CPAB CCRC

CANADIAN PUBLIC ACCOUNTABILITY BOARD
CONSEIL CANADIEN SUR LA REDDITION DE COMPTES

La pratique de l'audit dans le secteur des cryptoactifs

Points de vue sur les inspections

NOVEMBRE 2019

Ce que nous avons trouvé

Il y a actuellement 48 émetteurs assujettis canadiens qui exercent leurs activités au sein du secteur des cryptoactifs. Ces activités comprennent diverses stratégies de négociation de cryptoactifs et de cryptominage.

Le Conseil canadien sur la reddition de comptes (CCRC) a relevé des constatations importantes (déficience dans le cadre de l'application de normes d'audit généralement acceptées qui pourraient donner lieu à un retraitement de l'information financière de la société) dans sept des huit dossiers d'audit inspectés à ce jour. Des mesures correctives sont toujours en cours pour certains de ces audits.

Cinq déficiences les plus souvent relevées

1. Les auditeurs ne possédaient pas une connaissance suffisante des risques d'audit lorsqu'ils ont élaboré leur approche d'audit.
2. Les auditeurs se sont fiés à des renseignements obtenus des bourses de cryptomonnaie et des dépositaires sans en évaluer la fiabilité.
3. Pour les entités qui détiennent des cryptoactifs en garde autonome, les auditeurs n'ont pas obtenu de preuves suffisantes pour valider les affirmations des entités relativement à la propriété de ces actifs.
4. Les auditeurs n'ont pas évalué la fiabilité des renseignements obtenus des chaînes de blocs.
5. En ce qui concerne les entités effectuant du cryptominage, les auditeurs ayant limité leurs travaux d'audit à la vérification des cryptoactifs reçus dans la chaîne de blocs n'ont pas obtenu de preuves suffisantes.

1. Évaluation des risques durant la planification de l'audit

De nombreux auditeurs n'ont pas adéquatement compris les risques d'audit liés aux entités auditées.

Par exemple, pour les entités qui détiennent une vaste gamme de cryptoactifs, certains auditeurs n'ont pas su détecter les risques uniques à chaque catégorie importante, y compris si les renseignements obtenus de chaque chaîne de blocs pouvaient être utilisés comme éléments probants dans le cadre de leur audit.

Une cause fondamentale de nombreuses constatations d'inspection réside dans le manque de participation de spécialistes des chaînes de blocs et des procédures cryptographiques durant la phase de planification de l'audit pour aider les auditeurs à définir les risques d'audit et à concevoir une approche d'audit pertinente.

2. Fiabilité des renseignements obtenus des bourses de cryptomonnaie et des dépositaires

Lorsqu'une entité (entité utilisatrice) a recours à une bourse de cryptomonnaie ou à un dépositaire, elle suppose souvent que l'infrastructure sous-jacente du fournisseur de services fonctionnera de façon efficace pour protéger ses actifs et maintenir des dossiers adéquats sur les opérations sur cryptoactifs et les soldes.

De nombreux auditeurs d'entités utilisatrices (auditeurs utilisateurs) n'ont pas adéquatement compris la nature et l'importance des services offerts par les sociétés de services aux entités utilisatrices et leur pertinence dans le cadre des audits. Ces auditeurs se sont fiés, à tort, à de l'information obtenue de ces sociétés de services à titre de preuves dans le cadre de l'audit, notamment les données des opérations sur cryptoactifs et les dossiers de garde, sans effectuer de test supplémentaire.

La Norme canadienne d'audit (NCA) 402, *Facteurs à considérer pour l'audit d'entités faisant appel à une société de services*, traite de la responsabilité qui incombe à l'auditeur utilisateur d'obtenir des éléments probants suffisants et appropriés lorsque l'entité utilisatrice a recours à une ou plusieurs sociétés de services. La NCA 402 fournit des précisions sur la façon dont l'auditeur utilisateur applique la NCA 315, *Compréhension de l'entité et de son environnement aux fins de l'identification et de l'évaluation des risques d'anomalies significatives*, et la NCA 330, *Réponses de l'auditeur à l'évaluation des risques*.

Lorsque l'évaluation des risques d'un auditeur utilisateur repose sur l'attente d'un fonctionnement efficace des contrôles internes de la société de services pour aborder les risques pertinents pour l'audit de l'entité utilisatrice, il doit tester l'efficacité opérationnelle de ces contrôles directement ou se fier aux contrôles connexes effectués par d'autres auditeurs (par exemple, les rapports de l'auditeur d'une société de services).

3. Propriété des cryptoactifs

Le caractère pseudonyme des chaînes de blocs constitue un enjeu unique pour les auditeurs : il est difficile d'associer l'identité dans le monde réel du propriétaire d'un cryptoactif à la série de caractères alphanumériques qui représente l'identité pseudonyme du propriétaire dans la chaîne de blocs.

Un risque d'audit fondamental est que le propriétaire légitime d'un cryptoactif puisse partager sa clé privée avec d'autres. De nombreuses personnes qui ont accès à la clé privée pourraient ainsi prétendre être propriétaires des cryptoactifs en question.

Nous avons décelé des déficiences dans les travaux d'audit visant à vérifier si les cryptoactifs détenus en garde autonome par des entités étaient en fait leurs propres actifs. Les auditeurs ont bien vérifié que chaque entité avait accès aux clés privées qui contrôlaient les cryptoactifs en question. Toutefois, accès n'est pas nécessairement synonyme de propriété, et ces auditeurs n'ont pas su obtenir des preuves suffisantes dans le cadre de l'audit pour appuyer les affirmations de l'entité relativement à la propriété.

Dans la plupart des cas, les auditeurs doivent aussi vérifier la conception et l'efficacité opérationnelle de ces contrôles internes mis en place par la direction pour aider à valider les affirmations de l'entité quant à la propriété des cryptoactifs.

4. Fiabilité des dossiers des chaînes de blocs

Les protocoles de chaînes de blocs visent à rendre ces dernières résilientes à la falsification. Toutefois, les auditeurs ne peuvent supposer que tous les protocoles sont efficaces et que les renseignements consignés dans les chaînes de blocs des 3 050 cryptoactifs actuellement en circulation (veuillez vous référer à **CoinMarketCap** pour des renseignements plus récents) sont fiables.

Les auditeurs doivent identifier les risques liés à la fiabilité des renseignements des chaînes de blocs – par exemple, des opérations non valides pourraient être ajoutées à un registre de la chaîne de blocs et les opérations validées dans la chaîne de blocs pourraient ensuite être modifiées. Les auditeurs doivent ensuite évaluer les éléments du protocole de la chaîne de blocs qui abordent ces risques. Des constatations d'inspection importantes ont aussi été relevées chez des auditeurs qui n'ont pas effectué ces travaux et pour qui les renseignements des chaînes de blocs constituaient la principale source de données pour appuyer l'existence et la survenance des soldes et des opérations sur cryptoactifs d'importance.

Nous nous attendons à ce que les auditeurs demandent à des spécialistes des chaînes de blocs et des activités de cryptographie de les aider à concevoir et à mettre en œuvre une approche d'audit appropriée.

5. Produits tirés du cryptominage

Les entités qui font appel aux services de vérification des opérations pour les réseaux de chaînes de blocs (communément appelées cryptominage) reçoivent des cryptoactifs (comptabilisés à titre de produits) à l'achèvement et à l'ajout d'un bloc à la chaîne de blocs.

Les auditeurs qui ont limité leurs travaux d'audit de la comptabilisation des produits à la vérification des cryptoactifs reçus par les entités de la chaîne de blocs ont omis de tenir compte du risque que les produits puissent comporter des anomalies significatives en raison d'erreurs ou de fraude.

Une approche d'audit pertinente comprend l'acquisition d'une compréhension de la manière dont l'entité exerce ses activités de minage et l'évaluation de la capacité de l'équipement de minage de l'entité, des tendances de consommation d'électricité associée aux activités de minage, des arrangements du groupe de minage (le cas échéant) et d'autres facteurs pertinents pour appuyer la conclusion de l'auditeur selon laquelle les cryptoactifs reçus sont attribuables à l'entité (c.-à-d. les affirmations relatives à la propriété) et sont présentés de manière fidèle pour la période visée.

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