

Balado sur l'état des cryptoactifs

Épisode 2

Adam Rodricks:

Bonjour à tous et bienvenue! Je suis votre hôte, Adam Rodricks, et je suis heureux de vous accueillir aujourd'hui pour une série spéciale PodBytes de KPMG intitulée « Les cryptomonnaies : un état de la situation ». Si vous avez raté notre premier épisode, je vous encourage à l'écouter également.

Aujourd'hui, mes collègues des Services-conseils en technologie, Edwin, Kunal et Kareem se joignent à moi. Bienvenue à tous. Faisons d'abord quelques présentations. Nous commencerons par vous, Edwin. Dites à tout le monde ce que vous faites au sein du cabinet.

Edwin Isted:

Je m'appelle Edwin Isted, et je suis associé au sein des Services-conseils – Management de KPMG au Canada. Je travaille principalement dans le domaine des paiements, mais aussi dans celui des actifs numériques et de la chaîne de blocs.

Kunal Bhasin:

Bonjour Adam. Je suis ravi d'être de retour. Je m'appelle Kunal Bhasin et je suis directeur principal au sein de notre groupe Services-conseils-Gestion des risques et je codirige notre groupe Chaîne de blocs et cryptoactifs aux côtés de Kareem.

Kareem Sadek:

Je suis Kareem Sadek. Je suis associé au sein du groupe Services-conseils en Gestion du risque technologique de KPMG, et comme Kunal vient de le dire, je codirige le groupe Chaîne de blocs avec lui. C'est toujours un plaisir de discuter avec vous.

Adam Rodricks:

Et c'est un plaisir partagé. Kareem, je vais commencer par vous. Je pense que bon nombre de nos auditeurs connaissent bien les modèles classiques de dépositaires qui s'appliquent aux catégories d'actifs physiques et dématérialisées. Pouvez-vous nous présenter quelques-uns des modèles qui concernent sur les actifs numériques et expliquer en quoi ils diffèrent des modèles classiques?

Kareem Sadek:

En termes simples, les cryptoactifs sont stockés dans des chaînes de blocs. Pensez au bitcoin, l'actif, qui est enregistré dans la chaîne de blocs de l'entreprise Bitcoin. Pensez également à l'éther. L'éther est la cryptomonnaie d'Ethereum, qui est utilisée pour payer les transactions interagissant avec ces applications de finance décentralisée qui sont stockées sur Ethereum.

Voici un exemple que Mitch, l'un des membres de notre équipe, utilise tout le temps. La propriété de ces actifs repose sur des paires de clés public-privé. Pensez à la clé publique comme à une adresse courriel, où quelqu'un qui connaît mon adresse peut m'envoyer des messages. La clé privée est semblable au mot de passe du compte de messagerie, qui doit être utilisé chaque fois qu'une transaction est envoyée. Si mon mot de passe est compromis, n'importe qui peut envoyer des courriels à partir de mon compte. De même, si ma clé privée est volée, les cryptoactifs contenus peuvent être supprimés.

Edwin Isted:

Pour ce qui est des deux questions entourant les modèles de dépositaires, deux approches sont possibles : l'une est l'auto-garde, où vous vous occupez vous-même des clés, et l'autre, qui dépend d'un dépositaire dédié. L'auto-garde était l'intention initiale autour du bitcoin, où les utilisateurs détiendraient leurs propres clés pour contrôler leurs propres fonds. Cependant, à mesure que la valeur des cryptoactifs a augmenté et que les investisseurs institutionnels sont entrés dans le secteur (y compris ces investisseurs qui ont manifestement un mandat fiduciaire), de nombreux dépositaires de niveau institutionnel ont vu le jour. Ensemble, ces sociétés détiennent des centaines de milliards de dollars en cryptoactifs et fournissent des services à des investisseurs institutionnels en tant que clients.

Adam Rodricks:

Des centaines de milliards, ça dépasse l'imagination. Kunal, pouvez-vous décrire certains des avantages liés au recours à un dépositaire?

Balado sur l'état des cryptoactifs

Épisode 2

Kunal Bhasin:

Pensez aux transactions sur une chaîne de blocs, qu'il s'agisse de Bitcoin ou d'Ethereum. Toutes ces opérations sont de nature atomique et irrévocables; il est donc essentiel d'avoir en place les bons niveaux de contrôle pour s'assurer que le bon montant est envoyé ou reçu, et que les adresses des destinataires sont exactes.

Un dépositaire est avantageux pour ces organisations parce qu'elles disposent de technologies et de contrôles spécifiques, comme les systèmes de calcul multiséigneur ou multicorps qui augmentent la sécurité de ces opérations. En exigeant de multiples signataires ou en partageant la clé privée en plusieurs morceaux distincts et en disposant de contrôles appropriés pour les transactions, le risque que la clé privée puisse être compromise pour servir à une transaction illégitime est largement réduit.

Une autre raison pour laquelle les organisations ont tendance à avoir recours à un dépositaire est la réduction du temps de mise en marché. Imaginez qu'une entreprise cherche à réaliser une transaction en cryptomonnaie : si elles cherchent à établir à l'interne cette capacité de garde, le temps de mise en marché de ses placements augmente de beaucoup. Toutefois, si cette entreprise peut déjà compter sur les services d'un dépositaire qui dispose de l'infrastructure nécessaire, l'intégration avec ce dépositaire est une solution qui réduit le temps de mise en marché de près de la moitié ou plus.

Adam Rodricks:

Voilà qui est vraiment intéressant. J'aimerais examiner la question sous un autre aspect. Du point de vue d'un investisseur institutionnel, les avantages d'un dépositaire sont très clairs? Edwin, que faut-il prendre en considération lors de l'évaluation d'un dépositaire?

Edwin Isted:

Il y en a deux qui me viennent à l'esprit : l'une est le modèle opérationnel requis par l'institution pour la transaction et la couverture d'assurance du dépositaire. Selon la nature des activités de l'institution, il faut différents modèles pour que la transaction ait lieu.

Par exemple, un pupitre de négociation d'une grande institution financière effectuera des transactions plus actives qu'un gestionnaire d'actifs qui rééquilibre quotidiennement les produits de placement ou qu'un bureau de gestion familiale qui procède à une affectation stratégique à long terme. Ainsi, à mesure que la fréquence des transactions augmente, différents processus de gouvernance des clés privées sont en place pour maximiser la commodité tout en ne compromettant pas la sécurité.

Kunal Bhasin:

Une autre chose qui me vient à l'esprit, et ce sont les rapports d'attestation du centre de gestion de la sécurité (ou Security Operations center ou SoC) qui sont fournis par ces dépositaires. Il s'agit d'une pratique exemplaire que les dépositaires appliquent ces jours-ci, puisque la délivrance de rapports d'attestation en vertu du SoC 1 et 2 donne un aperçu de leur environnement de contrôle interne en ce qui a trait à la sécurité, à la protection des renseignements personnels, à la confidentialité, à la disponibilité, etc. Leurs clients utilisent ces rapports SoC pour examiner les pratiques actuelles de ces sociétés de garde et évaluer si elles sont en mesure de satisfaire aux exigences réglementaires et aux exigences internes de ces institutions.

Kareem Sadek:

C'est une belle introduction au sujet suivant : qu'arrive-t-il quand la sécurité est compromise? Nous parlons de ces rapports SoC; il s'agit d'essayer de répondre à certaines de ces attentes en matière de sécurité. Mais qu'arrive-t-il quand la sécurité est compromise?

Il est essentiel de disposer d'une couverture d'assurance complète. On en entend beaucoup plus parler de l'assurance et de son fonctionnement. Parmi les principales considérations relatives à la couverture, mentionnons les limites globales de la police, la question de savoir si une assurance supplémentaire est offerte et si le placement excède la limite. Il faut savoir aussi si la police couvre les actes malhonnêtes des employés, les vols et les cas de force majeure comme les inondations ou les pannes d'électricité qui peuvent compromettre les clés privées. Qui sont les assureurs qui proposent la police? Mais surtout, comment cette couverture d'assurance s'intègre-t-elle réellement à l'assurance existante de l'entreprise?



Balado sur l'état des cryptoactifs

Épisode 2

Kareem Sadek (continué):

Je pourrais en dire plus, mais j'aimerais bien entendre le point de vue de nos auditeurs. J'espère qu'ils nous contacteront parce que j'aimerais avoir une discussion plus approfondie à ce sujet et voir comment nous pouvons les aider dans leur parcours en matière de cryptoactifs.

Adam Rodricks:

On dirait qu'il y a pas mal de choses à considérer! Nous pourrions sans doute poursuivre la conversation, et c'est pour cette raison que nous proposons à nos auditeurs une série en quatre parties sur l'état de la situation des cryptomonnaies. L'épisode d'aujourd'hui est terminé. Il me reste à vous remercier pour votre temps et vos précieux conseils.

Joignez-vous à nous pour le prochain épisode de la série PodBytes de KPMG au Canada sur l'état des cryptoactifs. Nous accueillerons Kareem, Kunal et Mitch pour une discussion sur la preuve de réserves, un processus particulièrement intéressant qui permet de s'assurer que les actifs inscrits dans les livres internes correspondent aux actifs stockés dans les chaînes de blocs. Je suis Adam Rodricks. Merci beaucoup de votre écoute et à la prochaine