CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

POINTS DE VUE :

Application des Normes canadiennes d'audit (NCA) dans le secteur des cryptoactifs

L'AUDIT DES CRYPTOACTIFS : PERTINENCE ET FIABILITÉ DES INFORMATIONS PROVENANT D'UNE CHAÎNE DE BLOCS DEVANT SERVIR COMME ÉLÉMENTS PROBANTS

JANVIER 2020

Groupe de travail sur l'audit des cryptoactifs

L'ascension fulgurante et la volatilité des cryptoactifs suscitent un vif intérêt à l'échelle mondiale et font l'objet d'une surveillance accrue de la part des organisations, des investisseurs, des autorités de réglementation, des gouvernements et d'autres groupes ou personnes. Les états financiers d'une entité sont susceptibles de comporter des soldes de cryptoactifs et des transactions en cryptoactifs significatifs; les auditeurs doivent être au fait des défis qui se posent lors de l'audit de tels éléments. Comptables professionnels agréés du Canada (CPA Canada) et le Conseil des normes d'audit et de certification (CNAC) ont mis sur pied le Groupe de travail sur l'audit des cryptoactifs, qui réunit des représentants de cabinets d'audit et des autorités de réglementation de l'audit au Canada appelés à échanger leurs points de vue sur l'application des NCA lors de la pratique de l'audit dans le secteur des cryptoactifs.

Avertissement : Les points de vue exprimés dans le cadre de cette série de documents ne font pas autorité et n'ont pas été officiellement avalisés par CPA Canada, le CNAC, les autorités de réglementation de l'audit ou les cabinets représentés par les membres du Groupe de travail, qui peuvent par ailleurs avoir des points de vue différents sur la façon dont les indications suggérées dans le présent bulletin *Points de vue* devraient être mises en œuvre.

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

Les technologies qui sous-tendent les cryptoactifs peuvent être complexes; le contenu du présent bulletin *Points de vue* reflète cette réalité. Par souci de concision, les concepts techniques mentionnés ne sont pas tous expliqués. Bien souvent, l'audit des cryptoactifs requiert une expertise à l'égard de la technologie de la chaîne de blocs et des domaines connexes, notamment la cryptographie. Il est donc habituel pour l'auditeur d'utiliser les travaux d'un expert lors de l'audit des cryptoactifs.

Contexte

Selon la Norme canadienne d'audit (NCA) 330[1], l'auditeur doit concevoir et mettre en œuvre des procédures d'audit complémentaires dont la nature, le calendrier et l'étendue sont fonction de son évaluation des risques d'anomalies significatives au niveau des assertions.

1 NCA 330, *Réponses de l'auditeur à l'évaluation des risques.*

Comme les cryptoactifs ne sont pas des actifs corporels et que, par définition, ils n'« existent » que sous forme numérique dans une chaîne de blocs, les procédures d'audit requièrent habituellement l'utilisation d'informations tirées (ou établies à partir) d'une chaîne de blocs publique. Par exemple, lorsqu'il teste la réalité des transactions en cryptoactifs d'une entité et l'existence du solde de cryptoactifs à la clôture de l'exercice, l'auditeur peut utiliser une application informatique (souvent appelée « explorateur de blocs ») pour visualiser les informations enregistrées dans la chaîne de blocs devant servir comme éléments probants. Or, en pareil cas, la fiabilité des informations obtenues dépend de celle de la chaîne de blocs même et de l'explorateur de blocs employé, comme il est expliqué ci-après.

Le présent bulletin n'aborde qu'une des nombreuses questions qui se posent lors de l'application des NCA dans le secteur des cryptoactifs. L'application des normes d'audit et de déontologie, y compris celles relatives à l'indépendance, dans le secteur des cryptoactifs, soulève certaines difficultés non négligeables. Pour obtenir de l'information sur l'audit des cryptoactifs et comprendre certaines des autres difficultés auxquelles l'auditeur peut se heurter, veuillez lire le document de CPA Canada intitulé ***Facteurs à considérer pour l'audit des actifs et des transactions en cryptomonnaie***.

Question

Pour répondre à l'évaluation des risques d'anomalies significatives liés aux transactions en cryptoactifs et aux soldes de cryptoactifs figurant dans les états financiers de l'entité, quels sont, pour établir la pertinence et la fiabilité des informations provenant d'une chaîne de blocs publique devant servir comme éléments probants, les facteurs à examiner?

Étendue

Le présent bulletin *Points de vue* a pour sujet les informations provenant d'une chaîne de blocs publique devant servir d'éléments probants. Il traite essentiellement des informations qui sont tirées de la chaîne de blocs même, et non des autres éléments probants qui peuvent être requis. Il n'est pas non plus question, dans le présent bulletin, des contrats intelligents, qui peuvent ou non être soumis aux mêmes protocoles que la chaîne de blocs à laquelle ils se rattachent.

Lorsque les cryptoactifs d'une entité sont détenus par un tiers (p. ex., un dépositaire), certaines des informations devant servir comme éléments probants peuvent provenir de ce tiers plutôt que de la chaîne de blocs publique. Il n'est pas question, dans le présent bulletin, d'éléments probants qui pourraient être obtenus d'un tiers.

Points de vue

Selon la NCA 500[2], lorsque l'auditeur conçoit et met en œuvre des procédures d'audit, il doit tenir compte de la pertinence et de la fiabilité des informations devant servir comme éléments probants, y compris de celles provenant d'une source d'informations externe.

2 NCA 500, *Éléments probants.*

La pertinence des informations a trait au lien logique ou au rapport avec l'objectif de la procédure d'audit et, le cas échéant, avec l'assertion considérée. Par exemple, la chaîne de blocs fournit généralement des informations pertinentes quant à la réalité d'une transaction en cryptoactifs. Par contre, les informations provenant de la chaîne de blocs ne seront probablement pas pertinentes pour les besoins des tests de l'évaluation d'un cryptoactif ou des transactions hors chaîne[3] éventuelles.

La fiabilité des informations à utiliser comme éléments probants et, par conséquent, des éléments probants eux-mêmes, dépend de leur source, de leur nature et des circonstances dans lesquelles elles ont été obtenues. La fiabilité des informations provenant d'une chaîne de blocs devant servir comme éléments probants peut dépendre de ce qui suit :

- la source des informations (c.-à-d. la chaîne de blocs);
- le caractère approprié des ressources technologiques utilisées par l'auditeur, telles que les applications informatiques, pour obtenir directement ces informations (p. ex., l'explorateur de blocs).

Si l'auditeur ne dispose pas d'une base suffisante pour évaluer la fiabilité des informations provenant de la chaîne de blocs, il peut y avoir limitation de l'étendue de ses travaux, à moins qu'il puisse obtenir des éléments probants suffisants et appropriés en mettant en œuvre des procédures de remplacement. Par exemple, à l'heure actuelle, le recours à de nouvelles méthodes de cryptographie à des fins de confidentialité dans une chaîne de blocs, comme l'authentification à apport de connaissance nulle et la signature de cercle, peut empêcher l'auditeur d'obtenir les éléments probants appropriés. La NCA 705[4] prévoit des obligations en matière de rapport lorsque l'auditeur se voit imposer une limitation de l'étendue de ses travaux.

Selon la NCA 200[5], l'auditeur doit faire preuve d'esprit critique tout au long de la planification et de la réalisation de l'audit et être conscient que certaines situations peuvent conduire à des anomalies significatives dans les états financiers. L'esprit critique est indispensable à une appréciation critique des éléments probants, y compris les informations provenant d'une chaîne de blocs. Une telle appréciation critique consiste notamment à remettre en question les éléments probants contradictoires et incohérents ainsi que la fiabilité des informations.

L'auditeur doit, selon la NCA 500, déterminer quelles sont les modifications à apporter aux procédures d'audit ou les procédures d'audit supplémentaires à mettre en œuvre pour résoudre l'incohérence des éléments probants ou dissiper le doute sur leur fiabilité. La non-concordance des informations visualisées au moyen de deux explorateurs de blocs différents est un exemple d'incohérence entre les éléments probants obtenus d'une source et ceux obtenus d'une autre source. Il est également possible que l'auditeur en vienne à douter de la fiabilité de la chaîne de blocs elle-même, comme il est expliqué ci-après. Aux termes de la NCA 230[6], lorsque l'auditeur a identifié des informations qui ne concordent pas avec

3 Une transaction hors chaîne peut être décrite comme une transaction qui est réalisée à l'extérieur de la chaîne de blocs. Alors qu'une transaction réalisée dans la chaîne de blocs en est une qui modifie la chaîne de blocs et dont la validité est fonction de celle-ci, une transaction hors chaîne repose sur d'autres méthodes d'enregistrement et de validation.
4 NCA 705, *Expression d'une opinion modifiée dans le rapport de l'auditeur indépendant.*
5 NCA 200, *Objectifs généraux de l'auditeur indépendant et réalisation d'un audit conforme aux Normes canadiennes d'audit.*
6 NCA 230, *Documentation de l'audit.*

ses conclusions définitives sur une question importante, il doit consigner dans son dossier la façon dont il a traité les incohérences.

Chaîne de blocs

Lorsqu'il conçoit des procédures relatives à une chaîne de blocs dont il tirera des informations, l'auditeur peut prendre en considération ce qui suit :

- les caractéristiques de la chaîne de blocs (ce dont il est question plus loin);
- l'évaluation qu'il fait des risques d'anomalies significatives au niveau des assertions pour lesquels l'utilisation des informations constitue une question pertinente;
- les contrôles mis en place par l'entité à l'égard de la fiabilité des informations provenant d'une chaîne de blocs;
- la mesure dans laquelle ces informations contribuent à ramener le risque d'audit à un niveau suffisamment faible pour une assertion (p. ex., si les informations sont une source principale d'éléments probants ou sont destinées à compléter ceux provenant d'une autre source).

Bien que les informations devant servir comme éléments probants soient souvent plus fiables lorsqu'elles proviennent d'une source externe (comme ce peut être le cas d'une chaîne de blocs publique), certaines circonstances peuvent tout de même se répercuter sur leur fiabilité (p. ex., une chaîne de blocs peut ne pas fonctionner de la façon dont on pense généralement qu'elle fonctionne). Des généralisations quant aux caractéristiques de la technologie de la chaîne de blocs (suivant lesquelles, par exemple, les transactions enregistrées ne peuvent être modifiées) pourraient faire l'objet d'importantes exceptions (c.-à-d. qu'une généralisation pourrait ne pas s'appliquer dans le cas d'une chaîne de blocs en particulier). C'est en s'interrogeant sur les problèmes pouvant advenir relativement à une chaîne de blocs donnée et sur les caractéristiques de la chaîne de blocs ayant une incidence sur de tels problèmes que l'auditeur peut déterminer les sources probables d'informations inexactes ou incomplètes. Les problèmes éventuels et les caractéristiques présentés ci-après peuvent servir de cadre de référence pour l'appréciation de la fiabilité. Il ne s'agit toutefois que d'exemples; les cas de figure pourraient être plus détaillés ou des situations autres pourraient survenir.

Problèmes éventuels

- Des transactions non valides sont enregistrées dans la chaîne de blocs.
- Les données ne font pas l'objet d'un consensus au sein du réseau.
- Des transactions valides ne sont pas enregistrées correctement dans la chaîne de blocs.

Caractéristiques

- **Protocole ou algorithme cryptographique :** Il est important d'utiliser un protocole cryptographique robuste (qui soit fondé sur la technologie actuelle). Un protocole ou algorithme faible peut être une cause de déficiences dans la chaîne de blocs.
- **Modèle de consensus (p. ex., la « preuve de travail » ou « preuve d'enjeu ») :** Le consensus atteint au sein du réseau représente la « vérité » dans une chaîne de blocs (en termes de finalité probabiliste[7]). Le mécanisme en fonction duquel le protocole de consensus résout les divisions et embranchements qui se produisent couramment dans le cadre du processus de minage est important.

Certains autres problèmes éventuels peuvent avoir un effet moins direct sur la fiabilité des informations enregistrées dans une chaîne de blocs. Par exemple, une « attaque par la majorité » (souvent appelée « attaque des 51 % ») peut représenter un risque d'entreprise, car elle peut donner lieu au détournement des cryptoactifs de l'entité par un tiers. Une compréhension des risques d'entreprise auxquels est exposée l'entité accroît la probabilité d'identification des risques d'anomalies significatives, car les risques d'entreprise peuvent avoir des conséquences financières et, partant, une incidence sur les états financiers. Certaines caractéristiques de la chaîne de blocs peuvent être plus utiles pour répondre aux risques d'entreprise qu'aux risques liés à la fiabilité des informations sur la chaîne de blocs (p. ex., une puissance ou un taux de hachage supérieurs qui réduisent la probabilité d'une « attaque par la majorité »).

La NCA 315[8] exige que l'auditeur acquière une compréhension de l'entité et de son environnement. Pour ce faire, l'auditeur doit notamment comprendre le contrôle interne de l'entité, et ainsi disposer d'une base pour concevoir et mettre en œuvre des réponses à son évaluation des risques d'anomalies significatives. Lorsque l'audit porte sur des cryptoactifs, cette compréhension s'étend habituellement aux caractéristiques de la ou des chaînes de blocs sous-jacentes qui sont pertinentes en ce qui concerne leur fiabilité. Cette compréhension peut être acquise au moyen de sources variées, telles les suivantes :

- des documents et le code source publiés par les développeurs de la chaîne de blocs;
- des publications techniques ou sectorielles ainsi que les publications des membres de la communauté soutenant la chaîne de blocs;
- l'expérience acquise par l'auditeur dans l'exploitation d'un nœud de la chaîne de blocs, comme il est expliqué plus en détail à la rubrique « Source d'informations » ci-après;
- des entretiens avec des experts dans des domaines pertinents, comme la cryptographie, l'informatique ou la théorie des jeux;
- des entretiens avec la direction ou avec l'expert choisi par la direction.

7 Dans le contexte d'une chaîne de blocs, la finalité est l'affirmation selon laquelle tous les blocs valides ne feront pas l'objet d'une révocation une fois fixés à la chaîne de blocs. La finalité probabiliste désigne le type de finalité que procure un protocole fondé sur une chaîne, dans lequel la probabilité qu'une transaction soit annulée diminue de plus en plus à mesure que le bloc contenant cette transaction s'enchâsse profondément dans la chaîne.

8 NCA 315, *Compréhension de l'entité et de son environnement aux fins de l'identification et de l'évaluation des risques d'anomalies significatives*.

L'équipe de mission ainsi que les experts qui ne font pas partie de l'équipe et sont choisis par l'auditeur sont tenus de posséder collectivement la compétence et les capacités appropriées pour réaliser la mission d'audit, et d'avoir notamment acquis une compréhension de l'entité et de son environnement. Pour évaluer si l'équipe de mission dispose de la compétence et des capacités appropriées attendues d'elle, il est important de tenir compte de son expertise technique (y compris son expertise des technologies de l'information pertinentes) et de sa connaissance des secteurs dans lesquels le client exerce ses activités. L'auditeur peut juger nécessaire de faire appel à un expert pour obtenir l'aide nécessaire à l'acquisition de cette compréhension. Des indications sur l'utilisation des travaux d'un expert sont données dans la NCA 620[9].

Il se peut qu'un auditeur (ou un cabinet ou réseau) décide d'évaluer une chaîne de blocs à l'extérieur du contexte d'une mission. Il pourrait s'agir d'une approche efficiente et efficace, surtout si la chaîne de blocs en question en est une dont l'utilisation est répandue. Cela dit, il pourrait y avoir lieu d'apprécier le caractère approprié de cette évaluation au regard de la mission d'audit, notamment l'adéquation de la période visée par l'évaluation et le temps qui s'est écoulé depuis sa réalisation. Une mise à jour importante du code pourrait signifier que l'évaluation doit elle aussi être actualisée, et ce, surtout si le code ayant fait l'objet de la mise à jour n'est pas rétrocompatible.

Source d'informations

Un auditeur peut exploiter son propre nœud (souvent non destiné aux activités de minage) dans une chaîne de blocs au moyen de laquelle il obtiendra des éléments probants. Exécuter un nœud permet à l'auditeur de télécharger l'ensemble des blocs et des transactions et de les vérifier par rapport aux règles de consensus de la chaîne de blocs. Exécuter un nœud lui permet également d'obtenir des éléments probants de manière plus directe. L'auditeur peut aussi se servir d'une application informatique pour s'assurer que les transactions enregistrées auparavant dans la chaîne de blocs (pour un client en particulier ou de façon générale) ne changent pas au fil du temps. Les questions abordées à la rubrique « Ressources technologiques » ci-après peuvent s'avérer pertinentes lorsqu'une application informatique est utilisée.

Ressources technologiques

Comme il a été mentionné précédemment, l'explorateur de blocs est un exemple de ressource technologique pouvant être utilisée pour parcourir et afficher les informations enregistrées dans une chaîne de blocs. La fiabilité d'une telle application peut dépendre de divers facteurs. En effet, il faut déterminer si :

- l'application informatique a été développée expressément pour l'auditeur (ou le cabinet ou réseau), a été obtenue ou achetée auprès d'un fournisseur tiers ou appartient au domaine public – la compétence et la réputation du fournisseur de l'application peuvent être particulièrement pertinentes dans ce cas;

9 NCA 620, *Utilisation par l'auditeur des travaux d'un expert de son choix.*

- l'application informatique fonctionne adéquatement, en tenant notamment compte du risque que les informations soient lues ou affichées de façon inexacte;
- l'environnement informatique, qui comprend les infrastructures et les processus informatiques, prend en charge l'application informatique;
- des modifications ont été jugées nécessaires et ont été apportées à l'application informatique.

L'auditeur peut avoir besoin d'une formation pour utiliser adéquatement l'application informatique. De plus, pour être utilisées efficacement, certaines applications informatiques peuvent nécessiter des compétences spécialisées semblables à celles que posséderait un expert choisi par l'auditeur. Dans certains cas, l'auditeur pourrait devoir recourir à plus d'une application informatique pour obtenir des éléments probants suffisants, surtout s'il utilise une application informatique ayant été obtenue ou achetée auprès d'un fournisseur tiers ou appartenant au domaine public. Cependant, le fait de recueillir plus d'éléments probants ne compense pas nécessairement le manque de certitude quant à la qualité de l'application informatique.

Selon la NCA 220[10], l'associé responsable de la mission doit assumer la responsabilité de la qualité globale de chaque mission d'audit à laquelle il est affecté. Le fait que des ressources, notamment des ressources technologiques, suffisantes et appropriées soient disponibles pour réaliser l'audit est un facteur qui contribue à la qualité de l'audit.

10 NCA 220, *Contrôle qualité d'un audit d'états financiers.*

Remerciements

CPA Canada souhaite exprimer sa gratitude au Groupe de travail sur l'audit des crypto-actifs de CPA Canada et du Conseil des normes d'audit et de certification, qui lui a prêté assistance dans la rédaction et la revue de la présente publication. Le Groupe de travail est composé de représentants du Conseil canadien sur la reddition de comptes et des responsables provinciaux de l'inspection professionnelle, ainsi que de bénévoles provenant des cabinets canadiens suivants : BDO, Davidson & Company, Deloitte, EY, KPMG, MNP, PwC et Raymond Chabot Grant Thornton.

CPA Canada tient à remercier Raymond Chabot Grant Thornton d'avoir dirigé la rédaction de la présente publication pour le Groupe de travail.

Autres ressources

1. CPA Canada. *Facteurs à considérer pour l'audit des actifs et des transactions en crypto-monnaie.*
   www.cpacanada.ca/fr/ressources-en-comptabilite-et-en-affaires/audit-et-certification/normes-canadiennes-daudit-nca/publications/audit-actifs-transactions-cryptomonnaies
2. CPA Canada. *L'audit des cryptoactifs : Est-il nécessaire de tester les contrôles lors de la collecte d'éléments probants à l'appui de l'assertion relative aux droits (à la propriété)?*
   www.cpacanada.ca/fr/ressources-en-comptabilite-et-en-affaires/audit-et-certification/normes-canadiennes-daudit-nca/publications/tests-controles-cryptoactifs
3. *Manuel de CPA Canada*, NCA 315, NCA 330 et NCA 500.

Commentaires

Les commentaires sur le présent bulletin *Points de vue* et les suggestions pour les bulletins futurs doivent être adressés à :

Kaylynn Pippo, CPA, CA
Directrice de projets, Audit et certification
Recherche, orientation et soutien
Comptables professionnels agréés du Canada
277, rue Wellington Ouest
Toronto (Ontario) M5V 3H2
Courriel : kpippo@cpacanada.ca