La technologie de la chaîne de blocs et son incidence potentielle sur la profession d'auditeur et de certificateur

CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

AICPA®

UW CISA

La technologie de la chaîne de blocs et son incidence potentielle sur la profession d'auditeur et de certificateur

CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

AICPA®

UW CISA

AVERTISSEMENT

Le présent document, préparé par Comptables professionnels agréés du Canada (CPA Canada) et l'American Institute of Certified Public Accountants (AICPA), fournit des indications ne faisant pas autorité.

CPA Canada et l'AICPA déclinent toute responsabilité ou obligation pouvant découler, directement ou indirectement, de l'utilisation de ce document.

Table des matières

Sommaire

La chaîne de blocs a vu le jour en tant que noyau technologique de Bitcoin[1], l'écosystème de cryptomonnaie[2] décentralisé et fortement médiatisé proposé en 2008. L'attrait de la technologie de la chaîne de blocs repose sur son utilisation d'un réseau poste à poste[3] combiné à la cryptographie[4]. C'est grâce à cette combinaison que des parties qui ne se connaissent pas sont en mesure de conclure des opérations sans recourir à un intermédiaire de confiance traditionnel, comme une banque ou un réseau de traitement des paiements. Parce qu'elle permet d'éliminer l'intermédiaire et de tirer profit de la puissance des réseaux poste à poste, la technologie de la chaîne de blocs pourrait ouvrir la voie à de nouvelles façons de réduire considérablement les coûts des opérations ainsi que la période de règlement. Elle pourrait aussi transformer et bousculer une multitude de secteurs d'activité, des services financiers au secteur public en passant par les soins de santé. En conséquence, des sociétés de capital-risque et de grandes entreprises investissent dans la recherche et les essais relativement à la technologie de la chaîne de blocs afin de repenser les pratiques et modèles d'affaires traditionnels.

Ces dernières années, la technologie de la chaîne de blocs a largement dépassé les opérations en bitcoins et elle est maintenant mise à l'essai dans une vaste gamme d'applications commerciales et financières. Toutefois, cette technologie en est toujours à ses débuts et n'a pas encore fait ses preuves à l'échelle d'une entreprise, ce qui freine son potentiel de transformation. En outre, de nombreux cabinets comptables ont entrepris des initiatives axées sur les chaînes de blocs pour mieux comprendre les incidences de cette technologie. Il est important que la profession d'auditeur et de certificateur demeure au fait des nouveautés dans ce domaine, et nous encourageons les comptables professionnels agréés et les

1 Le terme « bitcoin » est utilisé pour désigner l'unité monétaire, alors que « Bitcoin » sert à décrire le concept lui-même ou le réseau complet conçu par Satoshi Nakamoto.

2 La cryptomonnaie peut se définir comme une forme de monnaie ou d'échange basée sur Internet (n'ayant rien à voir avec les billets de banque et les pièces de monnaie tangibles) qui présente des propriétés similaires à celles des monnaies physiques, mais qui permet des opérations instantanées et des transferts de propriété sans frontières.

3 L'informatique poste à poste ou les réseaux poste à poste s'appuient sur une architecture applicative distribuée qui partage les tâches entre les postes. Tous les participants s'engagent à parts égales dans l'application afin de former un réseau de nœuds poste à poste.

4 La cryptographie moderne s'appuie sur les mathématiques, l'informatique et le génie électrique pour assurer la sécurité des communications entre deux parties en présence d'un tiers.

Certified Public Accountants (collectivement, les CPA auditeurs) à s'intéresser à cette technologie. Le présent document vise à expliquer ce qu'est la technologie de la chaîne de blocs et à décrire son incidence potentielle sur l'audit des états financiers. On y traite notamment des nouveaux services de certification qui pourraient voir le jour et des nouveaux rôles que le CPA auditeur pourrait être appelé à jouer dans l'écosystème de la chaîne de blocs.

La technologie de la chaîne de blocs est porteuse de changements susceptibles de toucher tous les processus de tenue des comptes, y compris la façon dont les opérations sont déclenchées, traitées, autorisées, enregistrées et communiquées. Les changements apportés aux modèles et processus d'affaires pourraient se répercuter sur les activités administratives comme la communication de l'information financière et la préparation des déclarations fiscales. Les auditeurs indépendants devront eux aussi comprendre cette technologie lorsqu'elle sera déployée chez leurs clients. Le rôle et les compétences attendues des CPA auditeurs pourraient changer à mesure qu'émergeront de nouvelles techniques et procédures s'appuyant sur la chaîne de blocs. Par exemple, les méthodes visant à obtenir des éléments probants suffisants et appropriés devront être axées aussi bien sur les grands livres distincts traditionnels que sur les grands livres basés sur des chaînes de blocs. De plus, cette technologie pourrait favoriser l'uniformisation et la transparence de l'information financière et de la comptabilité, et donc une plus grande efficience dans l'extraction de données et l'analyse.

Pour la profession d'auditeur et de certificateur, cela signifie de nouveaux défis et de nouvelles perspectives. L'arrivée de la technologie de la chaîne de blocs ne viendra pas réduire l'importance des services traditionnels d'audit et de certification, mais elle pourrait modifier la stratégie du CPA auditeur. Tout comme les innovations actuelles en matière d'automatisation et d'analyse des données qui obligent la profession d'auditeur et de certificateur à s'adapter, la technologie de la chaîne de blocs pourrait elle aussi avoir une incidence significative sur la façon dont les auditeurs exécutent leurs missions. De plus, les CPA pourraient devoir élargir leurs compétences et leurs connaissances pour répondre aux demandes qui viendront assurément du monde des affaires à mesure que l'utilisation de la technologie de la chaîne de blocs se répandra.

Comptables professionnels agréés du Canada (CPA Canada), l'Association of International Certified Professional Accountants (AICPA) et le Centre pour l'intégrité de l'information et la certification des systèmes d'information de l'Université de Waterloo (UWCISA) encouragent la profession d'auditeur et de certificateur à poursuivre les discussions déjà entreprises en ce qui a trait à l'incidence de la technologie de la chaîne de blocs sur la profession et sur les normes d'audit.

L'ABC de la chaîne de blocs

Qu'est-ce que la technologie de la chaîne de blocs?

La chaîne de blocs est un registre numérique dans lequel sont inscrites les opérations effectuées entre diverses parties au sein d'un réseau. Il s'agit d'un registre distribué poste à poste basé sur Internet, qui contient l'ensemble des opérations effectuées depuis sa création. Tous les participants (particuliers ou entreprises) qui utilisent la base de données partagée sont des « nœuds » reliés à la chaîne de blocs[5], chacun conservant une copie identique du registre, dans lequel chaque écriture correspond à une opération – c'est-à-dire à l'échange d'une valeur (actif numérique représentant des droits, des obligations ou la propriété d'un bien) entre des participants. En réalité, de nombreux types de chaînes de blocs différents sont développés et mis à l'essai, mais la plupart suivent grosso modo ce cadre et ce mode de fonctionnement.

Lorsqu'un participant veut envoyer une valeur à un autre participant, tous les autres nœuds du réseau communiquent les uns avec les autres selon un mécanisme prédéterminé afin de vérifier si la nouvelle opération est valide. C'est ce qu'on appelle un algorithme de consensus[6]. Une fois l'opération acceptée par le réseau, toutes les copies du registre sont mises à jour. Habituellement, plusieurs opérations sont regroupées pour former un « bloc » qui est ajouté au registre. Chaque bloc contient des informations qui renvoient aux blocs précédents, et ainsi tous les blocs de la chaîne sont liés dans les copies identiques distribuées. Les nœuds participants peuvent ajouter de nouvelles opérations horodatées, mais il leur est impossible de supprimer ou de modifier les écritures une fois qu'elles ont été validées et acceptées par le réseau. Si un nœud modifiait un bloc précédent, son registre ne pourrait plus être mis à jour comme le reste du réseau et le nœud serait exclu de la chaîne de blocs. Une chaîne de blocs qui fonctionne comme il se doit est donc inaltérable, même s'il n'y a pas d'administrateur central.

5 La chaîne de blocs est gérée au moyen d'un réseau de nœuds. Lorsqu'un nœud accède à la base de données (c'est-à-dire à la chaîne de blocs), il télécharge sa propre copie du registre intégral.

6 Un algorithme est un processus ou un ensemble de règles servant à effectuer des calculs ou d'autres opérations de résolution de problèmes, souvent à l'aide d'un ordinateur. Pour qu'il y ait consensus, il faut que plusieurs nœuds s'entendent sur des valeurs. C'est à cela que sert un algorithme de consensus. Il existe différents types de mécanismes et d'algorithmes de consensus.

Caractéristiques de la chaîne de blocs

En tant que registre numérique distribué en temps quasi réel, la chaîne de blocs comporte plusieurs caractéristiques intéressantes qui, avec le temps, pourraient transformer divers secteurs d'activité :

Règlement en temps quasi réel	La chaîne de blocs permet le règlement des opérations en temps quasi réel, ce qui réduit le risque de non-paiement par l'une ou l'autre des parties.
Registre distribué	Le réseau distribué poste à poste contient un historique public des opérations. La chaîne de blocs est distribuée et largement accessible et conserve une preuve sécurisée que l'opération a bel et bien été réalisée.
Irrévocabilité	La chaîne de blocs contient une trace vérifiable de toutes les opérations qui la composent. Cela évite le double paiement des éléments suivis au moyen de la chaîne de blocs.
Résistance à la censure	Les règles économiques intégrées au modèle de la chaîne de blocs fournissent des avantages financiers aux participants indépendants, ce qui les incite à continuer de valider de nouveaux blocs. Cela signifie que la chaîne de blocs continue de croître sans « propriétaire ». Il serait également coûteux de la censurer.

Quels sont les avantages?

Un des principaux avantages de la technologie de la chaîne de blocs est qu'elle est distribuée. Dans les marchés financiers actuels, le transfert d'une valeur entre deux parties exige généralement l'intervention de tiers centralisés pour le traitement de l'opération, comme une banque ou un réseau de cartes de crédit. En assumant le rôle d'intermédiaires, les tiers réduisent le risque de contrepartie pour chacune des parties en cause, mais ils centralisent le risque de crédit sur eux-mêmes. Chacun de ces tiers centralisés tient son propre registre; les parties contractantes comptent sur ces tiers pour l'exécution exacte et sécuritaire des opérations. Les tiers perçoivent des frais pour la prestation de leurs services. À l'opposé, la chaîne de blocs permet aux parties de conclure l'opération directement entre elles, au moyen d'un seul registre distribué, ce qui élimine la nécessité de faire appel à des tiers centralisés.

En plus de son efficience, la chaîne de blocs possède d'autres caractéristiques distinctives qui en font une innovation marquante, dont la fiabilité. Si un nœud est mis hors ligne, le registre demeure facilement accessible pour tous les autres participants du réseau, puisque tous les nœuds actifs de la chaîne en détiennent une copie complète. La chaîne de blocs n'a donc pas de point de défaillance unique. En outre, chaque bloc de la chaîne renvoie au bloc précédent, ce qui empêche la suppression ou l'annulation d'une opération une fois qu'elle est inscrite dans la chaîne. Malgré l'ajout ou la suppression de nœuds, l'intégrité et la fiabilité du réseau seront préservées tant que celui-ci sera utilisé. De cette façon, nul ne contrôle à lui seul la chaîne de blocs, et nul ne peut la modifier ou la désactiver de son propre chef.

Les chaînes de blocs ne naissent pas toutes égales

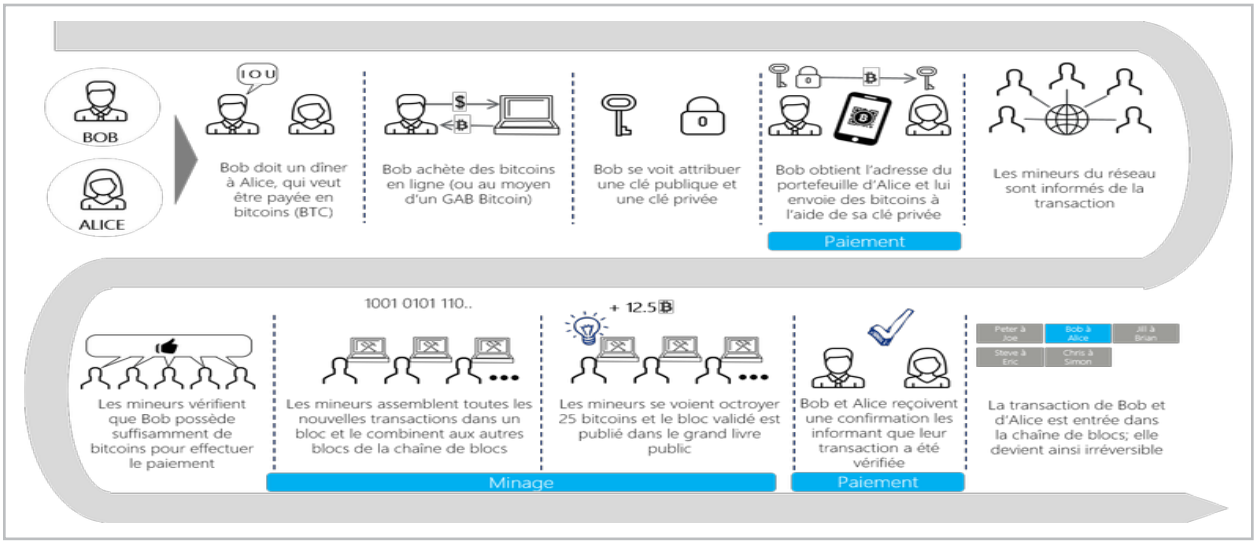
Les CPA auditeurs doivent savoir que la technologie de la chaîne de blocs est une nouvelle forme de base de données et que chaque nouvelle chaîne de blocs peut avoir des caractéristiques qui lui sont propres. Comme il s'agit d'une technologie émergente, il demeure possible que la mise en œuvre d'une chaîne de blocs donnée ne se montre pas à la hauteur des attentes. Il existe aujourd'hui deux principales catégories de chaînes de blocs : sans permission et avec permissions. Ce qui les distingue surtout, c'est la détermination des parties qui sont autorisées à y accéder. Une chaîne de blocs sans permission (ou « publique ») est accessible au public, c'est-à-dire à tous les internautes, tandis que la chaîne de blocs avec permissions (ou « privée ») est accessible à certains participants seulement.

La chaîne de blocs sans permission

Une chaîne de blocs sans permission est ouverte à quiconque souhaite l'utiliser. La chaîne de blocs Bitcoin en est un exemple; toute personne peut y participer en acceptant de retransmettre et de valider les opérations effectuées sur le réseau, le processeur de leur ordinateur devenant alors un nœud de la chaîne. Pour ce faire, il suffit de télécharger le logiciel et le registre Bitcoin à partir d'Internet. Comme la chaîne de blocs conserve la liste de toutes les opérations effectuées depuis le début, elle contient l'historique complet des opérations et les soldes des comptes de toutes les parties.

La figure 1 illustre le transfert de bitcoins (BTC) d'une personne à une autre. Lorsqu'une partie (l'acheteur) envoie des bitcoins (la valeur) à l'autre partie (le vendeur), la chaîne de blocs Bitcoin est mise à jour selon le processus suivant, qui implique un procédé dit de « minage[7] » :

FIGURE 1



Exemple d'une opération en bitcoins faisant appel à une chaîne de blocs publique (sans permission); paiement poste à poste sur le réseau Bitcoin. **Remarque :** Les chaînes de blocs avec permissions peuvent avoir des protocoles de consensus similaires ou non à l'opération décrite à la figure 1, selon l'entente conclue entre les participants.

7 Le minage est l'action d'ajouter de nouvelles opérations à la chaîne de blocs par la résolution de problèmes algorithmiques au moyen de ressources informatiques. Les participants à ce processus, appelés « mineurs », se voient accorder des bitcoins comme récompense puisqu'ils mettent leur capacité informatique à la disposition du réseau.

La chaîne de blocs sans permission a l'avantage de démontrer le plein potentiel de la technologie en offrant un accès universel, mais elle a aussi des inconvénients auxquels il est difficile de remédier. Par exemple, lors de la création d'une chaîne de blocs, la taille ou le volume des opérations est défini en fonction de la technologie la plus avancée à ce moment précis. À mesure que la technologie évolue, les réglages initiaux risquent de devenir des limites qui finiront par rendre la chaîne de blocs désuète, et cela pourrait se traduire par un ralentissement du traitement des opérations. Les utilisateurs des chaînes de blocs sans permission doivent aussi savoir que l'historique de leurs opérations est accessible à toute personne qui télécharge la base de données, et ce, aussi longtemps que la base de données demeurera active. Il peut être difficile pour un tiers d'identifier un participant dans la chaîne de blocs, mais s'il y parvient, il pourra voir l'historique complet des opérations de ce participant.

La chaîne de blocs avec permissions

Les limites des chaînes de blocs sans permission ont incité certaines organisations à envisager l'utilisation de chaînes de blocs privées, ou avec permissions, dont l'accès est réservé aux personnes ayant obtenu une permission auprès d'administrateurs désignés. Ces chaînes de blocs viennent résoudre certains des inconvénients des chaînes de blocs publiques, mais sacrifient aussi certains de leurs avantages potentiels (comme les transactions décentralisées, la large diffusion du registre et un environnement véritablement décentralisé, sans intermédiaires). Les chaînes de blocs avec permissions sont susceptibles d'intéresser en particulier les consortiums[8], qui peuvent souvent tirer avantage d'un système de registre partagé. Par exemple, les membres d'une chaîne d'approvisionnement pourraient juger utile d'avoir recours à une chaîne de blocs pour suivre les mouvements des marchandises.

Compte tenu des limites bien connues qui sont propres aux chaînes de blocs publiques, on s'attend à ce que l'utilisation des chaînes de blocs privées ou avec permissions se répande plus rapidement à court terme, particulièrement dans les entreprises. Par contre, on s'attend aussi à voir une plus grande adoption des chaînes de blocs publiques à plus long terme, lorsque les principales difficultés que pose cette nouvelle technologie sur les plans infrastructurel et technique auront été aplanies. Le changement de paradigme provoqué par la chaîne de blocs (et le niveau d'intérêt que suscitent les initiatives basées sur cette technologie) n'est pas sans rappeler, sous de nombreux aspects, le déploiement d'Internet dans les années 1990. Avec la technologie Internet, ce sont d'abord les intranets d'entreprise qui ont suscité le plus d'engouement, jusqu'à ce qu'une masse critique soit atteinte et que l'Internet destiné au grand public commence à offrir plus d'avantages pour compenser les risques perçus de la participation à un réseau ouvert.

8 Un consortium est un groupe d'organisations visant un objectif commun.

Évolution de la chaîne de blocs : les contrats intelligents

L'arrivée des contrats intelligents a marqué un tournant dans l'évolution de la technologie de la chaîne de blocs. Les contrats intelligents sont des codes informatiques qui sont emmagasinés dans une chaîne de blocs et qui exécutent des actions lorsque des conditions précises sont réunies. Ils permettent à des contreparties d'automatiser des tâches qui sont d'ordinaire effectuées manuellement par un intermédiaire externe. La technologie des contrats intelligents peut accélérer les processus d'affaires, réduire les erreurs opérationnelles et accroître l'efficience par rapport aux coûts.

Ainsi, deux parties peuvent conclure un contrat « intelligent » d'instruments dérivés pour couvrir les variations du prix du pétrole à la fin de l'exercice. Une fois les modalités du contrat convenues, celui-ci est annexé à la chaîne de blocs et les montants en cause sont déposés entre les mains d'un tiers et enregistrés dans une chaîne de blocs. À la fin de l'exercice, le contrat intelligent va chercher le prix du pétrole dans une source de confiance prédéfinie (appelée « oracle »), calcule le montant du règlement, puis transfère ce montant à la partie gagnante de la chaîne de blocs. .

Ethereum[9], la deuxième chaîne de blocs en importance (par sa capitalisation boursière), après Bitcoin, au moment où nous écrivons ces lignes, a été la première plateforme à exploiter le concept de contrat intelligent déployé et exécuté sur un réseau distribué (chaîne de blocs). Ethereum est un protocole public qui permet à toute personne accédant au réseau de la chaîne de blocs Ethereum de voir les modalités de chaque contrat, à l'exception de celles qui sont protégées par chiffrement. Cela peut poser problème dans le cas de contrats qui contiennent des renseignements sensibles (par exemple des contrats intelligents que conclut un fonds de couverture pour exécuter une stratégie de placement exclusive ou pour établir discrètement une position sur certaines actions). Cela dit, les développeurs s'emploient activement à créer des solutions pour assurer la confidentialité aux intervenants tout en leur permettant de tirer profit des chaînes de blocs publiques. Malgré ces limites perçues, les applications possibles des contrats intelligents suscitent un grand intérêt dans tous les secteurs d'activité parce qu'elles pourraient transformer le traitement et le règlement des contrats les plus variés, des contrats de couverture aux contrats à terme en passant par les paiements automatisés effectués en vertu de contrats de location.

Grâce aux contrats intelligents, il est possible d'automatiser le processus d'octroi des contrats et d'assurer le suivi et l'application des obligations contractuelles avec le moins d'intervention humaine possible. L'automatisation peut accroître l'efficience et réduire les délais de règlement ainsi que les erreurs. Puisque l'utilisation de la technologie des contrats intelligents nécessite la traduction en éléments logiques de toutes les modalités contractuelles, elle peut aussi favoriser le respect de ces modalités en levant certaines ambiguïtés.

9 www.ethereum.org

Au fil de l'évolution des contrats intelligents, il se pourrait que l'on découvre certains risques inhérents qu'il faudra atténuer. Par exemple, lors de l'établissement d'un contrat intelligent, les parties peuvent décider de ne pas traiter tous les résultats possibles, ou d'inclure une certaine marge de manœuvre afin de ne pas se limiter elles-mêmes. Cela pourrait mener à la conclusion de contrats intelligents comportant des vulnérabilités ou des erreurs susceptibles de produire des résultats inattendus sur le plan des affaires. En cas d'erreur, les parties pourraient trouver difficile de renégocier les modalités d'une entente et de les modifier. De plus, les contrats incomplets ou prévoyant une marge de manœuvre peuvent donner lieu à des problèmes ou à des litiges lors du règlement. Plus important encore peut-être, au moment où nous écrivons ces lignes, les contrats intelligents n'ont pas encore subi l'épreuve des tribunaux. Néanmoins, les contrats intelligents ajoutent à l'attrait de la chaîne de blocs et favorisent son adoption.

Quelles sont les applications de la chaîne de blocs?

La technologie de la chaîne de blocs a tout ce qu'il faut pour intéresser les secteurs d'activité les plus divers. Les applications les plus prometteuses se trouvent là où le transfert de valeurs ou d'actifs entre des parties est actuellement lourd et coûteux et nécessite de faire appel à un ou plusieurs organismes centralisés. On n'a qu'à penser au règlement des valeurs mobilières; à l'heure actuelle, celui-ci nécessite parfois des processus de compensation et de règlement pouvant prendre plusieurs jours et faisant intervenir de multiples intermédiaires financiers. Certains experts du secteur des services financiers estiment que ce secteur est en voie de se métamorphoser; les percées dans les technologies innovantes comme la chaîne de blocs devraient transformer ce secteur et ses effectifs avec l'automatisation d'un grand nombre d'activités actuellement réalisées par des humains.

Le tableau suivant décrit l'intérêt qu'ont manifesté certains secteurs d'activité pour la technologie de la chaîne de blocs et ses avantages transformateurs potentiels, intérêt qui s'est traduit par des investissements considérables effectués tant par les sociétés de capital-risque que par les grandes entreprises.

Services financiers	Plusieurs bourses dans le monde ont mis en œuvre une plateforme de chaîne de blocs qui permet l'émission et le transfert de titres de sociétés à capital fermé. De plus, un certain nombre de groupes bancaires étudient son utilisation aux fins du financement commercial, des paiements transfrontaliers et d'autres processus bancaires.
Produits de consommation et produits industriels	Certaines sociétés des secteurs des produits de consommation et des produits industriels envisagent d'utiliser la chaîne de blocs pour informatiser et suivre l'origine et l'historique des opérations pour diverses marchandises.
Sciences de la vie et soins de santé	Des organisations de soins de santé essaient de voir comment la chaîne de blocs pourrait les aider à sécuriser les dossiers médicaux électroniques, la facturation des soins médicaux, les réclamations d'assurance et d'autres documents.
Secteur public	Les gouvernements étudient la possibilité d'avoir recours à cette technologie pour la tenue de registres d'actifs comme les terrains et les participations dans des sociétés.
Énergie et ressources	Ethereum sert de base à l'établissement d'une technologie de réseau intelligent de distribution de l'électricité qui permettrait de transformer les surplus en actifs numériques négociables entre consommateurs.

Puisque toutes les entreprises assurent un suivi de l'information et sont confrontées aux défis du rapprochement des données avec des contreparties, la technologie de la chaîne de blocs peut être pertinente pour tous. Après les premières adoptions d'envergure, on pourrait assister à une transformation des processus d'affaires et des anciens systèmes patrimoniaux qui sont difficiles à tenir à jour.

L'incidence potentielle de la chaîne de blocs sur l'audit des états financiers et sur la profession de certificateur

Audit des états financiers

Aux yeux du public, les CPA auditeurs rehaussent la fiabilité de l'information des sociétés qu'ils auditent et contribuent au bon fonctionnement d'un système de marchés financiers de plusieurs milliers de milliards de dollars en offrant un niveau confiance plus élevé. Les CPA auditeurs respectent une réglementation, des codes de déontologie et des normes d'audit stricts, et sont indépendants des entités qu'ils auditent. Ils font preuve d'objectivité et d'esprit critique pour fournir une assurance raisonnable que les états financiers d'une entité sont exempts d'anomalies significatives et, selon la mission, que les contrôles internes de l'entité à l'égard de l'information financière fonctionnent efficacement.

Certaines publications ont laissé entendre que la technologie de la chaîne de blocs pourrait éliminer la nécessité même de faire appel à un CPA auditeur pour auditer les états financiers. Si toutes les opérations sont saisies dans une chaîne de blocs inaltérable, que reste-t-il à auditer pour le CPA auditeur?

Le fait de vérifier si une opération est bel et bien survenue est un élément fondamental de l'audit des états financiers, mais ce n'est certainement pas le seul. L'audit sert aussi à déterminer si les opérations enregistrées sont étayées par des éléments probants pertinents, fiables, objectifs, exacts et vérifiables. L'acceptation d'une opération dans une chaîne de blocs fiable peut constituer un élément probant suffisant et approprié pour certaines assertions contenues dans les états financiers, comme la réalité de l'opération (p. ex., la réalité du transfert, d'un vendeur à un acheteur, d'un actif inscrit dans la chaîne de blocs). Prenons l'achat d'un produit en bitcoins : le transfert des bitcoins est enregistré dans la chaîne de

blocs. Toutefois, il est possible que l'auditeur ne soit pas en mesure d'identifier le produit qui a été livré s'il se limite à l'information contenue dans la chaîne de blocs Bitcoin. Par conséquent, l'enregistrement d'une opération dans une chaîne de blocs peut ou non fournir des éléments probants suffisants et appropriés relativement à la nature de l'opération. Autrement dit, même si elle est inscrite dans la chaîne de blocs, l'opération peut être :

- non autorisée, frauduleuse ou illégale;
- intervenue entre des parties liées;
- liée à une entente parallèle « hors chaîne »;
- mal classée dans les états financiers.

De plus, de nombreuses opérations comptabilisées dans les états financiers représentent des valeurs estimatives qui diffèrent du coût historique. Les auditeurs devront donc envisager et mettre en œuvre des procédures d'audit à l'égard des estimations de la direction, même dans les cas où les opérations sous-jacentes sont enregistrées dans une chaîne de blocs.

Il se peut que l'adoption généralisée des chaînes de blocs permette l'obtention de données d'audit à partir d'emplacements centraux, et que les CPA auditeurs en viennent à élaborer des procédures pour obtenir des éléments probants à même ces chaînes. Toutefois, même pour les opérations inscrites dans les chaînes de blocs, le CPA auditeur devra tenir compte du risque que l'information soit inexacte en raison d'une erreur ou d'une fraude. Il en résultera de nouveaux défis, puisque la chaîne de blocs ne sera vraisemblablement pas contrôlée par l'entité faisant l'objet de l'audit. Après avoir extrait les données de la chaîne de bloc, le CPA auditeur devra déterminer si elles sont fiables en s'appuyant, par exemple, sur l'évaluation des contrôles généraux des TI (CGTI) liés à l'environnement de la chaîne de blocs. Il pourrait aussi être obligé d'acquérir une compréhension du protocole de consensus de la chaîne de blocs visée, d'en évaluer la fiabilité et, dans certains cas, de déterminer s'il y a un risque que ce protocole ait été manipulé. Étant donné que de plus en plus d'organisations envisagent l'utilisation de chaînes de blocs publiques ou privées, les CPA auditeurs doivent connaître l'incidence que pourrait avoir sur leurs audits cette nouvelle source d'information pour l'établissement des états financiers. Ils devront aussi évaluer les méthodes comptables de la direction concernant les actifs et les passifs numériques, qui ne sont pas pris en compte directement pour l'instant dans les normes internationales d'information financière et les principes comptables généralement reconnus des États-Unis. Ils devront s'interroger sur la façon d'adapter les procédures d'audit de manière à profiter des avantages de la chaîne de blocs et à tenir compte des nouveaux risques qui s'y rattachent.

Comment la chaîne de blocs fera-t-elle évoluer l'audit et la certification?

Malgré les complexités décrites plus haut, la technologie de la chaîne de blocs offre la possibilité de simplifier les processus d'audit et d'information financière. Actuellement, les rapprochements des comptes, balances des comptes, écritures de journal, extraits de grand livre auxiliaire et feuilles de calcul que reçoit le CPA auditeur se présentent sous toutes sortes de formes et sont produits parfois électroniquement, parfois manuellement. Une grande part du temps de planification de l'audit est donc consacrée à l'étude d'informations et de tableaux divers. Avec les chaînes de blocs, le CPA auditeur pourrait avoir accès aux données en temps quasi réel grâce à des nœuds en lecture seule. Il pourrait ainsi obtenir les informations nécessaires à la réalisation de l'audit dans un format uniforme.

Plus le nombre d'entités et de processus qui migrent vers les chaînes de blocs augmente, plus les gains en efficience qu'il devient possible de faire en accédant aux informations contenues dans ces chaînes sont grands. Par exemple, si une catégorie d'opérations importante pour un secteur d'activité était enregistrée dans une chaîne de blocs, il pourrait être possible pour le CPA auditeur de développer un logiciel lui permettant d'auditer en continu les organisations qui utilisent cette chaîne de blocs. Un bon nombre des tâches manuelles d'extraction de données et de préparation de l'audit qui sont très accaparantes pour la direction et le personnel de l'entité pourraient alors être éliminées. Or, l'accélération de la préparation de l'audit contribuerait à réduire le décalage entre la date d'une opération et la date de vérification – l'un des principaux défauts que l'on reproche à l'information financière. Cela aurait aussi pour effet d'accroître l'efficience et l'efficacité de la communication de l'information financière et de l'audit, car il serait plus facile pour la direction et les auditeurs de se consacrer aux opérations plus risquées et plus complexes tout en menant les audits de routine en temps quasi réel.

Avec l'informatisation fondée sur les chaînes de blocs, les auditeurs pourraient déployer davantage de capacités d'automatisation, d'analyse et d'apprentissage machine comme l'envoi automatique, en temps quasi réel, d'alertes aux parties concernées lorsque des opérations inhabituelles ont lieu. Les documents justificatifs comme les contrats, ententes, bons de commande et factures pourraient être chiffrés, puis enregistrés de façon sécurisée ou liés à une chaîne de blocs. Si les CPA auditeurs pouvaient accéder à des éléments probants inaltérables, la communication de l'information financière et l'audit s'en trouveraient probablement accélérés.

Même si l'audit est susceptible de devenir un processus plus continu, les auditeurs devront continuer d'exercer leur jugement professionnel lors de l'analyse des estimations comptables et des jugements portés par la direction dans la préparation des états financiers. En outre, dans les secteurs qui auront été automatisés, ils devront aussi évaluer et tester les contrôles internes visant à assurer l'intégrité des données pour toutes les sources d'information financière pertinente.

Quels nouveaux rôles les CPA seront-ils appelés à jouer dans l'écosystème de la chaîne de blocs?

Alors que les systèmes utilisant des chaînes de blocs viendront normaliser le traitement des opérations dans de nombreux secteurs d'activité, les CPA, notamment les CPA certificateurs, pourraient être en mesure de fournir une assurance aux utilisateurs de cette technologie. Grâce à leurs compétences, à leur indépendance, à leur objectivité et à leur expertise, les CPA pourraient être appelés à jouer certains rôles dans l'avenir.

Sans être exhaustive, la liste suivante fournit des exemples de nouveaux rôles qui pourraient s'ouvrir aux CPA; des contraintes réglementaires et professionnelles importantes pourraient se poser avant que les CPA puissent remplir ces fonctions.

Auditeur de contrats intelligents et d'oracles

Comme nous l'avons décrit plus haut, il est possible d'incorporer des contrats intelligents dans une chaîne de blocs afin d'automatiser certains processus d'affaires. Il se peut que des parties contractantes veuillent faire appel à un certificateur pour vérifier si la mise en œuvre de leurs contrats intelligents repose sur la logique d'affaires voulue. En outre, le CPA certificateur pourrait vérifier l'interface entre les contrats intelligents et les sources de données externes qui déclenchent les événements à enregistrer. Sans évaluation indépendante, les utilisateurs des technologies reposant sur la chaîne de blocs sont exposés au risque qu'il y ait des erreurs ou des vulnérabilités non relevées. Pour entreprendre ce nouveau rôle, le CPA certificateur aurait besoin de nouvelles compétences, telles que la compréhension du langage de programmation et des fonctions d'une chaîne de blocs. Ce type de rôle soulève également d'importantes questions pour la profession, dont les suivantes :

- Quels sont les types de compétences dont la profession a besoin pour assurer sa pertinence à cet égard?
- De quels facteurs dépendrait le risque de mission d'assurance?
- Jusqu'où va la responsabilité continue du certificateur une fois qu'un contrat intelligent est mis en œuvre dans une chaîne de blocs?

Dans le contexte de l'audit des états financiers, la direction aura la responsabilité d'établir des contrôles visant à vérifier si le code source du contrat intelligent est conforme à la logique d'affaires voulue. Le CPA indépendant chargé de l'audit d'une entité qui utilise une chaîne de blocs et des contrats intelligents devra probablement examiner les contrôles de la direction portant sur le code du contrat intelligent. Cela dit, de nombreuses sociétés pourraient choisir de réutiliser les contrats intelligents d'autres entités qui sont déjà présents dans une chaîne de blocs. Les prochaines normes et indications en matière d'audit devront peut-être tenir compte de cette technologie et clarifier le rôle du CPA auditeur à cet égard.

Auditeur de la société de services pour les chaînes de blocs avec permissions

Avant de lancer une nouvelle application sur une plateforme de chaîne de blocs déjà établie ou d'adhérer à un produit de chaîne de blocs existant, les utilisateurs du système pourraient demander une assurance indépendante à l'égard de la stabilité et de la robustesse de son architecture. Chaque participant pourrait bien sûr effectuer son propre contrôle préalable, mais il pourrait être plus efficient d'embaucher un CPA pour obtenir une telle assurance. En outre, certains éléments essentiels de la chaîne de blocs (p. ex. la gestion des clés de chiffrement) devraient être conçus de manière à inclure des CGTI perfectionnés fournissant une protection continue des renseignements sensibles, de même que des contrôles du traitement portant sur divers aspects (sécurité, disponibilité, intégrité du traitement, protection des renseignements personnels, confidentialité). Il pourrait être nécessaire de faire appel périodiquement à un tiers indépendant de confiance pour qu'il fournisse une assurance quant à l'efficacité des contrôles appliqués à une chaîne de blocs privée (p. ex. une chaîne de blocs établie par un consortium). Ce type de service soulève d'importantes questions pour la profession :

- Lors de la prestation de services de certification à l'égard d'une chaîne de blocs, qui est le client?
- Comment le CPA certificateur devrait-il évaluer les risques de mission dans le cas d'un système autonome?
- Comment les règles d'indépendance s'appliqueraient-elles aux utilisateurs d'une chaîne de blocs?

Fonction d'administrateur

Il peut être avantageux, dans le cas des chaînes de blocs avec permissions, de faire appel à un tiers indépendant de confiance, sans parti pris, pour exercer les fonctions d'administrateur central des droits d'accès. Celui-ci pourrait être chargé de la vérification de l'identité des participants ou d'un examen encore plus poussé auquel les participants devraient se soumettre avant de se voir accorder le droit d'accéder à une chaîne de blocs. Cet administrateur central pourrait valider la mise en application et la surveillance des protocoles de la chaîne de blocs. Si ces fonctions étaient effectuées par un utilisateur ou nœud de la chaîne de blocs, il pourrait en résulter un avantage indu venant éroder la confiance entre les membres du consortium. Puisque la raison d'être du rôle d'administrateur est de favoriser la relation de confiance au sein de la chaîne de blocs dans son ensemble, il faudra faire preuve de diligence au moment d'établir tant les fonctions que les obligations légales qui se rattachent à ce rôle. En tant que professionnel de confiance, un CPA indépendant peut être en mesure de s'acquitter de cette responsabilité. Toutefois, son rôle soulèverait de nouvelles questions pour la profession :

- Le certificateur qui assume un rôle aussi crucial est-il indépendant des participants à la chaîne de blocs?
- Le CPA pourrait-il réaliser l'audit des états financiers de ces participants?

Fonction d'arbitrage

Les ententes d'affaires peuvent être complexes et donner lieu à des litiges, même entre les parties les mieux intentionnées. Dans le cas d'une chaîne de blocs avec permissions, une fonction d'arbitrage pourrait être nécessaire à un certain moment pour régler les litiges entre les participants. Cette fonction rappelle celle de l'exécuteur testamentaire, rôle qui est habituellement assumé par différents professionnels compétents, dont les CPA certificateurs. Les participants à la chaîne de blocs pourraient avoir besoin de ce type de fonction pour faire appliquer certaines modalités contractuelles lorsque l'esprit du contrat intelligent s'éloigne d'un document juridique, d'une entente contractuelle ou d'une lettre officielle. D'autres considérations devraient être examinées pour déterminer si une fonction d'arbitrage est nécessaire. Si des CPA souhaitent assumer ce type de fonction, certaines questions cruciales se poseront, comme les suivantes :

- Quel est le cadre juridique applicable pour le règlement des litiges?
- Quelles compétences attend-on du CPA certificateur?
- Ce rôle pourrait-il donner lieu à des menaces imprévues pour l'indépendance en ce qui concerne les clients de missions d'attestation?

Conclusion

Il y a encore bien des inconnues quant à l'incidence qu'aura la chaîne de blocs sur la profession d'auditeur et de certificateur, notamment la vitesse à laquelle les changements se produiront. Des répercussions se font déjà sentir pour les CPA auditeurs dont les clients se servent de cette technologie pour enregistrer des opérations, et on s'attend à ce que le taux d'adoption de la chaîne de blocs continue de croître. Cela dit, à court terme, cette innovation ne remplacera pas la communication de l'information financière et l'audit des états financiers. Les états financiers audités sont essentiels à la bonne marche des affaires et jouent un rôle clé dans le financement par capitaux propres et par emprunt, la participation aux marchés financiers, les regroupements d'entreprises, le respect des exigences réglementaires et le fonctionnement efficace et efficient des marchés financiers. Les états financiers reflètent les assertions de la direction, notamment ses estimations, dont bon nombre ne peuvent être facilement résumées ou calculées dans des chaînes de blocs.

De plus, l'audit indépendant des états financiers renforce la confiance, qui est au cœur du fonctionnement du système des marchés financiers. L'érosion de cette confiance pourrait être néfaste pour la réputation d'une entité, le cours de l'action et la valeur pour l'actionnaire, et pourrait occasionner des amendes, des pénalités ou la perte d'actifs. Les utilisateurs des états financiers attendent des CPA auditeurs qu'ils effectuent un audit indépendant des états financiers, en faisant preuve d'esprit critique. Dans le cadre de ce type de mission, les CPA auditeurs exercent leur jugement pour déterminer s'ils ont acquis l'assurance raisonnable que les états financiers d'une entité, pris dans leur ensemble, sont exempts d'anomalies significatives, que celles-ci résultent de fraudes ou d'erreurs. Il serait surprenant que les chaînes de blocs viennent remplacer le jugement des CPA auditeurs. Toutefois, les CPA auditeurs doivent surveiller l'évolution de la technologie de la chaîne de blocs, car elle aura une incidence sur les systèmes informatiques de leurs clients. Les CPA auditeurs devront se tenir au fait des principes de base de cette technologie et travailler avec des experts pour évaluer les risques techniques complexes qui y sont associé.

Par ailleurs, les CPA auditeurs devront tenter de voir comment tirer profit de l'adoption de la technologie de la chaîne de blocs par leurs clients pour améliorer la collecte des données au cours de leur audit. Ils devront aussi se demander si cette technologie peut leur permettre

de créer des routines d'audit automatisées. La profession d'auditeur doit s'adapter et s'intéresser aux nouveaux défis et aux nouvelles perspectives que présente l'adoption généralisée de la chaîne de blocs. Les CPA auditeurs et certificateurs sont invités à suivre les progrès de la technologie de la chaîne de blocs et à saisir les occasions d'assumer de nouveaux rôles, d'apprendre et de tirer parti de leur capacité éprouvée à s'adapter à l'évolution rapide du monde des affaires.

Appel à l'action

La technologie de la chaîne de blocs s'inscrit dans l'informatisation des processus d'affaires, qui gagne en vitesse. CPA Canada et l'AICPA pressent les CPA, en particulier les CPA auditeurs, de continuer à surveiller l'évolution de cette technologie (voir les suggestions de lecture dans la section « **Autres sources d'information** »). Ils encouragent également les normalisateurs en audit et en comptabilité à surveiller la progression de la technologie de la chaîne de blocs dans l'écosystème des affaires. De nouvelles questions concernant les éléments probants, les contrôles internes, l'indépendance, l'évaluation des risques, la cybersécurité, etc., vont probablement se poser, et les normalisateurs devront s'y attarder. Enfin, la profession doit se pencher sur les compétences que devront acquérir les CPA pour être en mesure de répondre aux demandes du marché dans un monde des affaires où la technologie de la chaîne de blocs aura été largement adoptée. Elle devra, par exemple, envisager l'ajout de certains éléments au programme de formation des nouveaux CPA et aux obligations de formation continue des CPA expérimentés. L'innovation associée à cette technologie est inexorable; de nouvelles catégories d'actifs numériques se créent sans cesse pour occuper une place dans la chaîne de blocs. Vu leur rôle essentiel dans le bon fonctionnement des marchés en tant que certificateurs professionnels, les CPA se doivent de s'intéresser à cette nouvelle technologie, de contribuer à identifier les risques qu'elle présente, et de trouver des façons de tirer profit de ses avantages.

Autres sources d'information

Publication de CPA Canada – **Perturbation technologique des marchés financiers et de la communication de l'information? Aperçu de la chaîne de blocs**
CPA Magazine – **Chaîne de blocs pour les nuls, ou presque**
CPA Magazine – **Chaînes de blocs – 2e partie : le mécanisme à la loupe**
Publication de Deloitte – **Driving FinTech innovation in financial services**
Publication de Deloitte – **Blockchain: Enigma, Paradox, Opportunity**
Deloitte University Press – **Billets de blogue sur la chaîne de blocs** (en anglais seulement)
Page Web de Deloitte – **Break through with Blockchain: How can financial institutions leverage a powerful technology?**
Harvard Business Review – **The Truth about Blockchain**

Harvard Business Review – **The Blockchain Will Do to the Financial System What the Internet Did to Media**
Vidéo du Forum économique mondial – **What is Blockchain?**
Conférence TED de Don Tapscott – **How the blockchain is changing money and business**

Au sujet des auteurs

CPA Canada, l'AICPA et l'UWCISA tiennent à remercier les auteurs du présent document, c'est-à-dire William Bible, Jon Raphael et Peter Taylor de Deloitte & Touche LLP, et Iliana Oris Valiente, CPA, CA.

CPA Canada, l'AICPA et l'UWCISA souhaitent également souligner la contribution précieuse des professionnels suivants à la présente publication : Eric Piscini de Deloitte Consulting LLP, Mawadda Basir de Deloitte Canada, Malik Datardina de Deloitte Canada, Theo Stratopoulos de l'Université de Waterloo (Canada) et Juli-ann Gorgi, CPA, CA, M. Compt. de Toronto (Canada).

À propos de Deloitte

COMPTABLES
PROFESSIONNELS
AGRÉÉS
CANADA

277, RUE WELLINGTON OUEST
TORONTO (ONTARIO) CANADA M5V 3H2
TÉL. 416 977.3222 TÉLÉC. 416 977.8585
WWW.CPACANADA.CA