CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

Facteurs à considérer pour l'audit des actifs et des transactions en cryptomonnaie

CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

Facteurs à considérer pour l'audit des actifs et des transactions en cryptomonnaie

AVERTISSEMENT

La présente publication, préparée par Comptables professionnels agréés du Canada (CPA Canada), fournit des indications ne faisant pas autorité.

Elle n'a pas été approuvée par le Conseil des normes d'audit et de certification. CPA Canada et les auteurs déclinent toute responsabilité ou obligation pouvant découler, directement ou indirectement, de l'utilisation de ce document.

Table des matières

Sommaire

Les états financiers d'une entité sont susceptibles de comporter des éléments significatifs se rapportant aux cryptomonnaies. Le présent document est destiné aux auditeurs qui ont peu ou pas d'expérience en matière de cryptomonnaie et qui ne saisissent peut-être pas pleinement les défis qui se posent lors de l'audit de tels éléments. Les points saillants des questions abordées dans ce document sont énoncés ci-dessous.

- *Considérations relatives à l'acceptation et au maintien de la relation client*
  Les facteurs à prendre en considération comprennent par exemple :
  - l'intégrité du client, y compris l'objet visé par l'entité lorsqu'elle conclut des transactions en cryptomonnaie (par exemple, démontrer que les transactions ne visent pas le blanchiment d'argent ou d'autres activités illégales);
  - le niveau de compréhension de la direction en ce qui concerne les risques liés à la cryptomonnaie et le contrôle interne à l'égard des transactions et des soldes en cryptomonnaie;
  - la question de savoir si l'associé responsable de la mission s'est assuré que les participants à la mission (y compris les membres de l'équipe de mission et les experts externes choisis par l'auditeur) possèdent collectivement la compétence et les capacités qui sont nécessaires, en matière de technologie de l'information (TI) et de cryptomonnaie, pour réaliser la mission conformément aux normes professionnelles.

- *Acquisition d'une compréhension du système d'information de l'entité pour les transactions en cryptomonnaie*
  Les questions telles que la cryptographie et la **chaîne de blocs** sont complexes. Des sources de référence sont fournies pour permettre aux lecteurs d'obtenir des renseignements sur ces sujets. Un exemple simplifié de processus d'achat d'une **cryptomonnaie** est également fourni, de même qu'une brève description des différents types de **portefeuilles de cryptomonnaies.**

Ces derniers contiennent les clés cryptographiques privées et publiques de l'entité qui sont utilisées pour vendre de la cryptomonnaie, et ils servent à surveiller le solde de cryptomonnaie de l'entité.

- *Exemples de facteurs à considérer lors de l'identification et de l'évaluation des risques d'anomalies significatives dans les transactions et les soldes en cryptomonnaie*

  Neuf exemples de situations ou d'événements qui peuvent donner lieu à une anomalie significative sont fournis. Le document décrit brièvement les questions liées à la situation ou à l'événement en question, indique la ou les assertions connexes, et fournit des exemples de facteurs à considérer pour le contrôle interne. Les neuf exemples de situations ou d'événements sont les suivants :

  1. L'entité choisit d'avoir recours à une bourse de cryptomonnaies qui n'a pas de contrôles efficaces à l'égard des transactions qu'elle conclut pour le compte de l'entité ou à l'égard des soldes de cryptomonnaie maintenus dans les comptes de l'entité.
  2. L'entité a un portefeuille de cryptomonnaies qui n'a pas été comptabilisé.
  3. L'entité perd une clé privée et ne peut donc plus accéder à la cryptomonnaie qui s'y rattache.
  4. Une partie non autorisée obtient l'accès à la clé privée de l'entité et vole sa cryptomonnaie.
  5. L'entité donne une image trompeuse de la propriété d'une clé privée et donc de la cryptomonnaie qui s'y rattache.
  6. L'entité envoie de la cryptomonnaie à une adresse erronée, et la cryptomonnaie ne peut être recouvrée.
  7. L'entité conclut et enregistre une transaction en cryptomonnaie avec une partie liée qui ne peut être identifiée en raison de l'anonymat des parties à une chaîne de blocs.
  8. Le traitement des transactions en cryptomonnaie accuse des retards importants à la fin d'une période.
  9. Des événements ou des situations font en sorte qu'il est difficile de déterminer la valeur à laquelle une cryptomonnaie doit être enregistrée aux fins de la présentation de l'information financière.

Introduction

La détention de **cryptomonnaies** permet aux particuliers et aux entreprises de conclure des transactions directement entre eux, sans devoir recourir à des intermédiaires comme des banques ou d'autres institutions financières. Ces transactions en cryptomonnaies reposent sur la technologie de la chaîne de blocs. Pour découvrir en quoi consiste cette technologie et quelles sont ses répercussions sur l'audit, consultez la publication de CPA Canada intitulée ***La technologie de la chaîne de blocs et son incidence potentielle sur la profession d'auditeur et de certificateur***.

L'ascension fulgurante et la volatilité des cryptomonnaies 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 autres. Au cours de 2017, la capitalisation boursière des cryptomonnaies a augmenté de 547 G$ US, soit 3 038 %[1]. La cryptomonnaie la plus répandue et la plus largement utilisée est le bitcoin. Il y a cependant plus de 1 600 cryptomonnaies en circulation[2], et chacune d'entre elles possède ses propres caractéristiques et spécificités, ce qui en rend la compréhension, la comptabilisation et l'audit particulièrement difficiles.

Il est de plus en plus courant de voir des états financiers présenter les soldes de cryptomonnaie importants et de refléter les résultats de transactions en cryptomonnaie. Toutefois, de nombreux auditeurs ont peu ou pas d'expérience en matière de cryptomonnaie, de sorte qu'ils ne saisissent peut-être pas pleinement les défis qui peuvent se poser lors de l'audit de tels éléments. La présente publication, qui ne fait pas autorité, vise à fournir aux auditeurs des exemples de facteurs à prendre en considération :

1 https://coinmarketcap.com/fr/charts/.

2 https://coinmarketcap.com/fr/, en date du 19 juin 2018.

- lorsqu'ils déterminent s'il convient d'accepter ou de maintenir une mission d'audit dans le cas des entités qui se livrent à des transactions significatives en cryptomonnaie;
- lorsqu'ils identifient et évaluent les risques d'anomalies significatives dans les états financiers relativement aux transactions et aux soldes en cryptomonnaie.

Nous encourageons les auditeurs à continuer de suivre de près les faits nouveaux dans ce domaine, et nous invitons les lecteurs à nous faire part de tout commentaire ou point de vue qui pourrait nous aider à élaborer d'autres publications sur ce sujet.

Taryn Abate, CPA, CA, CPA (Illinois, États-Unis)
Directrice, Audit et certification
Recherche, orientation et soutien
CPA Canada
277, rue Wellington Ouest
Toronto (Ontario) M5V 3H2
Courriel : tabate@cpacanada.ca

Étendue

La présente publication se concentre exclusivement sur les missions d'audit portant sur des états financiers qui contiennent des soldes de cryptomonnaie significatifs. Elle ne traite pas d'autres types de missions, par exemple l'examen d'états financiers contenant des éléments significatifs se rapportant aux cryptomonnaies. Toutefois, les questions abordées dans la présente publication peuvent être adaptées au besoin par les professionnels en exercice qui réalisent d'autres types de missions.

La présente publication ne traite pas des procédures qui pourraient être mises en œuvre en réponse à l'évaluation des risques (c'est-à-dire les tests des contrôles et les procédures de corroboration). Certains cabinets d'audit explorent la nature, le calendrier et l'étendue de telles procédures. Les pratiques évolueront vraisemblablement à mesure qu'une plus grande expérience sera acquise.

La présente publication ne traite pas non plus de questions telles que l'audit :

- de passifs découlant d'ententes visant le paiement de sommes dues au moyen d'une cryptomonnaie;
- des états financiers d'une bourse de cryptomonnaies;
- des états financiers d'entités qui :
  - valident des transactions en cryptomonnaie dans une chaîne de blocs (c'est-à-dire des mineurs de cryptomonnaie);
  - font des premières émissions de cryptomonnaies (PEC) ou des premières émissions d'un jeton (PEJ);
- d'investissements dans des PEC et des PEJ;
- de contrôles liés à l'infrastructure soutenant une chaîne de blocs, par exemple le matériel et les logiciels utilisés pour exploiter un nœud;
- des aspects d'une charge ou d'un passif d'impôt sur le résultat qui peuvent être touchés par un manque de clarté quant à la façon dont les lois et les règlements fiscaux s'appliquent aux transactions et aux soldes en cryptomonnaie;

- des contrôles mis en place par un organisme de services (peut-être une bourse de cryptomonnaies) et des contrôles complémentaires conçus et mis en place par l'entité. Par exemple, le portefeuille de cryptomonnaies d'une entité peut être hébergé par une bourse de cryptomonnaies ou un autre type d'entité fournissant ce service, ce qui fait en sorte que l'organisme prend une part importante dans des transactions en cryptomonnaie et dans la garde des cryptomonnaies d'une entité.

Considérations relatives à l'acceptation et au maintien de la relation client

Selon la Norme canadienne de contrôle qualité (NCCQ 1), le cabinet doit établir, pour l'acceptation et le maintien de relations clients et de missions spécifiques, des politiques et procédures destinées à lui fournir l'assurance raisonnable qu'il n'acceptera ou ne maintiendra de relations clients et de missions que si les conditions suivantes sont respectées :

1. il est compétent pour réaliser la mission et en a les capacités, y compris le temps et les ressources;
2. il peut se conformer aux règles de déontologie pertinentes;
3. il a pris en considération l'intégrité du client, et il n'a pas eu connaissance d'informations qui le conduiraient à conclure à un manque d'intégrité du client.

L'audit des transactions en cryptomonnaie peut être complexe.
Avant d'accepter ou de maintenir une mission, avez-vous pris en considération tous les facteurs pertinents?

L'utilisation de la cryptomonnaie par une entité est susceptible d'être pertinente pour l'auditeur lorsqu'il détermine s'il convient d'accepter ou de maintenir une mission d'audit des états financiers d'une entité. Un auditeur peut se retrouver dans la situation où, par exemple, l'entité :

- a conclu pour la première fois des transactions significatives en cryptomonnaie;
- a changé de façon importante la nature de ses activités liées aux cryptomonnaies ou en a élargi la portée, par rapport aux années précédentes. Par exemple, une entité d'investissement qui, auparavant, se concentrait

essentiellement sur les véhicules de placement traditionnels peut décider qu'une part importante de son portefeuille de placements comprendra dorénavant des cryptomonnaies.

Voici des exemples de facteurs à prendre en considération relativement à l'acceptation ou au maintien d'une relation client.

Intégrité du client, y compris l'objet visé lors de la conclusion de transactions en cryptomonnaie

En ce qui concerne l'intégrité du client, l'auditeur doit par exemple vérifier s'il y a des indications selon lesquelles le client pourrait être impliqué dans des activités de blanchiment d'argent ou d'autres activités criminelles. Il existe des motifs légitimes, sur le plan des affaires, à l'utilisation de cryptomonnaies. Toutefois, des cryptomonnaies ont également été utilisées pour le recyclage des produits de la criminalité et le financement des activités terroristes et autres activités illégales. Ces types d'activités sont rendues possibles par l'anonymat des participants aux chaînes de blocs. De même, les bourses où des cryptomonnaies sont échangées contre des monnaies fiduciaires demeurent très peu réglementées (par exemple, certaines ne sont pas assujetties à des règlements qui s'appliquent aux banques, notamment les règles en matière de connaissance de la clientèle et de lutte contre le blanchiment d'argent ainsi que l'obligation de tenir un registre des transactions inhabituelles).

Ainsi, les procédures d'acceptation ou de maintien d'une mission suivies par un auditeur comprendraient probablement des demandes d'informations et des procédures connexes visant l'acquisition d'une compréhension de l'objet visé par l'entité lorsqu'elle conclut des transactions en cryptomonnaie pour la première fois ou lorsqu'elle change de manière considérable la nature ou l'étendue de ses activités liées aux cryptomonnaies. L'un des éléments clés à prendre en considération est la question de savoir si les transactions importantes de l'entité en cryptomonnaie sont effectuées dans le cadre normal de ses activités. Si l'auditeur identifie des transactions importantes en cryptomonnaie qui sortent du cadre normal des activités, il doit :

- évaluer si ces transactions donnent lieu à des risques importants[3];
- s'enquérir auprès de la direction de la nature de ces transactions et de la possibilité que des parties liées soient impliquées[4];

3 NCA 315, *Compréhension de l'entité et de son environnement aux fins de l'identification et de l'évaluation des risques d'anomalies significatives,* paragraphe 27.

4 NCA 550, *Parties liées*, paragraphe 16.

- évaluer si la justification économique (ou l'absence de justification économique) des transactions donne à croire qu'elles ont peut-être été conclues dans le but de présenter des informations financières mensongères ou de dissimuler un détournement d'actifs[5].

L'auditeur doit également demeurer attentif à l'existence possible de cas avérés ou suspectés de non-conformité aux textes légaux et réglementaires, y compris des activités de blanchiment d'argent ou d'autres activités illégales[6].

Niveau de compréhension du client en ce qui concerne les risques liés à la cryptomonnaie et les aspects pertinents du contrôle interne

Afin d'établir si les conditions préalables à la réalisation d'un audit sont réunies, l'auditeur doit obtenir, de la part de la direction, confirmation qu'elle reconnaît et comprend les responsabilités qui lui incombent relativement à certaines questions, parmi lesquelles :

- la préparation des états financiers conformément au référentiel d'information financière applicable, ce qui implique, le cas échéant, leur présentation fidèle;
- la mise en place des contrôles internes nécessaires pour permettre la préparation d'états financiers exempts d'anomalies significatives, que celles-ci résultent de fraudes ou d'erreurs[7].

Idéalement, le client doit comprendre les questions liées à la cryptomonnaie, y compris ses répercussions sur la présentation de l'information financière. Le client doit également avoir conçu et mis en place des contrôles à l'égard de ses transactions et de ses soldes en cryptomonnaie. Toutefois, l'auditeur peut se trouver dans une situation où un client potentiel n'a même pas mis en œuvre de processus servant à consigner ses transactions en cryptomonnaie. En pareille situation, il peut s'avérer très difficile, voire impossible, de procéder à l'audit des états financiers de l'entité.

5 NCA 240, *Responsabilités de l'auditeur concernant les fraudes lors d'un audit d'états financiers*, alinéa 33c).

6 NCA 250, *Prise en compte des textes légaux et réglementaires dans un audit d'états financiers*, paragraphe 16.

7 NCA 210, *Accord sur les termes et conditions d'une mission d'audit*, paragraphe 6.

Compétence et capacités des personnes qui participent à l'exécution de la mission[8]

Les transactions en cryptomonnaie et la gestion des actifs cryptomonétaires nécessitent souvent le recours à des systèmes cryptographiques et à des technologies de l'information (TI) très complexes. Dans certains cas, il peut s'avérer impossible d'auditer des transactions et des actifs liés aux cryptomonnaies sans s'appuyer sur le fonctionnement efficace des contrôles pertinents. De plus, les questions telles que l'évaluation des éléments se rapportant aux cryptomonnaies aux fins de la présentation de l'information financière peuvent nécessiter le recours à des experts en évaluation. Par conséquent, lorsqu'il décide s'il convient d'accepter ou de maintenir une mission d'audit d'états financiers qui contiennent des éléments et des transactions significatifs liés aux cryptomonnaies, l'associé responsable de la mission doit déterminer si les personnes qui participent à l'exécution de la mission (y compris les membres de l'équipe de mission et les experts externes choisis par l'auditeur) possèdent la compétence et les capacités qui sont nécessaires.

8 CSQC 1, *Contrôle qualité des cabinets réalisant des missions d'audit ou d'examen d'états financiers et d'autres missions d'assurance, paragraphe 31.*

Système d'information de l'entité pour les transactions en cryptomonnaie

Selon les Normes canadiennes d'audit (NCA), l'auditeur doit acquérir une compréhension du système d'information de l'entité[9], y compris les procédures suivies par l'entité, tant dans les systèmes informatisés que dans les systèmes manuels, pour le déclenchement, l'enregistrement, le traitement, la correction au besoin, le report au grand livre général et la communication dans ses états financiers.

Les cryptomonnaies majeures utilisent des chaînes de blocs publiques transparentes. Toutes les transactions sont enregistrées de façon permanente dans la chaîne de blocs. N'importe qui peut lire ou regrouper des transactions enregistrées. Ces transactions peuvent être consignées par exemple au moyen d'un numéro d'identification ou d'une adresse. On dit parfois que la technologie de la chaîne de blocs élimine la nécessité de faire confiance aux autres parties à la transaction. Même si cela peut être vrai jusqu'à un certain point, il existe néanmoins des défis et des risques associés à l'utilisation de cette technologie et des cryptomonnaies.

Certains aspects des procédures suivies par l'entité en ce qui a trait aux transactions en cryptomonnaie diffèrent considérablement de ce qui existe dans le cas des monnaies fiduciaires. Par exemple, les transactions en cryptomonnaie impliquent l'utilisation de la cryptographie, de **portefeuilles de cryptomonnaies**

9 NCA 315, paragraphe 18.

et d'une chaîne de blocs. Il est possible (quoique rare) qu'une organisation de cryptomonnaie utilise un système cryptographique autre qu'une chaîne de blocs (par exemple, le Ripple).

Pour mieux comprendre ces questions complexes, les lecteurs peuvent consulter les sources suivantes :

- CVMO – Les Ontariens et ls cryptomonnaies : un aperçu
- Banque du Canada – Exposé sur les monnaies électroniques
- US Congressional Research Service – Foire aux questions sur le bitcoin (en anglais)
- UWCISA – Bitcoin Process Flow – Guide à l'intention des comptables (en anglais)
- Nasdaq – Cryptocurrency And Your Small Business: What You Need To Know

Exemple d'achat en cryptomonnaie

La figure 1 montre un exemple simplifié de la façon dont une cryptomonnaie peut être achetée et la transaction, enregistrée. Cette figure et les commentaires qui la suivent sur les portefeuilles de cryptomonnaies sont destinés aux lecteurs qui ne maîtrisent pas le sujet des transactions en cryptomonnaie. Cette figure est générique; chaque entité peut suivre un processus différent de celui qui est illustré.

Il est possible de suivre un processus similaire à celui montré ci-dessous lors de la vente d'une cryptomonnaie. Par exemple, la cryptomonnaie pourrait être échangée contre une autre cryptomonnaie ou contre une monnaie fiduciaire.

D'autres transactions pourraient nécessiter, par exemple, l'utilisation de la cryptomonnaie pour la vente ou l'achat de biens ou de services.

FIGURE 1 – EXEMPLE SIMPLIFIÉ D'UNE TRANSACTION D'ACHAT EN CRYPTOMONNAIE

- La direction détermine le type de cryptomonnaie à acheter.
- Un **portefeuille de cryptomonnaies** est téléchargé auprès d'un fournisseur de services. Un mot de passe ou une phrase passe ainsi que d'autres mesures de sécurité considérées comme appropriées sont utilisés pour protéger le portefeuille contre les accès non autorisés (voir les renseignements sur les différents types de portefeuilles, dans la prochaine section du document).

- Le logiciel du portefeuille est utilisé pour générer la clé cryptographique privée de l'entité. Une clé publique est générée au moyen de la clé privée, et l'adresse de l'entité (identifiant à usage unique) est générée pour chaque transaction d'achat en cryptomonnaie à partir de la clé publique de l'entité.
- La direction établit un compte auprès d'une bourse ou **d'un courtier de cryptomonnaies**.
- Le montant désiré de cryptomonnaie est acheté à l'aide du portefeuille de cryptomonnaies en ligne (*hot wallet*) de l'entité (voir la section suivante).
- La transaction est authentifiée et est ensuite enregistrée de manière irréversible dans une chaîne de blocs. Les transactions peuvent être visualisées au moyen d'un explorateur de blocs (*block explorer*), lorsque celui-ci est disponible.
- Pour protéger la clé privée de l'entité de tout accès non autorisé par Internet, l'entité peut utiliser au moins une ou plusieurs méthodes de stockage à froid (à savoir un portefeuille hors ligne, ou *cold wallet*) pour stocker la clé privée et l'information connexe (par exemple, l'adresse à laquelle la clé privée est associée).
- Des copies de sauvegarde des clés cryptographiques de l'entité, en particulier des clés privées, ainsi que des mots de passe ou des phrases passe requis pour accéder à un portefeuille, sont créées et stockées en toute sécurité.
- La transaction en cryptomonnaie est enregistrée dans le système d'information financière de la société, pour ensuite être convertie dans la monnaie fonctionnelle de l'entité au taux de change approprié.
- Lors de la préparation des états financiers de l'entité, tous les ajustements nécessaires sont apportés au montant enregistré de l'actif en cryptomonnaie et aux transactions connexes, à des fins de conformité avec le référentiel d'information financière applicable (par exemple, les normes IFRS®). Pour de plus amples indications sur les répercussions comptables des cryptomonnaies, consultez la publication de CPA Canada intitulée ***Introduction à la comptabilisation des cryptomonnaies selon les normes IFRS***.

Portefeuilles de cryptomonnaies

Les transactions en cryptomonnaie nécessitent l'utilisation d'un logiciel, appelé portefeuille de cryptomonnaies, qui sert notamment :

- à stocker les clés de chiffrement privées et publiques de l'entité qui sont utilisées pour les transactions en cryptomonnaie;
- à interagir avec une ou plusieurs chaînes de blocs pour envoyer et recevoir des cryptomonnaies;
- à afficher le solde de l'entité, dans chaque cryptomonnaie, qui résulte des diverses transactions.

Si l'entité perd une clé privée qui ne peut être recouvrée, elle ne sera plus en mesure d'accéder à la cryptomonnaie associée à cette clé. Par conséquent, dans les faits, la cryptomonnaie sera perdue. De plus, si la clé privée d'une entité est obtenue par un tiers, elle peut être utilisée pour conclure des transactions non autorisées en cryptomonnaie qui ne peuvent pas être inversées. Le portefeuille de l'entité montrerait alors des transactions non autorisées par l'entité. La cryptomonnaie volée pourrait ne jamais être recouvrée.

Types de portefeuilles de cryptomonnaies

Portefeuille en ligne

Le portefeuille en ligne (*hot wallet*) est situé dans un appareil connecté à Internet (qui est soit hébergé, soit contrôlé par l'entité). Il faut utiliser un portefeuille en ligne pour envoyer une cryptomonnaie à une autre adresse (à savoir pour dépenser de la cryptomonnaie) et obtenir un aperçu à jour de l'ensemble des transactions et des soldes récents en cryptomonnaie de l'entité.

Portefeuille hors ligne

Le portefeuille hors ligne (*cold wallet*), ou portefeuille de stockage à froid (*cold-storage wallet*), n'est pas connecté à Internet. Voici quelques exemples de portefeuilles hors ligne :

- **Portefeuille matériel**
  Le portefeuille matériel (*hardware wallet*) est situé sur une clé USB ou un autre appareil. Les clés privées et publiques de l'entité sont générées dans l'appareil lorsqu'il est hors ligne, à l'aide d'un générateur de nombres aléatoires. Lorsque le portefeuille n'est pas connecté à Internet, la clé privée de l'entité n'est évidemment pas accessible par des tiers par le biais d'Internet. Cependant, la clé privée peut tout de même être perdue ou volée par d'autres moyens. Par exemple, l'appareil qui contient le portefeuille matériel

peut être perdu ou endommagé. De même, un portefeuille hors ligne devient temporairement un portefeuille en ligne (donc moins sûr) chaque fois que l'appareil qui contient le portefeuille hors ligne est connecté à Internet. La clé privée qui a été générée hors ligne est alors utilisée en ligne au cours de l'envoi de la cryptomonnaie à une autre adresse, de sorte qu'elle est temporairement exposée, par exemple, aux virus et aux logiciels malveillants. Toutefois, certains portefeuilles matériels sont dotés d'un processus qui génère une signature numérique hors ligne, de sorte que la clé privée n'apparaît jamais sur l'ordinateur ou l'autre appareil utilisé pour exécuter la transaction de vente.

- **Portefeuille papier**
  Un portefeuille papier (*paper wallet*) est un registre papier de la clé privée de l'entité et de l'information connexe. Lorsque l'ordinateur (ou autre appareil) de l'entité et l'imprimante sont hors ligne, un logiciel est utilisé pour générer un ensemble de clés privées et publiques ainsi que les adresses connexes liées à son portefeuille hors ligne. Les clés publiques et privées liées au portefeuille sont imprimées sur papier. Le montant de cryptomonnaie désiré est envoyé à partir du portefeuille en ligne de l'entité vers l'adresse de son portefeuille papier. Le montant transféré au portefeuille papier peut être réduit. La cryptomonnaie peut ensuite être envoyée à partir du portefeuille papier. Il est possible de le faire en inscrivant, dans le portefeuille en ligne de l'entité, l'adresse à laquelle la cryptomonnaie doit être envoyée, puis en numérisant ou en tapant la clé privée du portefeuille papier dans le portefeuille en ligne. Cette clé privée servira ensuite à générer la signature numérique pour la transaction. Pendant la courte période où la cryptomonnaie est envoyée, la clé privée du portefeuille papier n'est plus « hors ligne », de sorte qu'elle est exposée, par exemple, aux virus et aux logiciels malveillants.

Portefeuille hébergé sur une bourse

Un portefeuille hébergé sur une bourse (*exchange-hosted wallet*) est hébergé sur le serveur d'une bourse de cryptomonnaies. Le portefeuille est associé au compte de l'entité dans la bourse. Ce compte contient des renseignements permettant d'identifier l'entité. L'accès au compte et au portefeuille est protégé par un mot de passe. La bourse connaît la clé privée de l'entité qui est stockée dans le portefeuille, mais l'entité elle-même ne connaît pas sa clé privée. La bourse conclut des transactions en cryptomonnaie pour le compte de l'entité (en fonction des directives de l'entité ou de ce qui a autrement été convenu).

Exemples de facteurs à considérer lors de l'identification et de l'évaluation des risques d'anomalies significatives dans les transactions et les soldes en cryptomonnaie

Aux fins de l'identification de l'évaluation des risques d'anomalies significatives, l'auditeur doit, conformément aux NCA[10] :

- identifier les risques tout au long du processus d'acquisition d'une compréhension de l'entité et de son environnement, y compris des contrôles pertinents relatifs aux risques, en prenant en considération les catégories d'opérations, les soldes de comptes et les informations à fournir (y compris les aspects quantitatifs ou qualitatifs de ces informations) dans les états financiers;
- évaluer les risques identifiés et déterminer s'ils se répercutent de manière généralisée sur les états financiers pris dans leur ensemble et peuvent affecter de nombreuses assertions;
- faire un lien entre les risques identifiés et les problèmes pouvant survenir au niveau des assertions, en tenant compte des contrôles pertinents qu'il a l'intention de tester;
- examiner la probabilité de l'existence d'une anomalie, y compris la possibilité d'anomalies multiples, et déterminer si l'anomalie potentielle pourrait constituer une anomalie significative.

10 NCA 315, paragraphe 26.

Un risque d'anomalie significative dans un solde ou une transaction en crypto-monnaie peut être identifié dans les situations suivantes :

- il survient une situation ou un événement pertinent pour au moins une des assertions liées aux soldes et aux transactions en cryptomonnaie de l'entité;
- l'entité n'a pas mis en place de contrôle interne pour fournir une assurance raisonnable que les résultats de ces situations et événements sont consignés dans les comptes de l'entité et reflétés dans ses états financiers, comme l'exige le référentiel d'information financière applicable.

Ci-dessous sont exposés neuf exemples de situations ou d'événements qu'un auditeur serait susceptible de prendre en considération dans le cadre de la mise en œuvre de procédures visant à identifier et à évaluer les risques d'anomalies significatives dans les transactions et les soldes en cryptomonnaie, que celles-ci résultent de fraudes ou d'erreurs. Les informations fournies pour chaque exemple comprennent ce qui suit :

- une brève description de la situation ou de l'événement;
- les assertions connexes;
- des exemples d'aspects du contrôle interne qui pourraient aider à prévenir ou à détecter et corriger une anomalie significative. Ces exemples ne constituent pas une liste exhaustive des considérations relatives au contrôle interne.

Cette liste ne se veut pas exhaustive; d'autres situations et événements peuvent donner lieu à un risque d'anomalie significative dans les transactions ou les soldes en cryptomonnaie.

La figure 2 résume certaines situations ou certains événements, de même que les assertions pouvant être touchées.

FIGURE 2 – SOMMAIRE DES SITUATIONS OU ÉVÉNEMENTS ET DES ASSERTIONS POUVANT ÊTRE TOUCHÉES

Exemples de situations ou d'événements « problèmes pouvant survenir »	Exemples d'assertions auxquelles une anomalie possible peut être associée[11]					
	Exa	Exh	SP	Exi	R	D
1. L'entité choisit d'avoir recours à une bourse de cryptomonnaies qui n'a pas de contrôles efficaces à l'égard des transactions qu'elle conclut pour le compte de l'entité ou à l'égard des soldes de cryptomonnaie maintenus dans les comptes de l'entité.	×	×	×	×	×	×

11 NCA 315, paragraphe A129.

Exemples de situations ou d'événements « problèmes pouvant survenir »	Exemples d'assertions auxquelles une anomalie possible peut être associée[11]					
	Exa	Exh	SP	Exi	R	D
2. L'entité a un portefeuille de crypto-monnaies qui n'a pas été comptabilisé.		×				
3. L'entité perd une clé privée et ne peut donc plus accéder à la cryptomonnaie qui s'y rattache.						×
4. Une partie non autorisée obtient l'accès à la clé privée de l'entité et vole sa cryptomonnaie.				×		×
5. L'entité donne une image trompeuse de la propriété d'une clé privée et donc de la cryptomonnaie qui s'y rattache.				×	×	×
6. L'entité envoie de la cryptomonnaie à une adresse erronée, et la cryptomonnaie ne peut être recouvrée.						×
7. L'entité conclut et enregistre une transaction en cryptomonnaie avec une partie liée qui ne peut être identifiée en raison de l'anonymat des parties à une chaîne de blocs.	×	×				
8. Le traitement des transactions en crypto-monnaie accuse des retards importants à la fin d'une période.			×			
9. Des événements ou des situations font en sorte qu'il est difficile de déterminer la valeur à laquelle une cryptomonnaie doit être enregistrée aux fins de la présentation de l'information financière.	×					

Légende

Exa : Exactitude, évaluation et imputation
Exh : Exhaustivité
Exi : Existence
SP : Séparation des périodes
R : Réalité
D : Droits (propriété)

Remarque : Les assertions relatives aux informations à fournir ne sont pas abordées dans le présent document. De plus, les auditeurs peuvent utiliser des assertions autres que celles qui y sont mentionnées.

Vous trouverez ci-dessous des exemples de situations ou d'événements pouvant se traduire par un risque d'anomalie significative. **Cette liste n'est pas exhaustive.**

11 NCA 315, paragraphe A129.

Avez-vous l'expérience nécessaire pour auditer des soldes et des transactions significatifs en cryptomonnaie?

Si vous procédez à l'audit d'une entité ayant des soldes ou des transactions significatifs en cryptomonnaie, avez-vous évalué tous les risques d'anomalies significatives et toutes les assertions connexes?

Pensez-vous être en mesure d'obtenir des éléments probants suffisants et appropriés en concevant et en mettant en œuvre des réponses appropriées à ces risques?

1. **L'entité choisit d'avoir recours à une bourse de cryptomonnaies qui n'a pas de contrôles efficaces à l'égard des transactions qu'elle conclut pour le compte de l'entité ou à l'égard des soldes de cryptomonnaie maintenus dans les comptes de l'entité.**

   Assertions connexes : *n'importe laquelle des assertions est susceptible d'être touchée.*

   Il est courant pour une entité d'avoir recours à une bourse en ligne pour conclure des transactions en cryptomonnaie. De plus, dans certains cas, l'entité peut utiliser un portefeuille de cryptomonnaies hébergé sur cette bourse.

   Les caractéristiques de la bourse sélectionnée peuvent avoir des répercussions significatives pour toutes les assertions relatives à la cryptomonnaie qui sont indiquées ci-dessus. Les facteurs à prendre en considération lors du choix d'une bourse en ligne peuvent comprendre les suivants :

   - l'identité de ceux qui possèdent et exploitent la bourse, de même que leur réputation (par exemple, certaines bourses seraient impliquées dans des stratagèmes de manipulation de marché, lesquels consistent à gonfler le prix d'un titre par le biais de fausses déclarations, puis de larguer ou de vendre le titre à un nouvel investisseur, afin de moduler artificiellement les prix des cryptomonnaies);
   - le pays où est située la bourse. Ce facteur peut permettre de déterminer, par exemple, quels sont les lois et les règlements auxquels la bourse est assujettie, notamment les règlements contre le blanchiment d'argent qui exigent de la bourse qu'elle suive des protocoles de connaissance de la clientèle;
   - les cryptomonnaies et les monnaies fiduciaires dont la bourse autorise l'échange;

- les liquidités et le volume de transactions de la bourse;
- les contrôles que la bourse a mis en place relativement, par exemple, à la garantie fournie à l'égard des portefeuilles hébergés sur la bourse;
- la question de savoir si la bourse fournit un rapport de l'auditeur de la société de services sur l'efficacité de ses contrôles à l'égard des transactions et des soldes en cryptomonnaie pour le compte de ses clients. À l'heure actuelle, il est rare que des rapports de l'auditeur d'une société de services soient délivrés sur de tels contrôles. Toutefois, un certain nombre de bourses et d'auditeurs explorent la question des missions exécutées par les auditeurs des sociétés de services. Il est donc possible que de tels rapports soient délivrés plus fréquemment au cours des prochaines années.

Considérations relatives au contrôle interne

- L'entité peut attribuer la responsabilité de la sélection de la cryptomonnaie à acheter et de la bourse à utiliser à des membres du personnel qui connaissent bien le domaine et qui sont au fait des risques en cause ainsi que de la façon dont ils peuvent être atténués.
- La haute direction peut examiner et, s'il y a lieu, approuver les choix effectués.
- L'entité peut décider d'utiliser une authentification à deux facteurs au moins pour l'accès à son compte, ce qui atténuerait, dans une certaine mesure, le risque d'accès non autorisé au portefeuille de l'entité hébergé sur une bourse.

2. L'entité a un portefeuille de cryptomonnaies qui n'a pas été comptabilisé.

Assertion connexe : *exhaustivité, pour la comptabilisation à la fois des actifs cryptomonétaires et des transactions connexes.*

Il se peut qu'une entité auditée omette de comptabiliser un ou plusieurs de ses portefeuilles de cryptomonnaies (et la cryptomonnaie connexe qu'elle détient). Les actifs cryptomonétaires et les transactions connexes de l'entité n'auront alors pas été comptabilisés.

Le risque d'anomalie significative lié à l'exhaustivité des actifs cryptomonétaires et des transactions en cryptomonnaie peut être difficile à évaluer. Les clés publiques et les adresses qui s'y rattachent dans une chaîne de blocs ne rendent pas transparente l'identité des parties aux transactions. Qui plus est, il se peut que l'entité n'ait qu'une expérience limitée des transactions en cryptomonnaie. Par conséquent, l'auditeur est susceptible d'avoir

de la difficulté à obtenir des informations utiles étayant le fait qu'il s'attend à ce que des transactions importantes en cryptomonnaie n'aient pas été comptabilisées.

Si l'auditeur prend connaissance, au cours de l'audit, de l'existence d'un portefeuille n'ayant pas été comptabilisé précédemment, il peut y avoir des indices qui laissent croire que l'existence d'un tel portefeuille a délibérément été cachée. Cela peut être une indication d'un risque de fraude, y compris le risque de contournement des contrôles par la direction en ce qui concerne les portefeuilles de cryptomonnaies.

Considérations relatives au contrôle interne
Le défaut d'identifier un portefeuille détenu par l'entité peut être involontaire. Une entité peut posséder de nombreux portefeuilles, de telle sorte qu'il est possible que les contrôles relatifs à l'autorisation pour la création d'un portefeuille et le suivi ultérieur des portefeuilles ne fonctionnent pas efficacement. L'entité peut donc avoir perdu la trace d'un ou de plusieurs portefeuilles. L'établissement de responsabilités clairement définies en ce qui a trait à la création et au suivi des portefeuilles peut atténuer un tel risque.

3. L'entité perd une clé privée et ne peut donc plus accéder à la cryptomonnaie qui s'y rattache.

Assertion connexe : *droits (propriété) sur les actifs cryptomonétaires.*

Si l'entité perd une clé privée qui ne peut être recouvrée, elle ne pourra plus accéder à la cryptomonnaie associée à cette clé et ne sera donc plus en mesure d'établir ses droits de propriété. La cryptomonnaie associée à cette clé privée continuera toutefois d'exister dans la chaîne de blocs pertinente. Néanmoins, la cryptomonnaie associée à la clé privée n'existe plus en tant qu'actif de l'entité.

La perte d'une clé privée donne lieu à une anomalie significative si l'effet de la perte n'est pas adéquatement comptabilisé. Cependant, le risque d'anomalie significative peut survenir, par exemple, si les responsables du contrôle à l'égard de la clé privée n'ont pas connaissance de sa perte au moment où les états financiers sont établis, du fait qu'ils n'ont pas tenté de conclure de nouvelles transactions en cryptomonnaie. Toujours à titre d'exemple, les personnes responsables de la perte de la clé privée de l'entité peuvent avoir grandement intérêt à dissimuler cette perte ou à ne pas la signaler rapidement.

Considérations relatives au contrôle interne

- Contrôles visant à réduire le risque d'une perte d'accès à une clé privée
  Par exemple, des politiques et des procédures peuvent être mises en œuvre pour exiger qu'une copie de sauvegarde de la clé privée (et possiblement des clés publiques et des adresses qui s'y rattachent) soit conservée. Les copies de sauvegarde peuvent se trouver sur des appareils électroniques distincts. Il est également possible d'utiliser un portefeuille papier. Les clés privées et les mots de passe ou phrases passe stockés sur le dispositif de sauvegarde ou dans le portefeuille papier peuvent à leur tour être sauvegardés, afin d'aider à fournir une assurance raisonnable que l'entité ne perdra pas sa cryptomonnaie. En outre, la localisation du dispositif de sauvegarde ou du portefeuille papier doit être communiquée à plusieurs des personnes concernées (et non à une seule d'entre elles).

- Contrôles visant à réduire le risque que la perte d'une clé privée ne soit pas signalée et que la perte qui en résulte ne soit pas comptabilisée
  L'entité peut mettre en place des politiques et des procédures telles que l'établissement d'une séparation appropriée des tâches (c'est-à-dire que la responsabilité de la surveillance des actifs cryptomonétaires, du point de vue de la présentation de l'information financière, est exercée par des personnes qui ne participent pas à la réalisation des transactions en cryptomonnaie de l'entité). Ces politiques et procédures peuvent également exiger qu'une telle surveillance soit continue (par exemple, par le biais d'examens des portefeuilles de l'entité ou de l'utilisation d'un explorateur de blocs, s'il en existe un).

4. Une partie non autorisée obtient l'accès à la clé privée de l'entité et vole sa cryptomonnaie.

Assertions connexes : *droits (propriété) sur les actifs cryptomonétaires et existence des actifs pour l'entité.*

Les questions pertinentes pour le vol d'une clé privée sont semblables à celles exposées à l'exemple 3, ci-dessus, au sujet de la perte d'une clé privée.

Considérations relatives au contrôle interne

Les risques d'accès non autorisé à un portefeuille en ligne peuvent être atténués au moyen d'une authentification à deux facteurs au moins pour l'obtention de l'accès à un portefeuille. Le chiffrement du contenu d'un portefeuille peut ajouter un niveau de sécurité supplémentaire. De plus, le fait d'utiliser un portefeuille en ligne seulement pour la conclusion d'une transaction en cryptomonnaie et d'utiliser un portefeuille hors ligne pour

le stockage de la clé privée et des informations connexes de l'entité peut atténuer le risque d'accès non autorisé à la clé privée de l'entité par le biais d'Internet. En outre, l'entité peut décider de rendre accessible seulement une petite partie de sa cryptomonnaie à partir d'un portefeuille en ligne, et d'en stocker la majeure partie dans un portefeuille hors ligne.

5. **L'entité donne une image trompeuse de la propriété d'une clé privée et donc de la cryptomonnaie qui s'y rattache.**

   Assertions connexes : *droits (propriété) sur la cryptomonnaie, réalité (c'est-à-dire que l'événement ou la transaction lié à l'établissement de la propriété ne s'est pas produit) et existence du solde connexe.*

   Il est difficile de répondre au risque lié à la propriété, étant donné que, du fait de l'anonymat des parties à la transaction, la propriété d'une cryptomonnaie ne ressort pas de manière évidente de la chaîne de blocs. La possession d'une clé privée indique clairement, à un moment précis, la propriété de la cryptomonnaie à laquelle il est possible d'accéder au moyen de cette clé. Cependant, la propriété d'une clé privée n'est pas toujours attribuable à une seule entité. Il peut y avoir des cas où, par exemple, une clé privée (et la propriété de la cryptomonnaie qui s'y rattache) est partagée de façon légitime entre différentes parties. Aussi, il peut être difficile de déterminer si la clé privée (et la cryptomonnaie qui s'y rattache) est détenue par l'entité ou par une ou plusieurs personnes.

   En outre, un auditeur peut se trouver dans une situation lui laissant croire que l'entité auditée déclare frauduleusement qu'elle est seule à contrôler une clé privée et à détenir la cryptomonnaie qui s'y rattache. L'auditeur doit faire preuve d'esprit critique tout au long de l'audit, en étant conscient de l'existence possible d'une anomalie significative résultant d'une fraude, nonobstant le jugement que son expérience passée auprès de l'entité l'a amené à porter sur l'honnêteté et l'intégrité de la direction et des responsables de la gouvernance.

   Considérations relatives au contrôle interne
   Le système d'information de l'entité et ses contrôles connexes à l'égard de la création de ses portefeuilles peuvent fournir de la documentation sur la création de clés privées et sur leur utilisation aux fins des transactions en cryptomonnaie de l'entité. L'environnement de contrôle de l'entité, y compris ses énoncés de politique et son code d'éthique, peut également s'avérer pertinent.

6. L'entité envoie de la cryptomonnaie à une adresse erronée, et la cryptomonnaie ne peut être recouvrée.

Assertion connexe : *droits (propriété) sur les actifs cryptomonétaires.*

Chaque chaîne de blocs suit ses propres processus pour vérifier que les transactions en cryptomonnaie sont authentiques et qu'elles n'ont pas été reproduites (c'est-à-dire en validant leur algorithme de consensus). Toutefois, l'une des caractéristiques communes à toutes les chaînes de blocs est le fait que, une fois qu'une transaction est confirmée dans la chaîne de blocs, elle est irréversible. Cette caractéristique fait en sorte qu'une entité peut perdre une cryptomonnaie si elle est envoyée à une adresse erronée.

Un membre du personnel de l'entité auditée peut saisir une adresse erronée lors de l'envoi d'une cryptomonnaie. La partie qui reçoit la cryptomonnaie pourrait la retourner volontairement à l'entité auditée dans le cadre d'une nouvelle transaction, mais elle pourrait également décider de ne pas le faire, auquel cas la cryptomonnaie serait perdue.

Une anomalie se produit si la perte de la cryptomonnaie n'est pas comptabilisée adéquatement. Une telle situation peut survenir, par exemple, lorsque les responsables de la gestion de la cryptomonnaie ont grandement intérêt à tenter de dissimuler la perte ou à ne pas la signaler rapidement.

Considérations relatives au contrôle interne

- Contrôles visant à empêcher l'utilisation d'une adresse erronée
  Les politiques et les procédures mises en place par l'entité pourraient nécessiter à la fois un examen minutieux de chaque adresse avant l'envoi et le recours à un total de contrôle pour aider à prévenir les erreurs typographiques lors de la saisie d'une adresse. Certaines chaînes de blocs ont également chiffré un total de contrôle dans chaque adresse. De plus, l'entité peut envisager d'envoyer en premier lieu un très petit montant de cryptomonnaie au destinataire visé. L'adresse du destinataire peut donc être confirmée avant l'envoi du montant plus élevé. Le fait de recourir à un code QR (plutôt que de taper l'adresse ou de la copier-coller) peut également aider à prévenir les erreurs.
- Contrôles visant à aider à réduire le risque que la perte d'une cryptomonnaie ne soit pas communiquée et comptabilisée Les exemples de tels contrôles sont les mêmes que ceux présentés à l'exemple 3, ci-dessus.

7. L'entité conclut et enregistre une transaction en cryptomonnaie avec une partie liée qui ne peut être identifiée en raison de l'anonymat des parties à une chaîne de blocs.

Assertions connexes : *exactitude (y compris l'évaluation et l'imputation) pour les actifs et exhaustivité pour les informations à fournir.*

L'identité des acheteurs et des vendeurs de cryptomonnaie est souvent vue comme étant pseudonymique plutôt qu'anonyme. Il n'est pas possible d'obtenir des renseignements tels que le nom des acheteurs et des vendeurs simplement en regardant une adresse dans une chaîne de blocs. Toutefois, il existe des liens entre les adresses figurant dans une chaîne de blocs et l'identité des parties à une transaction, par exemple dans les registres des bourses et des courtiers utilisés par ces parties. Il est donc possible qu'un organisme de réglementation ou une autre partie soit en mesure d'obtenir de telles identités. Cependant, dans la plupart des cas, le nom des parties à une transaction n'est pas évident. Ainsi, il peut s'avérer difficile de déterminer clairement si l'entité auditée conclut des transactions en cryptomonnaie avec des parties liées que la direction n'a pas identifiées. De ce fait, les parties liées, les transactions avec des parties liées et les soldes qui en résultent sont susceptibles de ne pas être comptabilisés ou présentés conformément au référentiel d'information financière applicable.

Considérations relatives au contrôle interne
L'une des considérations globales consiste à se demander si l'environnement de contrôle et les activités de contrôle de l'entité relativement à l'identification des parties liées et à l'autorisation des transactions avec des parties liées s'appliquent aux transactions en cryptomonnaie. Les éléments à considérer peuvent comprendre, par exemple :

- les politiques et les procédures pour l'acquisition d'une connaissance appropriée des parties avec lesquelles l'entité conclut des transactions en cryptomonnaie;
- l'attribution des responsabilités au sein de l'entité pour l'identification, l'enregistrement, la synthèse et la communication, aux fins de l'information financière, des transactions avec des parties liées, y compris les transactions en cryptomonnaie.

8. Le traitement des transactions en cryptomonnaie accuse des retards importants à la fin d'une période.

Assertion connexe : *séparation des périodes.*

La vitesse à laquelle les chaînes de blocs qui soutiennent des cryptomonnaies traitent et confirment les transactions peut varier considérablement. Bien souvent, les transactions sont traitées en quelques minutes. Toutefois, dans certains cas, une transaction peut être retardée de plusieurs jours.

De tels retards peuvent survenir, par exemple, lorsque :

- les mineurs de cryptomonnaies accordent une faible priorité aux transactions de l'entité si les honoraires que l'expéditeur accepte de payer aux mineurs sont considérablement moindres que pour d'autres transactions, et si le volume des transactions pour lesquelles les honoraires sont plus élevés est important;
- les transactions ont été suspendues par la bourse qui héberge le portefeuille de cryptomonnaies de l'entité.

Considérations relatives au contrôle interne

L'entité peut mettre en œuvre des procédures pour surveiller les transactions en cryptomonnaie pendant les jours qui précèdent et qui suivent les dates de clôture, afin d'établir si les transactions sont comptabilisées au cours de la période appropriée.

9. Des événements ou des situations font en sorte qu'il est difficile de déterminer la valeur à laquelle une cryptomonnaie doit être enregistrée aux fins de la présentation de l'information financière.

Assertion connexe : *exactitude (y compris l'évaluation et l'imputation).*

Les référentiels d'information financière tels que les normes IFRS ne font pas expressément mention des cryptomonnaies. La publication de CPA Canada intitulée *Introduction à la comptabilisation des cryptomonnaies selon les normes IFRS* indique que certains ont soulevé des préoccupations selon lesquelles l'application d'IAS® 38 *Immobilisations incorporelles* et l'évaluation des cryptomonnaies au coût ne refléteraient pas la substance économique et ne fourniraient pas d'informations pertinentes aux utilisateurs des états financiers. Dans certains cas, la juste valeur des cryptomonnaies pourrait être comptabilisée ou présentée dans les états financiers.

Les facteurs particuliers à prendre en considération au sujet de l'évaluation des cryptomonnaies comprennent ce qui suit.

- Bon nombre de cryptomonnaies sont volatiles, et les marchés peuvent demeurer ouverts en tout temps. L'heure à laquelle l'entité publiante évalue la cryptomonnaie peut donc être importante. Par exemple, l'évaluation est-elle réalisée à 23 h 59 (fuseau horaire) le dernier jour de la période de présentation de l'information financière ou à la fermeture des marchés cette journée-là? Cet aspect peut représenter une méthode comptable importante, et l'entité est tenue de l'appliquer de manière uniforme.
- Comme dans le cas d'actions ou de marchandises, il y a des ordres d'achat et de vente, et un écart important est souvent constaté entre les prix respectifs. À tout moment, il peut être difficile d'échanger, dans un délai raisonnable, un montant important de cryptomonnaie contre une monnaie fiduciaire à un prix que le détenteur considère comme juste.
- Pour certaines cryptomonnaies, le volume des transactions est faible.
- Le prix auquel une cryptomonnaie est négociée de façon concurrente sur différentes bourses peut varier considérablement.
- La nature et l'étendue de la réglementation qui s'applique aux marchés des cryptomonnaies varient grandement d'un territoire à l'autre. Bien souvent, ces marchés sont peu réglementés, ce qui se traduit entre autres par un manque de clarté quant à la façon dont les prix sont présentés.

Si un volume important de transactions a récemment été observé sur des bourses relativement à une cryptomonnaie, les cours négociés peuvent constituer une preuve de la juste valeur. S'il y a récemment eu peu ou pas de transactions, les données d'entrée observables pertinentes peuvent comprendre les prix fixés pour les offres d'achat ou de vente lors d'un échange entre pairs. Toutefois, il peut y avoir des volumes élevés de transactions pour lesquelles les prix ne deviennent accessibles qu'à une date ultérieure. Par exemple, il existe des bourses sur lesquelles des transactions hors chaîne sont enregistrées temporairement dans un registre privé jusqu'à ce que les parties souhaitent que la transaction soit enregistrée dans une chaîne de blocs publique. De plus, l'entité peut décider de recourir à un modèle économique pour estimer la juste valeur d'une cryptomonnaie.

Considérations relatives au contrôle interne

L'entité pourrait mettre en œuvre des politiques et des procédures relatives à l'évaluation de cryptomonnaies aux fins de la présentation de l'information financière. Ces politiques peuvent exiger, par exemple, que le choix de la méthode d'évaluation et la formulation des hypothèses soient effectués par des membres compétents du personnel et qu'ils soient revus et approuvés par des membres du personnel qui ne sont pas responsables de l'autorisation des transactions en cryptomonnaie.

Conclusion

La présente publication vise à sensibiliser les auditeurs, de façon générale, aux différentes questions touchant l'évaluation des risques d'anomalies liés aux éléments des états financiers qui se rapportent aux cryptomonnaies. Comme il a été soulevé, il est essentiel que l'auditeur détermine si l'équipe de mission possède les capacités requises pour mener à bien les processus informatiques complexes liés à la cryptomonnaie. L'auditeur peut également se reporter à d'autres sources pour explorer plus en profondeur les questions abordées dans la présente publication, afin d'être mieux préparé à entreprendre des audits portant sur des montants significatifs de cryptomonnaie.

Annexe A – Où trouver des informations supplémentaires

Cette annexe fournit des liens vers des ressources supplémentaires pouvant être utiles :

1. CPA Canada. *Perturbation technologique des marchés financiers et de la communication de l'information? Aperçu de la chaîne de blocs.* https://www.cpacanada.ca/fr/ressources-en-comptabilite-et-en-affaires/domaines-connexes/technologies-et-gestion-de-linformation/publications/introduction-a-la-technologie-de-la-chaine-de-blocs.

2. CPA Canada. *La technologie de la chaîne de blocs et son incidence potentielle sur la profession d'auditeur et de certificateur.* https://www.cpacanada.ca/fr/ressources-en-comptabilite-et-en-affaires/audit-et-certification/normes-canadiennes-daudit-nca/publications/chaine-blocs-audit.

3. CPA Canada. *Introduction à la comptabilisation des cryptomonnaies selon les normes IFRS.* https://www.cpacanada.ca/fr/ressources-en-comptabilite-et-en-affaires/information-financiere-et-non-financiere/normes-internationales-dinformation-financiere-ifrs/publications/comptabilisation-cryptomonnaies-normes-ifrs.

Annexe B – Glossaire

Bourse de cryptomonnaies

Il s'agit d'une plateforme en ligne qui offre un marché numérique pour l'achat et la vente de cryptomonnaies ainsi que, dans certains cas, pour l'échange de cryptomonnaies contre des monnaies fiduciaires.

Chaîne de blocs

Dans la publication de CPA Canada intitulée *Perturbation technologique des marchés financiers et de la communication de l'information? Aperçu de la chaîne de blocs, le terme* « chaîne de blocs » est décrit, à la page 10, comme un registre d'opérations partagé, ou « distribué », sur un réseau d'ordinateurs participants. Puisque la technologie de la chaîne de blocs incorpore des communications poste à poste entre les ordinateurs participants, il n'est plus nécessaire de faire appel à un tiers central tel qu'une institution financière pour gérer le réseau. Les ordinateurs participant à une chaîne de blocs utilisent un processus automatisé pour valider le format de l'enregistrement d'une opération à inclure dans le « bloc » suivant. Une fois le « consensus » atteint, l'information est enregistrée dans un bloc.

Courtier de cryptomonnaies

Il s'agit d'un type de bourse de cryptomonnaies où les cryptomonnaies peuvent être achetées à un prix fixé par le courtier qui exploite la bourse.

Cryptomonnaie

L'Office québécois de la langue française définit la cryptomonnaie comme une « monnaie virtuelle sans lien avec une politique monétaire ou une banque, dont l'implémentation repose sur des algorithmes de chiffrement ». Les descriptions de la cryptomonnaie mettent parfois l'accent sur ses différences par rapport à la monnaie fiduciaire. Par exemple, dans le numéro de mars 2017 du bulletin

IFRS News de pwc, intitulé *Cracking the cryptocurrency code; or what is a 'bitcoin' anyway?*, on mentionne ce qui suit : [TRADUCTION] « la crypto-monnaie représente une méthode d'échange qui n'existe pas physiquement, mais plutôt sous forme numérique. Les cryptomonnaies ne sont pas liées à une monnaie sous forme physique ou garanties par un gouvernement, une banque centrale, une entité juridique, un actif sous-jacent ou une marchandise. »

Explorateur de blocs

Un explorateur de blocs sert à tirer de l'information d'une chaîne de blocs dans un format facilement lisible par l'humain (plutôt que par machine). L'information obtenue et le format utilisé varient en fonction de l'explorateur. Normalement, l'entité utilise un explorateur de blocs afin, par exemple, de vérifier des soldes liés à une adresse, de suivre l'historique de transferts de pièces, d'établir si une transaction a été acceptée et confirmée, et d'obtenir des statistiques sur la performance de la chaîne de blocs (par exemple, le temps que prend la confirmation des transactions).

Mineur et minage de chaîne de blocs

Un mineur de chaîne de blocs est une entité qui se livre au minage de chaîne de blocs. Le minage est l'action d'ajouter de nouvelles transactions à la chaîne de blocs par la résolution de problèmes algorithmiques au moyen de ressources informatiques. Les transactions comprennent l'achat et la vente de cryptomonnaies ainsi que la création de nouvelles cryptomonnaies. Les mineurs peuvent se voir accorder des honoraires en cryptomonnaie pour la capacité informatique qu'ils mettent à la disposition du réseau.

Portefeuille de cryptomonnaies

Un portefeuille de cryptomonnaies est un logiciel qui sert :

- à stocker les clés de chiffrement privées et publiques de l'entité qui sont utilisées pour les transactions en cryptomonnaie;
- à interagir avec une ou plusieurs chaînes de blocs pour envoyer et recevoir des cryptomonnaies;
- à afficher le solde de l'entité, dans chaque cryptomonnaie, qui résulte des diverses transactions.

Signature numérique

L'entité qui envoie la cryptomonnaie à l'entité acheteuse signe la transaction au moyen d'une signature numérique. La signature numérique établit que l'expéditeur possède la clé privée à laquelle est associée sa clé publique, sans révéler l'identité de cette clé privée. La clé privée de l'expéditeur établit son droit de propriété sur la cryptomonnaie envoyée (sous réserve d'une vérification effectuée par des mineurs de chaîne de blocs).

CPA
COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

277, RUE WELLINGTON OUEST
TORONTO, ON CANADA M5V 3H2
Tél. : 416 977.3222 Téléc. : 416 977.8585
WWW.CPACANADA.CA