CANADIAN PUBLIC ACCOUNTABILITY BOARD

CONSEIL CANADIEN SUR LA REDDITION DE COMPTES

CPAB

CCRC

# La pratique de l’audit dans le secteur des cryptoactifs

## Introduction

Bien des émetteurs assujettis évoluant dans le secteur canadien des cryptoactifs ont fait l’acquisition de portefeuilles de cryptoactifs significatifs ou se sont engagés dans des activités de cryptominage importantes au cours de leur plus récent exercice visé par un audit. La planification et l’exécution de ces audits ont d’ailleurs commencé.

Le CCRC publiera des communications pour exprimer son point de vue et ses attentes à l’égard des auditeurs dans le contexte de l’audit d’émetteurs assujettis évoluant dans le secteur des cryptoactifs.

Bien que la présente communication mette en lumière nos attentes à l’égard de plusieurs enjeux d’audit, elle ne doit pas être considérée comme un programme d’audit. Pour la planification et l’exécution de leurs audits, les auditeurs doivent plutôt se référer aux normes d’audit pertinentes.

## Existence des cryptoactifs et droits de propriété connexes

### Existence

Lorsqu’une entité s’appuie sur une chaîne de blocs pour étayer la réalité / l’existence des opérations sur des cryptoactifs / des soldes de cryptoactifs comptabilisés dans ses états financiers, ses auditeurs doivent démontrer qu’ils comprennent la façon dont ces opérations ont été comptabilisées dans le registre fondé sur la chaîne de blocs applicable.

Les protocoles et les procédés cryptographiques associés aux chaînes de blocs visent à accroître la résilience des registres fondés sur une chaîne de blocs face aux risques de falsification. L’efficacité de ces attributs varie toutefois d’une chaîne de blocs à l’autre, et les auditeurs ne peuvent s’appuyer sur ces registres sans avoir d’abord évalué la fiabilité des chaînes de blocs pertinentes aux fins de l’audit. Nous nous attendons à ce que les auditeurs fassent appel à des spécialistes de la chaîne de blocs et à des cryptographes pour qu’ils les

aident à comprendre et à évaluer les chaînes de blocs à l'appui des montants comptabilisés dans les documents comptables d'une entité présentant un risque d'anomalies significatives[1].

Les auditeurs doivent identifier les *risques* pertinents liés à la réalité / l'existence de cryptoactifs dans la chaîne de blocs et en consigner leur compréhension, y compris i) le risque que des opérations non valides soient enregistrées dans la chaîne de blocs; ii) le risque que des opérations validées n'y soient pas enregistrées; et iii) le risque que des opérations validées aient été modifiées ultérieurement. Ils doivent aussi identifier les *attributs* pertinents de la chaîne de blocs (p. ex., procédés cryptographiques, algorithmes de validation de chaînes de blocs et mécanismes de concertation) qui permettent d'atténuer ces risques, puis procéder à des vérifications leur permettant de s'assurer que ces attributs fonctionnent comme prévu.

Lorsqu'ils vérifient la réalité des opérations sur des cryptoactifs et l'existence des soldes de cryptoactifs de l'entité en fin d'exercice, les auditeurs utilisent généralement des outils appelés «explorateurs de blocs» pour examiner les informations consignées dans les registres fondés sur la chaîne de blocs. Ils doivent appliquer des procédures pour s'assurer que ces outils sont conçus et fonctionnent efficacement afin de permettre l'extraction des informations pertinentes de la chaîne de blocs.

### Droits de propriété

Les opérations sur des cryptoactifs assurent un certain degré de confidentialité, car les registres fondés sur la chaîne de blocs représentent l'identité des entités qui les ont réalisées par une séquence de caractères alphanumériques propre à chaque adresse publique.

Pour évaluer l'assertion de l'entité relative à la propriété, les auditeurs doivent concevoir une stratégie d'audit visant l'obtention d'éléments probants suffisants et appropriés à l'égard de la détention par l'entité des cryptoactifs associés à une adresse publique.

Ainsi, les auditeurs peuvent demander à la direction de transférer un certain solde de cryptoactifs entre des cryptoportefeuilles contrôlés par l'entité, puis inspecter l'enregistrement correspondant dans la chaîne de blocs afin de vérifier la réalité de l'opération. Ils peuvent aussi lui demander de signer des messages arbitraires pour prouver qu'elle a accès à la clé privée permettant de contrôler un cryptoactif.

Les procédures précitées peuvent s'avérer utiles pour vérifier l'accès d'une entité à une telle clé privée et le contrôle qu'elle exerce sur les actifs connexes. Les auditeurs ne doivent toutefois pas considérer pour autant que l'accès d'une entité à une clé privée signifie que cette entité détient les droits de propriété connexes. Il subsiste un risque que l'entité partage la séquence alphanumérique correspondant à cette clé privée avec des tiers, de telle sorte que d'autres entités ou personnes physiques pourraient revendiquer la détention des droits de propriété du même cryptoactif.

[1] NCA 620, *Utilisation par l'auditeur des travaux d'un expert de son choix, par. 7*

Nous nous attendons à ce que, dans le cadre de la plupart des audits de ce type, les auditeurs évaluent le risque de fausse déclaration sur les droits de propriété comme s'il s'agissait d'un risque de fraude et à ce qu'ils conçoivent des procédures permettant d'atténuer ce risque[2].

Bien qu'il soit nécessaire de concevoir des procédures de corroboration visant essentiellement à vérifier qu'une entité a accès à la clé privée contrôlant un cryptoactif, il est peu probable que de telles procédures suffisent à atténuer le risque de fraude.

À notre avis, des contrôles internes efficaces seront essentiels pour que la direction puisse affirmer à ses auditeurs que l'entité détient la propriété exclusive et légitime de ses cryptoactifs. Il sera très difficile pour les auditeurs d'atténuer le risque lié aux droits de propriété associés à de tels cryptoactifs sans comprendre et tester la conception de ces contrôles internes et l'efficacité de leur fonctionnement.

Voici quelques contrôles internes que les entités devraient avoir mis en place et que les auditeurs doivent tester :

- Exécution par les entités de cérémonies des clés[3] – La cérémonie des clés vise à faire en sorte que ces dernières soient générées de façon sécuritaire sur le plan cryptographique et que personne ne puisse en générer des copies non autorisées, de même qu'à s'assurer que les entités sont les propriétaires légitimes des cryptoactifs connexes. Le degré de complexité de la cérémonie des clés varie selon l'importance que revêtent les opérations sur des cryptoactifs pour une entité.

- Mise en place par les entités de contrôles d'accès à plusieurs signatures faisant en sorte que l'exécution de toute opération est préalablement soumise à plusieurs paliers d'approbation

- Mise en place par les entités de contrôles généraux informatiques visant à répondre aux risques liés aux TI dans le contexte des portefeuilles numériques

***Autres aspects à prendre en considération lorsque des clés privées sont détenues par un dépositaire indépendant***

En général, les bourses de cryptomonnaie réalisent des opérations pour le compte de clients en ayant sous leur garde les clés privées qui contrôlent les actifs; elles agissent à titre de courtiers et de dépositaires pour leurs clients.

Contrairement aux dépositaires du secteur des valeurs mobilières classiques, les dépositaires de cryptoactifs et les bourses de cryptomonnaie sont des entités relativement immatures qui demeurent largement non réglementées. À la connaissance du CCRC, aucun rapport de l'auditeur d'une société de services n'atteste l'efficacité des contrôles internes mis en place par

[2] NCA 240, *Responsabilités de l'auditeur concernant les fraudes lors d'un audit d'états financiers*
[3] Le *Statement on Auditing Standard* No. 70 (SAS 70), *Service Organizations*, de l'AICPA présente de l'information supplémentaire sur les cérémonies des clés.

les bourses de cryptomonnaie et les dépositaires. Le recours à des dépositaires indépendants génère des risques d'audit supplémentaires auxquels doit répondre l'auditeur.

S'il n'y a pas de rapport de l'auditeur d'une société de services portant sur l'efficacité des contrôles pertinents appliqués par une bourse ou un dépositaire et que la réalité des opérations ou l'existence des soldes de clôture représente un risque d'anomalies significatives, l'auditeur doit tester les contrôles internes directement chez le dépositaire ou à la bourse[4].

Nous observons également que plusieurs bourses de cryptomonnaie ont pour pratique d'amalgamer les actifs de leurs clients dans des portefeuilles boursiers. Lorsque des cryptoactifs sont amalgamés, la bourse de cryptomonnaie reflète dans ses registres les opérations sur ces cryptoactifs réalisés entre les acheteurs et les vendeurs, mais pas dans le registre fondé sur la chaîne de blocs applicable (c.-à-d. qu'il s'agit d'opérations hors chaîne). C'est pourquoi, pour les auditeurs, il est impossible en pratique de vérifier la réalité des opérations sur des cryptoactifs de l'entité en se référant à l'enregistrement correspondant dans la chaîne de blocs applicable.

## Produits tirés du cryptominage

Les mineurs de chaîne de blocs sont rétribués en contrepartie de la création de blocs d'opérations validées et de leur intégration à la chaîne de blocs. Un grand nombre d'entre eux regroupent leur puissance de calcul avec celle d'autres mineurs. D'après ce que nous savons, ces groupes de mineurs sont gérés à l'aide de protocoles programmés ou sont administrés par des sociétés ou personnes physiques indépendantes. Lorsqu'un groupe de mineurs ajoute un bloc à une chaîne de blocs et qu'il obtient la rétribution à laquelle donne droit celui-ci, chacun des mineurs participants reçoit sa part de celle-ci, qui est établie suivant l'une des différentes méthodes de répartition possibles.

L'auditeur d'un mineur de cryptoactifs doit élaborer une stratégie d'audit pour tester chacune des principales assertions relatives à la comptabilisation des produits, notamment la réalité, l'exactitude et l'exhaustivité des produits. Lorsqu'une entité tire des produits d'un groupe de minage, l'auditeur doit comprendre les modalités de l'entente conclue avec celui-ci et les risques connexes. Les tests que l'auditeur applique à l'égard de ces produits doivent comprendre des procédures visant à tester l'exactitude et l'exhaustivité des montants attribués à l'entité par le groupe de minage.

Il ne suffit pas à l'auditeur de limiter l'application de ses procédures d'audit des opérations génératrices de produits à la vérification de la rétribution reçue aux fins des activités de validation à l'égard du registre fondé sur la chaîne de blocs. Il doit comprendre comment les produits sont générés, puis élaborer une stratégie d'audit adaptée aux risques identifiés.

[4] NCA 402, *Facteurs à considérer pour l'audit d'entités faisant appel à une société de services*, par. 12

## Autres aspects posant des difficultés

### Dépréciation des actifs de minage

Plusieurs des émetteurs assujettis canadiens qui sont engagés dans des activités de cryptominage ont procédé à l'acquisition de matériel de minage lorsque le cours des cryptoactifs était beaucoup plus élevé qu'actuellement. Ainsi, entre janvier 2018 et le début décembre 2018, la valeur du bitcoin, du ripple et de l'ethereum a chuté d'environ 70 %, 90 % et 85 % respectivement.

La diminution importante du prix des cryptoactifs au cours de la dernière année doit être considérée comme un indice[5] que la valeur comptable du matériel de minage peut avoir subi une dépréciation et que la direction doit donc estimer la valeur recouvrable de ces actifs. Les auditeurs doivent exercer leur esprit critique si les estimations de la direction reposent sur des attentes irréalistes quant à l'évolution du prix des cryptoactifs et de la productivité du matériel de minage.

### Opérations avec les parties liées[6]

Les adresses publiques correspondant à une chaîne de blocs consistent en des séquences de caractères alphanumériques pouvant difficilement être associées aux identités réelles des parties ayant réalisé des opérations sur des cryptoactifs au cours de l'exercice visé par l'audit. Les auditeurs ont du mal à évaluer si la direction a correctement relevé et présenté dans les états financiers de l'entité toutes les opérations sur des cryptoactifs réalisées avec des parties liées.

Les auditeurs seront probablement amenés à considérer qu'il s'agit d'un secteur présentant un risque important. Il leur sera difficile d'obtenir des éléments probants suffisants et appropriés dans les cas où l'entité ne dispose pas de contrôles internes efficaces permettant d'identifier les parties liées et de relever les opérations sur des cryptoactifs réalisées avec celles-ci.

Les auditeurs doivent continuer de mettre en œuvre des procédures d'audit ciblées à l'égard des opérations réalisées avec des parties liées, y compris l'évaluation de la finalité économique des opérations sur des cryptoactifs et, lorsqu'il y a lieu, l'évaluation visant à établir si celles-ci ont été réalisées ou non selon des modalités équivalentes à celles qui prévalent dans le cas d'opérations soumises à des conditions de concurrence normale.

[5] IAS 36, *Dépréciation d'actifs*, par. 12(b)
[6] NCA 550, *Parties liées*

## Évaluation des cryptoactifs[7]

Si les entités évaluent leurs cryptoactifs à leur juste valeur, il est probable que leurs auditeurs considèrent que ces évaluations présentent un risque important.

Dans l'évaluation du caractère raisonnable des évaluations de cryptoactifs d'une entité, les auditeurs sont amenés à se demander s'il existe un marché actif pour ceux-ci (c'est-à-dire si une évaluation de niveau 1 peut être réalisée). Il peut parfois y avoir, pour un cryptoactif donné, plusieurs marchés répondant à la définition d'un marché actif, et chacun de ces marchés peut avoir des prix différents à la date d'évaluation. En pareilles situations, aux fins de la détermination de la valeur des actifs, l'entité doit identifier le marché principal (ou, à défaut, le marché le plus avantageux).

Pour déterminer la valeur de leurs cryptoactifs pour lesquels il existe des marchés actifs, certaines entités utilisent les cours obtenus auprès de fournisseurs de données qui compilent les cours de plusieurs bourses de cryptomonnaie. Les auditeurs doivent alors déterminer si ces cours sont des indicateurs raisonnables que l'entité sera en mesure de vendre le cryptoactif sur son marché principal à la date d'évaluation.

Il arrive souvent qu'aucun marché actif n'existe pour des cryptoactifs, auquel cas l'entité doit recourir à une technique d'évaluation permettant d'en déterminer la valeur. Nous nous attendons à ce que les auditeurs aient recours à des spécialistes de l'évaluation des cryptoactifs lorsqu'il s'agit de cryptoactifs pour lesquels il n'existe pas de marché actif.

## Événements postérieurs à la date de clôture[8]

Comme des risques importants sont liés à l'existence et à la propriété des cryptoactifs, les auditeurs doivent mettre en œuvre des procédures visant à permettre l'obtention d'éléments probants suffisants et appropriés attestant que les actifs n'ont pas été perdus ou compromis (ce qu'il faudrait communiquer dans les états financiers) au cours de la période s'échelonnant entre la date de la fin d'exercice et la date du rapport de l'auditeur. Ces procédures peuvent comprendre un bon nombre de procédures utilisées pour vérifier les soldes de cryptoactifs à la fin de l'exercice.

[7] IFRS 13, *Évaluation de la juste valeur*
[8] NCA 560, *Événements postérieurs à la date de clôture*

## Autres aspects à prendre en compte dans le cadre du processus d'acceptation des clients

Nous avons fait ressortir le fait que les opérations sur des cryptoactifs comportent des risques particuliers face auxquels les auditeurs doivent mettre au point une réponse d'audit globale. Nous avons aussi fait ressortir des cas où, selon nous, il peut s'avérer impossible d'auditer des actifs et opérations liés aux cryptomonnaies sans s'appuyer sur le fonctionnement efficace des contrôles pertinents.

Il nous apparaît évident qu'avant d'accepter des missions de ce type, les cabinets d'audit devront être bien conscients des risques d'audit auxquels ils sont appelés à faire face ainsi que du niveau d'expertise auquel ils devront recourir dans le cadre de l'audit[9]. Dans le cas des clients qu'ils ont déjà acceptés, il ne leur suffira pas d'affirmer que les risques d'audit liés à la présentation de l'information relative à ce nouveau secteur d'activité ne sont pas encore bien compris.

En outre, nous nous attendons toujours à ce qu'avant d'accepter de telles missions, les cabinets d'audit mettent en œuvre des procédures poussées en matière de connaissance de la clientèle.

## Observations finales

Nous encourageons les auditeurs à adopter une stratégie globale leur permettant de répondre aux risques d'audit particuliers qui sont propres au secteur des cryptoactifs. Nous les encourageons également à faire appel à des experts et à procéder aux consultations requises dans le cadre de l'élaboration de leur plan de mission.

Le CCRC prévoit de publier d'autres communications sur ce sujet tandis qu'il en apprendra davantage à cet égard et qu'il procédera à l'inspection d'audits d'émetteurs assujettis évoluant dans ce secteur.

[9] Pour plus d'information sur les exigences de contrôle qualité relatives à l'acceptation des clients, consultez les paragraphes 12 et 13 ainsi que les paragraphes A8 à A10 de la NCA 220, *Contrôle qualité d'un audit d'états financiers.*