CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

Transactions en cryptoactifs – Éléments à considérer par la direction et contrôles pour les petites et moyennes entreprises

AVERTISSEMENT

La présente publication, préparée par Comptables professionnels agréés du Canada (CPA Canada), fournit des indications ne faisant pas autorité.

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

Table des matières

Préface

Avez-vous déjà entendu parler de Bitcoin? Il s'agit d'un exemple de cryptoactif. À son apogée, un bitcoin était évalué à environ 20 089 dollars américains[1]. Les cryptoactifs s'appuient sur la technologie de la chaîne de blocs afin de permettre 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. Si votre entreprise envisage d'utiliser ou d'accepter des cryptoactifs comme mode de paiement, cette publication vous donnera un aperçu des cryptoactifs qui sont utilisés comme moyen d'échange et fera ressortir un certain nombre de considérations commerciales et de contrôles importants pour votre entreprise.

Déjà vers la fin de 2018, l'engouement suscité jusqu'alors par les cryptoactifs avait considérablement diminué; malgré tout, certaines entreprises continuent d'effectuer des investissements et des transactions impliquant des cryptoactifs. Cependant, nombre de professionnels du secteur qui soutiennent les petites et moyennes entreprises ne possèdent que peu d'expérience, voire pas du tout, en matière de cryptoactifs et pourraient donc ne pas être en mesure d'apprécier entièrement les risques associés aux transactions en cryptoactifs. En 2018 seulement, 1,7 milliard de dollars américains de cryptoactifs ont été volés[2]; il est donc primordial que les entreprises adoptent des pratiques rigoureuses en matière de sécurité afin de prévenir le vol de leurs cryptoactifs.

Les entreprises doivent également comprendre que les cryptoactifs ne sont pas garantis par le gouvernement et qu'ils doivent donc être considérés comme des actifs très spéculatifs. Contrairement aux entreprises technologiques qui ont fait faillite au début des années 2000, dans la foulée de l'éclatement de la bulle technologique, les cryptoactifs ne sont pas dotés d'un mécanisme permettant à leurs détenteurs ou acheteurs d'en connaître la valeur corporelle. Par conséquent, les entreprises doivent être au fait de cette réalité avant de se lancer dans les cryptoactifs.

Cette publication, qui ne fait pas autorité, vise à fournir aux professionnels du secteur travaillant au sein de petites et moyennes entreprises des indications à l'égard de certains des principaux enjeux auxquels sont aujourd'hui confrontées les organisations qui effectuent des transactions en cryptoactifs :

- détermination de la stratégie d'entreprise en ce qui a trait aux cryptoactifs;

1 Selon le site coinmarketcap.com, le prix sommet de 20 089 dollars américains pour un bitcoin a été atteint le 17 décembre 2017.

2 www.reuters.com/article/us-crypto-currency-crime/cryptocurrency-thefts-scams-hit-1-7-billion-in-2018-report-idUSKCN1PN1SQ

- considérations relatives au contrôle interne dans le contexte des activités liées aux cryptoactifs;
- examen d'un cadre réglementaire pour les cryptoactifs.

Cette publication fait partie d'un vaste ensemble de ressources offertes par CPA Canada relativement aux cryptoactifs. Pour en apprendre davantage sur les différentes méthodes pour comptabiliser les cryptoactifs en vertu des normes IFRS®, consultez la publication ***Introduction à la comptabilisation des cryptomonnaies selon les normes IFRS***. Pour obtenir des indications sur leur comptabilisation en vertu des NCECF, consultez plutôt la publication ***Introduction à la comptabilisation des cryptomonnaies selon les NCECF***. En ce qui concerne les répercussions des cryptoactifs sur l'audit des états financiers, reportez-vous à la publication ***Facteurs à considérer pour l'audit des actifs et des transactions en cryptomonnaie***. Pour en apprendre davantage sur la technologie sous-jacente de la chaîne de blocs, consultez la publication ***Introduction à la technologie de la chaîne de blocs***.

Au sujet des auteurs

CPA Canada tient à remercier les auteurs du présent document, Malik Datardina d'Auvenir et Michael Wong de CPA Canada, ainsi que les membres de son Comité consultatif sur les technologies de l'information pour leur contribution.

Commentaires

Nous vous prions de communiquer tout commentaire ou point de vue qui pourrait nous aider à élaborer d'autres publications sur ce sujet.

Michael Wong, CPA, CA
Directeur de projet
Recherche, orientation et soutien
CPA Canada
277, rue Wellington Ouest
Toronto (Ontario) M5V 3H2
Courriel : michaelwong@cpacanada.ca

Davinder Valeri, CPA, CA
Directrice
Recherche, orientation et soutien
CPA Canada
277, rue Wellington Ouest
Toronto (Ontario) M5V 3H2
Courriel : dvaleri@cpacanada.ca

Cryptoactifs : l'état de la situation

Victime d'un piratage en janvier 2018, la bourse de cryptoactifs Coincheck a perdu, du jour au lendemain, 500 millions de jetons NEM[3], d'une valeur de près de 500 millions de dollars[4]. La bourse conservait les actifs de ses clients dans ce que l'on appelle communément un **portefeuille en ligne** (*hot wallet*), et elle n'avait pas mis en œuvre de processus de **sécurité multisignature** (*multi-signature security*), ce qui s'est avéré être l'une des principales défaillances en matière de sécurité. Cet incident, conjugué à une multitude d'autres actes de piratage et atteintes à la sécurité, souligne l'importance, pour les entreprises, de mettre en place des contrôles rigoureux pour gérer les cryptoactifs et les transactions connexes.

Un **portefeuille en ligne** (*hot wallet*) est connecté à des réseaux externes, alors qu'un **portefeuille hors ligne** (*cold wallet*) ne l'est pas. Un **portefeuille multisignature** (*multi-signature wallet*) est un portefeuille qui prévoit un processus de sécurité multisignature et qui requiert de multiples approbations avant qu'une transaction ne soit traitée. La section « **Considérations relatives au contrôle interne dans le contexte des cryptoactifs** », ci-après, fournit des renseignements supplémentaires sur les types de portefeuilles et sur les circonstances dans lesquelles ils devraient être utilisés.

Aux fins de cette publication, le terme « cryptoactifs » s'entend uniquement des cryptoactifs qui sont utilisés comme moyen d'échange et qui se veulent une solution de rechange aux monnaies fiduciaires émises par un gouvernement. Par exemple, le bitcoin serait considéré comme un cryptoactif de ce type, alors que les contrats intelligents, qui ne fonctionnent pas principalement comme un moyen d'échange à usage général, ne le seraient pas.

La cryptobulle

La valeur et la popularité des cryptoactifs se sont accrues de manière exponentielle au cours des dernières années. La capitalisation boursière des cryptoactifs a augmenté, passant de 18 milliards de dollars américains au 31 décembre 2016 à 613 milliards de dollars américains au 31 décembre 2017, une croissance fulgurante de 3 406 %[5] qui a fait la une de

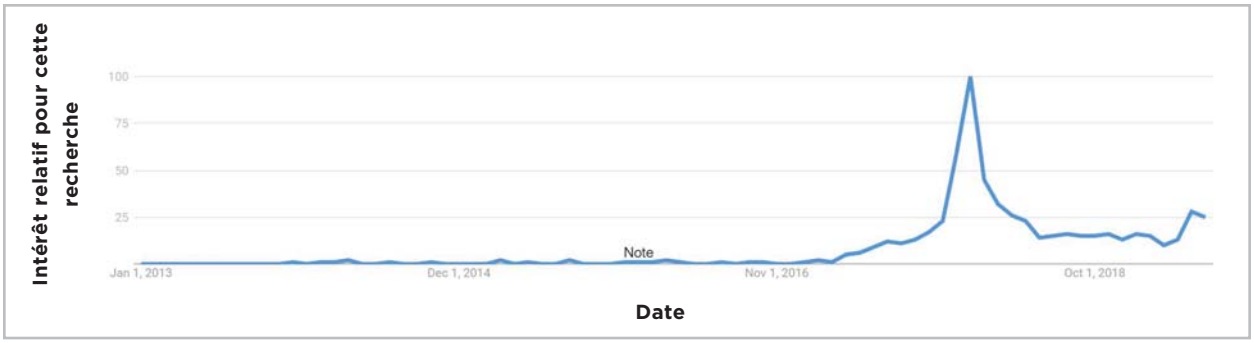
3 Lancé le 31 mars 2015, le NEM est un cryptoactif qui soutient la chaîne de blocs NEM.

4 http://fortune.com/2018/01/31/coincheck-hack-how/

5 https://coinmarketcap.com/fr/charts/

l'actualité, comme le démontre les articles intitulés *KFC Canada starts accepting Bitcoin for a bucket of chicken, immediately sells out*[6] et *Burger King Launches Crypto-asset 'Whoppercoin' in Russia*[7].

RECHERCHES DU TERME « CRYPTOMONNAIES » DANS GOOGLE DEPUIS 2013



Source : Google Trends
La popularité des cryptoactifs a bondi en 2017, comme en témoigne le pic de l'intérêt pour cette recherche dans Google à cette période. L'axe vertical représente l'intérêt pour cette recherche par rapport au point le plus élevé sur le graphique depuis 2013. La valeur de 100 représente le sommet de la popularité du terme. La valeur de 50 signifie que la popularité du terme a diminué de moitié.

La capitalisation boursière des cryptoactifs a atteint un sommet d'environ 829 milliards de dollars américains en janvier 2018, suivi d'une diminution substantielle alors qu'elle a chuté d'environ 698 milliards de dollars américains, soit 84 %, pour arriver à 131 milliards de dollars américains à la fin de décembre 2018[8].

Les cryptoactifs sont-ils tous égaux?

Il existe actuellement plus de 2 100 cryptoactifs différents[9], et ce nombre ne cesse d'augmenter car la création d'un cryptoactif est relativement facile. Bien que de nombreux cryptoactifs aient globalement des caractéristiques similaires (par exemple décentralisation et sécurité intégrée), ils ne doivent pas tous être traités de la même manière. Sans surprise, une analogie parfaite serait de comparer un panier de cryptoactifs à un panier de monnaies fiduciaires. Dans le monde des cryptoactifs, certains d'entre eux, notamment le bitcoin, sont utilisés à grande échelle, à l'instar du dollar américain, alors que de nombreux autres sont considérés comme des monnaies de marchés émergents et présentent un niveau de popularité plus faible et des risques plus élevés.

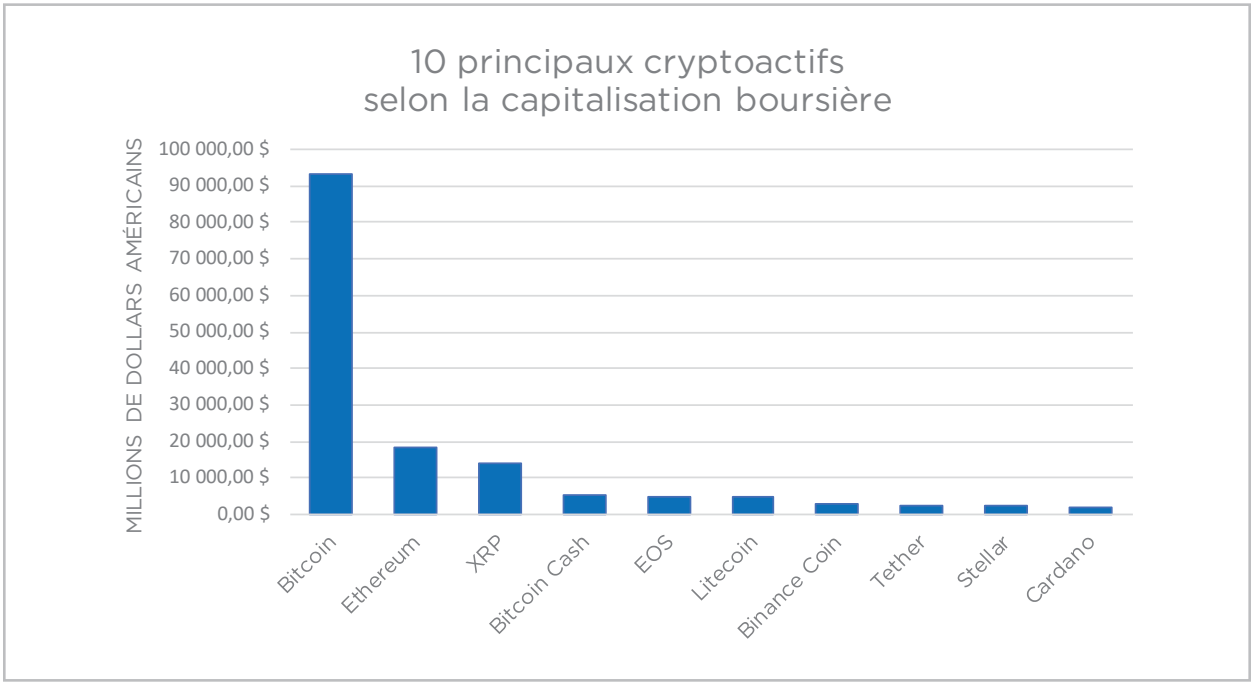
6 https://business.financialpost.com/news/retail-marketing/no-joke-kfc-canada-starts-accepting-bitcoin-for-a-bucket-of-chicken-immediately-sells-ou

7 http://fortune.com/2017/08/25/burger-king-russia-cryptocurrency-whoppercoin/

8 https://coinmarketcap.com/fr/charts/

9 https://coinmarketcap.com/fr/all/views/all/ au 16 janvier 2019

Les cryptoactifs les plus populaires sont Bitcoin et Ethereum. Bitcoin a été conçu comme un système de paiement numérique. Ethereum est similaire, mais il repose sur des capacités en matière de contrats intelligents et est parfois utilisé comme mécanisme de financement au moyen d'un processus appelé premières émissions de cryptomonnaies (PEC). Cette publication porte sur les cryptoactifs utilisés en tant que méthode de paiement et réserve de valeur, activités pour lesquelles Bitcoin constitue l'un des choix les plus populaires.



Source : coinmarketcap.com/fr au 18 avril 2019

Évolution de Bitcoin comme autre méthode de paiement

Avant l'engouement récent suscité par les cryptoactifs et Bitcoin, la possibilité d'acheter des biens avec des bitcoins était une nouveauté. À part les quelques adopteurs précoces, peu de particuliers ou de sociétés effectuaient des transactions avec des bitcoins. En 2010, un adopteur précoce a offert 10 000 bitcoins, alors évalués à environ 30 $ US, pour se faire livrer deux pizzas[10]. Ces 10 000 bitcoins valaient près de 137 millions de dollars américains à la fin de 2017; avec le recul, on peut dire que ces deux pizzas se sont avérées très dispendieuses!

Avance rapide jusqu'à 2018, où on constate que l'acceptation de bitcoins comme méthode de paiement a pris de l'ampleur, particulièrement auprès des commerçants et des fournisseurs de services en ligne. Parmi les organisations qui acceptent les bitcoins, il convient de

10 http://uk.businessinsider.com/bitcoin-pizza-10000-100-million-2017-11

mentionner notamment les magasins Shopify, Newegg, PayPal, Microsoft, et même l'État de l'Ohio (pour les impôts perçus par l'État). De plus, la ville d'Innisfil, en Ontario, a lancé un projet pilote en vertu duquel elle accepte le paiement des impôts fonciers en bitcoins. Bien que les détaillants traditionnels aient été plus lents à accepter les bitcoins, un service appelé eGifter permet aux acheteurs de se procurer en ligne, au moyen de bitcoins, des cartes-cadeaux qui peuvent ensuite être utilisées chez des détaillants populaires.

Cryptoactifs en main : Prochaines étapes?

Les cryptoactifs ne sont pas aussi largement acceptés que l'argent comptant ou les cartes de débit/crédit, et ils demeurent un créneau. À moins qu'ils ne soient détenus à des fins de placement spéculatif, les cryptoactifs sont habituellement convertis en monnaie fiduciaire. Il existe, pour les particuliers et les entreprises, un certain nombre de façons de convertir des cryptoactifs en monnaie fiduciaire :

- les guichets automatiques Bitcoin;
- les marchés de gré à gré ou les bourses en ligne de cryptoactifs;
- le troc ou l'échange avec un autre particulier;
- les systèmes de paiement en cryptoactifs.

Toutes ces méthodes d'échange fonctionnent à peu près comme celles qui s'appliquent aux monnaies fiduciaires. Par exemple, pour effectuer une transaction à un guichet automatique Bitcoin, il faut d'abord saisir le code de son portefeuille Bitcoin (semblable au NIP d'une carte de débit), puis effectuer un dépôt ou un retrait directement au guichet automatique. Une bourse en ligne de cryptoactifs fonctionne de façon similaire aux bourses de valeurs, à savoir que des intervenants du marché consentants peuvent acheter et vendre des cryptoactifs. En outre, comme avec l'argent comptant, il est possible de faire affaire directement avec une autre partie en balayant le code du portefeuille de cryptoactifs l'un de l'autre pour permettre l'échange de biens (le processus est similaire à ce qui se fait lorsqu'on balaye le code à barres sur son téléphone pour payer chez Starbucks). Enfin, un système de paiement en cryptoactifs aide les commerçants à convertir automatiquement les cryptoactifs, lorsqu'ils acceptent le paiement d'un client sous cette forme, en monnaie fiduciaire locale. Cette façon de faire est très semblable aux systèmes de paiement traditionnels qui facilitent l'acceptation des cartes de débit/crédit pour les entreprises.

Considérations commerciales relatives aux cryptoactifs

La première question que la direction devrait se poser lorsqu'elle décide d'utiliser ou non des cryptoactifs est la suivante : Quelle sera la principale finalité des cryptoactifs pour l'entreprise? Habituellement, la finalité des cryptoactifs se divise en deux grandes catégories : **transactionnelle** ou de **placement**. L'utilisation à des fins transactionnelles comprend notamment la facilitation et/ou l'acceptation de paiements en cryptoactifs, avec une durée minime de détention. L'utilisation à des fins de placement comprend le minage ou l'entreposage de cryptoactifs, la durée de détention s'étalant généralement sur le moyen ou le long terme[11]. Les considérations commerciales seront fonction de la principale utilisation des cryptoactifs par l'entreprise.

Finalité	Considérations commerciales	Considérations relatives au contrôle interne[12]
Transactionnelle	• Objectif : obtenir un avantage concurrentiel / se démarquer de la concurrence. • Risque de marché moins élevé que pour la détention à des fins de placement spéculatif. • Frais de traitement des transactions moins élevés que pour le traitement traditionnel des paiements. • Principal fournisseur de services : système de paiement en cryptoactifs.	• Nécessité d'un solide environnement de contrôle interne, mais appui important sur les systèmes de paiement en cryptoactifs. • Acquisition d'une compréhension du système de paiement en cryptoactifs utilisé (plus de renseignements ici). • Demande d'un rapport de l'auditeur de la société de services, s'il en existe un, et/ou d'éléments probants attestant du caractère approprié de la conception et du fonctionnement des contrôles pertinents émanant du système de paiement en cryptoactifs.

11 D'autres finalités ne sont pas prises en compte dans le cadre de cette publication, notamment les suivantes : partie agissant à titre de dépositaire, bourse, teneurs de marché et plateforme de négociation.

12 Les rapports d'auditeurs de sociétés de services concernant les systèmes de paiement en cryptoactifs et les bourses de cryptoactifs n'étaient pas accessibles à grande échelle au moment de la publication.

Finalité	Considérations commerciales	Considérations relatives au contrôle interne[12]
Placement	• Objectif : obtenir un rendement de placement. • Possibilité de détenir des cryptoactifs à court ou à long terme, en vue de faire des gains grâce aux changements de valeur des cryptoactifs. • Risque de marché plus élevé, mais rendement potentiel plus élevé comparativement aux catégories traditionnelles de placement comme les obligations gouvernementales. • Principal fournisseur de services : bourse de cryptoactifs.	• Nécessité d'un solide environnement de contrôle pour assurer la sûreté des cryptoactifs. • Acquisition d'une compréhension de la bourse de cryptoactifs utilisée (plus de renseignements ici). • Demande d'un rapport de l'auditeur de la société de services, s'il en existe un, et/ou d'éléments probants attestant du caractère approprié de la conception et du fonctionnement des contrôles pertinents de la bourse de cryptoactifs.

Utilisation à des fins transactionnelles

Si un système de paiement en cryptoactifs crédible est utilisé, les entreprises qui effectuent des transactions en cryptoactifs en vue de faciliter et/ou d'accepter des paiements peuvent s'attendre à des risques et à des avantages similaires à ceux associés à l'acceptation des cartes de crédit. Consultez la section « Contrôles internes et sécurité », ci-après, pour savoir quoi prendre en considération lors de l'évaluation de systèmes de paiement en cryptoactifs et de bourses de cryptoactifs. De nombreux systèmes de paiement en cryptoactifs permettent de convertir automatiquement et immédiatement en monnaie fiduciaire les paiements en cryptoactifs, réduisant ainsi le risque de marché lié à la détention des cryptoactifs. Étant donné que la valeur des cryptoactifs peut être extrêmement volatile, la conversion immédiate en monnaie fiduciaire constitue une stratégie pour atténuer ce risque.

Un autre élément à prendre en considération, en ce qui concerne les cryptoactifs, est la vitesse à laquelle les transactions sont confirmées dans leur chaîne de blocs respective. Le délai de confirmation d'une transaction conclue en cryptoactifs est habituellement plus long que celui des systèmes traditionnels de paiement comme VISA et MasterCard. Cette différence est due en grande partie à la nécessité de vérifier les transactions conclues en cryptoactifs au moyen d'un réseau décentralisé. Par exemple, les transactions en bitcoins requièrent habituellement six blocs de confirmation, ce qui peut prendre jusqu'à une heure, avant qu'elles ne soient considérées comme terminées. Ce délai peut être acceptable pour les transactions en ligne, mais peut difficilement s'appliquer dans le cas des détaillants

physiques. Toutefois, les systèmes de paiement en cryptoactifs misent sur des plateformes novatrices telles que GAP600, pour leur permettre de confirmer presque instantanément des transactions en bitcoins[13].

Sur le plan des coûts, les systèmes de paiement en cryptoactifs imposent habituellement des frais moins élevés que les systèmes de paiement par carte de crédit ou de débit. Selon une étude menée par la Fédération canadienne de l'entreprise indépendante (FCEI), les frais liés aux paiements par VISA ou MasterCard que paient les commerçants au Canada peuvent se chiffrer entre 1,65 % et 2,75 %[14], alors qu'ils sont habituellement moins élevés dans le cas des paiements en bitcoins. Par exemple, les frais associés à des transactions de base effectuées par le biais de BitPay et de Coingate sont de 1 %[15]. Une entreprise peut donc faire profiter ses clients des économies réalisées grâce à des frais de transaction moins élevés, et ainsi obtenir un avantage concurrentiel.

Bien que l'utilisation d'un système de paiement en cryptoactifs facilite le traitement des transactions et atténue certains risques liés aux cryptoactifs, elle n'est pas sans risque. Étant donné que les systèmes de paiement en cryptoactifs sont, pour la plupart, moins bien établis que les systèmes de paiement traditionnels, ils vont de pair avec un risque de liquidité et de crédit accru. Par conséquent, il est important de procéder à un contrôle diligent approprié en sélectionnant un système de paiement en cryptoactifs réputé et de confiance.

Utilisation à des fins de placement

Les entreprises utilisent également des cryptoactifs à des fins de placement, en ayant comme objectif d'obtenir un rendement de placement. Contrairement aux entreprises qui utilisent les cryptoactifs à des fins transactionnelles, celles qui se concentrent sur des activités de placement détiennent habituellement les cryptoactifs pendant plus longtemps, s'exposant par le fait même à des risques de marché beaucoup plus élevés. La détention de cryptoactifs peut également entraîner un risque plus élevé de vol interne et externe. Les entreprises concernées devront donc mettre en place des mesures renforcées de sécurité et de contrôle interne pour veiller à la sûreté de leurs portefeuilles de cryptoactifs et de leurs clés privées. Vous trouverez plus d'informations à ce sujet dans la section « Contrôles internes et sécurité », ci-après.

13 GAP600 est une plateforme qui utilise l'analyse de données pour calculer le risque de double paiement en bitcoins. Par conséquent, elle peut transmettre presque instantanément les confirmations de transactions en bitcoins aux systèmes de paiement.

14 www.cfib-fcei.ca/sites/default/files/pdf/5513.pdf

15 BitPay : https://bitpay.com/pricing
Coingate : https://coingate.com/accept-bitcoin

Les principaux coûts liés à la négociation et à la détention de cryptoactifs sont les frais de transaction appliqués par les bourses de cryptoactifs, tant pour la conversion en monnaie fiduciaire, ou à partir d'une telle monnaie, que pour les opérations d'achat ou de vente de cryptoactifs effectuées à la bourse. Les coûts engagés sont similaires aux frais de courtage encourus dans le cadre des transactions sur les marchés boursiers. La sélection d'une bourse de cryptoactifs réputée et de confiance est difficile, mais importante pour réduire les risques et s'assurer d'obtenir le meilleur prix. Outre les coûts, d'autres facteurs importants doivent être pris en considération lors de la sélection d'une bourse, soit sa liquidité et sa sécurité.

Que votre entreprise utilise des cryptoactifs à des fins transactionnelles ou de placement, il vous est fortement recommandé de commencer par :

- comprendre les risques et les avantages associés aux cryptoactifs;
- mettre en place un environnement solide de contrôle interne pour assurer la sécurité des portefeuilles de cryptoactifs et des clés privées, de même que l'intégrité des transactions sous-jacentes;
- consulter des experts du domaine, en ce qui a trait au traitement comptable et fiscal approprié;
- discuter avec vos auditeurs des incidences sur la mission d'audit.

Considérations relatives au contrôle interne dans le contexte des cryptoactifs

Contrôles internes et sécurité

Lorsqu'on envisage les risques associés aux cryptoactifs, la sécurité doit être au centre des préoccupations, et ce, pour une bonne raison. Contrairement aux fonds dans un compte bancaire dont la propriété est rattachée à la personne dont le nom figure sur le compte, la propriété des cryptoactifs est rattachée à un ensemble de clés privées et publiques représentées uniquement par une séquence de caractères alphanumériques. Quiconque a accès à la clé publique et à la clé privée correspondante peut accéder aux cryptoactifs. Habituellement, un portefeuille de cryptoactifs est utilisé pour conserver l'adresse publique d'un cryptoactif spécifique, et sert à envoyer et à recevoir le cryptoactif. Qui plus est, s'agissant de cryptoactifs tels que le bitcoin et l'ether, il faut savoir que ceux-ci peuvent facilement être convertis en espèces, en raison de la liquidité existante dans leurs marchés respectifs, ce qui les rend grandement vulnérables au vol. La question se pose de savoir s'il est possible de retracer des bitcoins volés, au moyen d'un registre ouvert. C'est effectivement le cas, puisque les transactions en bitcoins sont effectuées uniquement sous pseudonyme, et en aucun cas de façon anonyme. Des services tels que Chainanalysis peuvent aider les entreprises et les organismes d'application de la loi à faire enquête sur des fraudes et d'autres infractions criminelles. Le processus s'apparente toutefois au jeu du chat et de la souris. Des criminels précautionneux peuvent tirer parti de la pseudonymie pour blanchir de l'argent au moyen de mélangeurs qui remplacent les bitcoins volés par des bitcoins d'autres utilisateurs, de façon que les voleurs obtiennent une adresse propre que la chaîne de blocs ne peut relier à aucune des adresses à partir desquelles les bitcoins ont été volés[16]. Du fait de l'absence d'enregistrement de la propriété, de la pseudonymie et de la facilité de conversion de certains cryptoactifs en espèces, les cryptoactifs se comparent aux obligations au porteur, dans le cas desquelles, essentiellement, n'importe qui ayant accès à la clé privée peut contrôler les cryptoactifs et les utiliser comme bon lui semble.

16 www.theverge.com/2013/12/19/5183356/how-to-steal-bitcoin-in-three-easy-steps

Il n'est donc pas surprenant que de nombreux pirates aient volé des cryptoactifs à des entreprises. L'**annexe I** présente un résumé de plusieurs cas de piratage survenus récemment. En analysant ces cas de piratage pour comprendre ce qui avait mal fonctionné, il s'est avéré que plusieurs d'entre eux étaient liés à des problèmes de sécurité informatique qui n'étaient pas propres aux cryptoactifs.

- **Compréhension inadéquate de la technologie**
  Le piratage de Mybitcoins est survenu en raison d'une mauvaise compréhension de la manière dont Bitcoin garantit les transactions dans le bloc suivant. Ce genre de problème existe pour n'importe quelle technologie naissante, et il illustre bien comment l'utilisation de la technologie peut vous amener au bord du gouffre plutôt qu'en tête de peloton. Par conséquent, il est important de comprendre le protocole sous-jacent de la chaîne de blocs qui a été utilisé pour un cryptoactif, car tous les cryptoactifs ne sont pas conçus de la même façon.
- **Mauvaise analyse des risques**
  La mise en œuvre de contrôles nécessite une compréhension de l'équation des risques sous-jacents. Dans le cas de Linode et de Bitfloor, les pirates ont compromis des systèmes dont il avait été considéré qu'ils présentaient un risque faible. Ainsi, le piratage de Bitfloor est survenu en raison de l'idée reçue selon laquelle un ordinateur sans accès public présente un risque moins élevé et ne nécessite pas des contrôles de sécurité étendus.
- **Mauvaise configuration des contrôles**
  Les contrôles de sécurité tels que l'authentification multifactorielle sont efficaces lorsqu'ils sont établis de manière appropriée. L'authentification multifactorielle est une pratique de sécurité en vertu de laquelle l'utilisateur est tenu de fournir au moins deux éléments d'identification lorsqu'il tente de se connecter à un compte (par exemple, mot de passe et empreinte digitale). Toutefois, dans le cas de Inputs.io, les pirates ont utilisé de vieux comptes de courriels auxquels un deuxième élément d'identification approprié (par exemple, numéro de téléphone) n'était pas rattaché de façon à permettre le bon fonctionnement de l'authentification multifactorielle.

Avant de s'intéresser aux contrôles relatifs à Bitcoin, il est important de se rappeler que les cryptoactifs en sont encore à leurs balbutiements et que l'élaboration d'un ensemble définitif de pratiques exemplaires reste à faire. Toutefois, des experts comme Andreas Antonopoulos recensent plusieurs éléments à prendre en considération aux fins de la sécurité des cryptoactifs[17].

17 Andreas M. Antonopoulos. *Mastering Bitcoin: Programming the Open Blockchain*, 2e édition, O'Reilly Media, Inc., 2017.

- **Comprendre la bourse de cryptoactifs et/ou le système de paiement en cryptoactifs utilisé**
  Toutes les bourses de cryptoactifs ne s'équivalent pas. Certaines conservent les cryptoactifs de chaque utilisateur dans un portefeuille commun plutôt que dans des portefeuilles en ligne individuels. D'autres essaient d'économiser les frais de transaction en créant un système qui fait le suivi des transactions *au lieu* de s'appuyer sur la chaîne de blocs proprement dite. Les transactions de ce type sont habituellement appelées « transactions hors chaîne ». Par conséquent, l'information consignée dans un système qui fait le suivi uniquement des transactions hors chaîne ne tire pas profit du mécanisme de consensus ou d'autres protocoles de sécurité de la chaîne de blocs. Il est important d'effectuer des recherches adéquates avant de sélectionner une bourse appropriée.
- **Choisir un type de portefeuille approprié**
  Étant donné que les portefeuilles en ligne sont connectés à Internet, les pirates sont en mesure de compromettre les fournisseurs de portefeuille plus facilement et d'accéder aux cryptoactifs entreposés. Par conséquent, il n'est pas recommandé de conserver tous vos cryptoactifs dans un portefeuille en ligne. Les portefeuilles hors ligne constituent habituellement une meilleure option pour l'entreposage à long terme. Bien qu'ils puissent être moins pratiques que les portefeuilles en ligne, les portefeuilles hors ligne sont généralement plus sécuritaires parce qu'ils ne sont pas connectés à des réseaux externes. Il existe habituellement deux types de portefeuilles hors ligne : les portefeuilles papier (*paper wallet*) et les portefeuilles matériels (*hardware wallets*).
  — *Portefeuilles papier*
  Il peut sembler ironique qu'une manière sûre de protéger votre monnaie numérique puisse consister à imprimer votre clé privée et à la conserver dans un lieu sûr et sécuritaire. Cette méthode est toutefois sujette à un risque de destruction et de détérioration au fil du temps.
  — *Portefeuilles matériels*
  À la différence des téléphones intelligents et des ordinateurs, les portefeuilles matériels sont des dispositifs qui servent uniquement à entreposer de façon sécuritaire les clés privées pour accéder aux cryptoactifs. Le marché grand public en offre plusieurs comme Trezor One, Ledger Nano S et KeepKey. Les principaux avantages des portefeuilles matériels par rapport aux portefeuilles logiciels (*software wallets*) tiennent au fait que :
    - les clés privées sont conservées de façon sécuritaire sur des microcontrôleurs protégés et ne peuvent pas être transférées en fichier texte;
    - les clés privées ne sont pas en interaction avec des logiciels potentiellement vulnérables et sont moins vulnérables aux attaques de logiciels malveillants tels que les chevaux de Troie.

- **Conserver le contrôle de la clé privée**
  Les transactions effectuées en cryptoactifs s'appuient sur des clés publiques et privées. L'« adresse » publique de votre portefeuille est créée à partir d'un condensé de votre clé publique et permet à d'autres personnes d'effectuer des transactions avec vous. La clé publique est dérivée de la clé privée. Votre clé privée n'est ni plus ni moins que la « clé » de votre « maison », à votre « adresse » publique. Si vous perdez le contrôle de votre clé privée, vous perdez le contrôle de vos cryptoactifs. Par conséquent, vos clés privées doivent être gardées en sécurité à partir du moment où elles sont générées, et tout au long de la détention du portefeuille de cryptoactifs. Il n'est pas recommandé de partager une clé privée avec d'autres personnes.
- **Maintenir la sécurité physique des clés privées**
  Les portefeuilles hors ligne sont plus sécuritaires que les portefeuilles en ligne dans la mesure où des contrôles adéquats ont été mis en place relativement à la sécurité physique des clés privées. Par conséquent, malgré la nature numérique des cryptoactifs, leur sécurité physique n'en est pas moins importante. En effet, la sécurité physique des clés privées devrait être aussi perfectionnée et rigoureuse que s'il s'agissait d'autres sortes d'actifs à valeur élevée. Entre autres lieux d'entreposage possibles, mentionnons un coffre-fort ou une chambre forte dont l'accès est contrôlé.
- **Veiller à la bonne gestion des copies de sauvegarde de la clé privée**
  M. Antonopoulos indique dans son livre que [Traduction] « près de 7 000 bitcoins ont été perdus dans le cadre d'un projet bien connu de sensibilisation et de formation sur le sujet des bitcoins. Dans l'optique de prévenir le vol, les propriétaires avaient mis en œuvre une série complexe de sauvegardes chiffrées. Malheureusement, ils ont accidentellement perdu les clés de chiffrement, ce qui a rendu les sauvegardes inutiles et leur a fait perdre une fortune ». Comme pour d'autres systèmes informatiques, vous devez mettre en place des processus de sauvegarde appropriés (en vous assurant d'avoir accès aux sauvegardes) afin de protéger vos clés privées.
- **Diversifier les stratégies d'entreposage**
  Le fait de conserver tous vos cryptoactifs dans un seul et même portefeuille présente un risque élevé, étant donné que tous vos cryptoactifs seraient perdus si ce portefeuille était compromis. Envisagez d'utiliser une combinaison de différents types de portefeuilles et de fournisseurs, afin de réduire les répercussions si un portefeuille individuel vient à être compromis.
- **Envisager les portefeuilles multisignatures**
  Le concept des portefeuilles multisignatures n'est pas nouveau. L'une des pratiques exemplaires, en ce qui concerne la gestion des clés de chiffrement, est la « connaissance répartie » (c'est-à-dire que personne ne possède l'intégralité de la clé). Les portefeuilles multisignatures [Traduction] « garantissent la sécurité des fonds en exigeant plusieurs signatures pour effectuer un paiement. Les clés de signature doivent

être entreposées dans plusieurs endroits différents et se trouver sous le contrôle de différentes personnes. Dans le contexte d'une entreprise, par exemple, les clés devraient être générées de façon indépendante et détenues par plusieurs hauts dirigeants, de façon à assurer qu'une personne ne puisse à elle seule compromettre les fonds » (Antonopoulos, 2017). Les cérémonies de clés privées constituent une manière de générer de nouvelles clés. Reportez-vous à l'exemple ci-dessous, qui concerne la cérémonie des clés privées de Coinbase, pour de plus amples renseignements.

Cérémonies des clés privées – L'exemple de Coinbase[18]

Coinbase est une bourse de cryptoactifs qui est considérée comme l'une des bourses axées sur le consommateur les plus populaires aux États-Unis. La société traite des transactions et entrepose des cryptoactifs à l'échelle mondiale. De quelle façon une société comme Coinbase génère-t-elle ses clés privées?

La première étape du processus est de monter une tente Faraday. Une telle tente est conçue de manière à empêcher que les signaux électromagnétiques s'échappent ou soient interceptés par des pirates. La cérémonie des clés privées se déroule donc à l'intérieur de la tente Faraday, comme suit : un ordinateur portable Linux est choisi au hasard en tirant à pile ou face et est ensuite utilisé pour générer les clés privées. Les clés privées imprimées sont ensuite entreposées en lieu sûr dans un coffre-fort sécurisé. Une fois la cérémonie terminée, l'ordinateur portable utilisé pour générer la clé est détruit afin de prévenir la fuite de données.

Certaines des étapes suivies par Coinbase peuvent sembler extrêmes, mais elles font ressortir qu'il est important de protéger les clés privées dès le départ. Les entreprises devraient consulter des experts du domaine lorsqu'elles conçoivent leur cérémonie des clés privées.

Attentes de l'auditeur

Alors que les considérations relatives au contrôle mentionnées plus haut sont utiles pour renforcer la sécurité des cryptoactifs dans le cadre des activités de l'entreprise, les auditeurs pourraient devoir obtenir des éléments probants supplémentaires (y compris en ce qui concerne la conception et la mise en œuvre des contrôles) pour répondre aux risques spécifiques qui sont propres aux cryptoactifs. Les auditeurs pourraient également devoir effectuer des évaluations indépendantes pour comprendre la pertinence et la fiabilité des informations reçues grâce à la technologie sous-jacente de la chaîne de blocs.

18 www.wired.com/story/coinbase-physical-vault-to-secure-a-virtual-currency/

Concernant la sécurité de l'accès aux clés privées, les auditeurs peuvent demander à participer aux cérémonies des clés privées afin d'obtenir des éléments probants de la présence d'un solide environnement de contrôle, et ainsi s'assurer que les clés sont générées de manière sécuritaire du point de vue cryptographique et qu'aucune copie non autorisée n'a été faite. Dans le cas des cryptoactifs détenus sur une bourse ou un système de paiement, l'auditeur peut chercher à obtenir un rapport de l'auditeur de la société de services de la bourse ou du système de paiement; si un tel rapport n'est pas disponible ou si son étendue n'est pas appropriée pour les fins visées par l'auditeur, ce dernier peut envisager de tester directement les contrôles internes de la bourse ou du système de paiement.

Les transactions avec des parties liées constituent un autre aspect auquel il peut être nécessaire de porter une attention particulière. En raison de la nature pseudonymique des cryptoactifs, il peut être difficile d'associer des portefeuilles de cryptoactifs (constitués de séquences de caractères et de chiffres) à des entités dans le monde réel. Pour surmonter ce problème, il vous faut établir un environnement de contrôle efficace au sein de l'organisation. Vous devez également mettre en place des politiques et des procédures pour acquérir une connaissance suffisante des parties avec lesquelles votre entreprise conclura des transactions en cryptoactifs. En outre, vous devez attribuer, au sein de votre organisation, les responsabilités inhérentes à l'identification, à l'enregistrement et à la communication des transactions avec des parties liées.

Pour en apprendre davantage sur les répercussions des cryptoactifs sur l'audit, consultez la publication ***Facteurs à considérer pour l'audit des actifs et des transactions en cryptomonnaie*** de CPA Canada.

De nombreuses entreprises considèrent encore les cryptoactifs comme un nouveau territoire. Une extrême vigilance est donc nécessaire à l'égard de ce type d'actifs. En cas de doute, demandez des indications à des experts du domaine et à des conseillers afin de déterminer les contrôles requis pour sécuriser vos cryptoactifs.

Environnement réglementaire

Partout dans le monde, les autorités de réglementation et de surveillance affichent un grand intérêt à l'égard des cryptoactifs. Aux États-Unis, le Financial Stability Board (FSB), en collaboration avec le Committee on Payments and Market Infrastructures (CPMI), a conçu un cadre pour surveiller la stabilité financière des marchés de cryptoactifs. Dans un récent rapport, le FSB a indiqué que, bien que les cryptoactifs ne représentent pas un risque significatif pour la stabilité financière mondiale à l'heure actuelle, il est nécessaire de surveiller de près la situation, étant donné la rapidité à laquelle les marchés évoluent[19]. Alors qu'il n'existe pas encore de règles mondiales à l'égard des cryptoactifs, les gouvernements du monde entier ont adopté différentes stratégies pour les surveiller et les réglementer à l'échelle nationale. Ces réglementations ne cessent d'évoluer, au fur et à mesure du développement des cryptoactifs. Les entreprises qui envisagent une expansion dans le domaine des cryptoactifs doivent donc examiner soigneusement le cadre réglementaire des pays où elles prévoient d'aller de l'avant.

Bien qu'il existe des motifs d'affaires légitimes à l'utilisation de cryptoactifs, force est de constater que ceux-ci peuvent également être utilisés par des criminels pour exercer des activités illicites ainsi que pour orchestrer la mise en place de rançongiciels. Malheureusement, c'est souvent par suite d'une attaque par rançongiciel que les sociétés (et leurs consultants en informatique) en viennent à apprendre à connaître les cryptoactifs, étant donné qu'elles ont dû payer les pirates en bitcoins ou autres cryptoactifs pour récupérer l'accès à leur système et à leurs données. Les cryptoactifs peuvent également être utilisés pour perturber l'ordre établi. Ainsi, Satoshi Nakamoto (dont l'identité n'est pas vraiment connue[20]) a créé Bitcoin dans la foulée de la crise financière de 2008, qui avait vu la réputation du modèle de confiance centralisé être durement touchée du fait de la prise de risques excessifs de la part des institutions financières. D'ailleurs, avec Bitcoin, les cybermilitants n'en étaient pas à leur première tentative de créer une monnaie virtuelle visant à permettre aux particuliers de gagner une certaine indépendance par rapport à l'État et aux entreprises. Dans bien des cas, cela explique pourquoi les gouvernements du monde entier s'efforcent de réglementer les cryptoactifs.

19 www.fsb.org/wp-content/uploads/P160718-1.pdf

20 Satoshi Nakamoto est le nom utilisé par la personne ou le groupe, dont l'identité n'est pas connue, qui a créé Bitcoin et a rédigé un livre blanc sur le bitcoin, intitulé *The White Paper*.

Au Canada

Les cryptoactifs ne sont pas considérés comme ayant cours légal au Canada, et ils sont définis comme des marchandises en vertu des lois canadiennes. Toutefois, les paiements en cryptoactifs sont quand même assujettis à l'impôt en vertu de la *Loi de l'impôt sur le revenu*[21]. Pour en savoir plus sur leur comptabilisation selon les normes IFRS et sur les répercussions fiscales liées aux cyberactifs au Canada, consultez la publication ***Introduction à la comptabilisation des cryptomonnaies selon les normes IFRS*** de CPA Canada.

Bien que, au moment d'écrire ces lignes (juin 2019), le gouvernement fédéral canadien en soit encore à effectuer la mise au point définitive de la réglementation des cryptoactifs, cela n'a pas empêché les autorités de réglementation et les organismes fédéraux d'agir (vous trouverez, à l'**annexe III**, une liste de certaines des indications qui ont été publiées par les autorités de réglementation au Canada et aux États-Unis). À titre d'exemple, mentionnons que l'Agence du revenu du Canada (ARC) envisage sérieusement d'auditer les détenteurs de cryptoactifs et qu'elle leur a fait parvenir des questionnaires exhaustifs à remplir concernant leurs activités liées aux bitcoins au cours des dernières années[22]. De plus, des organismes tels que les Autorités canadiennes en valeurs mobilières (ACVM) ont publié des avis de leur personnel sur les émissions de cryptoactifs pouvant être considérées comme des placements de titres[23]. Par conséquent, les entreprises doivent se tenir au courant de l'évolution de la réglementation afin de garantir leur conformité aux lois et règlements canadiens.

À l'échelle internationale

Les pays dans le monde adoptent des approches différentes à l'égard des cryptoactifs. Certains, comme le Venezuela, les ont accueillis à bras ouverts et ont créé leur propre monnaie virtuelle, alors que d'autres, comme la Chine, en ont freiné l'utilisation par leurs citoyens.

La lutte de Beijing contre le bitcoin s'inscrit dans une tentative plus vaste qui vise à éradiquer les risques menaçant le système financier du pays. En 2017, de hauts représentants du pays ont fait circuler un projet de règles en matière de lutte contre le blanchiment d'argent concernant les échanges de bitcoins; un avertissement percutant, même si, selon des personnes au fait de ces questions, ces règles n'ont jamais été officialisées. En théorie, les monnaies virtuelles permettent à leurs détenteurs de contourner le système bancaire

21 www.loc.gov/law/help/cryptocurrency/canada.php

22 www.forbes.com/sites/ktorpey/2019/03/06/bitcoin-investors-targeted-with-audits-by-canadas-federal-tax-agency/#133439e1656e

23 https://lautorite.qc.ca/fileadmin/lautorite/reglementation/valeurs-mobilieres/0-avis-acvm-staff/2017/2017aout24-46-307-avis-acvm-fr.pdf

traditionnel de la Chine en vue de déplacer de l'argent à l'extérieur des frontières contrôlées par la capitale. Les autorités de réglementation chinoises pourraient donc avoir plus de difficulté à maintenir un contrôle serré sur le yuan[24].

Bien que la réglementation adoptée aux États-Unis soit minime relativement à l'utilisation des cryptoactifs, certains organismes gouvernementaux américains tels que la Federal Deposit Insurance Corporation (FDIC) et le Department of Justice (DOJ) ont pris des mesures réglementaires clés contre les organisations qui utilisent les bitcoins. Ainsi, la FDIC aurait mis de la pression sur les responsables de la conformité des banques afin qu'ils ne travaillent pas avec des organisations utilisant des bitcoins. Le DOJ a quant à lui lancé, en 2013, une initiative connue son le nom de *Operation Choke Point* visant à enquêter sur les banques faisant affaire avec des entreprises qui, sans forcément se livrer à des activités illégales, étaient considérées comme présentant un risque élevé de fraude et de blanchiment d'argent. Les entreprises visées par cette enquête comprenaient des fournisseurs légaux de services liés aux bitcoins. L'opération a eu le résultat escompté, qui était de couper l'accès aux services bancaires et financiers aux entreprises visées par une enquête, puisque le risque qu'elles fassent l'objet d'un audit par le DOJ a suffi à dissuader les institutions financières concernées de travailler avec ces entreprises[25].

Dans l'Union européenne (UE), les autorités financières ont souligné les risques associés aux cryptoactifs, mais n'ont pas encore proposé de règles significatives à cet égard. En janvier 2019, l'Autorité bancaire européenne (ABE) a publié un rapport dans lequel elle conseille à la Commission européenne de procéder à une évaluation approfondie de la question de savoir si des mesures réglementaires sont nécessaires à une approche commune des pays membres de l'UE à l'égard des cryptoactifs.

Bien que les cryptoactifs soient généralement conçus pour être sans frontières et accessibles à l'échelle mondiale, les mesures réglementaires actuelles et la réglementation en cours d'élaboration pourraient en limiter l'accessibilité. Toutefois, les cryptoactifs poursuivent leur essor et maintiennent leur avance sur l'élaboration des cadres réglementaires, faisant en sorte que les autorités concernées doivent rattraper leur retard. L'incertitude entourant la réglementation constitue donc un risque réel, et il est important de comprendre comment un organisme de réglementation appréhende les activités liées aux cryptoactifs, afin de mieux évaluer et anticiper les risques liés à la réglementation dans un pays donné.

La réglementation relative aux cryptoactifs finira par gagner en clarté. Malgré l'engouement initial qu'a suscité leur apparition, les cryptoactifs n'en sont encore qu'à leurs balbutiements. Comme dans le cas des obligations en matière de lutte contre le blanchiment d'argent et de connaissance de la clientèle, qui sont maintenant la norme au sein des institutions

24 www.wsj.com/articles/china-to-shut-bitcoin-exchanges-sources-1505100862

25 Vigna, Paul. *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order*, St. Martin's Press, Kindle Edition, p. 258-259.

financières, des procédures standards et des contrôles seront élaborés en temps opportun relativement aux cryptoactifs. D'ici là, la réglementation entourant les cryptoactifs naissants manquera de clarté dans la plupart des pays. C'est d'ailleurs pour cette raison, sans compter le fait que la position varie d'un pays à l'autre en matière de réglementation, que les entreprises ont de la difficulté à tirer parti de l'utilisation des cryptoactifs dans leurs activités. Pour le moment, les cryptoactifs demeurent un outil marginal pour les passionnés.

Annexe I – Analyse de cas de piratage de cryptoactifs

Piratage	Date	Ampleur des pertes	Résumé de l'incident	Ce qui a mal fonctionné
allinvain	Juin 2011	25 000 bitcoins, d'une valeur de 500 000 $ US	Cette attaque était l'un des premiers cas signalés de vol de bitcoins[26].	Un logiciel malveillant ayant compromis la sécurité du portefeuille a permis au pirate de transférer des bitcoins dans un autre portefeuille.
Mybitcoins[27]	Août 2011	154 406 bitcoins, d'une valeur de 2 millions de dollars américains	Mybitcoins offrait des services d'entreposage de portefeuilles à ses utilisateurs, et conservait la moitié des bitcoins par stockage à froid. Selon un message publié à l'intention de ses utilisateurs, Mybitcoins avait l'intention de leur rembourser ce qu'ils possédaient. Toutefois, rien n'indiquait clairement de quelle manière Mybitcoins pourrait restituer les bitcoins, étant donné que ses systèmes étaient compromis.	Un pirate a tiré parti du caractère inapproprié de l'interface des contrôles entre le système et le grand livre de la chaîne de blocs. Le site avait indiqué qu'une erreur humaine semblait être en cause, de même qu'une mauvaise compréhension de la manière dont Bitcoin garantit les transactions pour le bloc suivant de la chaîne.

26 www.forbes.com/sites/timworstall/2011/06/17/bitcoin-the-first-500000-theft/#74c5604d29b3

27 https://observer.com/2011/08/mybitcoin-spokesman-finally-comes-forward-what-did-you-think-we-did-after-the-hack-we-got-shitfaced/

Piratage	Date	Ampleur des pertes	Résumé de l'incident	Ce qui a mal fonctionné
Linode	Mars 2012	46 703 bitcoins, d'une valeur de 228 845 $ US	Plus de 43 000 des bitcoins volés appartenaient à Bitcoinica, une plateforme de négociation de bitcoins, et 3 094 autres bitcoins ont été soutirés du portefeuille virtuel de Marek Palatinus, un programmeur indépendant de la République tchèque. Ce dernier a indiqué en entrevue qu'un autre utilisateur de Bitcoin avec lequel il avait communiqué avait perdu 50 bitcoins à cause des mêmes pirates. De plus, Gavin Andresen, le programmeur en chef de Bitcoin, a perdu les cinq bitcoins qu'il avait entreposés dans un compte en ligne[28].	Un pirate a ciblé des portefeuilles Bitcoin entreposés sur des serveurs de Linode, après s'être attaqué à un portail de service à la clientèle.
Bitfloor	Septembre 2012	24 000 bitcoins, d'une valeur d'environ 250 000 $ US	Des serveurs ont été compromis, ce qui a permis au pirate d'accéder aux bitcoins et de les transférer. La grande majorité des bitcoins qui se trouvaient dans la bourse ont été volés pendant cette attaque[29].	Il a été possible d'accéder à la sauvegarde du portefeuille parce que Bitfloor a supposé que le risque de compromission était faible, étant donné que l'ordinateur utilisé pour la sauvegarde n'avait pas d'accès public.

28 https://arstechnica.com/information-technology/2012/03/bitcoins-worth-228000-stolen-from-customers-of-hacked-webhost/

29 www.nbcnews.com/technology/250-000-worth-bitcoins-stolen-net-heist-980871

Piratage	Date	Ampleur des pertes	Résumé de l'incident	Ce qui a mal fonctionné
Inputs.io[30]	Octobre 2013	4 100 bitcoins, d'une valeur de plus de 1 million de dollars américains	Inputs.io, qui était gérée par un développeur connu sous le nom de TradeFortress parmi les utilisateurs du bitcoin, a été piratée. La société exploitait également la banque de bitcoins CoinLenders, de même que le salon de clavardage CoinChat. Le développeur avait l'intention de rembourser les utilisateurs au moyen de bitcoins en stockage à froid ainsi qu'à partir de son propre compte.	Le pirate a contourné l'authentification multifactorielle en utilisant des comptes de courriel corrompus qui étaient faciles à réinitialiser du fait de l'absence de numéros de téléphone rattachés à ces comptes. Cette situation était attribuable à une faiblesse au niveau de l'hébergement du serveur.
BIPS[31]	Novembre 2013	1 295 bitcoins, d'une valeur de 650 000 $ US	Le principal système de paiement et détenteur de portefeuilles en ligne d'Europe a perdu 1 295 bitcoins. Selon la société située à Copenhague, les fonds volés lui appartenaient[32].	La société a été la cible de deux attaques successives qui, selon elle, étaient reliées. La première a consisté en une vaste attaque par déni de service, et la deuxième a entraîné la désactivation du site, la surcharge des commutateurs gérés et l'annulation de la connexion iSCSI aux réseaux de stockage sur les serveurs de BIPS.

30 www.theguardian.com/technology/2013/nov/08/hackers-steal-1m-from-bitcoin-tradefortress-site

31 www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency

32 www.coindesk.com/bitcoin-payment-processor-bips-attacked-1m-stolen

Piratage	Date	Ampleur des pertes	Résumé de l'incident	Ce qui a mal fonctionné
PicoStocks[33]	Juin et novembre 2013	1 300 bitcoins en juin et 5 896 bitcoins en novembre	Selon le magazine *Wired*, PicoStocks était un marché boursier non réglementé de bitcoins, prétendument constitué dans les îles Marshall. PicoStocks a essayé de contourner la réglementation fédérale des valeurs mobilières en fonctionnant comme s'il détenait lui-même les actifs et que les spéculateurs achetaient simplement des flux de dividendes.	Le magazine *Wired* a également indiqué que le piratage de juin 2013 résultait d'une sécurité déficiente. PicoStocks réutilisait les mêmes mots de passe pour une multitude de comptes, une pratique que le fondateur a lui-même qualifiée d'extrêmement stupide en s'attribuant la responsabilité du vol. Le magazine *Wired* a révélé que la deuxième attaque, commise en novembre, touchait à la fois des portefeuilles en ligne et hors ligne. Étant donné qu'un pirate en ligne ne peut pas accéder aux portefeuilles hors ligne, le vol est probablement venu de l'intérieur.

33 www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency

Piratage	Date	Ampleur des pertes	Résumé de l'incident	Ce qui a mal fonctionné
Mt. Gox[34]	Février 2014	850 000 bitcoins, d'une valeur de 450 millions de dollars américains	Un russe nommé Alexander Vinnik était le propriétaire et exploitant d'une bourse concurrente, appelée bitcoins-e. Le Federal Bureau of Investigation des États-Unis a affirmé que M. Vinnik avait, en connaissance de cause, accepté des bitcoins volés de la part de Mt. Gox, et qu'il les avait blanchis au moyen de sa propre bourse de bitcoins.	On croit qu'en juin 2011, l'ordinateur portable d'un auditeur a été corrompu, ce qui a permis à des pirates de modifier artificiellement la valeur nominale des bitcoins à un cent, puis d'en transférer environ 2 000 à partir de comptes de clients de la bourse et de les vendre. Quant au deuxième cas de piratage, on croit qu'il aurait commencé avant septembre 2011, lorsque la clé privée de Mt. Gox a été déchiffrée et semble avoir été volée par le biais d'un fichier wallet.dat copié, soit par un pirate, soit par une personne en interne.

34 https://blockonomi.com/mt-gox-hack/

Piratage	Date	Ampleur des pertes	Résumé de l'incident	Ce qui a mal fonctionné
Bitstamp	Janvier 2015	19 000 bitcoins, d'une valeur de 5,2 millions de dollars américains	Située au Royaume-Uni, Bitstamp est la deuxième plus importante bourse de bitcoins en dollars américains. Elle a interrompu ses activités après avoir découvert des preuves selon lesquelles près de 19 000 bitcoins, soit environ 5,2 millions de dollars, auraient été volés en ligne à son magasin opérationnel de bitcoins. La société a alerté ses utilisateurs au sujet de la possible attaque et les a mis en garde à l'égard d'éventuels transferts de bitcoins vers les anciennes adresses de dépôt de bitcoins de la société. Bitstamp a plus tard révélé que l'attaque avait touché moins de 19 000 bitcoins. Il s'est avéré que la véritable attaque avait en fait compromis les fonds opérationnels de la société, à savoir ses portefeuilles en ligne. La société a précisé que ses bitcoins étaient en grande partie en stockage à froid et étaient donc conservés de façon totalement sécuritaire[35].	Les fonds opérationnels de Bitstamp étaient entreposés dans un portefeuille en ligne, lequel a été compromis par des pirates. Le principal problème était la quantité de bitcoins entreposés dans le portefeuille en ligne, puisque les portefeuilles en ligne ne devraient pas être utilisés pour entreposer de grandes quantités de bitcoins. Les bitcoins qui avaient été entreposés dans des portefeuilles hors ligne n'ont pas été compromis.

35 https://arstechnica.com/information-technology/2015/01/bitcoin-exchange-bitstamp-claims-hack-siphoned-up-to-5-2-million/

Piratage	Date	Ampleur des pertes	Résumé de l'incident	Ce qui a mal fonctionné
Bitfinex	Août 2016	120 000 bitcoins, d'une valeur de 77 millions de dollars américains	Selon des commentaires formulés sur Reddit par Zane Tackett, directeur des affaires communautaires et du développement de produits chez Bitfinex, un total de 119 756 bitcoins ont été volés. La valeur moyenne d'un bitcoin étant de 650 $, cela représente plus de 77 millions de dollars[36].	Le défi posé par le piratage de Bitfinex réside dans le fait que la bourse utilisait BitGo, une approche multi-signature en matière de sécurité (autrement dit, il faut plus d'une signature pour exécuter une transaction). Dans un article renvoyant à une infographie de Bloomberg, on suppose que les pirates ont tiré parti de l'automatisation nécessaire pour obtenir la deuxième signature. Toutefois, rien n'a été confirmé quant à ce qui s'est véritablement passé[37].

36 https://arstechnica.com/information-technology/2016/08/bitcoin-value-falls-off-cliff-after-58m-in-btc-stolen-in-hong-kong-exchange-hack/

37 https://altcointoday.com/how-bitfinex-was-hacked/

Piratage	Date	Ampleur des pertes	Résumé de l'incident	Ce qui a mal fonctionné
QuadrigaCX	Février 2019	Cryptoactifs d'une valeur de 180 millions de dollars américains	Selon la BBC, les cryptoactifs semblent avoir été perdus à la suite du décès du chef de la direction de la société, qui était le seul à avoir accès aux cryptoactifs détenus en stockage à froid[38].	Les cryptoactifs ont été perdus en raison de l'absence d'une planification adéquate de la relève (c'est-à-dire qu'il n'y avait pas d'autre détenteur d'accès qui aurait pu accéder aux cryptoactifs en l'absence prolongée du principal détenteur d'accès). Qui plus est, la nature globalement non réglementée des bourses de cryptoactifs expose les acheteurs à de tels risques, puisqu'il n'existe actuellement aucune réglementation qui exigerait que ces bourses fassent l'objet d'audits indépendants ou d'examens par les autorités de réglementation.

38 www.bbc.com/news/world-us-canada-47203706

Annexe II – 10 questions à se poser lorsqu'il s'agit de considérer les cryptoactifs pour des petites et moyennes entreprises

1. Quelle est la finalité principale des cryptoactifs pour mon entreprise?
2. Mon entreprise a-t-elle consulté des experts du domaine au sujet des répercussions comptables, fiscales, légales et réglementaires liées à la conclusion de transactions en cryptoactifs? Les membres de mon entreprise comprennent-ils tous les risques associés aux cryptoactifs?
3. Mon entreprise fera-t-elle appel à un fournisseur de services liés aux cryptoactifs? Le cas échéant, ce fournisseur dispose-t-il d'un rapport de l'auditeur de la société de services ou d'une autre source d'assurance qui démontre le caractère adéquat des contrôles internes pertinents qui ont été mis en place au sein de son organisation?
4. Mon entreprise a-t-elle procédé à d'autres formes de contrôle diligent à l'égard du fournisseur de services liés aux cryptoactifs, afin de s'assurer que les critères qu'il applique en matière de sécurité, de fiabilité et d'intégrité répondent aux normes suivies par mon organisation?
5. Mon entreprise a-t-elle sélectionné le type approprié de portefeuille de cryptoactifs, et y a-t-il des contrôles d'accès adéquats à l'égard de ce portefeuille?
6. Les clés privées de mon entreprise sont-elles sûres? Sont-elles sauvegardées de manière sécuritaire, et est-il possible d'y avoir accès en l'absence du principal détenteur de clé? Mon entreprise a-t-elle procédé à une cérémonie des clés privées, et a-t-elle mis en œuvre des contrôles appropriés pour prouver la propriété des clés privées?
7. Mon entreprise a-t-elle élaboré et consigné des méthodes comptables appropriées relativement aux cryptoactifs?
8. Mon entreprise a-t-elle discuté avec les auditeurs des répercussions des cryptoactifs sur les missions d'audit? Quels autres éléments probants (y compris les contrôles internes) peuvent être nécessaires pour traiter les risques particuliers associés aux cryptoactifs?

9. Mon entreprise comprend-elle les obligations juridiques et les exigences réglementaires qui s'appliquent à l'échelle locale, en ce qui a trait aux transactions en cryptoactifs? Mon entreprise comprend-elle également les différences qui existent relativement au traitement des transactions en cryptoactifs dans les autres pays où elle exerce ses activités?
10. Les risques rattachés aux cryptoactifs et à la mise en œuvre des contrôles internes appropriés étant bien compris, mon entreprise est-elle à l'aise avec les risques résiduels à l'échelle de l'organisation?

Annexe III – Sélection d'indications réglementaires

Autorités canadiennes en valeurs mobilières (ACVM) / Commission des valeurs mobilières de l'Ontario (CVMO) / Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM)

- 24 août 2017 – Avis 46-307 du personnel des ACVM, *Les émissions de cryptomonnaies*
- 6 juin 2018 – Mise en garde des ACVM à l'intention des investisseurs : *Invitation à la prudence pour les Canadiens investissant sur des plateformes de négociation de cryptoactifs*
- 25 juin 2018 – Avis de l'OCRCVM 18-0119 – Avis administratif – Généralités – *Priorités de l'OCRCVM pour l'exercice 2019*
  - Annonce de la formation d'un groupe de travail sur la chaîne de blocs qui aura pour mandat de recommander des mesures réglementaires s'il y a lieu.
  - Consulter le secteur (Accenture) pour mieux comprendre les aspects réglementaires liés à l'innovation, à la technologie et à l'évolution des exigences des clients.
- 5 juillet 2018 – Avis 11-781 du personnel de la CVMO, *Notice of Statement of Priorities for 2018-2019*
  - Soutient l'innovation « fintech » grâce à la Rampe de lancement de la CVMO; identifie les occasions de moderniser la réglementation; continue à identifier les lacunes réglementaires découlant des développements concernant la cryptomonnaie, les premières émissions de cryptomonnaies et les chaînes de blocs.
- 10 juillet 2018 – Rapport des ACVM sur l'application de la loi 2017-2018, *L'application de la législation en valeurs mobilières dans un monde interconnecté*
  - Aborde la mise sur pied du Groupe d'intervention sur la fraude en matière d'investissement; la collaboration avec des plateformes numériques mondiales dans le but d'interdire la publicité sur les cryptomonnaies et les PEC; un premier recours intenté au Québec.
- 14 mars 2019 – Document de consultation 21-402 du Canada, *Projet d'encadrement des plateformes de négociation de cryptoactifs*

Securities and Exchange Commission (SEC) des États-Unis

- 11 décembre 2017 – Déclaration sur les cryptomonnaies et les premières émissions de cryptomonnaies (par le président de la SEC, Jay Clayton)
- 19 janvier 2018 – Déclaration conjointe des directeurs de l'application de la loi de la SEC et de la CFTC sur les mesures d'exécution relatives aux monnaies virtuelles
- 22 janvier 2018 – Publication, par le président de la SEC, d'un avertissement à l'intention des sociétés qui changent leur nom pour y intégrer les mots « bitcoin » ou « chaîne de blocs »
- 24 janvier 2018 – Publication, par les présidents de la SEC et de la CFTC, d'un article d'opinion dans le *Wall Street Journal* indiquant qu'ils surveillent étroitement les activités liées aux cryptomonnaies et qu'ils prendront les mesures nécessaires, au besoin
- 7 mars 2018 – Déclaration de la Division of Enforcement et de la Division of Trading and Markets sur les plateformes en ligne potentiellement illégales pour la négociation d'actifs numériques
- 6 juin 2018 – Déclaration du président de la SEC, Jay Clayton, qui laisse entendre à CNBC que le bitcoin n'est pas un titre
- 16 novembre 2018 – Déclaration sur l'émission et la négociation de titres / d'actifs numériques
- 29 novembre 2018 – Deux célébrités accusées d'avoir illégalement fait la promotion d'une émission de cryptomonnaie
- 12 décembre 2018 – De hauts dirigeants règlent le différend lié à une arnaque visant une première émission d'une cryptomonnaie
- 20 février 2019 – Une société règle le différend lié à une première émission d'une cryptomonnaie non enregistrée, après s'être autodéclarée à la SEC
- 3 avril 2019 – Déclaration sur le cadre de référence pour l'analyse des contrats d'investissement liés à des actifs numériques

Financial Industry Regulatory Authority (FINRA) des États-Unis

- 21 décembre 2017 – La FINRA avertit les investisseurs de ne pas se laisser piéger par les arnaques relatives aux cryptomonnaies
- 31 mai 2018 – Publication d'un article sur la compréhension des monnaies virtuelles
- 16 août 2018 – Mise en garde à l'intention des investisseurs sur les premières émissions de cryptomonnaies : les choses à savoir et des trucs éprouvés pour les investisseurs
- 6 septembre 2018 – Publication d'un article indiquant comment éviter de se faire piéger par les arnaques relatives aux cryptoactifs

- 11 septembre 2018 – La FINRA accuse un courtier de fraude et de distribution illégale de titres de cryptomonnaies non enregistrés
- 29 novembre 2018 – Publication d'un article sur la manière d'entreposer et de sécuriser les cryptomonnaies

North American Securities Administrators Association (NASAA)

- 4 janvier 2018 – Déclaration de la NASAA indiquant qu'il faut faire preuve de prudence en ce qui concerne les cryptomonnaies, les PEC et autres produits de placement connexes (complémentaire à la déclaration de la SEC)

CPA
COMPTABLES
PROFESSIONNELS
AGRÉÉS
CANADA

277, RUE WELLINGTON OUEST
TORONTO (ONTARIO) M5V 3H2
T. 416 977.3222 F. 416 977.8585
WWW.CPACANADA.CA