

# La technologie de chaîne de blocs - En survol

## Aperçu

Une chaîne de blocs est une base de données à écriture seule répartie sur un réseau d'ordinateurs reliés les uns aux autres et faisant appel à la cryptographie (encodage et décodage informatisés de renseignements) pour créer un registre public de transactions inviolable. La technologie de la chaîne de blocs est transparente, sécuritaire et décentralisée, ce qui signifie qu'aucun intervenant ne peut modifier le registre public. De plus, les opérations financières exécutées à l'aide de chaînes de blocs sont moins chères et plus rapides que celles réalisées par des établissements financiers traditionnels. Ces propriétés expliquent l'expansion rapide de cette technologie.

Bitcoin a été la première chaîne de blocs. Elle a été mise en œuvre en 2009 pour créer la cryptomonnaie « bitcoin » ayant pour but de remplacer les devises ou la monnaie fiduciaire (papier monnaie ou pièces de monnaie n'ayant pas de valeur réelle, mais légalisés par un gouvernement). En novembre 2016, sa capitalisation boursière s'établissait à 15 milliards de dollars CAD. Au cours des dernières années, un certain nombre de chaînes de blocs de deuxième génération ont été créées, Ethereum étant la plus connue d'entre elles. Les transactions réalisées à l'aide de la chaîne de blocs Ethereum sont de nature financière, mais elles peuvent également comprendre des rapports de bases de données polyvalents et des programmes appelés « contrats intelligents », qui peuvent être conclus directement dans la chaîne de blocs. Les contrats intelligents transforment les contrats commerciaux ou juridiques en programmes informatiques, appliquant les propriétés de la chaîne de blocs aux transactions commerciales. De plus, des **applications décentralisées** (« **DApps** ») cryptées de façon numérique peuvent reproduire la fonctionnalité d'applications vendues dans le commerce, mais dans un environnement décentralisé et peu coûteux. Les DApps sont des applications qui exécutent des contrats intelligents. Ces contrats peuvent porter, notamment, sur le covoiturage, le sociofinancement, des services notariés pour la conservation publique de données sur la propriété, des ventes d'électricité décentralisées, la gestion de tâches, des services de messagerie décentralisés (comme Twitter), l'identification et la tenue de dossiers et d'autres services gouvernementaux.

Le Financial Times : [How bitcoin and its blockchain work](#) et [The Ethereum Project](#)



Gouvernement  
du Canada

Horizons de politiques  
Canada

Government  
of Canada

Policy Horizons  
Canada

Canada 1

## Considérations stratégiques

La technologie de la chaîne de blocs constitue une solution numérique sécuritaire, transparente, rapide et abordable à de nombreux problèmes du gouvernement. Elle pourrait, entre autres choses, faciliter les paiements, la distribution de prestations, l'identification, la tenue de dossiers et la certification. Par contre, on craint que les cryptomonnaies comme le bitcoin puissent être utilisées pour accroître l'anonymat lors d'opérations criminelles, ce qui présente des [défis](#) sur le plan du droit et de la sécurité. Toutefois, d'après un [rapport](#) publié en 2015 par le gouvernement du Royaume-Uni, le bitcoin risque le moins d'être utilisé pour effectuer du blanchiment d'argent, puisque toutes les opérations effectuées avec des bitcoins sont publiques. Des innovations en lien avec la chaîne de blocs, comme la DAO sur Ethereum, pourraient être une occasion de faciliter le financement d'entreprises en démarrage. Une telle solution pourrait présenter de l'intérêt pour un pays comme le Canada, où les petites et moyennes entreprises jouent un rôle important dans l'économie. De même, le secteur des services assume un rôle de premier plan dans l'économie canadienne, et la technologie de la chaîne de blocs promet d'atténuer les frictions dans le commerce et les services numériques en réduisant les frais liés aux opérations financières. Pour les petites entreprises qui effectuent un très grand nombre de petites transactions, ces frais représentent un fardeau disproportionné.

La technologie de la chaîne de blocs a très souvent [battu des records de sociofinancement](#) en raison de l'intérêt manifesté par les investisseurs. Le milieu bancaire mondial, de même que des chefs de file des secteurs de la technologie et des communications, financent des projets dans le but d'apprendre comment se servir de cette innovation. Il s'agit essentiellement d'une technologie décentralisée, qui peut être perçue comme une menace pour les grandes institutions, notamment les gouvernements. Le bitcoin est une devise qui n'est soutenue par aucun pays et qui n'est contrôlée par aucune banque ni aucun joueur central. Contrairement à Internet, qui repose sur des serveurs installés en sol contrôlé par des États nations et appartenant à des entreprises, les logiciels décentralisés peuvent poser des défis juridiques entièrement nouveaux sur le plan des obligations, des droits et des territoires.

Bien que cette technologie ait été créée il y a seulement sept ans, les logiciels libres favorisent en raison de leur nature même, la distribution rapide et à grande échelle d'innovations liées à la chaîne de blocs. Il pourrait être risqué d'attendre de voir si les initiatives se concrétiseront, au lieu de se préparer en vue du moment où de telles ambitions deviendront très courantes.

## Avantages

La technologie de la chaîne de blocs pourrait contribuer à réduire le coût des services bancaires en proposant une solution de rechange à coût pratiquement nul. Prenons, par exemple, les transferts de fonds internationaux. Alors que de nombreux bureaux de change imposent des frais (peut être 2 % ou 3 %) sur le montant changé, les frais liés aux transactions en bitcoins varient entre [5 et 10 cents US](#), peu importe le montant changé. La rapidité de la transaction est un autre avantage. Au lieu du délai d'un à trois jours exigé par les banques pour exécuter des opérations financières, les chaînes de blocs peuvent effectuer des transactions en moins de [15 secondes](#). Le registre public décentralisé et transparent fourni par les chaînes de blocs peut donner la confiance nécessaire pour effectuer une transaction avec un inconnu sans avoir conjointement recours à une tierce partie de confiance,

comme une banque ou un avocat. De cette façon, les technologies de chaînes de blocs peuvent devenir un élément clé dans l'augmentation du nombre de transactions poste-à-poste rapides et peu coûteuses pour l'échange ou la vente de biens et de services, ce qui pourrait accroître le choix et l'offre sur le marché. Un certain nombre de secteurs d'activité envisagent d'utiliser des chaînes de blocs privées pour réduire leurs coûts et accroître la vitesse et la sécurité de leurs opérations. Globalement, la technologie de la chaîne de blocs pourrait augmenter le pouvoir d'achat des consommateurs en abaissant les frais de transaction dans toute la chaîne de valeur.

## Restrictions

L'une des conséquences des registres universels décentralisés est que toute erreur ou défaillance logicielle doit se produire au grand jour et sera donc rapidement découverte par la collectivité mondiale. Cette situation a donné lieu à des vols largement médiatisés, comme la défaillance du service de change de bitcoins [Mt. Gox](#) et le piratage de celui de [Bitfinex](#). Bien que les registres publics des chaînes de blocs soient cryptographiés et peu vulnérables à la plupart des formes de fraudes, il est possible que les services qui s'y rattachent soient tout aussi vulnérables aux attaques et aux vols que d'autres technologies numériques. Dernièrement, la découverte de défauts dans le code de l'un des produits dérivés les plus ambitieux d'Ethereum, la [DAO](#) (Digital Autonomous Organization), a démontré que même si la technologie de la chaîne de blocs promet d'être transformatrice, elle en est encore à ses balbutiements.

Les entreprises, les établissements et les endroits qui acceptent actuellement le bitcoin se font rares malgré une [expansion rapide](#), de sorte que cette devise ne peut certainement pas remplacer pour le moment les devises nationales et les services bancaires. Une mauvaise compréhension générale de la technologie et une pénurie de travailleurs hautement qualifiés et compétents représentent peut-être les obstacles les plus importants au déploiement à plus grande échelle de la technologie de la chaîne de blocs.

**Horizons de politiques Canada explore des avenir vraisemblables pour le Canada au cours des 10 ou 15 prochaines années dans les domaines de la gouvernance, de la durabilité, de l'infrastructure et de l'économie numérique. Pour de plus amples renseignements, veuillez communiquer avec nous à l'adresse [questions@horizons.gc.ca](mailto:questions@horizons.gc.ca).**

## Sources

[Les cryptomonnaies : pile ou face? Rapport du Comité sénatorial permanent des banques et du commerce](#)

[Device democracy: saving the future of the Internet of Things](#)

[Cryptocurrency 2.0 Report - CoinDesk](#)

## Gouvernement du Canada

La Banque du Canada acquiert une expérience pratique de la technologie.

Wall Street Journal – [Bank of Canada's Carolyn Wilkins Sees Potential for Blockchain, But Not Just Yet](#)

Horizons de politiques Canada – [www.horizons.gc.ca](http://www.horizons.gc.ca)

## Autres autorités

- [Blockchain to transform Estonia's e-residency by allowing shareholders to vote in shareholder meetings](#)
- [Georgia Pilots and Sweden Ponders – Is Blockchain the Future for Europe's Land Registries?](#)
- [Dubai to use blockchain technology for all government documents by 2020](#)
- [Chinese government's primary information technology ministry has published a research paper detailing blockchain's benefits](#)
- [Singapore's Central Bank Pairs Up With R3 to Create Blockchain R&D Center](#)
- [UK Government Trials Blockchain Welfare Payments System](#)
- [Blockchain Support Bill Passes Vote in US Congress](#)

## Meilleurs de leur catégorie

- [R3 Cev](#) dirige un partenariat regroupant 50 banques mondiales pour la mise au point d'une chaîne de blocs privée dont le nom de projet est « Corda ».
- [Bitnation](#) offre des services gouvernementaux et une aide d'urgence à ceux qui ont besoin de services de représentation, p. ex. les réfugiés ou des aspirants citoyens du monde.
- [Hyperledger](#) est un projet de normes et de protocoles ouverts entre des chefs de file de l'industrie, comme IBM, Cisco, Intel, la Bourse de Londres, etc., dirigé par la Linux Foundation.
- [Everledger](#) est une base de données sur les diamants utilisée pour contrer le vol et la fraude et faciliter l'application de la loi et des assurances.
- [Zcash](#) est une cryptomonnaie offrant une protection des renseignements personnels et une transparence sélective.
- [DAO](#), une organisation anonyme décentralisée, se voulait un ambitieux projet ayant pour but de créer une société décentralisée dont les membres auraient pu voter sur les nombreux projets que l'entreprise aurait financés.

*Le présent document propose un survol de certains enjeux émergents et de leurs répercussions potentielles sur la politique publique au cours des 10 à 15 prochaines années. Il ne vise pas à prédire l'avenir. L'objectif est de stimuler la réflexion et le dialogue et de soutenir l'élaboration d'une politique publique plus solide et durable à la lumière de divers scénarios futurs plausibles. Les opinions exprimées dans le présent document ne représentent pas forcément celles d'Horizons, du gouvernement du Canada ou des ministères et organismes participants.*

PH4-171/2016F-PDF  
978-0-660-07026-1

© Sa Majesté la Reine du Chef du Canada, 2016.