Tendances technologiques

Chaîne de blocs

Architecture d'entreprise, Direction générale du dirigeant principal de la technologie

Version 0.1
Date : 2019-5-8

Services partagés Canada | Shared Services Canada

Canada

Table des matières

Sommaire opérationnel

La chaîne de blocs est une liste de dossiers numériques (appelés blocs) qui sont liés de manière sécuritaire pour former une chaîne au moyen d'un chiffrement sécurisé et d'horodateurs. Les chaînes de blocs forment un grand livre numérique qui constitue un historique des transactions enregistrées auxquelles peuvent accéder de multiples utilisateurs, mais qui ne peuvent pas être modifiées individuellement.

La théorie derrière la chaîne de blocs a été décrite pour la première fois en 1991. On souhaitait alors créer un système dans lequel les documents pouvaient être horodatés et liés entre eux de manière numérique ou cryptographique. En 2008, une personne ou un groupe de personnes œuvrant sous le pseudonyme « Satoshi Nakamoto » a créé la première cryptomonnaie, le Bitcoin. La création du Bitcoin en 2008 a également mis à jour la technologie derrière cette cryptomonnaie : la chaîne de blocs. La chaîne de blocs permet de consigner les transactions de Bitcoins (en tant que grand livre partagé) et peut être utilisée pour consigner toute transaction et suivre les déplacements de tout élément d'actif corporel, incorporel ou numérique.

En raison de la méfiance croissante à l'égard du partage de données par certaines grandes entreprises et de la crise financière ayant eu lieu plus tôt pendant l'année, on recherche de plus en plus un moyen pour que chaque personne ait le contrôle de ses propres données et de son propre argent. Ce moyen devait être décentralisé et réduire la nécessité d'un intermédiaire, comme les banques, les courtiers ou les compagnies d'assurances. En tant que première technologie en son genre, la chaîne de blocs était révolutionnaire[i].

Bien que la technologie de la chaîne de blocs ait commencé à prendre de l'expansion depuis sa création, à ses débuts, les utilisateurs étaient exclusivement des particuliers. Il y a toujours des individus qui utilisent des cryptomonnaies comme le Bitcoin; toutefois, des entreprises comme Ethereum, Golem et Blockstack sont apparues et font également appel à la technologie de la chaîne de blocs pour la création de « contrats intelligents » entre des parties, le partage de la puissance de traitement des ordinateurs et le développement d'applications ouvertes, respectivement. Toutefois, la technologie est toujours considérée comme étant immature et sous-utilisée. Parmi les répondants au sondage mené par Gartner auprès des dirigeants principaux de l'information de 2018, seulement 1 % ont investi dans la technologie de la chaîne de blocs et déployé celle-ci[ii].

Sommaire technique

Les données et registres de transactions contenus dans une chaîne de blocs sont décentralisés, contrairement aux registres de transactions traditionnels, qui nécessitent souvent un intermédiaire comme une banque ou un autre administrateur et qui comportent la plupart du temps de multiples enregistrements d'une même transaction. Par exemple, dans le contexte d'un achat traditionnel, le consommateur a un

enregistrement de la transaction, tout comme le commerçant, le fournisseur et un vérificateur ou un comptable. La banque a également un enregistrement. Tous ces enregistrements sont conservés séparément. Le processus d'achat requiert donc que chacune des parties ait confiance que les autres parties ne modifieront ni ne perdront un enregistrement.

Dans une transaction dans la chaîne de blocs, chacune des parties concernées (appelées nœuds, utilisateurs ou mineurs) possède la même réplique d'un grand livre, qui est contenu dans la chaîne de blocs sur un réseau de pair à pair (ou de nœud à nœud). Ainsi, la banque et les bases de données traditionnelles de commerçants utilisées pour consigner et organiser les données dans le grand livre sont éliminées (p. ex., la date et l'heure de la transaction, le produit, l'acheteur).

Pour former un bloc ou une chaîne de blocs, chaque utilisateur a besoin d'un ordinateur spécialisé et d'un logiciel de minage. Une chaîne de blocs est gérée et vérifiée en collaboration sur un réseau auquel de multiples utilisateurs ou nœuds accèdent. Ces utilisateurs travaillent en collaboration et utilisent le minage et des « algorithmes de consensus » pour résoudre des problèmes mathématiques complexes. Un algorithme de consensus est un processus convenu de résolution de calculs, et plusieurs sont utilisés dans la technologie de la chaîne de blocs en fonction du type de calcul à résoudre et du type de données à vérifier.

En raison de sa nature décentralisée, ouverte et cryptographique, la chaîne de blocs permet aux personnes d'avoir confiance les unes envers les autres et de réaliser des transactions de pair à pair, ce qui élimine la nécessité des intermédiaires. Elle résiste aux attaques de piratage qui touchent les intermédiaires centralisés comme les banques parce que, pour réussir, l'attaquant doit pirater le bloc spécifique dans une chaîne ainsi que chacun des millions d'autres grands livres potentiels se trouvant sur le réseau en même temps. Une telle opération serait difficile, puisque les blocs sont sécurisés à l'aide de clés publiques et privées et doivent être vérifiés par de multiples utilisateurs et ordinateurs individuels. Même si cela était possible, l'attaquant devrait également mettre à jour toutes les transactions subséquentes de la chaîne et écraser toutes les autres copies du grand livre se trouvant sur le réseau pour assurer l'intégrité de la nouvelle chaîne.

Malgré la résistance naturelle aux attaques de la chaîne de blocs, la revue MIT Technology Review a signalé que de plus en plus de failles de sécurité apparaissent dans la cryptomonnaie et les plates-formes de contrats intelligents. Dans certains cas, les problèmes de sécurité sont au cœur de la conception des plates-formes. En obtenant le contrôle de la puissance de plus de la moitié des ordinateurs du réseau, un pirate a tenté de réécrire l'historique des transactions de la plate-forme d'échange de cryptomonnaie appelée Coinbase et de faire en sorte que la même cryptomonnaie puisse être dépensée plus d'une fois, pour une valeur totale de 1,1 million de dollars[iii].

Utilisation par l'industrie

L'utilisation la plus connue de la chaîne de blocs est liée aux cryptomonnaies, comme le Bitcoin. Cette monnaie numérique, lancée en 2009, ne fait pas appel à une autorité monétaire pour surveiller, vérifier ou approuver les transactions, mais se sert plutôt d'un réseau d'ordinateurs de pair à pair composé des appareils de ses utilisateurs pour le faire. La chaîne de blocs peut servir à toutes sortes d'opérations de coopération interorganisationnelles. En 2017, la revue Harvard Business Review a estimé que l'on s'attend à ce qu'environ 15 % des banques utilisent la chaîne de blocs[iv].

Même si le Bitcoin est la première et plus populaire technologie de chaîne de blocs, il ne s'agit que de l'une des quelque 700 applications qui utilisent le système de grand livre distribué au moyen de la chaîne de blocs. La chaîne de blocs est un grand livre numérique à partir duquel les organisations peuvent construire des applications dignes de confiance, par l'intermédiaire d'une chaîne de possession sécurisée pour les registres numériques.

Utilisation par le gouvernement du Canada

Actuellement, le Canada n'a pas de politique fédérale sur la chaîne de blocs. Bien qu'il s'agisse d'une importante technologie émergente, la manière dont le gouvernement pourrait s'en servir reste à déterminer. À l'heure actuelle, l'utilisation idéale de la chaîne de blocs par le gouvernement du Canada consisterait en un système de registres publics permettant de consigner les transactions sécurisées effectuées par de multiples parties dans le but de distribuer une source unique de faits non réfutables.

Selon Gartner, aucun gouvernement du monde n'a mis en place une véritable initiative reposant sur la chaîne de blocs. Toutefois, certains (État de la Géorgie, Hong Kong, Émirats arabes unis) réalisent des pseudo-initiatives et commencent à expérimenter avec la technologie[v]. Les notes du Conseil du Trésor du Canada soulignent certaines initiatives spécifiques : l'Estonie mise sur un partenariat avec une fondation de cybersanté pour accélérer des systèmes fondés sur la chaîne de blocs afin d'assurer la sécurité, la transparence et la vérifiabilité des dossiers de soins de santé des patients. Singapour utilise la chaîne de blocs pour empêcher les négociateurs de frauder les banques, au moyen d'un système unique de grand livre distribué axé sur la prévention des fraudes par fausse facture[vi].

En 2017, le rapport intitulé « The Blockchain Corridor: Building an Innovation Economy in the 2nd Era of the Internet » a été préparé; ce rapport traitait de façons de transformer le Canada en un centre mondial de « révolution de la chaîne de blocs ». Ce rapport, qui a été rédigé par un groupe de réflexion sur la haute technologie pour Innovation, Sciences et Développement économique Canada et partiellement financé par ce ministère, présente quelques propositions pour confirmer la position du Canada en tant que leader mondial dans la technologie de la chaîne de blocs. Le gouvernement du

Canada a annoncé, en juillet 2017, son intention d'exécuter au moins six projets pilotes retenus portant sur l'utilisation de la chaîne de blocs[vii].

Ces projets comprenaient l'établissement d'une commission sur l'économie numérique, qui se verra confier la tâche de formuler des recommandations solides sur la manière dont le Canada pourrait devenir un leader dans les technologies en développement comme la chaîne de blocs, l'informatique quantique, l'intelligence artificielle et les véhicules autonomes. Il est également recommandé d'inciter les gouvernements qui utilisent actuellement la chaîne de blocs à transformer leurs propres opérations et à donner des exemples de la manière dont cette technologie pourrait être bénéfique pour le secteur public du Canada et d'ailleurs dans le monde. Les gouvernements pourraient utiliser la chaîne de blocs afin de vérifier le paiement des impôts et gérer plus efficacement les services publics.

Répercussions pour Services partagés Canada

Proposition de valeur

Les technologies de collaboration comme la chaîne de blocs promettent la capacité d'améliorer les processus opérationnels qui s'exécutent entre les organisations et les entités et de diminuer de manière radicale le « coût de la confiance ». La chaîne de blocs pourrait donc offrir un rendement beaucoup plus élevé pour chaque dollar investi que les investissements internes traditionnels, mais elle nécessite la mise en place de nouvelles façons de collaborer avec les clients, les citoyens, les fournisseurs et les concurrents[viii].

La chaîne de blocs offre certains avantages au gouvernement du Canada, comme une réduction des coûts et de la complexité, une tenue de documents digne de confiance et un contrôle de la confidentialité axé sur les utilisateurs. Elle offre de grandes possibilités du point de vue d'une source unique de registres publics et du soutien de multiples collaborateurs et représente une technologie idéale pour les interactions plurigouvernementales. En raison de sa nature décentralisée et collaborative, elle pourrait bien s'harmoniser aux politiques et pratiques d'un gouvernement ouvert, qui visent à rendre les services, les données et les dossiers numériques du gouvernement plus accessibles aux Canadiens.

En éliminant le dédoublement et en réduisant le besoin d'intermédiaires, la technologie de la chaîne de blocs pourrait être utilisée par Services partagés Canada (SPC) pour accélérer certains aspects de la prestation de services. En ce qui concerne la chaîne de blocs, SPC devra relever un défi, celui de déterminer les meilleures solutions d'entreprise et comment elles traitent des aspects de la vie privée, de la confidentialité, de la vérifiabilité, du rendement et de l'adaptabilité.

Actuellement, certains organismes du gouvernement utilisent la chaîne de blocs de diverses façons. SPC pourrait peut-être appuyer les ministères et organismes suivants dans leurs initiatives visant à établir la manière d'utiliser la chaîne de blocs pour aider à régler certains enjeux :

Élections Canada – Applications pratiques pour faciliter la gestion de la liste électorale, la gestion sécurisée de l'identité et la gestion de la géographie électorale.

Centre d'analyse des opérations et déclarations financières du Canada – Explorer les utilisations liées au financement de la lutte contre le blanchiment d'argent et le terrorisme.

Sécurité publique Canada – Se pencher sur des utilisations diverses et à mauvais escient des monnaies virtuelles, à des fins d'extorsion ou de chantage, par exemple.

Ressources naturelles Canada – Utiliser en tant que registre public pour la divulgation des paiements en vertu de la *Loi sur les mesures de transparence dans le secteur extractif*.

Banque du Canada – Envisager un modèle de validation de principe avec Paiements Canada, les banques commerciales canadiennes et le consortium R3.

Innovation, Sciences et Développement économique Canada – Mobilisation des ministères fédéraux, des partenaires provinciaux, territoriaux et municipaux et des principaux acteurs de l'industrie.

Difficultés

Il existe des faiblesses en ce qui concerne la complexité de la technologie, des exigences informatiques et de stockage intensives ainsi qu'un besoin de logiciel commun à tous les nœuds. Il existe également des difficultés particulièrement importantes propres à un processus gouvernemental. Les actifs entièrement numériques dont il n'existe qu'une seule copie peuvent être détruits, et un réseau gouvernemental comportant de tels actifs serait une cible très en vue pour des auteurs malveillants[ix].

Il est important de se rappeler que la chaîne de blocs, même si elle constitue une innovation technologique dans le domaine des transactions ainsi qu'une chaîne de possession numérique, n'est pas une solution miracle aux difficultés en matière de transactions auxquelles le gouvernement du Canada est confronté.

La quantité de temps et d'énergie requise pour maintenir la chaîne de blocs et créer de nouveaux blocs est élevée, et il s'agit d'une critique fréquente à l'égard de cette technologie. Il ne faut que quelques millisecondes pour faire une entrée dans une base de données conventionnelle, comme SQL, comparativement à la chaîne de blocs, qui nécessite plusieurs minutes. En raison du temps requis et du besoin de multiples

ordinateurs pour vérifier les blocs, les chaînes de blocs consomment une quantité d'énergie énorme. Toutefois, à mesure que la technologie évolue, le temps nécessaire au processus de consensus de la chaîne de blocs se rapproche des trois minutes avec Ethereum, qui fait actuellement partie des chaînes de blocs les plus avancées disponibles. Même les chaînes de blocs plus anciennes, comme Bitcoin, sont plus rapides que les transactions financières traditionnelles, comme celles du marché boursier, dont la vérification et la finalisation peuvent prendre plusieurs jours. Malgré cela, les services ou transactions devant être exécutés rapidement pourraient ne pas convenir à la chaîne de blocs.

Il y a aussi certaines préoccupations relatives à la confidentialité. Puisque la chaîne de blocs est fondée sur le principe de la décentralisation et de la transparence, les données qui s'y trouvent sont techniquement accessibles à tous les utilisateurs du réseau, à condition qu'ils possèdent la puissance informatique et les connaissances nécessaires pour y accéder. Au lieu d'être identifiés sur le réseau par un nom, les utilisateurs ont une clé de chiffrage, qui est une suite de chiffres et de lettres en apparence aléatoire. Bien qu'il s'agisse d'une méthode plus privée qu'un nom ou une autre information démographique, les utilisateurs pourraient tout de même être identifiés par leur clé au fil du temps. De plus, un élément de données contenu dans un bloc pouvant comporter des renseignements personnels qu'une personne souhaite garder confidentiels, par exemple un dossier médical, pourrait ne pas convenir à la chaîne de blocs, puisque celle-ci est transparente et que les renseignements seront visibles pour les autres utilisateurs[x].

Considérations

En utilisant un algorithme de consensus convenu, les technologies de collaboration comme la chaîne de blocs fournissent la capacité d'améliorer les processus opérationnels qui s'exécutent entre les organisations et entités et de diminuer de manière radicale le « coût de la confiance ». Le coût de la confiance est diminué parce qu'il n'y a qu'un seul enregistrement de la transaction qui doit être conservé et que tous les intervenants ont confiance en cet enregistrement.

Dans une transaction traditionnelle, tous les intervenants doivent conserver un enregistrement de la transaction et, dans le cas d'un écart, il est plus difficile et coûteux de déterminer l'exactitude d'un enregistrement. Ainsi, la chaîne de blocs pourrait offrir un rendement beaucoup plus élevé pour chaque dollar investi que les investissements internes traditionnels. Toutefois, cette technologie nécessite la mise en place de nouvelles façons de collaborer avec les clients, les citoyens, les fournisseurs et les concurrents[xi].

Il faut réaliser plus de recherches pour comprendre les répercussions potentielles de la chaîne de blocs sur SPC en tant que fournisseur de services ainsi que sur l'usage requis par le gouvernement du Canada. SPC devrait envisager de cerner les secteurs clients où la chaîne de blocs pourrait être utilisée. Les ministères clients pourraient devoir cibler

eux-mêmes les secteurs dans lesquels les processus de la chaîne de blocs pourraient être utiles. Il sera difficile pour SPC de cerner les organisations partenaires et solutions d'entreprise qui nécessitent la tenue de projets pilotes prioritaires sur la chaîne de blocs et d'être en mesure de déterminer les ministères qui sont des chefs de file et la manière dont ils composent avec les questions de vie privée, de confidentialité, de vérifiabilité, de rendement et d'adaptabilité.

Enfin, SPC et le gouvernement du Canada devraient examiner les problèmes de capacités relatifs aux ressources, les capacités du réseau et le temps requis pour créer et maintenir des réseaux de chaînes de blocs par eux-mêmes. La chaîne de blocs n'est pas une technologie simple; il faudra des équipes spécialisées qui possèdent les ressources et le financement appropriés pour que cette technologie soit déployée comme tout autre service. SPC pourrait envisager de faire appel à des entreprises du secteur privé qui se spécialisent dans la chaîne de blocs en tant que service(BaaS ou *Blocks as a Service*) et déterminer les risques et les avantages sur le plan des coûts associés à l'externalisation de ce processus.

English	French
Figure 1. Hype Cycle for Blockchain Technologies, 2018	Figure 1. Rapport Hype Cycle sur les technologies de la chaîne de blocs, 2018
Expectations	Attentes
Time	Temps
Blockchain Wallet Platform	Plate-forme de portefeuille de la chaîne de blocs
Blockchain Interoperability	Interopérabilité de la chaîne de blocs
Postquantum Blockchain	Chaîne de blocs post-quantique
Smart Contract Oracle	Oracle des contrats intelligents
Zero Knowledge Proofs	Preuve à divulgation nulle de connaissance
Distributed Storage in Blockchain	Stockage distribué dans la chaîne de blocs
Smart Contracts	Contrats intelligents
Blockchain for IAM	Chaîne de blocs pour la gestion des identités et de l'accès
Blockchain PaaS	Chaîne de blocs à titre de PaaS
Blockchain for Data Security	Chaîne de blocs pour la sécurité des données
Decentralized Applications	Applications décentralisées
Consensus Mechanisms	Mécanismes de consensus
Metacoin Platforms	Plates-formes de Metacoin
Sidechains/Channels	Chaînes latérales/canaux
Multiparty Computing	Calcul multipartite
Cryptocurrency Hardware Wallets	Portefeuilles matériels de cryptomonnaie
Cryptocurrency Software Wallets	Portefeuilles logiciels de cryptomonnaie
Blockchain	Chaîne de blocs
Distributed Ledgers	Grands livres distribués
Cryptocurrency Mining	Minage de cryptomonnaie
Innovation Trigger	Déclencheur d'innovation
Peak of Inflated Exepctations	Pic des attentes exagérées
Trough of Disillusionment	Gouffre des désillusions
Slope of Enlightenment	Pente de l'illumination
Plateau of Productivity	Plateau de productivité
As of July 2018	En date de juillet 2018
Plateau will be reached:	Le plateau sera atteint :
Less than 2 years	dans moins de 2 ans
2 to 5 years	dans 2 à 5 ans
5 to 10 years	dans 5 à 10 ans
More than 10 years	dans plus de 10 ans
Obsolete before plateau	Désuet avant le plateau
Source: Gartner (July 2018)	Source : Gartner (juillet 2018)

Références

[i] George Gilder, *Life After Google: The Fall of Big Data and the Rise of the Blockchain Economy*, Gateway Editions, juillet 2018. (en anglais seulement)
[ii] David Furlonger et Rajesh Kandaswamy, *Hype Cycle for Blockchain Technologies, 2018*, juillet 2018. (en anglais seulement)
[iii] Mike Orcutt, *Once hailed as unhackable, blockchains are now getting hacked*, MIT Technology Review, 19 février 2019. (en anglais seulement)
[iv] Harvard Business Review, *A Brief History of Blockchain*, 2017. (en anglais seulement)
[v] Conférence téléphonique de Gartner.
[vi] Conseil du Trésor du Canada
[vii] Plan stratégique des opérations numériques de 2018 à 2022 – https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/plan-strategique-operations-numerique-2018-2022.html
[viii] Conseil du Trésor du Canada, *La chaîne de blocs : Cas d'utilisation optimaux pour le gouvernement du Canada*, 5.
[ix] Conseil du Trésor du Canada, 7.
[x] Henning Diedrich, *Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations*, septembre 2016. (en anglais seulement)
[xi] Conseil du Trésor du Canada, *La chaîne de blocs : Cas d'utilisation optimaux pour le gouvernement du Canada*, 5.