CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

POINTS DE VUE :

Application des Normes canadiennes d'audit (NCA) dans l'écosystème des cryptoactifs

AUDIT DES PRODUITS TIRÉS DU MINAGE D'ENTITÉS EXERÇANT DES OPÉRATIONS DE CRYPTOMINAGE

OCTOBRE 2022

Groupe de discussion 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 discussion sur l'audit des cryptoactifs, qui réunit des représentants du Conseil canadien sur la reddition de comptes (CCRC), des responsables provinciaux de l'inspection professionnelle, et des représentants du milieu universitaire et de cabinets canadiens appelés à échanger leurs points de vue sur l'application des NCA lors de la pratique de l'audit dans l'écosystème 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, le CCRC ou les cabinets et autres organisations représentés par les membres du Groupe de discussion, 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 ou de l'application 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 transactions en cryptoactifs ou des soldes de 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.

À l'heure actuelle, aucune section des Normes internationales d'information financière (IFRS) ne porte spécifiquement sur le minage de cryptoactifs. De manière générale, le secteur indique que des contrats ou des accords sont conclus entre le mineur et le groupe de minage ou la chaîne de blocs, qui se soldent par des produits des activités ordinaires comptabilisés selon IFRS 15. Toutefois, il faut examiner attentivement les faits et circonstances se rapportant à chaque accord ainsi que le traitement comptable connexe qui a été appliqué. Aux fins du présent document, nous supposons que la norme IFRS 15 s'applique; cependant, le lecteur doit garder à l'esprit que cette norme pourrait ne pas s'appliquer dans toutes les circonstances. En outre, dans le présent document, le terme « contrat » s'entend de tout type d'accord ou d'entente conclu entre un mineur et un groupe de minage.

Contexte

Tandis que le marché des cryptoactifs continue de prendre de l'ampleur, les défis auxquels font face les auditeurs pour obtenir une assurance à l'égard de cette catégorie d'actif complexe deviennent évidents. Il se peut que les procédures d'audit habituelles ne permettent pas d'obtenir des éléments probants appropriés lors de l'audit des soldes de cryptoactifs et des transactions en cryptoactifs. Les auditeurs pourraient devoir trouver d'autres façons de répondre aux risques propres à ce secteur émergent. Cependant, comme les cryptoactifs n'existent que depuis peu, les approches ou les indications habituelles relatives à l'audit – au Canada et ailleurs dans le monde – peuvent être difficiles à appliquer. Cela accroît inévitablement le risque de pratiques incohérentes entre les auditeurs ou les cabinets.

L'audit d'une entité de minage de cryptoactifs (cryptomineur) engendre des considérations particulières relatives à l'audit, certaines étant abordées dans le présent document. L'un des principaux défis de l'heure sur le marché est l'écart entre les attentes des cryptomineurs lors de l'audit de leurs états financiers et les responsabilités des auditeurs en conformité avec les NCA. Cette situation contribue au roulement des auditeurs auquel font face les entités de ce secteur.

Objet

Le présent document vise à :

- aider les auditeurs et les auditeurs éventuels de cryptomineurs (en particulier les mineurs dans le cadre de la preuve de travail) à comprendre les risques et les défis propres à l'audit des produits tirés du cryptominage;
- aider les cryptomineurs à comprendre les responsabilités de l'auditeur et ce qu'il faut pour faciliter la réalisation de l'audit.

En fournissant des indications ne faisant pas autorité aux auditeurs et à leurs clients (potentiels), nous souhaitons accroître la cohérence des pratiques afin de soutenir la réalisation d'audits de grande qualité.

Étendue

Le présent document traite plus particulièrement des facteurs à considérer pour l'audit des produits tirés du minage de cryptoactifs. Ces facteurs s'appliquent aux sociétés qui mènent leurs propres opérations de minage ou aux mineurs faisant partie d'un groupe. Les présentes indications ont été élaborées dans le contexte d'une société ouverte qui applique les normes IFRS, notamment afin d'illustrer certaines questions d'intérêt; cependant, les entités qui appliquent d'autres normes comptables peuvent aussi s'appuyer sur ces indications, dans la mesure où les dispositions comptables qu'elles suivent s'apparentent à celles énoncées dans les normes IFRS.

Foire aux questions (FAQ)

Les questions qui suivent sont traitées sous forme de FAQ :

1. Pourquoi peut-il être difficile d'auditer un cryptomineur?
2. À quoi un cryptomineur peut-il s'attendre de la part de l'auditeur lorsque ce dernier met en œuvre les procédures d'acceptation de la relation client en vue d'un audit?
3. Comme les transactions sont enregistrées dans la chaîne de blocs, l'auditeur peut-il simplement s'appuyer sur la chaîne de blocs même?
4. L'auditeur peut-il s'appuyer sur les transactions confirmées auprès du groupe de minage?
5. Quels types de contrôles, y compris les contrôles généraux informatiques (CGI), l'auditeur pourrait vouloir comprendre et tester?
6. Quels sont les contrôles généralement nécessaires à l'égard des actifs physiques de minage?
7. Quels autres facteurs faut-il prendre en considération lorsque le cryptomineur héberge des machines utilisées par des tiers?

Annexe – Exemples illustratifs

Deux exemples de procédures analytiques de corroboration sont présentés en annexe. Ces exemples, qui comportent divers degrés de complexité, illustrent les données qui peuvent être requises pour définir des attentes à un niveau de précision approprié.

Les questions abordées dans le présent document ne sont pas exhaustives, et les exemples fournis le sont à des fins d'illustration seulement. Le caractère approprié des procédures d'audit dépend des faits et circonstances propres à l'entité et des risques d'audit. L'approche adoptée doit être adaptée en conséquence.

Foire aux questions

1. Pourquoi peut-il être difficile d'auditer un mineur?

Le pseudo-anonymat de la chaîne de blocs peut poser des défis uniques pour l'audit et la mise en place par la direction d'un environnement de contrôle robuste. Il peut notamment être difficile pour l'entité de prouver qu'elle s'est acquittée de ses obligations de prestation (comme l'exigent les normes comptables sur la comptabilisation des produits) et de démontrer la propriété des actifs numériques.

La norme *Produits des activités ordinaires tirés de contrats conclus avec des clients*[1] énonce cinq conditions permettant de déterminer s'il y a lieu de comptabiliser des produits. L'émetteur assujetti s'appuie sur ces conditions pour déterminer quand il y a lieu de comptabiliser les produits tirés du minage, et l'auditeur en tient compte lorsqu'il met en œuvre des procédures d'audit à l'égard des produits. Il pourrait notamment être insuffisant pour la direction de s'appuyer simplement sur les cryptoactifs qu'elle a reçus pour justifier la comptabilisation de produits. Elle doit démontrer qu'elle

1 IFRS 15, *Produits des activités ordinaires tirés de contrats conclus avec des clients*, paragraphe 9.

s'est acquittée de son obligation de prestation (au sens d'IFRS 15), c'est-à-dire que l'entité de minage a fourni un service pour lequel elle a été dûment rétribuée, ce que l'auditeur doit vérifier. Autrement, il pourrait être difficile pour l'entité de démontrer qu'elle a gagné tous les produits comptabilisés ou qu'elle a reçu tous les produits auxquels elle a droit.

De plus, dans un audit des états financiers, l'auditeur est tenu d'identifier et d'évaluer les risques d'anomalies significatives résultant de fraudes[2]. Le modèle d'entreprise associé au minage de cryptoactifs présente des occasions uniques de perpétrer une fraude. En voici quelques exemples :

- Le mineur « simule » la génération de produits tirés de la puissance de hachage fournie au groupe de minage en se servant d'un accord distinct (p. ex., un accord d'emprunt, un accord conclu avec une partie liée) conclu avec une autre partie en vue du dépôt de cryptoactifs ou de frais d'opérations dans ses portefeuilles de primes de minage. Si l'auditeur n'est pas informé de cet accord, le mineur pourrait tenter de présenter les actifs empruntés qu'il a reçus à titre de produits dans ses états financiers.
- Une personne au sein de l'entité accède, sans l'autorisation de la direction, au matériel de minage et redirige une partie de la puissance de hachage vers un portefeuille qui n'est pas affilié à la société. Cette activité mène à une diminution des produits de l'entité et au détournement de ses actifs (par le vol de puissance de hachage, de primes ou d'électricité).
- Un groupe de minage ne fournit pas à l'un de ses participants la quote-part des primes de minage qui lui revient, ce qui a pour effet de diminuer sa rétribution et de réduire les produits de l'entité.

Cette liste d'exemples n'est pas exhaustive, mais elle illustre les occasions de fraudes propres au secteur du minage de cryptoactifs. Les procédures de corroboration pourraient ne pas fournir à elles seules à l'auditeur les éléments probants nécessaires pour répondre à ces risques; l'auditeur pourrait alors devoir s'appuyer sur la mise en place par l'entité des contrôles internes appropriés pour atténuer ces risques[3].

2. À quoi un cryptomineur peut-il s'attendre de la part de l'auditeur lorsque ce dernier met en œuvre les procédures d'acceptation de la relation client en vue d'un audit?

Compte tenu des difficultés sur le plan de l'audit dans le secteur, l'auditeur peut devoir mettre en œuvre des procédures additionnelles pour respecter les exigences du cabinet en matière d'acceptation de la relation client. Il pourrait s'agir de procédures approfondies afin de comprendre les opérations de l'entité, notamment des tests de cheminement des contrôles et l'obtention et l'analyse de contrats. Ces procédures visent à évaluer l'environnement et la structure de contrôle actuels afin de déterminer si l'entité a mis en place les processus, les systèmes et les contrôles appropriés pour présenter les résultats de ses activités de minage. Ces informations peuvent aider l'auditeur à déterminer s'il peut s'attendre à obtenir des éléments probants suffisants et appropriés

2 NCA 240, *Responsabilités de l'auditeur concernant les fraudes lors d'un audit d'états financiers*, paragraphes 17 et 24.

3 NCA 330, *Réponses de l'auditeur à l'évaluation des risques*, paragraphe 8b).

à l'égard des états financiers pris dans leur ensemble. Si ces procédures ne sont pas mises en œuvre avant l'acceptation de la relation client, l'auditeur pourrait devoir se retirer de la mission ultérieurement s'il n'est pas en mesure d'obtenir des éléments probants suffisants et appropriés.

Pour ce qui est des contrôles, l'auditeur peut procéder à des demandes d'informations à l'égard d'aspects comme la comptabilisation des produits, l'exhaustivité des produits, y compris les considérations relatives à la fiabilité des données sous-jacentes, aux actifs de minage, à la lutte contre le blanchiment d'argent, à la connaissance du client, aux parties liées, etc. Il peut également demander des informations concernant les fournisseurs de services qui sont concernés par les cryptoactifs de l'entité, tels que les dépositaires ou les plateformes de négociation de cryptoactifs. L'auditeur peut envisager de réaliser des tests des contrôles préalables afin d'évaluer l'efficacité de leur conception et de leur fonctionnement avant l'acceptation. La complexité des systèmes peut également nécessiter le recours à l'informatique, à la chaîne de blocs ou à d'autres spécialistes pour l'évaluation des contrôles.

L'auditeur peut demander un échantillon de contrats, comme ceux qui sont conclus avec un groupe de minage. La structure de ces accords peut être très complexe et influer grandement sur l'audit et la comptabilité, deux éléments que l'auditeur doit comprendre.

En outre, l'auditeur peut poser des questions sur les sources de financement ainsi que sur la structure de direction et de gouvernance de l'entité, y compris le niveau d'expérience de la direction en matière d'information financière et de cryptoactifs. Le manque d'expérience de la direction dans l'un ou l'autre de ces aspects peut entraver le processus d'acceptation de la relation client de l'auditeur.

Dans bien des cas, ces procédures nécessitent plus de temps que les procédures d'acceptation de la relation client dans d'autres secteurs, possiblement moins complexes. Les entités doivent être au fait de cette réalité lorsqu'elles envisagent de retenir les services d'un cabinet d'audit. L'auditeur pourrait aussi devoir mettre en œuvre ces procédures approfondies annuellement afin de respecter les exigences du cabinet en matière de maintien de la relation client.

Il est fortement recommandé que la direction mette en place des activités de contrôle et des structures de gouvernance appropriées et vérifiables avant de s'entretenir avec un auditeur potentiel, puisqu'elles favorisent un environnement de contrôle robuste. C'est particulièrement vrai pour les émetteurs assujettis qui ont aussi des obligations d'attestation à l'égard de l'efficacité du fonctionnement des contrôles.

3. Comme les transactions sont enregistrées dans la chaîne de blocs, l'auditeur peut-il simplement s'appuyer sur la chaîne de blocs même?

Remonter jusqu'à la chaîne de blocs peut permettre de valider que le cryptoactif existe, mais pas que l'obligation de prestation[4] est remplie. Ce n'est donc pas une façon d'obtenir des éléments probants suffisants à l'appui de la comptabilisation des produits.

4 IFRS 15, paragraphe 31.

La chaîne de blocs ne permet pas non plus de démontrer l'exhaustivité des produits, puisqu'elle n'indique pas la part des produits à laquelle l'entité a réellement droit. Autrement dit, la chaîne de blocs ne montre que le transfert d'un cryptoactif à l'entité.

Enfin, c'est à l'entité qu'il revient de démontrer que le cryptoactif dans la chaîne de blocs lui appartient réellement étant donné que la chaîne de blocs en soi ne peut confirmer la propriété. L'accès à un portefeuille de cryptoactifs ne prouve pas, à lui seul, la propriété. Pour de plus amples indications sur la propriété, consulter la publication sur la **collecte d'éléments probants à l'appui de l'assertion relative à la propriété** de CPA Canada.

Les éléments probants recueillis grâce à la chaîne de blocs devront être conjugués à d'autres procédures d'audit afin d'obtenir des éléments probants sur l'exhaustivité et la réalité des produits.

Ces procédures peuvent notamment consister en ce qui suit :

- Procédures portant sur le contrôle à l'égard des systèmes de suivi internes visant à mesurer la puissance de hachage
- Procédures portant sur le contrôle à l'égard du matériel de minage de l'entité
- Confirmation auprès du groupe de minage (si un tel groupe est utilisé)
- Utilisation par l'auditeur des analyses effectuées par la direction dans son environnement de contrôle afin d'appuyer ses procédures analytiques
- D'autres procédures de corroboration, comme l'évaluation des produits attendus selon d'autres variables vérifiables. Un exemple d'analyse de cette nature est présenté en **annexe**; il est possible de combiner cette analyse à d'autres méthodes et éléments probants afin de répondre aux exigences relatives à la comptabilisation des produits en ne s'appuyant pas uniquement sur les montants reçus comme éléments probants.

Il convient de noter que l'utilisation d'une procédure analytique de corroboration exige beaucoup de travail de la part de l'auditeur. L'analyse requiert un degré de précision élevé et l'évaluation de la pertinence et de la fiabilité de toutes les données significatives exige beaucoup de travail en raison du profil de risque des cryptoactifs.

Enfin, si l'auditeur utilise des outils pour évaluer la chaîne de blocs, il doit également en déterminer la fiabilité[5]. Pour connaître les facteurs que l'auditeur peut considérer pour établir la fiabilité d'une chaîne de blocs (en tant que source d'informations) et le caractère approprié des ressources technologiques, comme les explorateurs de blocs (qui sont utilisés pour afficher les informations enregistrées dans une chaîne de blocs), consulter la publication ***Pertinence et fiabilité des informations provenant d'une chaîne de blocs*** de CPA Canada.

5 NCA 500, *Éléments probants*, paragraphe 9.

4. L'auditeur peut-il s'appuyer sur les transactions confirmées auprès du groupe de minage?

Si l'auditeur prévoit d'utiliser les confirmations de tiers, il doit évaluer la pertinence et la fiabilité des informations[6]. À la date de la présente publication, la plupart des groupes de minage de cryptoactifs au Canada n'ont pas de rapports sur les contrôles, comme un rapport sur les contrôles au niveau du système ou de l'organisation (SOC) 1. Lorsqu'il y a un rapport SOC 1 de type 2, l'auditeur peut l'utiliser pour déterminer si les informations présentées par l'exploitant du groupe de minage font l'objet de contrôles qui sont adéquatement conçus et mis en œuvre et qui fonctionnent efficacement[7]. Lorsque l'auditeur n'est pas en mesure d'utiliser un rapport SOC 1 de type 2, il doit trouver d'autres moyens de vérifier la fiabilité des informations fournies par le groupe (vérification externe des données d'entrée, conformité aux documents de la direction, etc.)[8]. Ce processus ramène souvent l'auditeur aux systèmes utilisés par l'entité pour faire le suivi du pouvoir de hachage et démontrer la satisfaction de l'obligation de prestation génératrice de produits. Pour de plus amples indications sur les tiers fournisseurs de services, consulter la publication ***Considérations liées aux tiers fournisseurs de services*** de CPA Canada.

Il est important que l'auditeur comprenne bien la relation entre l'entité auditée et le groupe afin d'évaluer les éléments probants requis pour auditer les produits tirés du groupe. Dans certains cas, l'auditeur peut réaliser l'audit sans la participation du groupe, mais il devra comprendre les mécanismes utilisés par celui-ci pour mesurer les primes et les répartir entre les participants.

L'auditeur doit aussi mettre en œuvre des procédures pour s'assurer que les produits tirés des cryptoactifs proviennent réellement du groupe et non d'autres sources, ce qui pourrait être un indice de fraude, comme il est expliqué à la question 1.

5. Quels types de contrôles, y compris les contrôles généraux informatiques (CGI), l'auditeur pourrait vouloir comprendre et tester?

L'entité doit pouvoir démontrer qu'elle s'est acquittée de son obligation de prestation liée aux produits tirés du cryptominage. Elle ne peut pas s'appuyer uniquement sur la chaîne de blocs ou les versements du groupe pour comptabiliser les produits. L'auditeur doit s'assurer de comprendre les contrôles mis en place par la direction à l'égard des produits tirés du minage, qui peuvent être très sophistiqués. Outre les contrôles à l'égard des produits, l'auditeur peut s'attendre à retrouver une combinaison des contrôles suivants :

- Contrôles physiques à l'égard du matériel de minage
- Systèmes de suivi du minage
- Contrôles liés à la lutte contre le blanchiment d'argent ou à la connaissance du client lors de l'achat ou de la vente de cryptoactifs ou de la conclusion de contrats générateurs de produits liés au minage
- CGI

6 NCA 500, paragraphe 7.

7 NCA 402, *Facteurs à considérer pour l'audit d'entités faisant appel à une société de services*, paragraphe 17.

8 NCA 402, paragraphes 12b) à 12d).

Si l'entité détient des cryptoactifs découlant d'activités de minage, elle devrait avoir mis en place des contrôles à l'égard des portefeuilles, notamment concernant la séparation appropriée des tâches, la création de clés privées et la gestion du cycle de vie, ainsi que d'autres contrôles à l'égard de l'existence, et des droits et obligations.

Certains CGI standard revêtent une importance accrue en raison des risques liés au détournement de cryptoactifs. La section qui suit présente une liste non exhaustive des types de contrôles qu'une entreprise de minage devrait normalement mettre en place. Chaque entreprise de minage est unique et peut structurer ses contrôles de différentes façons en vue d'atteindre les mêmes objectifs.

- **Contrôles d'accès logique** à l'égard de l'attribution, de l'examen périodique et de la révocation des comptes d'utilisateurs. Doivent notamment être pris en considération les noms d'utilisateurs et les mots de passe permettant l'accès au matériel de minage, l'endroit où sont définis les membres du groupe et les portefeuilles de primes, ou le logiciel de gestion collective, le cas échéant. Un membre de la direction doit approuver l'autorisation d'accès initiale, et la preuve de cette approbation doit être conservée. La revue périodique des accès consiste à obtenir une liste des utilisateurs pour chaque machine ainsi que tout logiciel utilisé pour gérer l'ensemble des machines, et à demander à un membre de la direction de passer en revue la liste des utilisateurs et le niveau d'accès accordé. Si des employés quittent l'entreprise ou changent de rôle, il faut conserver la preuve que leur accès utilisateur a été révoqué, généralement dans les 24 heures ou moins suivant l'événement.
- **Contrôles sur les modifications** du code de programmation utilisé dans les opérations.
  - Lorsqu'un client emploie des codes personnalisés, les programmeurs ne doivent pas avoir accès à la version de production du code. Le code doit plutôt être migré de l'environnement de développement vers un référentiel de codes. Un groupe de test doit récupérer le code dans le référentiel et le mettre en œuvre dans un environnement de test ou d'acceptation par l'utilisateur afin d'en tester le fonctionnement. Une fois les tests d'acceptation par l'utilisateur réussis, le code est mis en œuvre dans l'environnement de production par un administrateur de système autre que le programmeur.
  - Lorsque le client emploie un logiciel acheté, il faut réaliser des tests d'acceptation par l'utilisateur similaires avant de migrer le logiciel dans l'environnement de production.
  - Un système de suivi de l'intégrité des fichiers doit être utilisé pour détecter les modifications apportées au logiciel ou aux configurations des serveurs et des machines de minage afin de détecter les modifications non autorisées, y compris celles apportées aux configurations du groupe de minage et au portefeuille de primes.
- **Contrôles de gestion des opérations,** notamment la surveillance des machines de minage, de la consommation d'énergie ou des interruptions, et le processus de suivi afin que les mineurs arrêtés puissent reprendre la production. Cela permettra de réduire le risque que le matériel de minage soit à tort considéré comme étant en panne, tandis que sa puissance de hachage est détournée par des employés à des fins personnelles.

6. Quels sont les contrôles généralement nécessaires à l'égard des actifs physiques de minage?

Grâce à des procédures de contrôle, les auditeurs devront peut-être obtenir des éléments probants à l'égard de l'existence des actifs significatifs utilisés dans les opérations de minage. Les contrôles peuvent notamment être associés à ce qui suit :

- Les restrictions limitant l'accès physique au matériel
- Le dénombrement et l'inspection physique réguliers du matériel
- L'achat et la cession du matériel
- Le suivi du temps de fonctionnement et des interruptions
- Les obligations en vertu d'un contrat d'achat d'énergie, etc.

7. Quels autres facteurs faut-il prendre en considération lorsque le cryptomineur héberge des machines utilisées par des tiers?

L'hébergement d'une opération de cryptominage requiert une infrastructure considérable; il n'est donc pas rare que les mineurs hébergent leur propre matériel de minage en plus de celui de tiers ou qu'ils louent leur matériel à des tiers. La complexité s'accroît lorsque l'entité visée par l'audit héberge des machines pour d'autres entités. Par exemple, comment la société vérifie-t-elle comme il se doit l'apport relatif de chaque machine afin de veiller à l'attribution et à la répartition adéquates des cryptoactifs? Cela indique encore une fois la nécessité pour l'auditeur de bien comprendre tous les accords conclus en matière de minage pour pouvoir identifier et évaluer les risques et de mettre en place une stratégie d'audit appropriée.

Les accords d'hébergement peuvent soulever diverses questions liées à la présentation de l'information financière (et considérations relatives à l'audit), entre autres concernant la répartition des produits et des charges, et la propriété des actifs.

Annexe – Exemples illustratifs

Analyse des produits tirés du minage de bitcoins

Voici des exemples de procédures analytiques de corroboration qu'un auditeur peut préparer pour prédire les produits qui devraient être tirés du minage de bitcoins. Le caractère approprié des procédures d'audit dépend des faits et circonstances propres à l'entité et des risques d'audit identifiés dans le cadre de la mission. La stratégie et les procédures d'audit sont adaptées en fonction de ces faits et circonstances.

Le réseau Bitcoin est calibré de façon qu'un nouveau bloc soit découvert toutes les 10 minutes environ. Si la capacité de minage en ligne augmente et que le temps requis entre la découverte des blocs passe à moins de 10 minutes, le réseau rehausse automatiquement le niveau de difficulté afin que le minage d'un bloc nécessite plus de travail, pour que la durée moyenne soit à nouveau de 10 minutes. Inversement, si la capacité de minage en ligne diminue et que le temps requis entre la découverte des blocs dépasse 10 minutes, le niveau de difficulté est rabaissé pour revenir à une durée moyenne de 10 minutes. Grâce à ce mécanisme d'autoajustement, environ 144 nouveaux blocs sont ajoutés au réseau Bitcoin chaque jour, comme l'indique l'équation D présentée dans l'exemple 1 plus bas.

Le calcul de la rétribution reçue en contrepartie de la découverte d'un nouveau bloc repose sur un modèle prédéterminé incorporé dans la chaîne de blocs Bitcoin. Cette rétribution est réduite de moitié tous les 210 000 blocs, ce qui équivaut à environ 4 ans. La rétribution, qui était de 50 bitcoins en 2009, est passée à 25 en 2013, puis à 12,5 en 2015, et est maintenant de 6,25 bitcoins depuis 2020, comme il est indiqué dans les exemples illustratifs.

Étant donné la nature du minage, les rétributions qu'une organisation reçoit pour ses activités de minage en solo, c'est-à-dire qu'elle mine seule et ne partage pas sa capacité informatique ni ses primes avec d'autres, sont foncièrement inégales. Pendant certaines périodes, l'organisation ne recevra rien du tout, puis elle réussira à miner un bloc, ce qui lui procurera, pour un temps, des revenus nettement plus élevés que la moyenne à long terme. De ce fait, les revenus tirés de petites opérations de minage en solo sont très difficiles à prédire et se prêtent mal à cette analyse. Les mineurs font souvent partie de groupes, qui mettent en commun la puissance informatique de plusieurs milliers d'ordinateurs de minage appartenant à différentes entités et qui partagent les revenus. De cette façon, les revenus sont répartis de façon beaucoup plus égale et se prêtent bien à l'analyse. Habituellement, l'exploitant du groupe exige le paiement de frais, par exemple 1 %, pour couvrir les dépenses liées à l'administration du groupe. Le mineur doit déduire ces frais de ses revenus attendus.

L'auditeur doit valider toutes les données d'entrée importantes de ce modèle, notamment le taux de hachage de la machine, du client et du réseau, les frais d'administration du groupe de minage, le cours du bitcoin, la consommation réelle d'électricité par machine, la consommation totale d'énergie par facture de services publics et les derniers revenus provenant du groupe de minage. La consommation réelle d'électricité sert également à vérifier les déclarations de la direction concernant le temps d'utilisation de la machine. Il faut ensuite comparer les produits attendus aux résultats réels, et analyser les écarts afin d'en déterminer la source et le caractère raisonnable compte tenu du seuil de signification du client.

Exemple 1

Le premier exemple illustre le calcul des produits annuels attendus d'un seul ordinateur de minage ayant une puissance de hachage de 110 terahash par seconde (Th/s) et une consommation énergétique de 3 250 watts. Le taux de hachage est la mesure de la puissance de calcul de l'ordinateur de minage; plus le taux est élevé, plus l'est également la puissance de minage. Les ordinateurs de minage peuvent avoir différents taux de hachage. Il faut donc ajuster ce taux selon le matériel utilisé dans une opération de minage donnée. Dans cet exemple, on présume que le temps de fonctionnement de l'ordinateur seul est de 100 %.

Exemple 2

Le deuxième exemple illustre les pourcentages de temps de fonctionnement par mois de 20 ordinateurs de minage. Les machines 1 à 4 sont vendues à la fin de l'exercice, de sorte qu'elles présentent, à la fin de l'exercice, un taux de fonctionnement de 0 %; les machines 15 à 20 sont achetées en cours d'exercice, de sorte qu'elles présentent, au début de l'exercice, un taux de fonctionnement de 0 %. Les autres pourcentages de temps de fonctionnement tiennent compte des problèmes techniques, des pannes d'électricité, de l'entretien et de la mise en veille volontaire des machines par le mineur. Le calcul du total des équivalents machine figure en bas, ainsi que les produits annuels attendus pour le groupe et la consommation d'électricité prévue.

EXEMPLE 1 : RÉSULTATS ATTENDUS POUR UNE MACHINE AVEC UN TEMPS DE FONCTIONNEMENT DE 100 %

Mois (2021)	Taux de hachage – client (Th/s) A	Taux de hachage – réseau (Th/s) B[9]	Nombre de jours par mois C	Blocs par mois D = C x 144	Prime par bloc (BTC) E	Frais d'administration F	Produits attendus (BTC) G = (A/B) x D x E x (1-F)	Cours du bitcoin ($ CA) H[10, 11]	Produits attendus ($ CA) I = G x H	Heures J = C X 24	Puissance (watts) K	Consommation d'électricité (kWh) L = J x K / 1 000
Jan	110	149 196 972	31	4 464	6,25	1 %	0,02036	44 064	897	744	3 250	2 418
Fév	110	155 100 116	28	4 032	6,25	1 %	0,01769	58 315	1 032	672	3 250	2 184
Mar	110	159 601 625	31	4 464	6,25	1 %	0,01904	68 467	1 304	744	3 250	2 418
Avr	110	157 234 579	30	4 320	6,25	1 %	0,01870	71 385	1 335	720	3 250	2 340
Mai	110	161 245 123	31	4 464	6,25	1 %	0,01884	57 123	1 076	744	3 250	2 418
Juin	110	120 098 019	30	4 320	6,25	1 %	0,02448	43 867	1 074	720	3 250	2 340
Juil	110	100 355 391	31	4 464	6,25	1 %	0,03028	42 881	1 298	744	3 250	2 418
Août	110	120 709 404	31	4 464	6,25	1 %	0,02517	57 390	1 445	744	3 250	2 418
Sep	110	136 607 014	30	4 320	6,25	1 %	0,02152	58 345	1 256	720	3 250	2 340
Oct	110	149 109 956	31	4 464	6,25	1 %	0,02038	71 330	1 454	744	3 250	2 418
Nov	110	160 886 125	30	4 320	6,25	1 %	0,01828	76 494	1 398	720	3 250	2 340
Déc	110	173 191 889	31	4 464	6,25	1 %	0,01754	63 546	1 115	744	3 250	2 418
Total							**0,25228**	**713 207**	**14 684**			**28 470**

9 Source des moyennes mensuelles du taux de hachage du bitcoin (Th/s) : www.blockchain.com/charts/hash-rate

10 Source des moyennes mensuelles des cours du marché en dollars américains dans les échanges importants de bitcoins : www.blockchain.com/charts/market-price

11 Source des moyennes mensuelles des taux de change pour la conversion du dollar américain en dollar canadien : www.banqueducanada.ca/taux/taux-de-change

EXEMPLE 2 : RÉSULTATS ATTENDUS POUR 20 MACHINES AVEC UN TEMPS DE FONCTIONNEMENT VARIABLE

Mois (2021)	Eqn	Jan	Fév	Mar	Avr	Mai	Juin	Juil	Août	Sep	Oct	Nov	Déc	Total
Produits – temps de fonctionnement de 100 % par machine ($ CA)	**A**	897	1 032	1 304	1 335	1 076	1 074	1 298	1 445	1 256	1 454	1 398	1 115	14 684
Consommation d'électricité (kWh) – temps de fonctionnement de 100 % par machine	**B**	2 418	2 184	2 418	2 340	2 418	2 340	2 418	2 418	2 340	2 418	2 340	2 418	28 470
Machine 1		96 %	95 %	95 %	96 %	99 %	93 %	98 %	100 %	17 %	0 %	0 %	0 %	
Machine 2		97 %	99 %	99 %	95 %	97 %	95 %	96 %	96 %	96 %	9 %	0 %	0 %	
Machine 3		93 %	95 %	95 %	98 %	99 %	95 %	99 %	100 %	93 %	2 %	0 %	0 %	
Machine 4		93 %	96 %	95 %	94 %	97 %	98 %	96 %	94 %	98 %	95 %	14 %	0 %	
Machine 5		97 %	98 %	94 %	96 %	94 %	99 %	95 %	100 %	97 %	96 %	12 %	17 %	
Machine 6		97 %	99 %	95 %	97 %	99 %	97 %	94 %	98 %	99 %	95 %	95 %	94 %	
Machine 7		96 %	97 %	95 %	93 %	97 %	97 %	97 %	95 %	99 %	97 %	99 %	95 %	
Machine 8		94 %	93 %	97 %	97 %	98 %	96 %	98 %	97 %	100 %	94 %	93 %	97 %	
Machine 9		94 %	99 %	99 %	96 %	99 %	100 %	96 %	95 %	94 %	94 %	97 %	98 %	
Machine 10		99 %	99 %	93 %	99 %	100 %	96 %	94 %	99 %	94 %	99 %	100 %	97 %	
Machine 11		93 %	97 %	97 %	93 %	95 %	94 %	98 %	97 %	95 %	100 %	94 %	97 %	
Machine 12		95 %	97 %	93 %	94 %	97 %	98 %	99 %	96 %	98 %	96 %	94 %	99 %	
Machine 13		98 %	95 %	100 %	94 %	99 %	96 %	98 %	96 %	96 %	93 %	96 %	93 %	
Machine 14		95 %	94 %	97 %	100 %	99 %	95 %	100 %	98 %	99 %	96 %	99 %	98 %	
Machine 15		0 %	4 %	94 %	95 %	94 %	94 %	96 %	98 %	97 %	96 %	96 %	96 %	
Machine 16		0 %	0 %	7 %	97 %	99 %	98 %	93 %	93 %	98 %	99 %	97 %	94 %	
Machine 17		0 %	0 %	0 %	16 %	97 %	96 %	100 %	94 %	99 %	98 %	95 %	95 %	
Machine 18		0 %	0 %	0 %	0 %	17 %	95 %	94 %	98 %	96 %	100 %	97 %	97 %	
Machine 19		0 %	0 %	0 %	0 %	0 %	17 %	98 %	100 %	99 %	98 %	97 %	93 %	
Machine 20		0 %	0 %	0 %	0 %	0 %	0 %	8 %	96 %	95 %	96 %	97 %	93 %	
Total des équivalents machine	**C**	**1337 %**	**1357 %**	**1445 %**	**1550 %**	**1676 %**	**1749 %**	**1847 %**	**1940 %**	**1859 %**	**1653 %**	**1472 %**	**1453 %**	
Produits attendus ($ CA)	**D = A x C**	11 993	14 004	18 843	20 693	18 034	18 784	23 974	28 033	23 349	24 035	20 579	16 201	238 522
Consommation d'électricité prévue (kWh)	**E = B x C**	32 329	29 637	34 940	36 270	40 526	40 927	44 660	46 909	43 501	39 970	34 445	35 134	459 248

Remerciements

CPA Canada souhaite exprimer sa gratitude au Groupe de discussion sur l'audit des cryptoactifs 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 discussion est composé de représentants du Conseil canadien sur la reddition de comptes, des responsables provinciaux de l'inspection professionnelle, d'universitaires et de bénévoles provenant des cabinets canadiens suivants : BDO, Deloitte, Davidson & Company, EY, KPMG, MNP, PwC et Raymond Chabot Grant Thornton.

CPA Canada tient à remercier PwC, qui a dirigé la rédaction du présent document, et EY, qui a fourni les exemples illustratifs au nom du groupe de discussion.

Autres ressources

Consultez la page Ressources sur la chaîne de blocs et les cryptoactifs pour les CPA de CPA Canada; vous y trouverez les articles suivants ainsi que d'autres ressources pertinentes pour les CPA :

1. Facteurs à considérer pour l'audit des actifs et des transactions en cryptomonnaie (2018)
2. Points de vue (audit des cryptoactifs) : Tests des contrôles et assertion relative à la propriété (2020)
3. Points de vue (audit des cryptoactifs) : Pertinence et fiabilité des informations provenant d'une chaîne de blocs (2020)
4. L'audit des cryptoactifs : considérations liées aux tiers fournisseurs de services (série Points de vue) (2021)

Commentaires

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

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