CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

POINTS DE VUE :

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

L'AUDIT DES CRYPTOACTIFS : AUDIT DES ÉTATS FINANCIERS D'ENTITÉS FAISANT APPEL À UN TIERS FOURNISSEUR DE SERVICES POUR DES TRANSACTIONS EN CRYPTOACTIFS OU LA DÉTENTION DE CRYPTOACTIFS

MARS 2021

Groupe de travail sur l'audit des cryptoactifs

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

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

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

Contexte

Les entités qui détiennent des cryptoactifs peuvent faire appel à différents tiers de l'écosystème (ou du secteur) des cryptoactifs pour divers services, y compris :

- la réalisation de transactions en cryptoactifs pour leur compte;
- la détention d'un solde de cryptoactifs pour leur compte[1];
- des services de portefeuille.

1 Certains des risques et des exemples de contrôles dont il est question dans le présent document peuvent ne pas s'appliquer lorsque les cryptoactifs sont détenus uniquement à titre de garantie.

Les tiers qui fournissent ces services peuvent être des plateformes de négociation, des dépositaires ou des fournisseurs de portefeuilles.

Il est important que l'entité utilisatrice et l'auditeur comprennent que, compte tenu de la nature de la technologie, ces services peuvent ne pas être aussi simples que ceux fournis par un tiers fournisseur de services habituel comme un fournisseur de services de paie ou un dépositaire d'actifs traditionnels. Par ailleurs, il se peut que ces tiers fournisseurs de services ne soient pas aussi avertis que d'autres; autrement dit, que leur environnement de contrôle n'ait pas atteint le même degré de maturité, y compris en ce qui concerne la conception de contrôles appropriés.

Pour étayer son évaluation des risques et planifier des procédures d'audit complémentaires, l'auditeur doit acquérir une compréhension suffisante du contrôle interne de l'entité à l'égard de l'information financière, y compris la manière dont l'entité a recours aux services de tiers dans le cadre de son fonctionnement. Ces tiers peuvent être ou ne pas être considérés comme des sociétés de services pour l'entité utilisatrice faisant l'objet de l'audit, selon la façon dont cette dernière interagit avec eux. L'auditeur devra exercer son jugement afin de déterminer, en premier lieu, si le tiers est une société de services et, en second lieu, s'il y a lieu, les procédures à mettre en œuvre pour comprendre quels contrôles de la société de services sont pertinents pour l'audit.

Lorsque l'auditeur conçoit et met en œuvre des procédures d'audit, il doit tenir compte de la pertinence et de la fiabilité des informations devant servir comme éléments probants, y compris celles provenant de tiers qui sont des sociétés de services. Compte tenu des étapes de maturité des sociétés de services dans cet écosystème, un rapport sur les contrôles d'une société de services (SOC) ne sera pas nécessairement disponible. Par ailleurs, même lorsqu'un rapport SOC est disponible :

- il pourrait ne pas couvrir tous les contrôles jugés pertinents pour l'audit;
- il pourrait ne pas couvrir suffisamment la période auditée;
- l'auditeur de l'entité utilisatrice pourrait ne pas être assuré de la compétence professionnelle de l'auditeur de la société de services.

Dans ces circonstances, en tant qu'auditeur, vous devriez déterminer si vous pouvez mettre en œuvre d'autres procédures d'audit afin d'obtenir des éléments probants en réponse à l'évaluation des risques d'anomalies significatives. Si tel n'est pas le cas, vous devriez modifier votre opinion.

Étendue

Ces indications visent :

- à aider les auditeurs d'états financiers qui comportent des soldes de cryptoactifs et/ou des transactions en cryptoactifs significatifs et dans le cas desquels l'entité (« entité utilisatrice ») a recours aux services d'un tiers (par exemple, une plateforme de négociation, un dépositaire ou un fournisseur de portefeuilles) pour des transactions en cryptoactifs et/ou la détention de cryptoactifs;

- à mettre l'accent sur les considérations relatives à l'auditeur de l'entité utilisatrice. Il se peut que l'entité utilisatrice doive prendre en compte d'autres risques d'entreprise avant de faire appel à un tiers, mais ces considérations dépassent le cadre de ces indications.

Ces indications ne visent pas :

- à fournir une liste exhaustive des contrôles pertinents se rapportant aux objectifs de contrôle donnés en exemple;
- à traiter de la pertinence et de la fiabilité des informations provenant d'une chaîne de blocs publique devant servir comme éléments probants[2];
- à couvrir toutes les dispositions de la NCA 402[3]; nous nous attarderons plutôt sur les aspects qui peuvent faire l'objet de considérations particulières dans l'écosystème des cryptoactifs.

Aux fins du présent bulletin, le terme « cryptoactifs » s'entend uniquement du sous-ensemble spécifique des cryptoactifs qui sont achetés, vendus ou transférés sur une plateforme de négociation, ou qui sont détenus à des fins de placement. Il peut y avoir d'autres risques d'audit associés aux jetons utilitaires et aux contrats intelligents, qui ne sont pas abordés dans le présent bulletin.

Les cryptoactifs dont il est question dans le présent bulletin n'ont pas de substance physique et ne sont généralement pas liés à une monnaie ou garantis par un gouvernement, une banque centrale, une entité juridique, un actif sous-jacent ou une marchandise. La détention de cryptoactifs 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.

Le présent bulletin ne traite pas de questions telles que l'audit de ce qui suit :

- les états financiers d'une plateforme de négociation, d'un dépositaire ou d'un fournisseur de portefeuilles de cryptoactifs[4];
- les états financiers d'entités (voir la note de bas de page 4) qui :
  - — valident des transactions en cryptoactifs dans une chaîne de blocs (c'est-à-dire des mineurs),
  - — font des premières émissions de cryptomonnaies (PEC) ou des premières émissions de jetons (PEJ),
  - — concluent des contrats intelligents;
- les conclusions relatives à la méthode de comptabilité pour les cryptoactifs.

2 Pour de plus amples indications à ce sujet, veuillez consulter le document *Pertinence et fiabilité des informations provenant d'une chaîne de blocs* de CPA Canada.

3 NCA 402, *Facteurs à considérer pour l'audit d'entités faisant appel à une société de services*

4 Sauf dans la mesure où ce type d'entité fait appel à un tiers pour lui fournir l'un des services décrits dans le présent bulletin.

Question

Pour répondre à l'évaluation des risques d'anomalies significatives liés aux transactions en cryptoactifs et aux soldes de cryptoactifs figurant dans les états financiers de l'entité utilisatrice, il faut se poser plusieurs questions.

- Quels sont les facteurs à prendre en considération lors de l'audit lorsqu'un tiers détient des cryptoactifs pour le compte de l'entité, lorsque les transactions sont effectuées sur la plateforme de négociation d'un tiers ou lorsqu'un tiers fournit des services de portefeuille à l'entité?
- Quels sont certains des facteurs particuliers relatifs aux cryptoactifs que l'auditeur pourrait prendre en considération lors de l'acquisition d'une compréhension de la nature et de l'importance des services fournis par le tiers ainsi que de leur effet sur le contrôle interne de l'entité?
- Quels contrôles peuvent être pertinents pour l'audit à l'égard du dépositaire, de la plateforme de négociation ou du fournisseur de portefeuilles, et de quelle manière les éléments probants pourraient-ils être obtenus?

Le présent bulletin aborde chacun des aspects suivants :

PARTIE 1

1. Compréhension de l'écosystème des cryptoactifs
2. Compréhension de la nature des services fournis par le tiers, y compris la question de savoir si un tiers est une société de services
3. Stratégies pour acquérir une compréhension des contrôles pertinents de la société de services et les évaluer

PARTIE 2

1. Identification des risques et des contrôles pertinents de la société de services

PARTIE 1

Compréhension de l'écosystème des cryptoactifs

L'écosystème des cryptoactifs a évolué et inclut plusieurs types de tiers. Voici des exemples de ces entités et des services qu'elles fournissent :

- *Plateformes de négociation* – Ces entreprises permettent aux utilisateurs d'acheter, de vendre, de détenir et d'échanger des cryptoactifs et des monnaies « fiduciaires » traditionnelles. Elles génèrent et gèrent les clés cryptographiques qui sont nécessaires pour utiliser, vendre ou transférer les cryptoactifs dans les chaînes de blocs qu'elles soutiennent. Vous trouverez de plus amples informations sur les plateformes de négociation ci-après[5].

5 Le document de consultation conjoint 21-402 des ACVM et de l'OCRCVM, *Projet d'encadrement des plateformes de négociation de cryptoactifs,* indique que les *plateformes de négociation* facilitent l'achat et la vente ou le transfert de cryptoactifs.

- *Dépositaires* – À l'instar des dépositaires de titres de capitaux propres, ces entreprises détiennent des cryptoactifs pour le compte d'utilisateurs tels que des fonds de couverture, des gestionnaires d'actifs et d'autres entités.
- *Fournisseurs de portefeuilles* – Ces organisations se spécialisent dans la conception et la mise en œuvre de solutions de gestion de clés cryptographiques pour aider à protéger contre le vol ou la destruction des clés privées hautement sensibles qui se rattachent à des adresses publiques dans une chaîne de blocs.

Les plateformes de négociation de cryptoactifs permettent aux utilisateurs d'acheter, de vendre ou de transférer des cryptoactifs. Certaines plateformes de négociation permettent également aux utilisateurs de conserver les cryptoactifs dans un portefeuille sur leur système. Cette caractéristique donne lieu à une distinction importante entre deux types de plateformes de négociation de cryptoactifs que vous pourriez rencontrer, soit les plateformes *gardiennes* et les plateformes *non gardiennes.*

- Les **plateformes de négociation gardiennes** permettent aux utilisateurs de conserver leurs cryptoactifs sur leur système, leur permettant d'accéder à leur fonds et de procéder à des négociations ou à des transactions rapidement. Les services de garde de ces plateformes incluent la protection des actifs qui se trouvent dans leur système.
- Les **plateformes de négociation non gardiennes** ne prennent pas la garde des cryptoactifs de leurs utilisateurs en conservant pour eux un portefeuille dans leur système. Les utilisateurs peuvent plutôt utiliser différentes technologies de portefeuille afin de signer personnellement (et de façon numérique) les transactions en vue d'autoriser un achat ou une vente.

Une deuxième distinction importante peut être faite entre ces deux types de plateformes de négociations de cryptoactifs, selon que la plateforme est *centralisée* ou *décentralisée*.

Les **plateformes de négociation centralisées (PNC)** permettent aux utilisateurs d'utiliser les monnaies fiduciaires (comme le dollar canadien, le dollar américain ou l'euro) pour acheter des cryptoactifs. Ce type de plateforme donne lieu à des frais de transaction ou d'utilisation lorsque les utilisateurs se servent de monnaies fiduciaires pour acheter des cryptoactifs (ou l'inverse), se servent de cryptoactifs pour acheter d'autres cryptoactifs, ou réalisent des transactions sur la plateforme de négociation.

En outre, les PNC se caractérisent généralement par le fait qu'elles permettent les négociations qui ont lieu « sur la plateforme », mais pas dans la chaîne de blocs. Les transactions qui sont effectuées entre les utilisateurs sur la plateforme (négociations indépendantes), ou entre la plateforme et l'utilisateur (dépôts, retraits ou transferts, y compris les transactions dans le cadre desquelles la plateforme est la contrepartie), ne sont pas nécessairement toutes enregistrées dans le registre distribué du réseau de la chaîne de blocs concerné.

Cela peut être d'une importance cruciale si vous êtes un auditeur d'états financiers et que vous mettez en œuvre des procédures de corroboration. Si la PNC ne peut pas permettre à ses entités utilisatrices et à leurs auditeurs de vérifier que ces transactions – qui sont réglées en interne au sein de la plateforme et en dehors de la chaîne de blocs publique – existent et sont présentées de manière exhaustive et exacte, cela pourrait avoir pour effet que l'auditeur ne dispose pas d'éléments probants suffisants. Certaines plateformes de négociation conservent les cryptoactifs dans des portefeuilles individuels, alors que d'autres les conservent dans un compte général qui mélange ou regroupe les actifs des clients. Les auditeurs doivent tenir compte des répercussions de ces circonstances lorsqu'ils déterminent quelles procédures d'audit supplémentaires pourraient être requises.

À l'inverse, les **plateformes de négociation décentralisées (PND)** ne permettent pas l'accès aux monnaies fiduciaires, mais elles facilitent les transactions entre les personnes, de pair à pair. Bien que nombre de PND imposent des frais de transaction internes à la fois aux vendeurs et aux acheteurs, les utilisateurs peuvent aussi être tenus de payer, pour le traitement de leurs transactions, des frais de transaction externes au réseau de la chaîne de blocs sur lequel ils négocient. Les véritables PND ne seraient probablement pas considérées comme des sociétés de services, raison pour laquelle elles ne sont pas prises en considération dans le présent bulletin.

En tant qu'auditeur, il est important que vous connaissiez bien l'entité faisant l'objet de l'audit et les tiers avec lesquels elle interagit. Bien qu'il en soit indubitablement de même pour tous les audits, c'est d'autant plus important dans le cas des entités utilisatrices du secteur des cryptoactifs, étant donné la complexité de cet écosystème et des différents types de tiers impliqués.

Compréhension de la nature des services fournis par le tiers, y compris la question de savoir si un tiers est une société de services

Il incombe à la direction d'établir des contrôles appropriés à l'égard des services fournis par le tiers. Il peut notamment s'agir d'établir des processus et des contrôles pour la sélection des tiers fournisseurs de services, de s'assurer que des membres du personnel ayant les compétences pertinentes passent en revue les rapports SOC, et de mettre en place des contrôles complémentaires de l'entité utilisatrice.

Comme c'est le cas pour d'autres catégories d'actifs telles que les titres de participation et les biens immobiliers, les cryptoactifs doivent être contrôlés. En tant qu'auditeur, vous devez tenir compte des assertions contenues dans les états financiers relativement à l'actif (exactitude, évaluation et imputation, exhaustivité, existence, séparation des périodes, droits [et propriété]).

Vous devez ensuite acquérir une compréhension des contrôles internes pertinents pour l'audit. Cette compréhension vous servirait à identifier les risques d'anomalies significatives au niveau des assertions pour les catégories d'opérations, les soldes de comptes et les informations à fournir correspondantes dans les états financiers, et à déterminer la nature, le calendrier et l'étendue des procédures d'audit complémentaires conçues pour répondre à ces risques. Il est important de noter que les contrôles pertinents pour l'audit peuvent englober à la fois ceux établis par l'entité

et ceux mis en place par le tiers. Les plateformes de négociation de cryptoactifs, les dépositaires et les fournisseurs de portefeuilles fournissent souvent aux entités utilisatrices des services pertinents sur le plan financier, et les auditeurs des entités utilisatrices doivent tenir compte des risques d'anomalies significatives pertinents.

En tant qu'auditeur, pour acquérir une compréhension de la façon dont l'entité utilisatrice a recours aux services d'un tiers dans le cadre de son fonctionnement, vous devez comprendre :

- la nature des services fournis par le tiers (c'est-à-dire négociation, garde ou portefeuille) et leur importance pour l'entité utilisatrice, y compris leur incidence sur le contrôle interne de l'entité utilisatrice;
- la nature et le caractère significatif des opérations traitées ou des comptes ou processus d'information financière affectés par les services que le tiers fournit;
- le degré d'interaction (par exemple, direction et surveillance, ou autonomie) entre les activités du tiers et celles de l'entité utilisatrice;
- la nature des relations entre l'entité utilisatrice et le tiers, y compris les conditions contractuelles pertinentes pour les services fournis par le tiers.

En acquérant cette compréhension, vous devez également déterminer si le tiers est effectivement une société de services. Selon les Normes canadiennes d'audit (NCA), une société de services est une tierce organisation (ou une subdivision d'une tierce organisation) qui fournit aux entités utilisatrices des prestations qui font partie intégrante du système d'information de ces entités pertinent pour l'information financière.

Il y a de bonnes chances que bien des contrôles de la société de services fassent partie de ce système, ou des contrôles y afférents, notamment ceux mis en place pour la sauvegarde des actifs. Les prestations fournies par la société de services font partie du système d'information de l'entité utilisatrice si elles concernent l'un quelconque des éléments suivants :

a) le cheminement, dans le système d'information de l'entité utilisatrice, des informations relatives aux catégories d'opérations importantes, aux soldes de comptes importants et aux informations à fournir importantes, peu importe que les étapes soient effectuées manuellement ou à l'aide de l'informatique, et peu importe la provenance de ces informations (grand livre général et livres auxiliaires, ou autre). Cela comprend les prestations fournies par la société de services qui influent sur la façon :
   — dont les opérations de l'entité utilisatrice sont déclenchées et dont les informations les concernant sont enregistrées, traitées, corrigées (au besoin), incorporées dans le grand livre général et communiquées dans les états financiers,
   — dont les informations sur les événements ou les situations, autres que les opérations, sont saisies, traitées et fournies par l'entité utilisatrice dans les états financiers;

b) les documents comptables, les comptes spécifiques contenus dans les états financiers de l'entité utilisatrice et les autres documents justificatifs qui concernent le cheminement des informations décrit au point a);

c) le processus d'information financière utilisé pour préparer les états financiers de l'entité utilisatrice à partir des documents comptables mentionnés au point b), y compris en ce qui concerne les informations à fournir et les estimations comptables se rapportant à des catégories d'opérations importantes, à des soldes de comptes importants et à des informations à fournir importantes;

d) l'environnement informatique de l'entité qui est pertinent au regard des points a) à c) ci-dessus.

Par le passé, les auditeurs d'états financiers ne considéraient pas certaines fonctions exercées par des banques ou des bourses comme étant le fait de sociétés de services. Dans ces cas, les prestations se limitent habituellement à l'exécution des opérations expressément autorisées par le client, par exemple le traitement par une banque des opérations d'un compte chèque ou l'exécution d'ordres par un courtier en valeurs mobilières.

De même, dans un environnement de cryptoactifs, une entité peut donner son autorisation pour qu'une opération soit effectuée par le biais de la plateforme de négociation d'un tiers, tout en conservant la responsabilité de s'assurer qu'elle a été effectuée comme prévu (par exemple, en obtenant des éléments probants à l'appui de l'exécution de l'opération dans la chaîne de blocs), sans s'appuyer sur des informations reçues de la plateforme du tiers pour étayer la comptabilisation de l'opération dans ses livres et registres. Dans ces circonstances, l'auditeur pourrait ne pas considérer ces tiers comme des sociétés de services.

Par ailleurs, les services de fiducie des banques qui placent et gèrent des actifs pour le compte d'autres parties peuvent déclencher et exécuter certaines opérations, et tenir les livres et les registres qui s'y rattachent. Dans ces circonstances, les opérations qui ont une incidence sur l'entité utilisatrice sont, du moins en partie, physiquement et opérationnellement distinctes de celles de l'entité utilisatrice. Selon la nature et l'importance de ces opérations, il peut ne pas être faisable en pratique pour l'entité utilisatrice de mettre en place des contrôles efficaces sur ces opérations. Dans ces circonstances, ces services de fiducie des banques peuvent être considérés comme des sociétés de services pour l'entité utilisatrice.

Dans un environnement de cryptoactifs, les circonstances suivantes peuvent survenir :

- L'entité utilisatrice peut faire appel à une plateforme de négociation d'un tiers afin d'exercer des fonctions similaires, comme la tenue des registres pour les opérations exécutées et les actifs détenus. L'entité utilisatrice peut ensuite mettre à jour de façon périodique (par exemple, mensuellement, trimestriellement) ses propres registres financiers en se fondant sur les relevés fournis par la plateforme de négociation du tiers.
- L'entité utilisatrice peut effectuer des transactions directement avec la plateforme de négociation du tiers. Par exemple, l'entité utilisatrice pourrait souhaiter vendre des cryptoactifs à un certain prix, et la plateforme de négociation du tiers pourrait acheter directement les actifs, plutôt que de faciliter une transaction avec une autre partie indépendante. Dans ces circonstances, si aucune transaction n'est effectuée au moyen de la chaîne de blocs, il se peut que l'entité utilisatrice ne dispose d'aucun élément indiquant que la transaction a été effectuée comme il avait été demandé et qu'elle doive donc s'appuyer sur un relevé de la plateforme de négociation gardienne.

- La plateforme de négociation du tiers peut mélanger tous les cryptoactifs dans un seul portefeuille qui comprend également les actifs d'autres entités, et faire un suivi interne de la répartition des éléments du compte entre chaque entité. Il se peut que la transaction n'implique pas de mouvement de l'actif et qu'elle ne génère pas une entrée dans la chaîne de blocs. L'entité utilisatrice est donc tributaire de la plateforme de négociation du tiers.

En pareils cas, il est probable que l'entité utilisatrice s'appuie sur les contrôles de la plateforme de négociation du tiers dans le cadre de son système d'information pertinent pour l'information financière.

Les dépositaires d'actifs ont souvent été considérés comme des sociétés de services en raison des fonctions qu'ils exécutent. En ce qui a trait aux cryptoactifs, les entités utilisatrices peuvent faire appel à un tiers afin qu'il leur fournisse une installation de stockage sécuritaire pour leurs actifs moyennant des frais. Pour déterminer si le tiers est une société de services, vous pourriez devoir déterminer qui contrôle effectivement la sauvegarde des actifs.

Certaines plateformes de négociation qui détiennent des cryptoactifs d'une entité pour leur compte en appui à la négociation exercent un rôle de dépositaire des actifs en plus de celui de négociateur. Par exemple, vous pourriez établir que la plateforme de négociation ne joue qu'un rôle d'intermédiaire dans le cadre des opérations (un peu comme une bourse), mais vous devrez tout de même déterminer si la plateforme est un dépositaire d'actifs, étant donné qu'elle peut détenir une quantité significative des cryptoactifs d'une entité.

Il peut y avoir des circonstances limitées où il n'existe aucune relation avec une société de services. L'auditeur de l'entité utilisatrice peut déterminer que c'est le cas lorsque tout ce qui suit s'applique :

- une entité utilisatrice autorise l'exécution d'opérations par une plateforme de négociation indépendante ou par un dépositaire;
- les activités de la plateforme de négociation ou du dépositaire se limitent au traitement des opérations pour le compte de l'entité utilisatrice;
- ni la plateforme de négociation ni le dépositaire ne tiennent à jour les documents comptables de l'entité utilisatrice, ne gèrent des actifs, ou ne déclenchent, comptabilisent ou traitent des opérations à titre de mandataire de l'entité utilisatrice.

Même lorsque vous concluez qu'il n'existe aucune relation avec une société de services, vous devez vous conformer aux exigences de la NCA 315[6] et de la NCA 330[7] pour vous assurer d'obtenir des éléments probants en réponse aux risques d'anomalies significatives.

Une partie de jugement intervient pour déterminer si un tiers est une société de services. Un tiers peut être considéré comme une société de services relativement à une entité, mais pas pour une autre, selon la nature des opérations qui sont effectuées entre les différentes entités.

6 NCA 315, *Identification et évaluation des risques d'anomalies significatives*

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

Si vous avez déterminé que le tiers est une société de services qui a des contrôles pertinents pour l'audit, vous devez alors tirer profit de votre compréhension de la nature et de l'importance des services fournis pour :

- identifier et évaluer les risques d'anomalies significatives;
- concevoir et mettre en œuvre des procédures d'audit en réponse à ces risques.

Stratégies pour acquérir une compréhension des contrôles pertinents de la société de services et les évaluer

À titre d'auditeur de l'entité utilisatrice, vous pouvez être en mesure de répondre à vos besoins en matière de certification relativement aux contrôles de la société de services qui sont pertinents pour l'audit en vous procurant et en examinant un rapport SOC qui traite des rapports sur les contrôles d'une société de services pertinents pour le contrôle interne à l'égard de l'information financière des entités utilisatrices.

Les rapports SOC 1 sont généralement plus susceptibles d'être pertinents, puisqu'ils traitent du contrôle interne à l'égard de l'information financière. Toutefois, selon son étendue, un rapport SOC 2 portant sur les contrôles en matière de sécurité, d'accessibilité, d'intégrité du traitement, de confidentialité ou de protection des renseignements personnels peut également fournir des informations pertinentes pour vous en tant qu'auditeur de l'entité utilisatrice.

Deux types de rapports sont disponibles pour les missions SOC 1 et SOC 2 :

- Un **rapport de type 1** fournit des éléments probants quant à la question de savoir si des contrôles ont été conçus et mis en place à un moment précis.
- Un **rapport de type 2** (qui correspond habituellement plus aux besoins de l'auditeur de l'entité utilisatrice) fournit des éléments probants quant à la question de savoir si des contrôles ont fonctionné de manière efficace tout au long de la période visée par le rapport.

Peu importe le type de rapport SOC que vous obtenez, vous devrez prendre en considération les facteurs qui suivent pour évaluer le rapport et déterminer s'il traite effectivement des risques pertinents pour l'audit de l'entité utilisatrice[8] :

- l'étendue des travaux de l'auditeur de la société de services;
- le type de rapport délivré et son caractère approprié, compte tenu de vos exigences en tant qu'auditeur de l'entité utilisatrice;
- la période couverte, car, étant donné le rythme des changements dans l'écosystème des cryptoactifs, vous pourriez avoir besoin d'éléments probants sur les contrôles jusqu'à la clôture de l'exercice ou à une date s'en rapprochant.

Vous devrez également prendre en considération (et, au besoin, tester) les contrôles complémentaires de l'entité utilisatrice.

8 La partie 2 du présent bulletin comprend des exemples de risques et de contrôles d'une société de services dans l'écosystème des cryptoactifs, et peut aider l'auditeur d'une entité utilisatrice à évaluer si le rapport SOC traite des risques pertinents pour l'audit de l'entité utilisatrice.

En tant qu'auditeur de l'entité utilisatrice, il vous incombe d'obtenir des éléments probants en réponse aux risques d'anomalies significatives, peu importe si un rapport SOC est obtenu ou non.

Par exemple, vous devez acquérir une compréhension de la nature et de l'importance des prestations fournies par la société de services ainsi que de leur incidence sur les aspects du contrôle interne de l'entité utilisatrice pertinents pour l'audit qui soit suffisante pour vous fournir une base appropriée aux fins de l'identification et de l'évaluation des risques d'anomalies significatives. Si vous n'êtes pas en mesure d'acquérir une compréhension suffisante auprès de l'entité utilisatrice et qu'un rapport SOC n'est pas disponible, vous devez acquérir cette compréhension en mettant en œuvre une ou plusieurs des procédures suivantes :

- contacter la société de services, par l'entremise de l'entité utilisatrice, afin d'obtenir certaines informations précises;
- visiter la société de services et mettre en œuvre des procédures qui fourniront les informations nécessaires sur ses contrôles pertinents;
- faire appel à un autre auditeur afin qu'il mette en œuvre des procédures qui fourniront les informations nécessaires sur les contrôles pertinents de la société de services.

Habituellement, vous appliquez ces procédures en effectuant des demandes d'informations, en association avec des inspections ou des observations, qui soient suffisantes pour déterminer que les contrôles pertinents ont été mis en place.

De plus, lorsque votre évaluation des risques repose sur l'attente du fonctionnement efficace des contrôles de la société de services et qu'un rapport de type 2 n'est pas disponible[9], vous devez, en tant qu'auditeur de l'entité utilisatrice, obtenir des éléments probants sur l'efficacité du fonctionnement de ces contrôles en mettant en œuvre une ou plusieurs des procédures suivantes :

- effectuer des tests appropriés des contrôles au sein de la société de services;
- faire appel à un autre auditeur afin qu'il effectue des tests des contrôles pour vous au sein de la société de services.

Si vous n'êtes pas en mesure de mettre en œuvre les procédures nécessaires pour obtenir des éléments probants en réponse à l'évaluation des risques d'anomalies significatives lorsqu'un rapport SOC n'est pas disponible, il vous faudra exprimer, dans le rapport que vous délivrez en tant qu'auditeur de l'entité utilisatrice, une opinion modifiée conformément à la NCA 705[10].

La partie 2 du présent bulletin donne des indications pratiques visant à vous aider, en tant qu'auditeur utilisateur, relativement à deux aspects :

- l'acquisition d'une compréhension des services fournis (y compris le contrôle interne) par une société de services dans l'écosystème des cryptoactifs;
- la réponse à l'évaluation des risques d'anomalies significatives.

9 Le rapport de type 1 est actuellement plus fréquent dans l'écosystème des cryptoactifs, étant donné que ce secteur n'est pas encore parvenu à maturité.

10 NCA 705, *Expression d'une opinion modifiée dans le rapport de l'auditeur indépendant*

PARTIE 2

Identification des risques et des contrôles pertinents d'une société de services

Avant même d'évaluer la conception et la mise en place des contrôles de la société de services fournissant des prestations à l'entité utilisatrice, vous devez, en tant qu'auditeur de l'entité utilisatrice, identifier quels sont les contrôles pertinents. Cette section du présent bulletin précise des sujets d'intérêt possibles dans le contexte d'un audit d'états financiers comportant des soldes de cryptoactifs significatifs ou des transactions en cryptoactifs significatives, y compris des scénarios de risque et les assertions connexes ainsi que des exemples de contrôles.

Cette section donne des exemples de risques possibles et de contrôles qui peuvent être pertinents pour l'audit et dont vous voudrez vous assurer qu'ils sont inclus dans le rapport SOC lorsque, à titre d'auditeur de l'entité utilisatrice, vous êtes en mesure d'obtenir un tel rapport.

Cette section donne également des exemples que vous pourriez prendre en considération pour acquérir votre compréhension directement (par exemple, l'exécution de vos propres tests des contrôles pertinents pour l'audit de la société de services, si cela est possible) lorsque, compte tenu de vos besoins, le rapport SOC n'est pas suffisant à lui seul.

Il convient de noter que les sujets et les scénarios de risque connexes ne sont pas exhaustifs, et que l'identification de ceux qui sont pertinents pour un audit d'états financiers dépendra des faits et circonstances propres à l'entité utilisatrice donnée.

La légende pour les assertions contenues dans les états financiers est la suivante :

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

Gestion des clés cryptographiques

La conclusion de transactions portant sur des cryptoactifs requiert habituellement l'utilisation de clés cryptographiques qui doivent être générées, stockées, utilisées et finalement mises hors service de manière sécuritaire. Si les clés cryptographiques sont compromises (par exemple, en cas d'atteinte à la sécurité ou de destruction fortuite) ou perdues, les actifs pourraient être détournés ou rendus inaccessibles, les registres pourraient être altérés, et des transactions non autorisées pourraient être traitées. Par conséquent, la gestion des clés cryptographiques tout au long de leur cycle de vie (génération, stockage, utilisation et mise hors service) est une responsabilité cruciale qui incombe aux plateformes de négociation, aux dépositaires et aux fournisseurs de portefeuilles.

À titre d'auditeur de l'entité utilisatrice, vous devrez acquérir une compréhension des contrôles relatifs à la gestion des clés cryptographiques lorsque la société de services à laquelle l'entité a recours utilise des technologies de la chaîne de blocs. Cette compréhension sera probablement pertinente pour le contrôle interne à l'égard de l'information financière d'une entité utilisatrice lorsque les clés cryptographiques servent à authentifier et à valider des opérations financières, à transférer des actifs entre les participants, et à modifier des données pertinentes sur le plan financier. L'utilisation et le contrôle appropriés de la cryptographie sous-tendent la confiance que les réseaux de chaînes de blocs cherchent à offrir.

Voici des exemples de questions importantes susceptibles de devoir être prises en compte relativement à la gestion des clés cryptographiques. Cette liste ne se veut pas exhaustive, et vous devrez tenir compte des faits et circonstances propres à l'entité utilisatrice :

- Quels sont les objets cryptographiques (clés privées, clés symétriques, dispositifs de matériel inviolables, etc.) qui existent?
  - Les objectifs cryptographiques du réseau de la chaîne de blocs peuvent comprendre le stockage *en ligne* et *hors ligne* des clés cryptographiques, deux possibilités qui nécessitent de faire différents compromis techniques en ce qui concerne la vitesse d'accès par rapport à la protection contre la perte ou le vol.
  - Les clés cryptographiques plus sensibles peuvent être complètement *isolées* de toute connectivité au réseau.
  - Des dispositifs de matériel inviolables peuvent être utilisés pour renforcer la protection.
- De quelle manière les clés cryptographiques sont-elles gérées?
  - Contrôles associés à l'accès (logique et physique) aux clés cryptographiques et à leur sécurité : ces contrôles sont nécessaires à chaque étape du cycle de vie d'un objet cryptographique, qui comprend la génération, le stockage, l'utilisation et la mise hors service des clés.
  - Contrôles mis en place par l'entité utilisatrice pour gérer l'accès à la plateforme du tiers : l'accès non autorisé à des clés privées (ou la copie de telles clés) peut donner lieu à des transactions non autorisées, au vol d'actifs connexes et à la falsification de données.
  - Contrôles de séparation des tâches à l'égard des clés privées : dans certains cas, les clés cryptographiques privées peuvent être divisées en plusieurs parties, dont un sous-ensemble peut être utilisé pour récupérer la clé cryptographique d'origine. Ce processus est appelé la « fragmentation ». Les « fragments » de clés peuvent être distribués aux dépositaires responsables afin d'assurer une séparation plus tranchée des responsabilités.
  - Création de sauvegardes sécurisées : si la clé d'origine est perdue, les cryptoactifs demeurent accessibles.

TABLEAU 1 : EXEMPLES DE RISQUES ET DE CONTRÔLES – GESTION DES CLÉS CRYPTOGRAPHIQUES

Sujet	Risque / Scénario d'un problème pouvant survenir	Exa	Exh	SP	Exi	R	D	Exemple de types de contrôles
Gestion des clés	Compromission ou perte de clés cryptographiques				X		X	Contrôles à l'égard de la génération, du stockage, de l'utilisation et de la mise hors service des clés de manière sécuritaire.

Garde, tenue de registres, exécution d'ordres et opérations des clients

Les entités utilisatrices peuvent s'appuyer sur une société de services en ce qui a trait aux contrôles relatifs à la garde, à la tenue de registres, à l'exécution d'ordres et à la réalisation efficace des opérations des clients. Par conséquent, il peut être nécessaire pour la société de services de disposer de contrôles qui répondent :

- aux rapprochements entre la chaîne de blocs et les documents internes de chaque entité;
- à la tenue efficace de registres;
- à l'autorisation et la validation des interactions et des opérations des clients (y compris les dépôts, les transferts et les retraits);
- à la prévention du mélange d'actifs (lorsque les actifs sont détenus dans des portefeuilles distincts, ou tenue de registres exacts lorsque les actifs de plusieurs clients sont mélangés dans un ou plusieurs portefeuilles);
- à l'ouverture de compte et à l'exécution d'ordres.

Dans certains cas, les plateformes de négociation peuvent détenir des cryptoactifs pour le compte de l'entité et effectuer des transactions avec elle uniquement grâce à leurs propres fonctions de tenue de registres. Cette intervention accrue de la société de services a une incidence sur le risque, en particulier lorsque les transactions avec cette partie se font hors chaîne.

Vous pouvez déterminer si les objectifs de contrôle et les contrôles correspondants qui ont trait aux mécanismes de consensus et aux protocoles associés à la chaîne de blocs sont pertinents pour le contrôle interne de l'information financière de l'entité utilisatrice et, par conséquent, pour l'audit. Lorsque les registres distribués de la chaîne de blocs désignent la propriété des actifs, une défaillance dans les mécanismes de consensus pourrait entraîner la perte d'actifs. De même, si les contrôles à l'égard des mécanismes de consensus ne sont pas efficaces, ils pourraient donner lieu à des versions redondantes et incohérentes des registres distribués de la chaîne de blocs entre les participants, ce qui pourrait aboutir à un désaccord entre eux quant à la question de savoir qui possède les actifs ou si les données sont valides.

Dans de nombreux réseaux publics de chaînes de blocs, il se peut que la société de services (et l'entité utilisatrice) ne soit pas en mesure de contrôler des caractéristiques de la chaîne de blocs qui pourraient avoir une incidence sur elle (et sur l'entité utilisatrice), par exemple les mécanismes de consensus, les fourchettes et les mises à niveau de contrats[11]. Étant donné que le fonctionnement des mécanismes de consensus échappe souvent au contrôle direct de l'organisation, le rôle de la société de services peut se limiter à faire le suivi des questions et à y répondre. L'entité utilisatrice peut également avoir besoin que des contrôles soient en place pour faire un suivi du réseau et confirmer que celui-ci ne fait pas l'objet de manipulations, si la société de services n'exécute pas déjà cette fonction.

TABLEAU 2 : EXEMPLES DE RISQUES ET DE CONTRÔLES – GARDE, TENUE DE REGISTRES, EXÉCUTION D'ORDRES ET OPÉRATIONS DES CLIENTS

Sujet	Risque / Scénario d'un problème pouvant survenir	Exa	Exh	SP	Exi	R	D	Exemple de types de contrôles
Garde[12]	La société de services n'assure pas la garde de suffisamment de cryptoactifs pour répondre aux dépôts des clients. Elle n'est donc pas en mesure de s'acquitter de ses obligations envers les clients.	X			X		X	La société de services effectue un rapprochement entre les cryptoactifs dans la chaîne de blocs et ses livres et registres internes. Remarque : Cela suppose que l'auditeur de l'entité utilisatrice a obtenu des éléments probants pour valider que les informations stockées dans la chaîne de blocs sont fiables (voir la note de bas de page 11).

11 Pour de plus amples indications à ce sujet, veuillez consulter le document intitulé *Pertinence et fiabilité des informations provenant d'une chaîne de blocs* de CPA Canada.

12 Pour de plus amples indications à ce sujet, veuillez consulter le document intitulé *Tests des contrôles et assertion relative à la propriété* de CPA Canada.

Sujet	Risque / Scénario d'un problème pouvant survenir	Exa	Exh	SP	Exi	R	D	Exemple de types de contrôles
Tenue de registres	L'entité utilisatrice comptabilise des cryptoactifs ou des transactions en cryptoactifs qui sont inexacts, qui n'existent pas, qui sont incomplets ou à l'égard desquels elle ne dispose pas de contrôles suffisants sur la tenue des registres, y compris des contrôles sur les transactions hors chaîne.	X	X	X	X	X	X	La société de services dispose de contrôles sur les ventes et les achats de cryptoactifs entre l'entité utilisatrice et les clients, notamment un mécanisme par lequel, lorsque des opérations sont exécutées, elles sont automatiquement enregistrées dans le système de négociation. La société de services dispose de contrôles sur la tenue appropriée des soldes des clients, notamment le suivi des mouvements touchant ces soldes.
Relevés de clients	L'entité utilisatrice s'appuie sur des relevés de clients fournis par la société de services qui sont incomplets ou inexacts.	X	X	X	X	X	X	La société de services dispose de contrôles pour déterminer si les relevés de clients fournis à l'entité utilisatrice sont exhaustifs et exacts.
Validation des interactions des clients	En raison des risques associés aux changements dans les comptes de clients, certains clients perdent des fonds ou ne sont pas au courant de changements apportés à leur compte.	X			X			Les clients de la société de services reçoivent un avis automatisé lorsque des opérations ou des changements sont effectués dans leur compte, lequel avis comprend les coordonnées à utiliser pour signaler les opérations douteuses ou non autorisées.
Retrait de fonds	La société de services ne repère pas des cas où les clients retirent une quantité de fonds excédant leur solde actuel.	X			X			Avant de procéder à l'opération, la société de services effectue une validation automatisée afin de confirmer que le compte du client dispose de fonds suffisants.

Sujet	Risque / Scénario d'un problème pouvant survenir	Exa	Exh	SP	Exi	R	D	Exemple de types de contrôles
Regroupement de fonds	L'entité utilisatrice ne dispose pas de contrôles appropriés à l'égard des regroupements de fonds.	X			X		X	La société de services dispose de contrôles qui séparent de façon appropriée les cryptoactifs de chaque client de ses propres avoirs et de ceux des autres clients.
Ouverture de compte client	La société de services ne respecte pas les protocoles de connaissance du client.				X		X	La société des services dispose de contrôles sur l'inscription des clients, notamment des procédures de vérification de l'identité en cas d'ouverture d'un compte.
Exécution d'ordres	La société de services ne dispose pas de contrôles efficaces pour traiter les ordres.	X		X	X			La société de services dispose de contrôles afin de s'assurer que les ordres et/ou les échanges ouverts sont traités de manière exhaustive et exacte et en temps opportun lorsque l'événement déclencheur approprié survient.
Protocoles et mécanismes de consensus	Défaillance non détectée des mécanismes de consensus.				X		X	La société de services dispose de contrôles de suivi visant à confirmer qu'il n'y a pas eu de manipulation du registre distribué.

Opérations de sécurité visant l'infrastructure informatique

Comme pour la plupart des systèmes, une défaillance de la gestion de la sécurité fondamentale peut conduire à une panne et à une perte de contrôle à l'égard des registres numériques. Des contrôles efficaces de l'accès au système, de la gestion des changements et des opérations sont essentiels.

En tant qu'auditeur de l'entité utilisatrice, vous pourriez devoir déterminer à qui incombe la responsabilité de gérer les permissions d'accès à la plateforme du tiers et déterminer si les contrôles répondent adéquatement :

- à la gestion de l'identité et de l'accès, y compris la création et le maintien des comptes de participant, de même qu'à l'accès privilégié;
- à la sécurité de l'infrastructure (que ce soit dans un environnement sur site ou infonuagique);

- à la sécurité des données contenues dans différentes composantes de stockage des données (que ce soit dans un environnement sur site ou infonuagique);
- à la gestion des incidents de sécurité.

TABLEAU 3 : EXEMPLES DE RISQUES ET DE CONTRÔLES – OPÉRATIONS DE SÉCURITÉ VISANT L'INFRASTRUCTURE INFORMATIQUE

Sujet	Risque / Scénario d'un problème pouvant survenir	Exa	Exh	SP	Exi	R	D	Exemple de types de contrôles
Sécurité de l'infra-structure informatique	La défaillance des contrôles de l'infrastructure informatique a entraîné une perte de contrôle à l'égard des registres numériques.				X		X	Contrôles généraux informatiques visant l'accès au système, la sécurité du système, le développement du système, la gestion des changements et les opérations informatiques.

Une fois que vous avez acquis une compréhension des contrôles pertinents de la société de services, y compris les éléments probants indiquant qu'ils fonctionnent efficacement (lorsque votre évaluation des risques tient compte de cette attente), il se peut que vous déterminiez que vous devrez obtenir, directement auprès de la société de services, des informations sur certaines procédures de corroboration. En réponse au risque d'anomalies significatives, vous devrez déterminer si ces informations sont pertinentes et fiables.

Conclusion

L'écosystème des cryptoactifs continue de progresser. L'interaction des entités avec les plateformes de négociation, les dépositaires et les fournisseurs de portefeuilles donne lieu à des risques qui sont pertinents pour les auditeurs d'états financiers, particulièrement en ce qui a trait aux questions comme i) la gestion des clés cryptographiques; ii) la garde, la tenue de registres, l'exécution d'ordres et les opérations des clients; et iii) les opérations de sécurité visant l'infrastructure informatique.

En tant qu'auditeur de l'entité utilisatrice, vous devrez continuer de mettre à jour votre compréhension de l'entité, et plus particulièrement de son recours à des tiers dans le contexte de la détention ou de la négociation de cryptoactifs, en vue d'étayer votre évaluation des risques et de planifier des procédures d'audit complémentaires pour obtenir des éléments probants en réponse aux risques d'anomalies significatives identifiés.

Remerciements

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

CPA Canada tient à remercier Deloitte d'avoir dirigé la rédaction de la présente publication pour le Groupe de travail.

Autres ressources

1. CPA Canada. ***Facteurs à considérer pour l'audit des actifs et des transactions en cryptomonnaie*** (www.cpacanada.ca/fr/ressources-en-comptabilite-et-en-affaires/audit-et-certification/normes-canadiennes-daudit-nca/publications/audit-actifs-transactions-cryptomonnaies), 2018.
2. CPA Canada. ***L'audit des cryptoactifs : Est-il nécessaire de tester les contrôles lors de la collecte d'éléments probants à l'appui de l'assertion relative aux droits (à la propriété)?*** (www.cpacanada.ca/fr/ressources-en-comptabilite-et-en-affaires/audit-et-certification/normes-canadiennes-daudit-nca/publications/tests-controles-cryptoactifs), 2020.
3. CPA Canada. ***L'audit des cryptoactifs : Pertinence et fiabilité des informations provenant d'une chaîne de blocs devant servir comme éléments probants*** (www.cpacanada.ca/fr/ressources-en-comptabilite-et-en-affaires/audit-et-certification/normes-canadiennes-daudit-nca/publications/fiabilite-informations-chaine-blocs), 2020.
4. *Manuel de CPA Canada,* NCA 315, NCA 330 et NCA 402.

Commentaires

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

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