L'échange CCRC

La pratique de l'audit dans le secteur des cryptoactifs

Existence de cryptoactifs détenus par des tiers

Le Conseil canadien sur la reddition de comptes (CCRC) est préoccupé par la qualité des éléments probants que se procurent certains auditeurs lorsqu'ils vérifient l'existence de cryptoactifs détenus en garde par des tiers. Le présent rapport explique les éléments probants dont les auditeurs doivent tenir compte lors des audits des états financiers d'émetteurs assujettis qui ont recours à des dépositaires pour protéger leurs cryptoactifs.

Introduction

De par leur nature, les cryptoactifs sont plus vulnérables au vol ou à la perte[1] que les actifs traditionnels. Souvent, les émetteurs assujettis dont le modèle commercial implique la détention de cryptoactifs significatifs confient la garde de leurs cryptoactifs à des tiers externes, spécialisés dans l'offre de services de garde de cryptoactifs (collectivement, les « dépositaires »). Par dépositaires, on entend les plateformes de négociation de cryptoactifs (plateformes chargées d'acheter, de vendre ou de garder des cryptoactifs) et autres dépositaires tiers.

À propos du CCRC

Le CCRC est l'organisme indépendant de réglementation des audits des sociétés ouvertes du Canada. Chargé de superviser les audits des états financiers des émetteurs assujettis qu'effectuent des cabinets d'experts-comptables inscrits, le CCRC contribue à maintenir la confiance du public en l'intégrité de l'information financière, et s'engage à protéger le public investisseur du Canada.

Nous sommes préoccupés par la qualité des éléments d'audit probants que se procurent certains auditeurs lorsqu'ils vérifient l'existence de cryptoactifs détenus par des dépositaires. Les principales constatations suite à de nombreuses inspections révèlent l'un des thèmes récurrents : les auditeurs ne comprennent pas suffisamment les risques associés aux accords d'externalisation de la garde des cryptoactifs des émetteurs assujettis. Par conséquent, ces auditeurs ont mis en œuvre des procédures d'audit insuffisamment adaptées aux risques. Par exemple, le CCRC a identifié des constatations importantes suite à des inspections où les auditeurs se sont appuyés sur l'information provenant des dépositaires (par exemple, des confirmations d'audit et des relevés de compte des clients) comme seule source de preuves d'audit en vue de confirmer l'existence de cryptoactifs détenus par les dépositaires aux dates du bilan des émetteurs assujettis.

Il faut que les auditeurs reconnaissent que le fait d'externaliser la garde des cryptoactifs auprès de dépositaires ne signifie pas nécessairement que ces actifs seront en sécurité. S'appuyer sur les déclarations des dépositaires comme seule source d'éléments probants ne constitue pas une réponse adéquate des auditeurs aux risques élevés associés à l'affirmation de l'existence d'un cryptoactif. Les réponses d'audit appropriées comprennent souvent l'évaluation et le test des contrôles pertinents chez les dépositaires. Il s'agit de contrôles relatifs à la manière dont le dépositaire protège les cryptoactifs des clients et veille à ce que les registres portant sur les soldes et transactions des clients sont complets et exacts.

[1] En raison du fait que les clés privées des cryptoactifs sont susceptibles d'être perdues ou volées, et ce, qu'elles soient détenues soit directement, soit par un tiers.

Affirmation d'une existence

Lorsque les dirigeants inscrivent au bilan de l'émetteur assujetti les cryptoactifs détenus par les dépositaires, ils affirment que l'émetteur assujetti possède lesdits actifs, et que ceux-ci existent bien à la date du bilan (ils n'ont été ni perdus, ni volés alors qu'ils étaient sous la garde du dépositaire). L'affirmation d'une telle existence constitue fondamentalement une déclaration selon laquelle ces actifs sont prêts à être transférés sans délai (c'est-à-dire retirés) hors des portefeuilles que conservent les dépositaires à la date du bilan de l'émetteur assujetti.

Le présent rapport s'intéresse à l'affirmation d'une existence lorsque les émetteurs assujettis conservent la propriété des cryptoactifs qu'ils ont transférés à des dépositaires pour en assurer la garde (encadré 1).

Encadré 1

Impact sur les droits de propriété en cas d'externalisation de la garde de cryptoactifs

L'externalisation de la garde de cryptoactifs auprès de dépositaires soulève une question comptable complexe : les cryptoactifs continuent-ils d'appartenir à l'émetteur assujetti, ou bien les droits de propriété sont-ils passés au dépositaire?

La réponse dépend d'une analyse des concepts de « contrôle » et d'« avantages » si l'on cherche à déterminer quelle partie – l'émetteur assujetti ou le dépositaire – est soumise aux risques et avantages substantiels liés au fait d'être propriétaire. Le groupe de discussion sur les IFRS (voir page 9) du Conseil des normes comptables (CNC) du Canada a publié des directives sur les facteurs à prendre en compte, du point de vue du dépositaire, quand il faut déterminer si ce dernier est propriétaire des cryptoactifs qu'il est chargé de protéger. Les auditeurs peuvent trouver ces directives également utiles lorsqu'ils évaluent la détermination de la propriété du point de vue de l'émetteur assujetti.

Tâches requises de la part des auditeurs utilisateurs

La Norme canadienne d'audit (NCA) 402 décrit les exigences d'audit concernant les audits d'états financiers d'entités utilisatrices qui se procurent les services d'organismes de services. Dans le présent rapport, nous décrivons certaines des exigences de la NCA 402 qui s'appliquent aux auditeurs (auditeurs utilisateurs) dans le cadre des audits des états financiers d'émetteurs assujettis ayant fait appel aux services de dépositaires pour protéger leurs cryptoactifs.

Pour chaque accord significatif de services de garde, les auditeurs utilisateurs sont tenus d'effectuer, entre autres, les opérations suivantes :

- **Identifier et évaluer les risques ->** Comprendre en profondeur la nature et l'importance des services de garde que fournissent tous les dépositaires détenteurs de cryptoactifs importants, et ce, afin d'éclairer leur identification et leur évaluation des risques d'anomalies significatives.
- **Répondre aux risques évalués ->** Concevoir et mettre en œuvre des procédures d'audit répondant à ces risques.

Le présent rapport n'a pas pour objectif de détailler toutes les considérations ou procédures que les auditeurs doivent appliquer au cours de leurs audits. Il revient aux auditeurs utilisateurs de comprendre les exigences de la norme NCA 402, ainsi que de consulter des experts internes ou externes lorsque ces exigences ne sont pas claires.

Identifier et évaluer les risques

Il est extrêmement important que les auditeurs utilisateurs comprennent en profondeur les accords de garde significatifs afin d'éclairer leur identification et leur évaluation des risques d'anomalies significatives liées à l'affirmation de l'existence de cryptoactifs détenus chez les dépositaires.

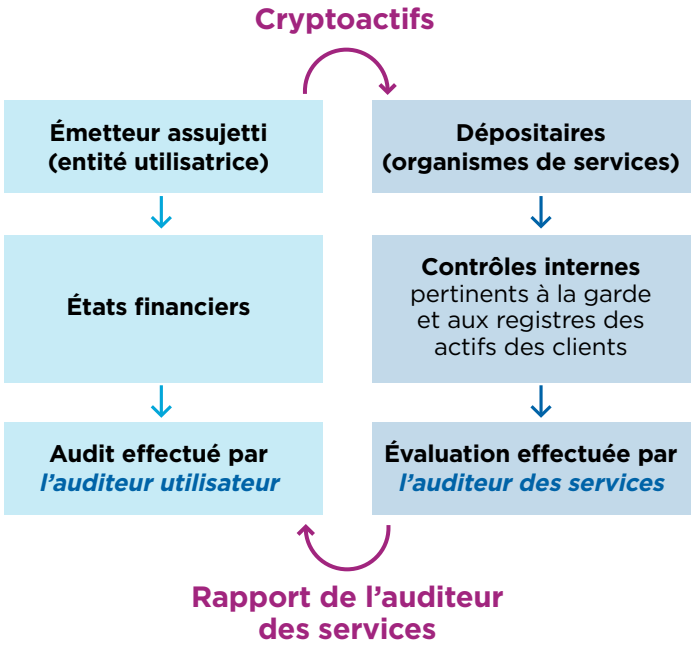
Se procurer et étudier le contrat des services de garde

Afin de comprendre ce qui suit, les auditeurs utilisateurs doivent se procurer et étudier le contrat (l'accord relatif au niveau de services) entre le dépositaire et l'émetteur assujetti :

- Les cryptoactifs détenus par le dépositaire se trouvent-ils sur un compte distinct (c'est-à-dire séparé des cryptoactifs d'autres clients, et doté d'une adresse unique sur la chaîne de blocs), ou bien sont-ils amalgamés aux cryptoactifs d'autres clients (ce que l'on appelle un compte omnibus)? Souvent, les dépositaires amalgament les cryptoactifs de leurs clients dans un compte omnibus, doté d'une adresse unique sur chaîne de blocs. Aux yeux des dépositaires, cette méthode simplifie la gestion des clés et constitue un moyen plus rentable de gérer les cryptoactifs de leurs clients. Cependant, les comptes omnibus engendrent de nouveaux risques. Par exemple, les clients perdent la possibilité de surveiller les mouvements de leurs cryptoactifs lorsqu'ils sont amalgamés dans des comptes omnibus, et les clients doivent se fier aux engagements du dépositaire indiquant que le dépositaire agira d'une manière convenue (par exemple, il s'engage à ne pas utiliser les cryptoactifs des clients à ses propres fins d'investissement, etc.).
- Le dépositaire a-t-il le droit de faire usage des cryptoactifs des clients (par exemple, gage, renouvellement d'un gage, hypothèque, renouvellement d'une hypothèque, vente, prêt, intérêt, prise d'intérêt, etc.) pour ses propres besoins d'investissement? Cela pourrait donner lieu à une discordance entre la durée des actifs du dépositaire (les investissements) et les passifs du dépositaire (les dépôts des clients), ce qui entraînerait alors l'incapacité du dépositaire à honorer en temps voulu les demandes de retrait de l'émetteur assujetti.
- Le dépositaire a-t-il confié la responsabilité de protéger les cryptoactifs de ses clients à un autre dépositaire externe (dépositaire secondaire)? Lorsque cette responsabilité est confiée à un dépositaire secondaire, l'auditeur utilisateur doit également comprendre les dispositions relatives aux services dudit dépositaire secondaire, les risques qui découlent du recours à chaque dépositaire secondaire (ce qui inclut de comprendre les contrôles pertinents du dépositaire secondaire), et savoir réagir à ces risques.
- Le contrat comporte-t-il une clause d'indemnisation qui précise les recours de l'émetteur assujetti en cas de perte ou de vol des cryptoactifs sous la garde du dépositaire?
- Quelle est la couverture d'assurance dont dispose le dépositaire pour indemniser les clients en cas de perte ou de vol de leurs cryptoactifs?
- L'auditeur utilisateur dispose-t-il d'un droit d'accès aux documents comptables du dépositaire relatifs à l'émetteur assujetti (détails du compte, historique des transactions, contrôles connexes)?
- Le contrat prévoit-il une communication directe entre l'auditeur utilisateur et l'auditeur du dépositaire (auditeur des services)?

Se procurer et étudier le rapport de l'auditeur des services

Les auditeurs utilisateurs sont également tenus d'acquérir une connaissance des contrôles pertinents[2] mis en place chez chaque dépositaire chargé de protéger un montant significatif des actifs de l'émetteur assujetti (les cryptoactifs) afin d'éclairer l'évaluation des risques relatifs au contrôle, évaluation que feront les auditeurs utilisateurs[3]. Les contrôles pertinents sont ceux qui traitent des risques significatifs, ainsi que des risques que des procédures de fond ne suffisent pas à atténuer. En général, les contrôles pertinents qui se rapportent spécifiquement à l'affirmation de l'existence de cryptoactifs se classent dans l'une des deux catégories suivantes :



- Contrôles relatifs à la protection des cryptoactifs des clients (perte ou vol). Par exemple, le dépositaire disposera généralement de contrôles liés à la gestion des clés cryptographiques des portefeuilles dits « chauds » et « froids »[4].
- Contrôles relatifs à la tenue des registres des soldes des clients (soldes des cryptoactifs). Par exemple, le dépositaire peut effectuer des rapprochements périodiques entre les données de la chaîne de blocs et les livres et registres internes du dépositaire ayant trait aux cryptoactifs des clients détenus dans des comptes omnibus.

  Pour comprendre les contrôles pertinents, les auditeurs utilisateurs se procureront et étudieront généralement les rapports pertinents des auditeurs des services, qui définissent la portée et les tests connexes des missions de contrôle d'une société de services (SOC) pour les dépositaires concernés. Les missions SOC sont effectuées par des auditeurs que les dépositaires engagent directement (ce sont les auditeurs des services). Il existe plusieurs types de missions d'assurance SOC[5] (SOC 1, SOC 2, SOC 3, etc.). Chacune vise un objectif particulier et s'adresse à différentes parties prenantes. Le type de mission SOC qui répond le mieux[6] aux besoins d'un auditeur utilisateur est une mission SOC 1. En effet, elle porte précisément sur les contrôles de l'organisme de services qui s'appliquent au contrôle interne de l'entité utilisatrice en matière de rapports financiers. Par ailleurs, il existe deux types de rapports SOC 1 :

- Un rapport de type 1 atteste que les contrôles ont été conçus efficacement et mis en œuvre à un moment donné.
- Un rapport de type 2 atteste que l'efficacité de la conception, de la mise en œuvre et du fonctionnement des contrôles tout au long de la période que couvre le rapport. Les auditeurs utilisateurs exigent un rapport de type 2 quand ils ont l'intention de s'appuyer sur les contrôles des dépositaires dans leurs méthodes d'audit au moment où ils testent l'existence des cryptoactifs détenus par les dépositaires.

[2] CAS 315 (révisée) : *Identification et évaluation des risques d'anomalies significatives,* alinéa 26 (a) et CAS 402, alinéa 10.

[3] CAS 315 (révisée) : Alinéa 34.

[4] Veuillez également consulter l'article de la série Points de vue rédigé par le Groupe de discussion sur l'audit des cryptoactifs, qui explique les contrôles dont doivent disposer les dépositaires afin de protéger adéquatement les actifs de leurs clients. Constitué par CPA Canada et le Conseil des normes d'audit et de certification du Canada (CNAC), le Groupe de discussion sur l'audit des cryptoactifs comprend aussi des représentants de cabinets d'audit, des universitaires et le CCRC.

[5] Un ensemble disparate de normes canadiennes, américaines et internationales s'appliquent aux missions SOC. Consultez les directives non officielles du Conseil des normes d'audit et de certification du Canada (CNAC), qui expliquent les normes applicables dans chaque juridiction aux divers types de missions SOC.

[6] Le CCRC reconnaît l'existence possible de contrôles testés par les auditeurs des services dans le cadre des missions SOC 2, contrôles qui peuvent être pertinents aux auditeurs utilisateurs durant leurs audits des états financiers des émetteurs assujettis.

Répondre aux risques évalués

Il existe un faible degré d'interaction[7] entre l'émetteur assujetti et le dépositaire en ce qui concerne les activités de sauvegarde des cryptoactifs de l'émetteur assujetti par le dépositaire. Les auditeurs évaluent le degré d'interaction pour comprendre l'importance des contrôles du dépositaire. Un faible degré d'interaction fait référence à la capacité limitée d'un émetteur assujetti à mettre en œuvre ses propres contrôles pour atténuer les risques associés à la capacité du dépositaire à protéger les actifs de l'émetteur assujetti. Par conséquent, les contrôles du dépositaire deviennent particulièrement importants, car, pour protéger ses actifs, l'émetteur assujetti est obligé de s'en remettre entièrement à l'efficacité des contrôles de protection du dépositaire.

Dans la plupart des cas, il sera impossible aux auditeurs utilisateurs de répondre aux risques élevés associés à l'affirmation de l'existence des cryptoactifs (pour les cryptoactifs détenus par les dépositaires) s'ils se contentent de réaliser des procédures de fond. Souvent, les auditeurs utilisateurs devront se fier aux tests de l'efficacité opérationnelle des contrôles pertinents chez les dépositaires, tests effectués par les auditeurs des services. Lorsque des rapports SOC 1 de type 2 sont disponibles aux dépositaires qui détiennent des montants significatifs de cryptoactifs de l'émetteur assujetti, l'auditeur utilisateur doit se les procurer, et évaluer si les contrôles figurant dans les rapports répondent de manière adéquate aux risques qu'a évalués l'auditeur utilisateur. Lorsque les rapports SOC 1 de type 2 ne sont pas disponibles, l'auditeur utilisateur devra tester directement les contrôles chez les dépositaires concernés, ou engager un autre auditeur qui effectuera ces tests en son nom.

On peut trouver des situations où les contrôles figurant dans les rapports SOC 1 de type 2 ne répondent pas de manière adéquate aux risques élevés identifiés par l'auditeur utilisateur, qui ne reçoivent aucune réponse adéquate par la seule mise en œuvre de procédures de fond. Par exemple, l'auditeur utilisateur peut comprendre que le dépositaire a le droit contractuel de faire usage (par exemple, gage, renouvellement d'un gage, hypothèque, renouvellement d'une hypothèque, vente, prêt, intérêt, prise d'intérêt, etc.) des cryptoactifs des clients pour ses propres besoins d'investissement (ainsi, pour remporter un rendement), mais le rapport SOC 1 ne comporte aucun contrôle lié à la gestion actifs-passifs (ALM) du dépositaire. Les contrôles ALM répondent au risque que le dépositaire ne soit pas en mesure d'honorer les demandes de retrait des clients parce que les investissements du dépositaire (les investissements réalisés à partir des dépôts des clients) ne peuvent pas être réalisés dans le même délai (comme des demandes de retrait). Pour répondre à ce risque, l'auditeur utilisateur peut avoir besoin d'engager l'auditeur des services dans le but d'effectuer des procédures spécifiques comprenant, par exemple, l'évaluation de la conception et de l'efficacité opérationnelle des contrôles ALM si de tels contrôles existent.

Acceptation ou poursuite de la mission d'audit

Avant d'accepter ou de poursuivre une mission d'audit, les auditeurs doivent se demander s'ils seront en mesure de mener à bien cette mission d'audit lorsque l'émetteur assujetti aura confié la garde de cryptoactifs significatifs à des dépositaires dont les contrôles internes n'ont pas encore subi l'examen d'auditeurs des services (les rapports SOC 1 de type 2 ne sont pas disponibles). Au moment d'accepter ou de poursuivre une mission d'audit, le fait de prévoir des discussions avec la direction et le comité d'audit sur les accords d'externalisation de l'émetteur assujetti permet aux cabinets d'anticiper et de répondre aux obstacles qui pourraient influencer l'achèvement de leurs missions d'audit en temps voulu.

[7] Les alinéas 9 (c) et A7 de la NCA 402 expliquent que l'auditeur doit comprendre le degré d'interaction entre les activités de l'organisme de services et celles de l'entité utilisatrice.

Pour en savoir plus

Consultez notre site Internet au www.cpab-ccrc.ca et inscrivez-vous à notre liste de diffusion.
Suivez-nous sur Twitter — @CPAB_CCRC.

www.cpab-ccrc.ca / Courriel : info@cpab-ccrc.ca

cpab ccrc
Canadian Public Accountability Board
Conseil canadien sur la reddition de comptes