de recherche, le niveau de créativité, le bassin d'expertise qui se développe, le type de problématique que l'on tente de régler et l'ampleur du potentiel applicatif que l'on attribue à l'industrie des chaînes de blocs.

4.2 Les universités s'impliquent

L'implication et la participation d'établissements d'enseignement prestigieux témoignent de l'intérêt envers les cryptomonnaies et l'usage cryptographique appliqué à la chaîne de blocs. Voici quelques exemples d'universités hautement reconnues en Europe et en Amérique et les programmes offerts :

- **MIT Management Executive Education:** Blockchain technologies: Business Innovation and Application[76]
- **University of Oxford**: Oxford Blockchain Strategy Programme[77]
- **Stanford Engineering**: Cryptocurrencies and Blockchain technologies[78]
- **London School of Economics and Political Science**: Cryptocurrency Investment and Disruption[79]
- **Harvard University**: Introduction to Blockchain and Bitcoin[80]

Au Québec, des initiatives de recherche et développement sont également en cours dans nos universités. Premièrement, mentionnons l'initiative du professeur Jeremy Clark[81] du Concordia Institute for Information Systems Engineering. Son équipe de recherche est composée d'étudiants et de diplômés, dont six étudiants et étudiantes au doctorat et une au postdoctorat. Une liste de publications riches et pertinentes sur le sujet de l'usage cryptographique appliqué aux chaînes de blocs et qui couvre une période de plus de dix ans est disponible en ligne[82]. Les travaux de recherche visent les sujets suivants :

- Systèmes de vote vérifiables d'un bout à l'autre
- Bitcoin, Blockchain et Fintech
- TLS et le modèle de confiance CA
- Cryptographie appliquée
- Sécurité utilisable

[76] https://executive.mit.edu/openenrollment/program/blockchain-technologies-business-innovation-and-application/ (05/10/2018)
[77] https://www.sbs.ox.ac.uk/programmes/oxford-blockchain-strategy-programme (05/10/2018)
[78] https://online.stanford.edu/courses/cs251-cryptocurrencies-and-blockchain-technologies (05/10/2018)
[79] http://www.lse.ac.uk/study-at-lse/Online-learning/Courses/Cryptocurrency-Investment-and-Disruption (05/10/2018)
[80] https://online-learning.harvard.edu/course/introduction-blockchain-and-bitcoin (05/10/2018)
[81] https://users.encs.concordia.ca/~clark/index.php (07/10/2018)
[82] https://users.encs.concordia.ca/~clark/academic.php (07/10/2018)

Les deux cours[83] enseignés par le professeur Clark à l'automne 2018 s'intitulent : Bitcoin & Blockchain Technology et Data Structures and Algorithms.

Mentionnons une deuxième initiative, soit celle du groupe de recherche FUSEE[84] de l'école de technologie supérieure (ETS). FUSEE est dirigée depuis décembre 2017 par le professeur Kaiwen Zhang du Département de génie logiciel et des TI de l'ETS. Son expertise se situe à l'intersection des systèmes distribués, du réseautage et de la gestion de données. Son équipe est composée de 14 étudiants diplômés de deuxième ou de troisième cycle universitaire. Cinq membres de l'équipe actuelle possèdent un Ph.D. dont l'expertise dans le domaine de l'usage cryptographique appliqué aux chaînes de blocs est fort enviable.

« Si, la recherche fondamentale sur la sécurité des bitcoins est importante pour M. Zhang, son intérêt réside plutôt dans la recherche et le développement d'applications soutenues par cette même technologie, mais qui seraient différentes de la cryptomonnaie, dans des domaines tels que la santé, l'éducation ou l'Internet des objets.[85] »

M. Zhang est résolu à développer de nouveaux usages appliqués à la chaîne de blocs. Voici quelques exemples de projets[86] :

- « Protocole de consensus pour échanger des données cryptées entre des machines qui appartiennent à différentes organisations permettront de faire en sorte que tout le monde pourra avoir accès aux mêmes informations et que celles-ci seront confidentielles et sécurisées. »
- Les « smart contracts » garantissent que les transactions sont traitées de façon fiable et uniforme, peu importe l'utilisateur. Le chercheur avance même que les archives conservées dans les études de notaires vont perdre leur utilité, car tous ces documents pourront être conservés dans ces fameux « blocs. »

Grâce à ces initiatives universitaires, le Québec peut participer à la R et D dans un domaine émergent et développer une expertise locale dans un domaine où celle-ci est rare, pointue et multidisciplinaire. La création de chaires de recherche et de pôles d'innovation peut contribuer à faire rayonner de telles initiatives en mettant en commun talent, expertise et capitaux.

[83] https://users.encs.concordia.ca/~clark/courses/1803-6630/index.html (07/10/2018)
[84] https://fuseelab.github.io/ (05/10/2018)
[85] http://prof-ets.etsmtl.ca/lets-accueille-le-professeur-kaiwen-zhang-expert-de-la-blockchain/ (07/10/2018)
[86] http://prof-ets.etsmtl.ca/lets-accueille-le-professeur-kaiwen-zhang-expert-de-la-blockchain/ (07/10/2018)

4.3 Authenticité

Problématique visée

L'authentification de documents tels que les diplômes universitaires est une tâche essentielle mais encombrante pour les recruteurs en ressources humaines. Une solution chaîne de blocs peut offrir un environnement en ligne transparent et permettre en quelques clics d'attester de la véracité d'un document éliminant ainsi toute possibilité de fraude.

Exemple de projet

Le MIT (Massachussetts Institute of Technology) a mis en ligne le site suivant : https://credentials.mit.edu/ et permet à l'aide d'une clé publique associée à un diplôme d'en vérifier l'authenticité directement sur une chaîne de blocs.

4.4 Énergie

Problématique visée

La chaîne de blocs peut bénéficier aux producteurs d'énergie en modernisant leurs infrastructures actuelles (avec des grilles intelligentes) mais aussi permettre à de nouveaux marchés de se créer. Cet aspect peut potentiellement servir aux producteurs d'énergie tant au niveau de ses propres installations, mais aussi pour comprendre l'évolution des modèles d'affaires des autres acteurs et partenaires commerciaux situés dans d'autres juridictions. Les solutions chaînes de blocs visent notamment à augmenter l'efficacité des règlements financiers entre les producteurs d'énergie, les intermédiaires qui vendent cette énergie et les consommateurs. La simplification et la standardisation des transactions énergétiques entre les contreparties ainsi que la démocratisation de l'accès aux données énergétiques par le consommateur sont des exemples de bénéfices recherchés par les projets chaînes de blocs liés à l'industrie de l'énergie.

Exemple de projet

Scanergy[87] : il s'agit d'un projet qui a reçu du financement[88] de l'Union européenne et qui vise à adresser la prolifération des "prosumers". C'est-à-dire des consommateurs (par exemple, des maisons qui deviennent des agents autonomes producteurs d'énergie via l'énergie solaire) et qui renvoient de l'énergie dans le réseau. Ceci aurait un impact direct sur la distribution européenne d'énergie. Scanergy vise à répondre à ces problématiques.

- Permettre des transactions efficientes/intelligentes entre les "prosumers" tout en faisant

[87] http://scanergy-project.eu/ (19/09/2018)

[88] Ce projet reçu du financement venant de l'union européenne (Seventh programme for research, technological development and démonstration) subvention # 324321

face à la dynamique de l'offre et la demande.

- Le système prévoit une strate d'intégration pour l'infrastructure énergétique actuellement en place et permettre une coordination presque en temps réel de l'énergie produite et consommée par les habitations, les quartiers et les municipalités.

- Le projet vise une meilleure utilisation de l'énergie renouvelable et une meilleure gestion des gaz à effets de serre (quantification, réduction, meilleure qualité de l'air)

Plusieurs projets liant le secteur de l'énergie à l'industrie de la chaîne de blocs sont en cours. La chaîne de blocs peut servir à exécuter en temps réel, de manière bidirectionnelle des contrats numériques ce qui augmente la transparence en accélérant le flux d'information et en automatisant des décisions pour les producteurs ou les distributeurs énergétiques.

4.5 Financement immobilier

Problématique visée

Plusieurs propriétaires et investisseurs souhaitent minimiser la friction et accéder à des ''pools de liquidité'' sur les marchés internationaux. Le marché immobilier est typiquement reconnu comme un marché moins liquide. La problématique adressée vise à morceler un actif immobilier en titre d'équité et le rendre accessible numériquement.

Exemple de projet[89]

Août 2018 – Le complexe immobilier St.Regis Aspen est l'une des premières propriétés d'envergure aux États-Unis à tester la ''tokenisation''. C'est-à-dire de morceler un actif immobilier réel et en le numérisant à l'aide d'un jeton (token) afin de créer un nouveau véhicule d'accès et de liquidité. Aspen Digital envisage vendre 18 millions de tokens à un prix initial de 1$/token afin de convertir en crypto (token) une portion de la propriété évaluée à 224 millions de dollars. La plateforme Ethereum est utilisée pour permettre l'émission desdits tokens.

Ce même type de financement via la numérisation d'une partie d'un actif réel est aussi en cours de test pour un tableau de Andy Warhol[90]. Cette transaction offre la possibilité d'acheter avec des bitcoins jusqu'à 49% de l'œuvre "14 Small Electric Chairs" et d'utiliser un contrat intelligent sur Ethereum pour numériser l'actif. La numérisation d'actifs réels ouvre des possibilités pour plusieurs classes d'actifs et non pas seulement en immobilier.

[89] http://fortune.com/2018/08/23/hotel-real-estate-aspen-blockchain-ethereum-st-regis-indiegogo/ (19/09/2018)
[90] https://www.forbes.com/sites/billybambrough/2018/06/07/andy-warhol-art-to-be-sold-via-blockchain-for-cryptocurrency-including-bitcoin/#4492908e250d (19/09/2018)

4.6 Centre d'hébergement de données et sites web

La chaîne de blocs sécurise l'accès à la donnée et non la donnée elle-même.

Problématique visée

L'architecture actuelle du web est soutenue par des serveurs centralisés. Cette centralisation peut représenter une faiblesse puisque le serveur (donc son contenu) est vulnérable à un piratage, à une catastrophe naturelle ou à une décision de son propriétaire de le fermer. La problématique visée est la centralisation et une solution décentralisée pourrait être une perspective novatrice pour y arriver.

Exemple de projet

Septembre 2018 – CloudFlare's IPFS Gateway[91] (InterPlanetary File System) est un réseau décentralisé qui tente de répondre à cette situation. Il s'agit d'un réseau pair-à-pair qui est composé de milliers d'ordinateurs à travers le globe et dont la fonction est d'entreposer et de partager des morceaux de fichiers dans le réseau via un protocole de registre distribué. Il y a actuellement plus de 5 milliards de fichiers qui ont été téléchargés sur IPFS.

L'hébergement (données et sites web) ne se fait plus seulement en un lieu centralisé, mais est maintenant aussi possible en morcelant les fichiers et en les distribuant sur des milliers d'ordinateurs. Ceci représente une transformation marquée du modèle d'affaires des centres de données traditionnels. Un autre exemple de ce type d'infrastructure est Filecoin[92]. L'entreposage est distribué et décentralisé ce qui rend le piratage pratiquement impossible puisque chaque ordinateur du réseau devrait être piraté pour y arriver.

[91] https://blog.cloudflare.com/distributed-web-gateway/ (19/09/2018)

[92] https://filecoin.io/ (19/09/2018)

4.7 Services financiers

Les transformations potentielles de la chaîne de blocs dans l'industrie des services financiers sont si vastes qu'une étude spécifique et volumineuse pourrait y être dédiée. L'article suivant résume bien l'ampleur du changement technologique qui est devant nous. Précisons que cet article traite de la "blockchain de bitcoin".

"The "killer app" for the early Internet was email; it's what drove adoption and strengthened the network. Bitcoin is the killer app for the blockchain.[93] *"*


Harvard Business Review

TECHNOLOGY

The Blockchain Will Do to the Financial System What the Internet Did to Media

by Joichi Ito, Neha Narula, and Robleh Ali

MARCH 08, 2017 **UPDATED** MARCH 09, 2017

4.8 Soins de santé

Problématiques visées

- Agréger l'ensemble des données médicales d'un patient sous un même identifiant.
- Conserver en toute sécurité les données confidentielles liées au dossier médical.
- Améliorer la sécurité entourant le partage du dossier médical entre professionnels (généralistes à spécialistes ou entre établissements hospitaliers).
- Dépersonnaliser les données médicales pour respecter la confidentialité individuelle, mais aussi pour permettre aux chercheurs d'accéder aux données de manière anonyme.
- Assurer l'authenticité des médicaments et déjouer les contrebandiers.
- Accélérer les délais de traitement des réclamations d'assurances.

[93] https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media (19/09/2018)

Exemple de projet[94]

De nombreux projets sont en cours de réalisation pour répondre à chacune des problématiques identifiées ci-dessus. Le projet MedRec offre la particularité d'être soutenu par des centres de calcul. Par contre, leur dépense énergétique (puissance de calcul) n'est pas récompensée en cryptomonnaie mais plutôt en accès à des données médicales agrégées et anonymes. Les centres de calcul sont des laboratoires de recherche qui développent de nouveaux médicaments et pour qui ces données ont beaucoup de valeur.

Cet exemple a spécifiquement été choisi pour illustrer qu'un mineur de cryptomonnaie (un centre de calcul) peut prendre plusieurs formes. Pour certains l'actif monétaire que représente le bitcoin justifie la dépense énergétique, pour d'autres c'est l'accès à la donnée.

4.9 Traçabilité alimentaire

Problématique visée

Lorsqu'un produit alimentaire est contaminé, l'identification de sa source peut être longue et lourde d'un point de vue administratif. Dans certains cas, une réduction des délais d'identification peut sauver des vies. L'absence de registre numérique est problématique.

Exemple de projet[95]

Août 2017- Nestlé, Unilever, Walmart et d'autres géants de l'alimentation ont fait un partenariat avec IBM afin de développer une solution utilisant la chaîne de blocs pour tracer les sources de contaminations alimentaires. Ce nouvel outil a l'objectif de permettre aux fournisseurs de denrées alimentaires de pouvoir:

- Identifier l'origine, suivre les déplacements et identifier la provenance de produits contaminés en quelques secondes.
- Partager rapidement et en toute confiance de l'information dans un réseau sécurisé.
- Réduire la contamination alimentaire via la traçabilité source-magasin numérique.

Walmart vise par exemple la bactérie E. coli et ses fournisseurs ont jusqu'en 2019 pour implanter la plateforme chaîne de blocs développée par IBM au cours des 18 derniers mois[96].

[94] https://cointelegraph.com/news/data-security-insurance-how-blockchain-is-disrupting-the-health-industry (Dernière consultation 19/09/2018)
[95] https://www.cnbc.com/2017/08/22/ibm-nestle-unilever-walmart-blockchain-food-contamination.html (Dernière consultation 19/09/2018)
[96] https://www.cnbc.com/2018/09/24/walmart-is-going-to-use-blockchain-to-stop-the-spread-of-e-coli-in-lettuce.html?__source=facebook%7Ccrypto+ (25/09/2018)

4.10 Traçabilité maritime

Problématique visée

La modernisation et la numérisation d'un registre dont l'origine remonte au 18e siècle qui permettrait d'authentifier et de vérifier en temps réel l'information sur la flotte maritime.

Exemple de projet[97]

Septembre 2018- La firme Lloyd's Register (LR) qui, en 1764, avait créé le premier registre de navires a annoncé vouloir utiliser une solution chaîne de blocs pour moderniser ses activités. L'objectif est de fournir aux souscripteurs et aux marchands:

- De l'information immuable et vérifiable afin d'augmenter leur confiance mutuelle.
- Un partage d'information en temps réel afin de traiter de manière plus dynamique les fonctions d'assurance, de financement et de paiement.
- Un processus efficace, sécuritaire et digne de confiance pour encadrer de manière numérique les transactions maritimes.

4.11 Traçabilité des services postaux

Problématique visée

Puisque les interactions de la vie quotidienne se passent de plus en plus en ligne, la sécurité est une priorité prépondérante des particuliers, des entreprises et des gouvernements. Les outils actuels ne procurent pas aux utilisateurs le niveau de confiance et de sécurité souhaité. Il y a un écart entre les solutions qui étaient adaptées à un contexte face à face et la nouvelle réalité qui est souvent numérique.

Exemple de projets[98] [99]

Mars 2018 - Les services postaux américains (USPS) souhaitent implanter une architecture numérique de confiance qui inclurait l'inscription, la vérification de l'utilisateur, un système de clés publiques et privées pour l'accès au compte, un courriel afin de signer avec une clé privée l'information sensible et une chaîne de blocs pour gérer le registre des utilisateurs.

L'Agence des douanes et protection de la frontière américaine (CBP)[100] et les géants du transport UPS[101] et Fedex[102] sont des exemples d'entreprises ou d'agences gouvernementales qui développent également une expertise en chaîne de blocs.

---

[97] https://www.lr.org/en/events/classification-register-updated-for-the-digital-age/ (19/09/2018)

[98] https://cointelegraph.com/news/usps-files-patent-to-use-blockchain-tech-in-user-identity-verification (19/09/2018)

[99] https://www.uspsoig.gov/sites/default/files/document-library-files/2016/RARC-WP-16-001.pdf (19/09/2018)

4.12 Transaction immobilière

Problématique visée

- Réduire le temps pour négocier et conclure la transaction.
- Réduire drastiquement la période de temps requise pour compléter les étapes du processus de vente ou d'achat (incluant le transfert de fonds).
- Éliminer le besoin de faire des tâches manuelles.

Exemple de projet[103]

Septembre 2018 - La société japonaise immobilière Ruden Holdings qui est inscrite à la Bourse de Tokyo (TYO : 1400) a construit une plateforme de règlement pour les transactions immobilières. Un test a été effectué en utilisant le bitcoin comme moyen de règlement, des contrats intelligents et le réseau-test NEM pour horodater le contrat. Le listing, l'offre d'achat, la négociation, le règlement en cryptomonnaie, la conversion de la cryptomonnaie vers la devise locale (Yen), et les documents notariés (registre de propriété et autres documents) ont été exécutés et partagés promptement.

4.13 Autres projets

L'objectif de la section qui s'achève visait à illustrer de manière concrète quelques exemples de problématiques et de transformations qui s'opèrent actuellement grâce à l'industrie des chaînes de blocs. Voici toutefois une liste d'industries qui n'ont pas été couvertes, mais qui étudient ou développent actuellement des solutions chaînes de blocs :

Manufacturier automobile, système de votes, assurance, industrie du jeu, médias sociaux, gestion de l'identité, programme de fidélisation, créateur de contenu, publicité, organisme de charité, environnement et services financiers.

Tous partagent un désir de simplifier leurs processus, de moderniser ou numériser leurs opérations puis d'augmenter la confiance des intervenants à l'aide d'un processus transparent et vérifiable. Les possibilités qu'offrent les chaînes de blocs stimulent la créativité pour résoudre des problèmes concrets et bien réels de notre époque.

---

[100] https://cointelegraph.com/news/us-customs-and-border-protection-to-test-blockchain-shipment-tracking-system (19/09/2018)

[101] http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220180232693%22.PGNR.&OS=DN/20180232693&RS=DN/20180232693 (19/09/2018)

[102] https://www.ccn.com/tracking-key-shipments-fedex-is-testing-with-blockchain/ (19/09/2018)

[103] https://news.bitcoin.com/japanese-company-btc-smart-contracts-real-estate/?utm_source=Japanese%20Company%20Trials%20BTC&utm_medium=telegram&utm_campaign=Telegram%20Channel (19/09/2018)

Plusieurs de ces solutions risquent de rencontrer le même type d'embûches. Par exemple, plusieurs différents standards pourraient être développés pour une même problématique ce qui fragmenterait le potentiel d'adoption. Il pourrait y avoir aussi des difficultés rencontrées afin d'atteindre l'immuabilité numérique et des défis règlementaires locaux dans un contexte d'entreprise internationale.

Ces embûches seraient plus facilement adressées dans un contexte collaboratif et innovant. Un pôle d'expertise en chaîne de blocs regroupant des intervenants compétents et au savoir diversifié ne peut qu'accélérer et dynamiser la recherche de solutions, et ce, dans un contexte simultané à plusieurs industries.

Finalement, la quantité d'exemples et de projets en cours à travers un large éventail d'industries témoigne d'un fort potentiel de développement économique à travers la R et D et de création d'emplois.

5. Impacts économiques

5.1 Impacts économiques et technologiques pour le Québec

Première question du mandat : Quels sont les impacts économiques et technologiques pour le Québec associés au déploiement de l'industrie de la chaîne de blocs? Le rapport d'analyse illustrera le changement technologique profond qui se déroule et exposera une évaluation des perspectives d'emplois et des impacts économiques qui en découlent;

« Such a fundamental restructuring of a core part of the economy is a big challenge to incumbent firms that make their living from it. Preparing for these changes means investing in research and experimentation. Those who do so will be well placed to thrive in the new, emerging financial system.[104] *»*

Harvard Business Review, Mars 2017

Les impacts économiques et technologiques pour le Québec s'expriment à la fois sur le plan quantitatif et qualitatif. Il s'agit notamment pour le Distributeur d'électricité de pouvoir diversifier son portefeuille de clients. C'est la possibilité d'accueillir des entrepreneurs qui sont prêts à dépenser pour acheter de l'énergie dans le cadre de leur activité commerciale et qui en plus offrent de la flexibilité (possibilité de délestage, s'établir dans des régions éloignées des centres urbains ou dans des usines abandonnées). C'est la possibilité que ces entrepreneurs s'établissent et réinvestissement localement.

Outre les recettes de ventes d'électricité, l'apport de capitaux privés, les impôts des entreprises, les impôts fonciers, la possibilité de développer en sol québécois et en français une expertise de pointe, c'est l'opportunité d'encourager et de supporter des entrepreneurs qui sont des pionniers et des explorateurs dans cette industrie émergente.

Il s'agit également de prendre en considération les bouleversements que le marché de l'emploi pourrait subir. Si les projets à usage cryptographique appliqué à la chaîne de blocs tels qu'illustrés à la section 4 émergent avec succès de l'étape de R et D, les emplois actuels seront modifiés et d'autres seront créés. L'impact sur la dynamique du marché du travail est plus large que celle associée à la création directe d'emplois par les centres de calcul. Ces nouvelles technologies pourraient transformer les modèles d'affaires existants, augmenter la productivité et la compétitivité des entreprises québécoises et permettre à de nouvelles entreprises de voir le jour. Les prévisions quantitatives et qualitatives de tels impacts dépassent le cadre du présent mandat.

---

[104] https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media (21/09/2018)

La section 3 de ce rapport a entre autres, présenté le potentiel du protocole Bitcoin (ainsi que sa monnaie) à titre de solution numérique potentiellement adaptée aux besoins monétaires et transactionnels particuliers d'autres développements technologiques tels que l'Internet des objets et l'intelligence artificielle.

La section 4 a présenté les changements technologiques possiblement profonds qui se développent et a exposé la nouvelle plateforme que représente « l'usage cryptographique appliqué à la chaîne de blocs » comme un moteur de R et D de manière simultanée dans plusieurs industries. L'identification de problématiques commerciales et de nouvelles avenues pour y remédier inspire la créativité entrepreneuriale, créé un terreau fertile à l'innovation et possiblement une vague d'innovation à venir. Voici quelques statistiques supplémentaires illustrant le potentiel estimé:

Le World Economic Forum a prédit en 2015 que d'ici 2027, 10% du PIB mondial serait entreposé à l'aide de la technologie blockchain[105]. Voici quelques exemples d'impact positif y étant relatés :

- Inclusion financière des pays émergents.
- Désintermédiation des institutions financières (les échanges se font sur la blockchain).
- Une explosion du nombre d'actifs pouvant être négociés sur la blockchain.
- Augmentation de la transparence.

Selon la firme de recherche Tractica, les revenus des entreprises utilisant la technologie blockchain vont surpasser les 20 milliards de dollars d'ici 2025[106]. Les principaux secteurs sujets à l'adoption sont les suivants :

- Finance
- Secteur manufacturier
- Gouvernement
- Santé
- Assurance

Deloitte a effectué un sondage à la fin du premier trimestre de 2018 auprès de chefs d'entreprises ayant des revenus annuels supérieurs à 500 millions de dollars et situés dans 7 différents pays[107]. On peut notamment y lire que :

- 52% mettent l'emphase sur les chaînes à permission, 44% sur les chaînes internes et 44% sur les chaînes publiques. (le total dépasse 100% car les projets ne sont pas mutuellement exclusifs)

[105] http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf (30/09/2018)
[106] https://www.tractica.com/newsroom/press-releases/enterprise-blockchain-revenue-to-surpass-20-billion-by-2025/ (30/09/2018)
[107] https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-2018-global-blockchain-survey-report.pdf (30/09/2018)

- 16% des entreprises prévoient investir plus de 10 millions de dollars et 23% entre 5 et 10 millions de dollars pour les initiatives blockchain dans la prochaine année.

- 53% travaillent sur des cas d'utilisation blockchain liés à la chaîne d'approvisionnement, 51% liés à l'Internet des objets, 50% à l'identité numérique, 44% aux enregistrements numériques et 40% aux cryptomonnaies.

RBC Marché des Capitaux[108] a publié en janvier 2018 un rapport de recherche estimant le potentiel des cryptomonnaies et des chaînes de blocs à 10 billions de dollars (en anglais, 10 trillions). Les principaux éléments font référence à :

- Ordinateur mondial sécuritaire par-dessus lequel bâtir une couche d'applications.

- Entrepôt de valeur.

- Virements internationaux.

- La notion de « Fat Protocols » (modèle d'affaires inverse à ce qui existe aujourd'hui).

- Mining (plus spécifiquement centre de calcul et preuve de travail).

Développer l'expertise localement est non seulement essentiel afin de naviguer adéquatement à travers les transformations technologiques qui se produisent mais représente aussi une opportunité pour le Québec de devenir un chef de file et un pôle d'innovation pour ces nouvelles technologies. Autrement, les capitaux privés seront déployés ailleurs et l'expertise qui l'accompagne ne sera pas développée au Québec, et ce, au risque de devoir importer cette expertise dans le futur. Une revue des offres d'emplois sous la rubrique blockchain affichées sur la plateforme LinkedIn[109] montre que 46% des emplois actuellement disponibles sont en Ontario, 26% en Colombie-Britannique et seulement 8,7% au Québec.

Le Québec est pourtant uniquement positionné pour accueillir ces entrepreneurs, favoriser le développement de centres d'expertise et maximiser les retombées pour l'ensemble des Québécois.

5.2 Importance d'un environnement commercial compétitif

Deuxième question du mandat : En quoi est-il important de conserver un environnement commercial compétitif, notamment à travers des tarifs d'électricité, afin que cette industrie émergente puisse se développer au Québec?

Imaginez que des scientifiques aient découvert un nouveau minerai et qu'ils l'estiment précieux. Ce minerai est disponible à plusieurs endroits dans le monde mais au Québec un ensemble de facteurs rendent sa prospection locale naturellement attrayante.

[108] https://ca.rbcwealthmanagement.com/documents/77054/77074/Crypto+Currency+%26++Blockchain+Technology+-+A+Decentralized+Future+RBC+Capital+Markets+Jan+2018.pdf/594fcb18-1b28-48c1-920f-74938c59cc90 (05/10/2018)

[109] linkedin.com en date du 1er octobre 2018. Recherche "Blockchain" au Canada et par province.

Imaginez à présent être en 1994 et qu'un entrepreneur souhaite construire un entrepôt qui ne contiendra essentiellement que des équipements qui supportent des serveurs informatiques. Cet entrepreneur est peut-être l'un des futurs géants du web.

Ce que Bitcoin représente à titre de client énergétique, c'est un hybride de ces deux situations. C'est une commodité numérique qui a des propriétés apparentées à l'or et qui est sécurisée par sa dépense énergétique.

Une nouvelle utilisation de l'électricité a été découverte. Des entrepreneurs de différentes tailles souhaitent s'établir ici, investir du temps et des capitaux privés afin de développer cette nouvelle utilisation. L'électricité a une valeur spéciale pour eux parce qu'elle est au cœur de la sécurité de l'actif numérique qu'ils protègent.

Selon l'état d'avancement 2017 du plan d'approvisionnement 2017-2016 [110] (déposé le 31 octobre 2017), les surplus moyens annuels prévus par le Distributeur sont de l'ordre de 9,76 Twh:

TABLEAU 6 :
BILAN EN ÉNERGIE

En TWh	2018	2019	2020	2021	2022	2023	2024	2025	2026
Besoins	182,1	183,8	185,9	185,5	187,3	188,5	190,3	190,6	191,6
Électricité patrimoniale	178,9	178,9	178,9	178,9	178,9	178,9	178,9	178,9	178,9
Approvisionnements postpatrimoniaux	16,7	17,0	17,5	17,8	18,1	18,5	19,0	19,3	19,7
• Base et cyclable - HQP	3,1	3,1	3,1	3,2	3,4	3,7	4,2	4,4	4,5
• Énergie rappelée - HQP	-	-	-	-	0,1	0,4	0,8	0,9	0,9
• Appel d'offres de long terme - HQP	-	0,0	0,0	0,0	0,1	0,2	0,2	0,2	0,2
• Éolien	11,2	11,3	11,4	11,4	11,4	11,4	11,4	11,4	11,3
• Biomasse et petite hydraulique	2,3	2,5	2,9	3,2	3,2	3,2	3,2	3,2	3,2
Achats d'énergie	0,0	0,0	0,0	0,0	0,1	0,1	0,1	0,2	0,6
Surplus	(13,4)	(12,1)	(10,4)	(11,1)	(9,7)	(8,9)	(7,6)	(7,6)	(7,0)

Du point de vue d'un fournisseur d'énergie, il y a plusieurs avantages à considérer les centres de calcul comme clients.

Flexibilité :

Ces centres n'ont pas besoin d'être installés près des grands centres urbains, peuvent diversifier l'économie des régions ou donner une deuxième vie à des usines abandonnées. De plus, il est possible de négocier une période de délestage en période de pointe hivernale. Puisque les activités de minage sont décentralisées et réparties dans de nombreuses juridictions à travers le globe certains centres de calcul peuvent être entièrement éteints sans que les opérations du réseau global ne soient compromises. Ces périodes de délestage auront toutefois un effet négatif sur la profitabilité des centres de calcul en tenant compte des coûts fixes inhérents (bâtisse, salaire, assurance, autre).

[110] http://www.regie-energie.qc.ca/audiences/Suivis/SuiviR-3986-2016_PlanAppro2017-2026/HQD_SuiviPlanAppro2017-2026_31oct2017.pdf (03/10/18)

Prévisibilité économique :

Le minage de bitcoins est l'une des rares industries où la rentabilité peut-être prédite avec précision lorsque toutes les variables économiques sont connues. Il y a donc peu de hasard puisque ces variables (prix du bitcoin, coût et efficacité de l'équipement et puissance de calcul) sont transparentes, accessibles et connues. La donnée manquante actuellement est le prix de l'électricité.

Le fait que des entrepreneurs privés soient prêts à déployer des capitaux significatifs pour participer à cette industrie est un fort signal de marché. Le Distributeur a donc le potentiel de servir des clients qui effectuent leur calcul de rentabilité avec une précision élevée.

Diversification du portefeuille de clients du Distributeur:

Ce nouveau type d'utilisation de l'électricité pourrait diversifier les sources de revenus du Distributeur d'énergie. On peut aussi voir l'option protectrice (hedge) qui est implicitement liée à ce secteur d'activité. Nous avons vu que la nuance entre le centre de calcul et le centre de données pouvait s'amincir, que des modèles d'affaires pouvaient être bouleversés (décentralisation des modèles d'affaires) et que le bitcoin représente pour certains de l'or numérique (compétition à l'or à titre de valeur refuge). Exprimé différemment, avoir ce type de clients est une option de protection à long terme sur ce qu'ils pourraient bouleverser.

Il est important de conserver un environnement commercial compétitif pour permettre à cette industrie de se développer. L'annexe 6 présente la convergence potentielle d'une partie des activités des centres de données et des centres de calcul et l'annexe 7 présente la compétition qui s'opère autour des projets de grande envergure.

Outre la monétisation des surplus d'Hydro-Québec, un environnement compétitif favorisera la possibilité de réaliser un projet structurant pour le Québec en bénéficiant non seulement des ventes d'électricité, du développement de l'expertise locale, mais aussi du levier économique et de l'effet multiplicateur que peuvent représenter les investissements en R et D.

L'opportunité de maximiser les revenus en augmentant significativement les prix pour ce nouveau type de client peut être attrayante dans une optique à court terme. Par contre, ce scénario est accompagné d'au moins trois conséquences :

- Risque que les projets soient déployés ailleurs qu'au Québec et que le Distributeur ne récolte pas les recettes des ventes d'électricité.
- Diminution de la compétitivité des clients du Distributeur par rapport à leurs compétiteurs internationaux. La dynamique économique démontrée en page 8 illustre comment un tarif non compétitif fragilise la compétitivité des centres de calcul et par conséquent celui des revenus attendus par le Distributeur.
- Diminution de la marge bénéficiaire des centres de calcul ce qui limite le potentiel de réinvestissement en R et D. Si les projets sont quand même déployés ici, le potentiel de redéploiement des bénéfices en R et D aura été redirigé vers une facture d'électricité plus élevée ce qui priverait le Québec d'un levier économique à l'effet multiplicateur.

5.3 Impacts du dossier R-4045-2018

Troisième question du mandat : Quels sont les impacts que pourrait avoir la demande du Distributeur dans le dossier R-4045-2018 sur le développement de l'industrie de la chaîne de blocs, notamment sur la compétitivité des entreprises du Québec?

L'industrie associée à l'usage cryptographique appliqué aux chaînes de blocs est émergente et peu connue. Elle a été taxée au Québec de mesures protectrices et d'un tarif non compétitif qui, tels qu'exposés aux sections 1 et 2, étaient peut-être basés sur des prémisses et des informations inexactes ou devant être nuancées, notamment en ce qui concerne l'utilité de la dépense énergétique, de la dynamique économique du minage de cryptomonnaie (vs l'aspect simultané des demandes) et le fait que les clients dans la nouvelle catégorie proposée n'ont pas un profil de consommation énergétique similaire.

Ces mesures pourraient avoir un effet négatif sur le développement de l'industrie de la chaîne de blocs au Québec. Voici quelques exemples de l'impact que les mesures proposées dans le dossier R-4045-2018 pourraient avoir sur la compétitivité des entreprises au Québec.

- Introduction d'une complexité administrative et non efficace d'une tarification à l'usage.
- Dissuader les entrepreneurs de s'établir au Québec. L'annexe 7 présente quelques transactions récentes et démontre que la compétition s'installe et que des régions éloignées peuvent bénéficier de ce nouveau type de clients.
- Brimer le potentiel de diversification des activités commerciales et du type de client desservi des centres de données. Veuillez consulter l'annexe 6 pour obtenir de l'information à ce sujet.
- Diminution de la diversité économique des entreprises du Québec.
- Diminution de la compétitivité du Québec sur le marché de l'emploi et de l'expertise.
- Diminution de la compétitivité des centres de calcul comparativement aux compétiteurs internationaux. Revoir la dynamique économique et la considérer dans le contexte de vente d'énergie à des partenaires internationaux qui pourraient la revendre à des centres de calcul.
- Création d'un potentiel précédent basé sur l'usage à l'intérieur d'une même industrie et qui cible un amalgame de technologies existantes.
- Création d'une injustice pour deux types de clients (peut-être au sein de la même entreprise):
    - Ceux qui utilisent la preuve de travail verront leur bénéfice net réduit. Ceci risque d'étouffer le potentiel de réinvestissement local en R et D. Ces clients sont ceux dont le modèle de revenus est démontré.
    - Ceux qui développent des projets (sans la preuve de travail) auraient quand même un tarif non-compétitif. Ceci risque d'étouffer la R et D locale de projets qui ne sont pas énergivores et dont le modèle de revenus est en développement.
- Brimer le potentiel de diversification, l'exploration de nouveaux marchés et être à l'extérieur du flux d'informations et de transactions.

6. Conclusion

Un nouvel usage de l'électricité a émergé à travers l'assemblage de technologies déjà existantes. Cet assemblage a de la valeur aux yeux de plusieurs comme en témoigne le nombre élevé de demandes d'énergie simultanées qu'a reçues le Distributeur.

La nouveauté de l'industrie de l'usage cryptographique appliqué aux chaînes de blocs et l'information insuffisante dont le Distributeur disposait à ce propos ont mené à deux problématiques de base.

La première problématique est que la quantité élevée de MW demandés en électricité combinée à la manière simultanée dont ces demandes ont été présentées n'a pas tenu compte de la dynamique économique du minage de cryptomonnaie. Même si ces MW avaient été octroyés, il est peu probable qu'ils aient pu être déployés par les centres de calcul de cryptomonnaie de manière économiquement viable. Le défi semble lié au caractère simultané des demandes formulées et non pas vers la matérialisation du déploiement d'une telle demande énergétique.

La deuxième problématique est l'hypothèse selon laquelle tous les clients de la catégorie proposée sont de grands consommateurs d'énergie. Ce rapport a exposé que le profil de consommation ne serait pas utile pour la détection des variations de charge ciblant l'ensemble de l'usage cryptographique appliqué aux chaînes de blocs. D'une part, certains usages et applications ne consomment pas beaucoup d'énergie. D'autre part, le profil de consommation énergétique de la preuve de travail varie en fonction du succès de son réseau.

Rappelons qu'un réseau en santé (tel qu'illustré par le taux de hachage) a attiré un montant significatif d'investissement en infrastructure et a un schème de monétisation confirmé. Ce n'est pas le cas de plusieurs projets sous l'appellation usage cryptographique appliqué à la chaîne de blocs qui sont encore à l'étape de R et D. Un tarif non compétitif aurait pour effet de diminuer la compétitivité des clients du Distributeur en forçant ceux-ci à éteindre leur équipement avant d'autres.

Par conséquent, les mesures proposées (bloc dédié et tarification à l'usage) par le Distributeur seront difficilement applicables. De plus, il peut y avoir une convergence entre les activités de clients existants (centres de données) et de nouveaux clients (centres de calcul), car ceux-ci partagent certaines caractéristiques similaires et intersections de leurs activités.

Les centres de calcul sont de nouveaux clients potentiels pour le Distributeur. La nature de leurs activités fait en sorte qu'ils peuvent être localisés à l'extérieur des grands centres urbains, qu'ils peuvent donner une deuxième vie à des usines désaffectées et qu'une période de délestage peut être envisagée au besoin advenant une pointe hivernale.

Outre les recettes de ventes d'électricité, les retombées fiscales et la création d'emplois, le Québec pourrait bénéficier d'investissement R et D venant de capitaux privés et permettant de développer un bassin d'expertise locale dans cette industrie émergente. Le fait que des entrepreneurs veulent y investir temps et argent est un fort signal de marché. Ils y voient de la valeur.

ANNEXE 1 : Commentaires sur le rapport de KPMG

Cette annexe vise à nuancer, préciser ou apporter un complément d'information à l'étude de KMPG intitulée « Analyse économique des installations de minage d'actifs cryptographiques.[111]»

Section 1 : preuve de travail

L'étude KPMG indique que :

- *«Comme ce système preuve de travail est plus complexe et coûteux à opérer, il ne constitue pas la voie privilégiée pour les autres types d'application de la technologie blockchain.[112]»*

Ce commentaire suppose que le potentiel "blockchain" puisse se développer en isolation. C'est l'assemblage de technologies interreliées (réseau pair-à-pair, preuve de travail, cryptographie et chaîne de blocs) qui permet à une infrastructure telle que celle de Bitcoin d'exister. La chaîne de blocs est une résultante. L'immuabilité, la décentralisation et les transactions sans organe de contrôle sont atteintes à l'aide d'une interaction complexe entre plusieurs concepts qui se renforcent l'un et l'autre ; cryptographie, théorie des jeux (incitatif financier) et informatique distribuée.

La récompense associée au système preuve de travail offre un schème de monétisation démontré. La pérennité financière des entreprises qui consomment une grande quantité d'électricité est soutenue par cette monétisation. Les autres applications représentent des projets à l'étape de la conception et du développement.

De plus, ce commentaire suppose qu'une autre méthode de consensus distribué à grande échelle (pour remplacer la preuve de travail) est actuellement disponible et fonctionnelle. Trouver une alternative à la preuve de travail est un problème ouvert en science informatique. La preuve de travail est la seule solution de consensus distribué à grande échelle actuellement connue et fonctionnelle.

- *«Dans de telles éventualités (crise de confiance, scandale, freins politiques ou règlementaires), la puissance de calcul des appareils supportant le réseau Bitcoin pourrait être redirigée en partie vers d'autres actifs cryptographiques.[113]»*

Cette hypothèse aurait mérité que l'on explique dans quelle mesure les risques cités pourraient avoir un impact sur le réseau Bitcoin mais pas sur les autres actifs cryptographiques utilisant le même algorithme. C'est aussi ignorer la force et la résilience d'un réseau informatique dont l'historique se développe depuis bientôt dix ans et qui a reçu des investissements colossaux par les participants à son écosystème.

[111] Présentée à Direction Grands clients et Direction Développement des affaires – Québec, Vice-présidence – Clientèle, Hydro-Québec Distribution le 26 février 2018

[112] Section 1.3 p. 4

[113] Section 1.3 p. 4

- *« On ne peut donc éliminer le risque que les entreprises qui s'établiraient au Québec pour réaliser du minage de bitcoins, ou certaines d'entre elles, réduisent, voire ferment leurs opérations si le contexte change.[114] »*

C'est exact. Il s'agit par contre d'un risque d'entreprise présent dans toutes les industries. Le fait que des entrepreneurs veulent déployer des capitaux privés, comme démontré par les demandes simultanées qu'a reçues le Distributeur est un signal de marché important.

Section 2 : autres commentaires

- *« Il existe peu d'informations complètes ou rigoureuses sur les activités des installations de minage de bitcoin, au Québec comme ailleurs. Ce type d'activité est non seulement relativement nouveau, mais entouré d'un certain « secret ».[115] »*

Le secteur est certes relativement nouveau, mais l'information qui décrit en détail toutes les variables économiques de l'industrie du minage est abondante sur le web. L'information permettant de dresser un portrait assez précis des variables économiques associées au minage n'est pas secrète. Par exemple ; le protocole d'émission, les règles de consensus, la difficulté de calcul, l'efficacité et le coût de l'équipement informatique et la composition des « pools de mineurs » sont disponibles de manière transparente et gratuite sur le web. Il est possible que des entreprises privées n'aient pas souhaité dévoiler le profil d'emploi de leurs activités et cela peut être le cas dans n'importe quelle industrie compétitive.

- *« La « blockchain » est une nouvelle technologie habilitante qui...[116] »*

La « blockchain » n'est pas une technologie en soi. La plupart des projets « blockchain » ne font qu'utiliser des signatures cryptographiques et des bases de données distribuées pour réaliser des opérations qui, la plupart du temps, n'ont pas besoin des propriétés intrinsèques d'une "vraie" blockchain tels que l'immuabilité, la décentralisation et l'absence de censure.

- *« Si la technologie blockchain et le bitcoin ont été construits ensemble, l'utilisation de cette technologie peut s'appliquer à bien d'autres domaines et intéresser de nombreux acteurs différents (entreprises, institutions financières, gouvernements).[117]»*

La blockchain n'est pas sous-jacente à bitcoin, la blockchain existe parce qu'il y a bitcoin. C'est une résultante. Il y a des banques parce qu'il y a de l'argent. Mais l'argent (peu importe la forme) a existé avant les banques. La blockchain de bitcoin a émergé et se perpétue uniquement parce que le marché lui attribue de la valeur. Le seul cas d'utilisation qui fonctionne actuellement est l'échange d'une ressource numérique décentralisée et les applications qui peuvent exploiter la nature immuable d'une telle blockchain. Le reste des applications potentielles liées à la blockchain sont pour la plupart soit au stade de la recherche et développement ou sont des solutions à l'architecture fermée qui s'apparente à un schème de signatures cryptographiques avec une base de données distribuée.

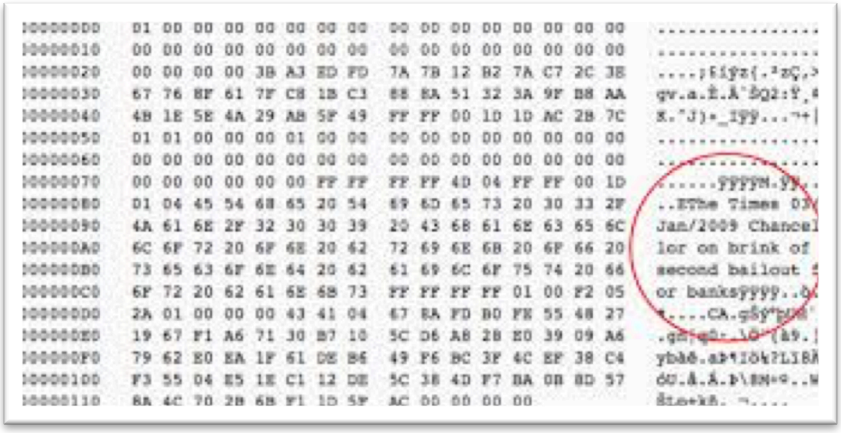
[114] Section 1.3 p. 4
[115] Section 1.3 p. 3
[116] Section 2.1 p. 5
[117] Section 2.1 p. 6

- *« Par exemple, un réseau privé ne requiert en général que quelques serveurs pour fonctionner, alors qu'un réseau comme celui de Bitcoin ou d'Ethereum utilise des centaines de milliers de machines.[118] »*

Un réseau privé est un environnement centralisé (avec permission) et ne correspond donc pas à la définition d'un réseau distribué, décentralisé, immuable sans organe de contrôle. Comparer un réseau privé à des réseaux ouverts est pour le moins paradoxal. Il s'agit de deux propositions distinctes et non comparables. La différence est aussi grande qu'entre l'Intranet et l'Internet. Par ailleurs, cette phrase omet le fait qu'initialement bitcoin était miné avec des ordinateurs personnels (CPU) et que c'est sa popularité qui a fait croitre la puissance de calcul. Au départ, Bitcoin était un projet informatique essentiellement soutenu par quelques développeurs bénévoles.

- *«Ces cryptomonnaies ont émergé en 2009 et elles sont particulièrement en expansion depuis 3-5 ans, à la fois en nombre et en utilisation.[119] »*

Une seule monnaie a émergé en 2009: bitcoin.



Le bloc de la genèse (le bloc #0) est daté du 3 janvier 2009. On peut y lire la mention « 03/Jan/2009 Chancellor on brink of second bailout for banks »

- *« Comme toute autre application blockchain, les cryptomonnaies exigent que toutes les transactions soient signées cryptographiquement de manière à les individualiser pour ne pas les imiter. [120]»*

Ce n'est pas pour qu'elles ne soient pas imitées, c'est pour qu'elles ne soient pas dépensées deux fois. L'innovation majeure du protocole Bitcoin est d'avoir trouvé une solution au problème ouvert en science informatique appelé « le problème des Généraux byzantins ». Cette solution a permis la rareté numérique sans intermédiaire de confiance.

- *« L'importance relative de la capitalisation du bitcoin dans l'ensemble des cryptomonnaies diminue par ailleurs. Elle dépassait 90% au cours de l'année 2016 et est tombée à près de 60% en moyenne pendant l'année 2017[121] »*

[118] Section 2.1 p. 7
[119] Section 2.1 p. 7
[120] Section 2.1 p. 7

Ce commentaire omet que la notion de puissance de calcul témoigne de la popularité d'un réseau (plus que sa capitalisation). Par ailleurs, le nombre de ICO a drastiquement augmenté depuis 2016. Les ICO (Initial Coin Offering) n'ont pas nécessairement de produits ou de chaînes de blocs en activité. Ils sont plus apparentés à un hybride entre le financement participatif et le capital de risque. Ce commentaire omet également le fait que d'autres cryptomonnaies (altcoin) utilisant la preuve de travail ont été lancées ou "forkée" du réseau Bitcoin comme ce fut le cas en août 2017 avec Bcash. Il aurait été plus significatif de considérer l'importance relative des monnaies utilisant la preuve de travail dans un contexte énergétique.

- *« Chaque bloc est validé par les nœuds du réseau appelés les « mineurs ». [122]»*

Ceci est inexact. Un mineur peut être un nœud, mais un nœud n'est pas nécessairement un mineur. À titre d'illustration, il y a actuellement 9947 nœuds[123] sur le réseau Bitcoin mais des millions de machines à miner. Quelqu'un peut décider d'exécuter un nœud complet (full node) pour contribuer à la décentralisation du réseau en hébergeant l'historique complet de la chaîne de blocs de bitcoin sur son ordinateur. Cet acte peut être effectué par quiconque, ne requiert pas de matériel informatique spécialisé, n'est pas énergivore et est effectué de manière volontaire sans obtenir de bitcoins en compensation.

- *« Toute la chaîne est mise à jour en continu sur des périodes très courtes. [124]»*

Ceci est inexact et porte à croire que le réseau recalcule en permanence la validité de la chaîne ce qui serait un calcul lourd et non nécessaire. « Toute » la chaîne n'est pas mise à jour en continu. Au contraire, le processus de validation qui est effectué par la preuve de travail n'est associé qu'à l'ajout des nouveaux blocs (qui contiennent les nouvelles transactions). Toutes transactions ou tous blocs existants peuvent être validés sans calcul (sans preuve de travail) grâce à l'utilisation des signatures cryptographiques et de l'arbre de Merkle[125].

- *« Contrairement à d'autres cryptomonnaies, le bitcoin exige des systèmes de calcul plus puissants. [126]»*

Cet aspect est présenté comme négatif. Pourtant, cette augmentation de la difficulté de calcul est ce qui témoigne des investissements dans le réseau. Les entrepreneurs investissent en infrastructure Bitcoin dans l'expectative d'un retour sur l'investissement. Revoir au besoin la section sur la dynamique économique.

- *« La demande accrue, et en particulier la hausse de la valeur du bitcoin, ont augmenté sensiblement la rentabilité potentielle des activités de minage.[127] »*

---

[121] Section 2.1 p. 7 note 6
[122] Section 2.1 p. 8
[123] https://bitnodes.earn.com/ (29/09/18)
[124] Section 2.1 p. 8
[125] https://en.bitcoinwiki.org/wiki/Merkle_tree (30/09/18)
[126] Section 2.1 p. 8
[127] Section 2.1 p. 9

La relation entre le prix du bitcoin et la profitabilité n'est pas directe. Il manque une variable essentielle à considérer : la puissance de calcul nécessaire en fonction du taux de hachage. Au besoin, revoir la section sur la dynamique économique. En résumé, il est possible que le prix du bitcoin baisse et que la rentabilité augmente (et inversement). Il est très important de comprendre cette dynamique.

- *« La rémunération du mineur, qui obtient la création d'un nouveau bloc (évènement qui arrive toutes les dix minutes), est elle-même divisée par 2 à tous les 2016 blocs (soit environ tous les 4 ans).*[128]*»*

La rémunération (récompense) du mineur est composée de nouveaux bitcoins et des frais associés aux transactions contenues dans le bloc. L'émission d'un nouveau bloc oscille autour de dix minutes en fonction de la puissance de calcul et est ramenée à dix minutes à chaque 2016 blocs (soit environ deux semaines). Tous les quatre ans, soit à chaque 210,000 blocs, la récompense par bloc (les nouveaux bitcoins) est divisée par deux. Revoir au besoin la courbe d'émission de la devise bitcoin dans la section de la dynamique économique.

- *«Au début 2018, pour une installation au Québec, les experts estimaient que le seuil de rentabilité correspondait à un prix de bitcoin se situant entre 3 000 et 4 000$ pour un opérateur existant.*[129]*»*

Il aurait été intéressant d'obtenir les sources et les hypothèses utilisées (efficience des machines et taux de hachage en vigueur lors de cette estimation). Le taux de hachage est ajusté à chaque 2016 blocs et par conséquent le seuil de rentabilité également.

- *« Une telle concentration défierait le principe même de décentralisation alors que le réseau Bitcoin en particulier est déjà très centralisé au goût de certains.*[130] *»*

Ce commentaire est particulier compte tenu du fait que l'étude parle abondamment des projets blockchain, de la technologie blockchain, des réseaux privés qui sont centralisés alors que bitcoin est le cas d'utilisation prouvé, fonctionnel, décentralisé, immuable et résistant à la censure. Des événements récents comme le « fork » de bitcoin cash (bcash) et UASF ont démontré que Bitcoin est un réseau décentralisé où les utilisateurs sont en contrôle. De plus, les fabricants d'équipement de minage sont directement incités à être honnêtes puisqu'une partie de leurs revenus et de leurs actifs dépendent de l'industrie du minage bitcoin.

[128] Section 2.1 p. 9
[129] Section 2.1 p. 9 note 9
[130] Section 2.2 p. 15

ANNEXE 2 : Cadre d'estimation du réseau Bitcoin

(au 24 mars 2018)

Hypothèses:

- Les mineurs débranchent les machines non profitables (minent à 0$ mais pas à perte). C'est-à-dire que des équipements soit peu ou soit très efficace, sont utilisés pour former la fourchette d'estimation de la consommation totale du réseau.
- Le calcul est effectué seulement pour le réseau Bitcoin.
- Le coût de refroidissement est exclu.
- Toutes les sources énergétiques sont considérées.
- D'autres types d'équipements existent. Ceux représentés proviennent du plus grand fabricant[131] de chips ASIC pour le minage de bitcoin. Les informations utilisées à propos de la performance proviennent du site des fabricants.

Données :

	AntMiner s9i[132]	AntMiner S7[133]
Taux de hachage	14 500 GH/sec	4 730 GH/sec
Consommation	0,09414 watt/ GH	0,25 watt/ GH
En watt	1 365 watts	1 183 watts
Limite inférieure / supérieure	2 187 MW	5 809 MW

Calculs :

AntMiner s7

Bitcoin hashrate[134]/ s7 hashrate	=	nombre de mineurs
23 236 729 000 / 4 730	=	4 912 628 mineurs s7
Nb de mineurs * consommation	=	consommation totale des mineurs
4 912 628 x 1 183	=	5 809 182 250 watts 5 809 Mégawatts

AntMiner s9i

Bitcoin hashrate / s9 hashrate	=	nombre de mineurs
23 236 729 000 / 14 500	=	1 602 533 mineurs s9i
Nb de mineurs * consommation	=	consommation totale des mineurs
1 602 533 x 1 365	=	2 187 505 668 watts 2 187 Mégawatts

Remarquez que plus la machine (miner) est efficace moins le MW nécessaire pour miner un bitcoin est élevé. Au moment de faire ces calculs, les AntMiner S7 étaient encore profitables, mais on remarque leur consommation énergétique plus élevée comparativement aux AntMiner S9.

[131] https://www.bitmain.com/ (24/03/2018)
[132] https://shop.bitmain.com/antminer_s9_asic_bitcoin_miner.htm?flag=specifications (24/03/18)
[133] https://www.bitcoinmining.com/bitcoin-mining-hardware/ (24/03/18)
[134] https://blockchain.info/fr/charts/hash-rate (24/03/18)

(au 10 octobre 2018)

Hypothèses:

- Le Avalon A921 est un équipement offert par le fournisseur Canaan Creative mais est actuellement en rupture de stock. Sa présence dans le rapport vise à illustrer la compétition, le progrès de l'efficacité des chips spécialisées et l'impact sur la consommation.
- Le calcul est effectué seulement pour le réseau Bitcoin.
- Le coût de refroidissement est exclu.
- Toutes les sources énergétiques sont considérées.
- Les informations utilisées à propos de la performance proviennent du site des fabricants.

Données :

	Avalon A921[135]	AntMiner S9i[136]
Taux de hachage	20 000 GH/sec	14 500 GH/sec
Consommation	0,089 watt/ GH	0,09414 watt/ GH
En watt	1 780 watts	1 365 watts
Limite inférieure / supérieure	5 244 MW	5 547 MW

Calculs :

AntMiner s9i

Bitcoin hashrate[137] / s9i hashrate	=	nombre de mineurs
58 923 572 000 / 14 500	=	4 063 695 mineurs s9i
Nb de mineurs * consommation	=	consommation totale des mineurs
4 063 695 x 1 365	=	5 547 065 068 watts 5 547 Mégawatts

Avalon A921

Bitcoin hashrate / A921 hashrate	=	nombre de mineurs
58 923 572 000 / 20 000	=	2 946 179 mineurs A921
Nb de mineurs * consommation	=	consommation totale des mineurs
2 946 179 x 1 780	=	5 244 197 908 watts 5 244 Mégawatts

Remarquez qu'entre le 24/03/18 et le 10/10/18, le taux de hachage du réseau Bitcoin a plus que doublé (2.54x). De nouveaux équipements comme par exemple, le Avalon A921, peuvent compenser une partie de l'augmentation du taux de hachage avec une meilleure efficacité. On peut s'attendre à ce que l'équipement qui n'est plus rentable soit éventuellement remplacé. Le Canaan Avalon A9[138] n'est pas encore disponible mais les attentes sont; un taux de hachage de 30 000 GH/sec et une consommation de 1 720 watts. Notez que ceci n'est ni une revue exhaustive de produits disponibles ou une recommandation mais une illustration du potentiel d'augmentation d'efficacité attendue.

[135] https://canaan.io/product/avalonminer-921/ (11/10/18)
[136] https://shop.bitmain.com/antminer_s9_asic_bitcoin_miner.htm?flag=specifications (11/10/18)
[137] https://blockchain.info/fr/charts/hash-rate (11/10/18)
[138] https://bitcoinexchangeguide.com/canaan-avalon-a9/ (12/10/18)

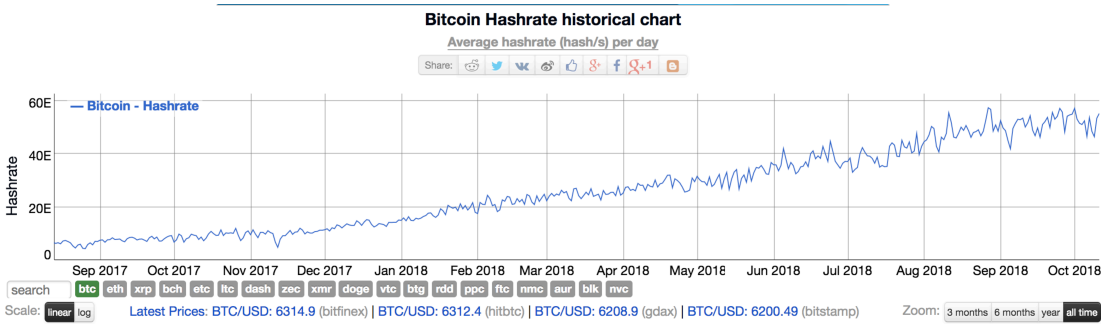
ANNEXE 3 : Principales cryptomonnaies utilisant la preuve de travail (28 septembre 2018) [139]

Bien que leur proposition à valeur ajoutée diffère, et que les algorithmes de hachage utilisés peuvent être différents, certaines cryptomonnaies ont en commun d'utiliser la preuve de travail. Remarquez les différences d'échelles Mega/Tera/Exa hash/secondes.
Avec 52,163 Ehash/s Bitcoin est de loin la cryptomonnaie dont le réseau est le plus supporté.

Le taux de hachage à la hausse est un indicateur d'investissements en infrastructure dans le réseau.

Données :

Crypto	Taux de hachage	Capitalisation
Bitcoin (BTC)	52,163 Ehash/sec	115 105 130 099 $ US
Ethereum (ETH)	266,18 Thash/sec	23 014 749 263 $ US
Bcash (BCC)	4,249 Ehash/sec	9 376 725 920 $ US
Litecoin (LTC)	264,535 Thash/sec	3 618 044 690 $ US
Monero (XMR)	606,701 Mhash/sec	1 928 854 499 $ US



[139] https://bitinfocharts.com/ (12-10-18)

ANNEXE 4 : Appuis institutionnels

La couverture des initiatives locales et internationales s'activant à l'intersection de l'écosystème de la cryptomonnaie et de l'écosystème financier traditionnel est si riche qu'il ne sera possible que d'en couvrir une petite partie dans le cadre du présent document. Voici quelques exemples d'initiatives d'acteurs majeurs de l'écosystème traditionnel.

Cboe Global Markets[140]
Décembre 2017 – L'une des plus grandes sociétés de places boursières au monde a été la première à offrir la possibilité d'utiliser un produit dérivé traditionnel soit un contrat à terme (*futures*) pour exprimer une anticipation à la hausse ou à la baisse sur le prix du bitcoin. Bien que non adossé à des bitcoins physiques, ce fut l'un des premiers pas témoignant de la reconnaissance du phénomène de Bitcoin par la finance traditionnelle.

Groupe TMX (propriétaire de la Bourse de Toronto)[141]
Mars 2018 – Le groupe TMX a annoncé le lancement de Shorcan Digital Currency Network qui offrira un service de courtage spécialisé autour de Bitcoin et d'Ethereum. Le TMX a souligné l'importance de cette étape dans l'exécution de sa stratégie numérique visant à répondre aux besoins des clients tant dans les marchés traditionnels que non traditionnels.

Intercontinental Exchange (NYSE : ICE)[142]
Août 2018 - La place boursière américaine ICE (spécialisée dans les produits dérivés) a annoncé le lancement de Bakkt. Bakkt sera une plateforme pleinement règlementée où il sera possible de négocier des contrats à terme (*futures)* adossés à des bitcoins physiques. L'objectif est d'offrir aux consommateurs et aux institutions la possibilité d'acheter, vendre, entreposer ou dépenser sans friction leurs actifs numériques.

Goldman Sachs / Morgan Stanley / Citigroup/ Bank of America [143] [144] [145]
Goldman Sachs évalue la possibilité de lancer un pupitre de transaction d'actifs numériques et aussi d'offrir un service de gardien de valeur. Citigroup veut offrir la possibilité à ses clients d'investir indirectement dans le bitcoin et la cryptomonnaie en général via des reçus d'actifs numériques. Morgan Stanley vise la clientèle institutionnelle avec un pupitre de swap (dérivés) adossé au prix du bitcoin. Et Bank of America a déposé une demande de brevet pour un service de gardien de valeur de cryptomonnaie en août 2018.

---

[140] http://ir.theice.com/press/press-releases/all-categories/2018/08-03-2018-133022149 (22/09/2018)
[141] https://www.thestar.com/business/2018/03/23/tmx-to-launch-cryptocurrency-platform-focusing-on-bitcoin-ether.html (22/09/2018)
[142] http://ir.theice.com/press/press-releases/all-categories/2018/08-03-2018-133022149 (22/09/2018)
[143] https://www.bloomberg.com/news/articles/2018-08-06/goldman-is-said-to-consider-custody-offering-for-crypto-funds?utm_content=crypto&utm_medium=social&utm_campaign=socialflow-organic&utm_source=twitter (22/09/2018)
[144] https://dailyhodl.com/2018/09/15/goldman-sachs-morgan-stanley-citigroup-and-nyse-owner-prepare-to-back-bitcoin-and-crypto/ (22/09/2018)
[145] http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220180240112%22.PGNR.&OS=DN/20180240112&RS=DN/20180240112 (03/10/2018)

ANNEXE 5 : Pourquoi Bitcoin sera difficile à répliquer

Pour répliquer l'unicité ou déloger Bitcoin, il s'agira de trouver une innovation encore plus grande que ce qu'il représente et non une amélioration de protocole. Il faudra également comprendre les éléments et les circonstances exceptionnelles qui ont mené à sa création.

Bitcoin est un phénomène unique, qui a émergé et dont la valeur a été attribuée spontanément par ses utilisateurs grâce à une technologie fonctionnelle et ayant de la valeur aux yeux de ceux-ci. Reproduire ce phénomène sera non seulement extrêmement difficile, voire impossible et excessivement couteux.

Capital monétaire

- Aucun capital n'a été levé pour développer Bitcoin.
- Aucun capital n'a été dépensé pour en faire la promotion (conférence, publicité).
- Sa valeur lui a été attribuée de manière spontanée par le marché.

Effet réseau

- Parce que la technologie a fonctionné dès le premier jour, elle a organiquement attiré d'autres joueurs et a grossi rapidement, et ce, sans que le bitcoin n'ait de valeur initialement.

- La taille actuelle du réseau confère à Bitcoin sa sécurité. Maintenant que le "chemin est tracé", s'il était possible de retourner dans le passé, il serait possible d'attaquer le réseau en mobilisant plus de la moitié de la puissance de calcul (attaque 51%). Ceci aurait probablement été possible dans les premiers temps de Bitcoin (quand la puissance de calcul était faible) mais parce que la valeur économique du réseau était insignifiante, ce type d'attaque ne s'est pas matérialisé.

Décentralisation

- Équilibre entre les mineurs, les codeurs et les utilisateurs sans qu'aucun d'entre eux ne puisse le contrôler.

- Une réplique de Bitcoin serait planifiée "top down" et ne pourrait se soustraire au contrôle de son créateur. Nakamoto a travaillé anonymement pendant deux ans et s'est effacé du processus. Il n'a plus d'influence sur les décisions et personne ne compte sur lui pour trouver des solutions.

- Personne n'est essentiel dans Bitcoin.

Longévité

- Monument d'immuabilité dispendieux à reproduire.

ANNEXE 6 : Convergence centres de données et centres de calcul

Il existe plusieurs similitudes entre les centres de données et les centres de calcul. Ces similitudes font en sorte que certains centres de données qui cherchent à diversifier leurs activités commerciales ou à séduire de nouveaux marchés se tournent naturellement vers le marché de la cryptomonnaie et des chaînes de blocs.

Un premier exemple est celui de Cogeco Peer 1. François Rémy, blogueur au journal Les Affaires a relaté[146] que l'entreprise a fait un virage vers la blockchain et "exploite depuis mai 2018 les principaux nœuds de la plateforme open-source décentralisée DigitalBits". Les propos du président de Cogeco Peer 1 laissent peu de doute sur l'avenir de la cryptomonnaie et des chaînes de blocs, ni sur le croisement des activités des centres de données et des centres de calcul ;

> *«La blockchain va sous-tendre une large partie d'Internet et c'est la tâche d'une entreprise d'infrastructures web comme la nôtre de fournir cet Internet sur chaînes de blocs», avait déclaré Philippe Jetté, le président de Cogeco Peer 1.* [147] *»*

Un deuxième exemple est celui de l'entreprise eStruxture qui, en septembre 2017, annonçait un investissement de 150 millions de dollars dont les principaux investisseurs sont la Caisse de dépôt et placement du Québec, Canderel et Fengate. L'investissement vise à transformer l'ancienne imprimerie de The Gazette en un centre de données[148].

Environ neuf mois plus tard, le président et directeur général d'eStruxture a partagé en entrevue[149] sa vision et les projets de l'entreprise. Il est intéressant de constater que malgré son scepticisme face aux cryptomonnaies, il voit le potentiel des chaînes de blocs et affirme que les serveurs de l'entreprise sont déjà en train de miner des cryptomonnaies qui jouent un rôle dans l'intelligence artificielle.

L'industrie de la chaîne de blocs pourrait d'ailleurs bouleverser l'industrie des centres de données et pourrait aussi créer de nouveaux types de centres de calcul. L'exemple de MedRec (p. 41) a la particularité de proposer un incitatif financier différent de bitcoin.

[146] http://www.lesaffaires.com/blogues/francois-remy/cogeco-s-inquiete-du-tarif-blockchain-dhydro-quebec/604011et (24/09/2018)
[147] http://www.lesaffaires.com/blogues/francois-remy/cogeco-s-inquiete-du-tarif-blockchain-dhydro-quebec/604011et (24/09/2018)
[148] http://www.lapresse.ca/techno/201712/06/01-5146067-un-centre-de-donnees-dans-lex-imprimerie-de-the-gazette.php (24/09/2018)
[149] https://www.capremedia.com/will-estruxture-expand-into-calgary (24/09/2018)

Certaines différences existent entre les besoins des centres de calcul et les centres de données.

1. Sécurité

Les centres de données ont des besoins de sécurité car ils abritent de l'information qui peut être d'une grande importance. Les centres de données qui hébergent les données de l'armée, des gouvernements ou banques sont très sécurisés. Les centres de calcul produisent un actif monétaire et sont donc également très sensibles à la sécurité. Les centres de calcul ont un risque lié à la sécurité qui n'est pas présent chez les centres de calculs. Il existe un marché secondaire pour le matériel informatique utilisé par les centres de calcul (contrairement aux serveurs informatiques traditionnels). Des malfaiteurs pourraient vouloir dérober et revendre le matériel informatique. On peut donc dire que les besoins en sécurité sont plus élevés pour les centres de calcul.

2. Refroidissement

Les centres traditionnels de données ont des besoins plus lourds à supporter en matière de refroidissement. Les centres de calcul peuvent refroidir à l'air. L'indicateur d'efficacité énergétique (le pue)[150] est un ratio entre l'énergie totale consommée par le centre d'exploitation et l'énergie totale consommée par l'équipement informatique. Ce ratio est meilleur pour les centres de calculs. Dit différemment, l'énergie des centres de calcul est utilisée pour l'équipement de manière très efficace puisqu'une plus grande partie de l'énergie est consommée par l'équipement informatique (au lieu de refroidir).

À titre d'exemple, Bitfury et Bitfarms, qui sont des leaders mondiaux en minage de cryptomonnaie, rapportent respectivement un indicateur d'efficacité énergétique moyen de 1,05[151] et de 1,06[152]. La moyenne (roulante 12 mois)[153] des grands centres de données de Google se situe à 1,12 pour chacune des cinq dernières années. Le centre Google le plus efficient a un indicateur d'efficacité énergétique moyen de 1,09 (le moins efficient a une moyenne de 1,21 pour les 5 dernières années).

3. Délestage

Il est possible de procéder au délestage avec les centres de calcul. L'activité de minage de cryptomonnaie n'est pas centralisée auprès d'un fournisseur. Il s'agit plutôt d'un réseau international composé de plusieurs joueurs ayant la même fonction. Une interruption chez certains centres de calcul est possible sans mettre en péril les opérations de validation de la chaîne de blocs. L'effet de la période de délestage est un impact négatif sur la profitabilité des centres de calcul et non sur la viabilité des opérations. Cette flexibilité est non négligeable pour tenir compte de la pointe hivernale.

4. Connectivité

Les centres de calcul ont des besoins moins élevés en matière de connectivité. C'est ce qui permet de déployer ces centres en dehors des grands centres urbains sans affecter leur efficacité.

[150] https://fr.m.wikipedia.org/wiki/Indicateur_d%27efficacit%C3%A9_%C3%A9nerg%C3%A9tique (24/09/2018)
[151] https://bitfury.com/content/downloads/03_20_18_bitfury_norway_datacenter_release.pdf (24/09/2018)
[152] Citation de Pierre-Luc Quimper, Président des opérations, fondateur et directeur, Bitfarms (25/09/2018)
[153] https://www.google.com/about/datacenters/efficiency/internal/ (24/09/2018)

ANNEXE 7: Compétition pour attirer les projets d'envergure

En janvier dernier, RBC Marché des capitaux[154] a estimé à 10 billions de dollars le potentiel du marché de la cryptomonnaie et de la technologie blockchain. On peut notamment y lire que la puissance de calcul déployée pour sécuriser le réseau (via la preuve de travail) est déjà un marché de plusieurs milliards de dollars. Cette opportunité économique a été comprise par plusieurs producteurs énergétiques comme en témoignent les annonces suivantes ;

- Une aluminerie abandonnée appartenant à la société Alcoa[155] située dans le nord de l'État de New York sera convertie dans l'un des plus grands centres de calcul au monde. Ce sont 435 MW que pourra exploiter l'entreprise CoinMint. L'influx de capital qui accompagne cette annonce est de l'ordre de 700 millions de dollars et ce sont 150 emplois directs qui seront créés au courant des 18 mois suivants.

- En 2008, Bitmain Technologies Ltd a annoncé[156] le lancement d'un centre de données blockchain à Rockdale au Texas. Il s'agit d'un investissement de 500 millions de dollars sur une période initiale de sept ans. Le communiqué relate également la création de 400 emplois au cours des deux premières années du projet. Remarquons la nuance de terminologie utilisée dans le communiqué : "Blockchain Data Center".

- L'entreprise de cryptomonnaie ontarienne Hut8 a annoncé en juillet dernier l'ouverture d'un deuxième centre de calcul au Canada portant ainsi sa capacité totale à près de 67 MW[157]. Ce nouveau centre de calcul sera bâti au coût de 100 millions de dollars et déploiera 42 MW[158] à Medicine Hat en Alberta.

- Avec moins de 100 habitants, la municipalité de Ocean Falls en Colombie-Britannique est devenue une ville fantôme après la fermeture de son usine de papier, il y a près de 40 ans. Dotée d'un barrage hydroélectrique pouvant déployer 13 MW, elle alimente deux villes voisines. Durant les pointes hivernales, à peine le tiers de sa capacité est utilisée. Un centre de calcul de bitcoin s'y est installé[159].

Le Québec est avantageusement positionné pour attirer et retenir les centres de calcul. Les surplus énergétiques, l'énergie propre et renouvelable, le contexte politique stable, le régime de taxation clair et le climat froid sont des avantages compétitifs que proposent les régions nordiques telles que le Canada et le nord-ouest des États-Unis. Diversifier l'économie des régions, développer un pôle

[154] https://ca.rbcwealthmanagement.com/documents/77054/77074/Crypto+Currency+%26++Blockchain+Technology+-+A+Decentralized+Future+RBC+Capital+Markets+Jan+2018.pdf/594fcb18-1b28-48c1-920f-74938c59cc90 (27/09/2018)

[155] https://www.cnbc.com/amp/2018/06/05/bitcoin-miner-revamps-alcoas-aluminum-factory.html?__twitter_impression=true (24/09/2018)

[156] https://www.businesswire.com/news/home/20180806005156/en/Bitmain-Chooses-Rockdale-Texas-Newest-Blockchain-Data (24/09/2018)

[157] https://cointelegraph.com/news/canada-bitcoin-miner-hut-8-becomes-largest-by-capacity-after-second-site-opening/amp (24/09/2018)

[158] https://news.coinsquare.com/digital-currency/hut-8-bitcoin-mining-farm-alberta/ (27/09/2018)

[159] https://www.bloomberg.com/news/features/2018-09-04/the-bitcoin-boom-reaches-a-canadian-ghost-town (27/09/2018)

d'expertise en cryptomonnaie et chaînes de blocs, monétiser des surplus énergétiques, revitaliser des usines désaffectées et récolter les recettes fiscales des entreprises ne sont là que quelques bénéfices que retirent les régions étant favorablement positionnées pour accueillir les centres de calcul.

L'entreprise Bitfarms qui est déjà en activité au Québec fait partie de ces projets d'envergure. Dans le document intitulé Demande d'intervention de Bitfarms dossier R-4045-2018 (étape 2), on peut y lire qu'un total de 27,5 MW sont actuellement déployés dans les quatre centres situés au Québec (Farnham, Saint-Hyacinthe, Cowansville et Notre-Dame de-Stanbridge). Les emplacements utilisés sont d'anciennes usines qui ont été revitalisées. Certaines d'entre elles étaient désaffectées depuis plusieurs années.

L'entreprise Bitfarms souhaite prendre de l'expansion et a fait l'annonce de projets d'envergure notamment à Sherbrooke où un investissement de 250 millions de dollars a été annoncé. Bitfarms vise également à développer des projets à Magog, Saint-Jean-sur-Richelieu, Baie-Comeau, Thetford Mines et Jonquière totalisant plusieurs centaines de millions de dollars et des centaines d'emplois.

L'incertitude entourant le prix de l'électricité, une variable déterminante, a forcé la suspension temporaire desdits projets.

Pour conclure sur la section de l'environnement compétitif pour attirer les projets d'envergure, mentionnons un autre type d'alimentation en énergie renouvelable qui a attiré l'attention de centres de calcul.

Au Maroc, la société Soluna[160] a annoncé en septembre 2018 la construction d'une ferme d'éoliennes de 36 MW sur un terrain qui pourrait permettre jusqu'à 900 MW de production. Par contre, un réseau robuste de transmission de l'énergie qui sera produite vers la grille de distribution n'est pas disponible. Cette situation pourrait freiner le développement de cette source d'énergie par manque de monétisation à court et moyen terme. Par contre, avec une connexion Internet, il est possible de miner de la cryptomonnaie et rentabiliser les opérations en attendant d'être connecté à la grille du réseau de distribution. Lorsque questionné au sujet de la volatilité du prix, le PDG de Soluna, a mentionné qu'il souhaite diversifier ses activités graduellement pour inclure des applications chaînes de blocs qui ne sont pas des cryptomonnaies. Il a également mentionné que leur centre de calcul aurait l'option d'utiliser leur plateforme informatique à haute densité pour alimenter notamment l'intelligence artificielle et l'apprentissage automatique.

[160] https://arstechnica.com/information-technology/2018/09/construction-to-begin-on-36-megawatt-moroccan-wind-farm-for-bitcoin-mining/ (27/09/2018)

ANNEXE 8 : Documents consultés pour la rédaction du rapport d'analyse

Documents consultés pour les sections 1 et 2

- HQD-2 doc 1 en liasse NO : R-4045-2018 annexe B : Demande amendée d'Hydro-Québec Distribution (« Distributeur ») de fixation de tarifs et conditions de service pour l'usage cryptographique appliqué aux chaînes de blocs;
- HQD-2 doc 1 : Réponses du Distributeur à la DDR #1 de la Régie;
- HQD-2 doc 1.1 : Réponses du Distributeur à la DDR #2 de la Régie;
- HQD-2 doc 1.2 : Réponses du Distributeur à la DDR #3 de la Régie;
- HDQ-2 doc 5 : Réponses du Distributeur à la DDR #1 de Bitfarms;
- HQD-2 doc 7 : Réponses du Distributeur à la DDR #1 de Cogeco;
- HQD-1 doc 6 : Réponses du Distributeur à l'engagement #2 pris lors de l'audience devant la Régie de l'énergie
- Demande d'intervention de Bitfarms dossier R-4045-2018 (étape 2)
- Version administrative du décret n° 646-2018
- Analyse économique des installations de minage d'actifs cryptographiques par KPMG daté du 26 février 2018 (ci-après appelé Rapport KPMG)

OCTONOMICS

Elisabeth Préfontaine
MBA, CFA, CAIA, CBP
Fondatrice

ep@octonomics.com