Balado sur l'état des cryptoactifs

Épisode 13

Adam Rodricks:
Bonjour tout le monde et bienvenue à ce nouvel épisode de la série de balados de KPMG au Canada sur l'état des cryptoactifs. Nous sommes de retour avec un épisode très spécial axé sur la fraude et les crimes financiers. Pour l'épisode d'aujourd'hui, je suis ravi d'accueillir Amrit Dev et Liezel Pistorius, directrices principales en Juricomptabilité et en studio avec nous pour la première fois pour diriger notre discussion. Comment allez-vous aujourd'hui?

Amrit Dev:
Très bien, merci Adam.

Liezel Pistorius:
Ça va à merveille. Merci Adam. Je suis très heureuse d'être ici aujourd'hui.

Adam Rodricks:
Tout le plaisir est pour nous. Et ils sont rejoints par quelqu'un qui n'a plus besoin qu'on le présente, mais nous le ferons tout de même : Kunal Bhasin, directeur, Services-conseils – Risques technologiques et un habitué de notre balado. Kunal, comment allez-vous aujourd'hui?

Kunal Bhasin:
Très bien Adam. Je suis ravi d'être ici. Merci à tous!

Adam Rodricks:
Je vais commencer avec nos nouveaux invités, Liezel et Amrit. J'aimerais commencer comme le font la plupart des films de super héros, par l'histoire de vos origines. Comment avez-vous été amenées à offrir des services de juricomptabilité à des organisations aux prises avec des crimes financiers?

Amrit Dev:
Merci Adam. Bonjour à tous, ici Amrit. Je travaille en juricomptabilité et dans le domaine de la criminalité financière depuis 6 à 7 ans. Quand j'ai commencé au sein de l'équipe Juricomptabilité de Toronto chez KPMG, j'ai eu la chance de commencer ma carrière dans un domaine qui me tient à cœur depuis toujours. J'ai récemment fait connaissance avec le secteur des cryptoactifs en travaillant dans la division de l'application des mesures législatives à la Commission des valeurs mobilières de l'Ontario, et c'est là que j'ai acquis une expérience pratique des questions liées aux cryptoactifs.

J'ai travaillé sur diverses escroqueries où l'arnaqueur disparaît avec votre argent (« rug pull »), sur des cas de piratage, d'activités non enregistrées, et de manipulation du marché qui avaient tous un lien avec la finance décentralisée (DeFi). Je suis donc ravie d'être ici aujourd'hui pour parler de criminalité financière et du secteur des cryptoactifs avec l'équipe. Je passe la parole à Liezel.

Liezel Pistorius:
Merci Amrit. Je suis aussi directrice principale en Juricomptabilité chez KPMG depuis environ huit ans maintenant, et je cumule 14 années d'expérience dans le secteur numérique, toujours chez KPMG. Ce qui m'a amenée à travailler dans ce domaine en particulier, c'est une famille très fortunée, qui m'est arrivée avec un énorme problème un jour dans une situation très personnelle et émotive, pour me demander de l'aider à récupérer ses investissements en cryptoactifs. Ce client n'avait plus accès à ses investissements, ne savait plus comment faire pour y accéder et se demandait même s'il reverrait un jour la couleur de son argent.

Je voulais aider ces personnes, essayer de récupérer leurs cryptoactifs, et c'est vraiment là que j'ai fait mon entrée en scène dans le secteur. Et évidemment, j'ai misé sur mes compétences en enquêtes technologiques et en réponse aux incidents, que j'ai acquises au fil des ans en juricomptabilité, en tant que professionnelle de ce domaine.

Donc oui, j'espère continuer à soutenir de nombreux particuliers et organisations dans ce secteur.

Adam Rodricks:
J'adore ça, merci d'avoir partagé votre histoire avec nous. Nous avons donc deux personnes passionnées en studio avec nous aujourd'hui.

La première question que nous examinerons consiste à savoir s'il y a matière à s'inquiéter. Quelle est la prévalence de la fraude et des crimes financiers dans le secteur des cryptoactifs?

Balado sur l'état des cryptoactifs

Épisode 13

Amrit Dev:
Je serai heureuse de me lancer en premier en répondant à cette question. La criminalité financière a de toute évidence gagné le secteur des cryptoactifs et est en augmentation ces dernières années.

Malgré le ralentissement du marché, le volume des transactions illicites dans la chaîne de blocs a augmenté en 2022, atteignant un sommet historique de 20 milliards de dollars. Et c'est d'après le rapport sur le crime de Chainalysis 2023. Ce que je trouve intéressant à propos de ce chiffre de 20 milliards, c'est qu'il n'inclut pas les faillites que nous avons vues l'année dernière de plusieurs grandes entreprises de crypto.

En réalité, quand on avance le chiffre de 20 milliards, on sous-estime vraiment la fraude et les crimes financiers qui se produisent dans ce secteur. Ce qui nous donne l'espoir aux professionnels en juricomptabilité, c'est notre capacité à retracer l'activité illicite dans une large mesure. En effet, chaque transaction enregistrée dans la chaîne de blocs est un enregistrement permanent de ce qui s'est passé et du moment où cela s'est produit. Et c'est quelque chose qui était compliqué à faire en finance classique, car nous traitons souvent avec différentes entités qui stockent des données sous différents formats.

La capacité de retracer une transaction sur la chaîne de blocs est ce qui nous permet de voir qu'une grande partie des 20 milliards de volumes illicites dont j'ai parlé plus tôt peut être attribuée à des transactions impliquant des entités qui ont été sanctionnées l'année dernière. Et je suis sûr que nous parlerons des sanctions un peu plus tard aujourd'hui.

Nous observons également l'évolution du type de crime financier dans le secteur. On est passé du piratage de bourses centralisées à un nombre en croissance d'exploits dans le secteur de la finance décentralisée, et plus de la moitié de ces coups d'éclat se produisent sur des ponts entre chaînes, selon Token Terminal.

Dans l'ensemble, la fraude et le crime financier continuent d'être un risque dans ce domaine, surtout compte tenu des contrôles typiques (inaudibles) tels que la séparation des actifs des clients, les règles sur les dépositaires, la conformité à la connaissance du client et les procédures de lutte contre le blanchiment d'argent font souvent défaut.

Mais j'aimerais aussi entendre ce que pense Liezel à ce sujet.

Liezel Pistorius:
Rapidement, beaucoup d'entre vous savent peut-être que l'environnement numérique a changé après la pandémie. Je ne veux pas revenir à la pandémie, mais en fin de compte, une bonne part de ce que nous faisons aujourd'hui sur le plan numérique a radicalement changé.

Et dans le monde de la criminalité financière, nous avons vu des augmentations spectaculaires. Amrit vient de citer le rapport Chainalysis, mais parmi les cas que nous voyons, une des façons les plus courantes d'utiliser les cryptoactifs pour commettre une fraude ou un crime financier consiste à payer des pots-de-vin ou des commissions occultes en cryptomonnaie.

Il y a aussi les actifs mal acquis qui sont convertis en cryptomonnaies afin de rapidement cacher les fonds mal acquis. Le blanchiment d'une partie des produits de la fraude au moyen de cryptomonnaies, puis aussi le détournement d'actifs en cryptomonnaie en général, est l'un des principaux méfaits que nous avons observés.

Et nous allons certainement parler plus en détail de ces sujets au cours du balado. Kunal a certainement des choses importantes à ajouter. Kunal, c'est à vous.

Kunal Bhasin:
Merci Liezel. Je suis d'accord avec tout ce que vous et Amrit avez mentionné. Le crime financier a existé et pratiquement sous toutes les formes depuis qu'il existe des d'instruments financiers, et les cryptoactifs ne font pas exception.

Vous savez, comme il s'agit d'une technologie relativement nouvelle, qui peut être utilisée comme moyen de paiement et de transfert de valeur au-delà des frontières, cela a bien certainement attiré l'attention de nombreux acteurs illicites par le passé, et ça continue.

En même temps, il importe de se rappeler que la transparence qu'apporte la nature même de cette technologie permet de retracer et de surveiller les transactions illicites et d'enquêter sur elles.

Balado sur l'état des cryptoactifs

Épisode 13

Kunal Bhasin:
Dans une certaine mesure, la possibilité d'éviter l'implication des institutions dans ces transactions illicites existe pour un grand nombre d'acteurs du marché.

Donc, même si je suis tout à fait d'accord et que le crime financier en ce qui concerne les cryptoactifs et la fraude liée aux cryptoactifs est en hausse, cela nous motive encore davantage.

Et je dis que nous, par nous, je veux dire, toutes les institutions et les organismes de réglementation. Nous sommes motivés à instaurer plus de clarté réglementaire sur la façon dont les programmes de lutte contre le recyclage des produits de la criminalité et le financement des activités terroristes au sein de ces organisations peuvent être modifiés pour surveiller et suivre ces activités illicites et les garder à l'œil.

Adam Rodricks:
Très bien dit, Kunal. Liezel a très bien amené le sujet. Si elle continue, je vais devenir inutile. Alors permettez-vous de passer au sujet suivant.

Amrit, ma prochaine question s'adresse à vous? Je veux parler un peu de la façon dont fonctionnent les mixeurs de cryptoactifs. En 2022, nous avons vu l'augmentation des sanctions imposées par le Bureau du contrôle des avoirs étrangers, mais quelle est l'incidence réelle des sanctions imposées aux mixeurs sur le risque financier?

Amrit Dev:
Merci Adam. Je pense que Kunal y a fait allusion dans sa réponse.

Avant de répondre à votre question sur les mixeurs de cryptomonnaies, je veux souligner l'évolution du blanchiment d'argent dans le secteur des cryptos. Quand Bitcoin est apparu pour la première fois, nous pensions que les transactions seraient intraçables et anonymes. Cette idée fausse a depuis volé en éclat, car de nombreux cybercriminels ont été arrêtés au cours des dernières années, grâce aux techniques de traçage qui sont maintenant destinées à examiner les mouvements dans la chaîne de cryptoactifs.

Le ministère de la Justice des États-Unis a récemment récupéré plus de la moitié des 4,3 millions de rançongiciels payés par Colonial Pipeline en 2021.

Par conséquent, nous avons vu des cybercriminels à la recherche de nouvelles façons d'améliorer le pseudo-anonymat de leurs transactions et de blanchir leurs cryptoactifs illicites. Ce que cette méthode repose sur des services, appelés mixage de cryptomonnaies. Cela ne veut pas dire que la seule raison d'être des mixeurs est le blanchiment d'argent. Il y a aussi des usages légitimes auxquels je ne m'attarderai pas aujourd'hui.

Pour répondre à votre question, en quoi consiste le mixage de cryptomonnaies? Les services de mixage de cryptomonnaies sont des services qui combinent vos cryptoactifs avec ceux d'autres utilisateurs pour brouiller la source de fonds. Les mixeurs se servent à cette fin de contrats intelligents qui exécutent de multiples combinaisons de transactions de différents montants, ce qui fait que l'utilisateur reçoit un résultat final qui est relié au mixeur, et pas nécessairement l'adresse à partir de laquelle les fonds ont été déposés.

De cette façon, les mixeurs brisent la chaîne de possession et rendent le traçage des fonds plus difficile.

Je réponds ensuite à la deuxième partie de votre question sur l'impact des sanctions des mixeurs sur le risque financier. Permettez-moi tout d'abord d'expliquer en quoi consistent les sanctions. Des agences comme le Bureau du contrôle des avoirs étrangers aux États-Unis et ses équivalents dans d'autres pays appliquent des sanctions contre des individus et des entités considérés comme des menaces à la sécurité nationale.

Traditionnellement, l'application des sanctions repose sur la coopération des institutions financières classiques, et désormais sur les bourses de cryptomonnaies qui respectent les lois.

Comme nous l'avons dit plus tôt, il y a eu en 2022 un nombre accru de sanctions dans le secteur des cryptomonnaies. Et l'une des plus remarquables, était peut-être celle qui a été imposée Tornado Cash, un mixeur mieux connu pour avoir servi à blanchir des fonds volés par des cybercriminels associés à la Corée du Nord.

Balado sur l'état des cryptoactifs

Épisode 13

Amrit Dev:
Il faut savoir que les transactions associées aux services sanctionnés représentent un risque important pour les entreprises en matière d'observation fiscale, y compris les amendes et les accusations criminelles potentielles. Et ces amendes peuvent aller de milliers de dollars à plusieurs millions, y compris des peines de prison allant jusqu'à 30 ans.

L'an dernier, des bourses centralisées ont conclu des règlements avec le Bureau qui concernaient leur la responsabilité éventuelle dans des transactions effectuées sur leur plateforme par des entités visées par des sanctions.

Ainsi, le filtrage des sanctions devient l'un des contrôles de plus en plus importants pour les entreprises qui présentent un risque en matière de cryptoactifs. C'était là la réponse longue à votre question. Je vais passer la parole Kunal et Liezel pour qu'ils puissent ajouter quelque chose au besoin.

Adam Rodricks:
Pas de commentaires, alors je poursuis. Ma prochaine question s'adresse à Liezel.

J'aimerais en savoir un peu plus sur la façon dont les criminels utilisent réellement les cryptoactifs dans le cadre des attaques par rançongiciel.

Mais avant d'aller plus loin, peut-être pourrait-on commencer par définir ce qu'est un rançongiciel.

Liezel Pistorius:
Oui, c'est un bon commencement en effet. Et Amrit y a brièvement fait allusion quand nous avons parlé des mixeurs de cryptoactif. Disons d'abord que les rançongiciels dans le domaine des cryptomonnaies ne sont pas très différents qu'ailleurs dans le monde numérique, c'est exactement la même chose.

Pour répondre à votre question, un rançongiciel est essentiellement un logiciel malveillant conçu pour infiltrer les systèmes d'une organisation ou d'une personne. Ils visent davantage les organisations, car leur but ultime est d'infiltrer et de perturber de grandes organisations où la valeur des rançons peut être plus élevée. Les rançongiciels servent deux objectifs.

D'abord et avant tout, il s'agit de perturber les opérations, en prenant le contrôle des données et de l'information d'une organisation. Il s'agit de bloquer l'accès pour que plus personne n'ait le contrôle. Ensuite, ils sont utilisés pour extorquer des fonds aux organisations infiltrées. Donc, qu'il y ait ou non des cryptomonnaies en jeu, c'est à cela que servent des rançongiciels.

Revenons à la façon dont les criminels utilisent les cryptoactifs dans le cadre de ces attaques par rançongiciels. Lorsque l'attaque a fonctionné et que les criminels ont accès aux systèmes de l'organisation, ils utilisent les machines infectées pour mettre l'organisation devant un ultimatum. Elle doit payer la rançon non seulement pour que ses systèmes soient déverrouillés, mais aussi pour que les renseignements personnels qui se trouvent parmi ses données ne soient pas divulgués. Toute l'information liée aux renseignements personnels est très sensible, très privée, ce sont des numéros d'assurance sociale, des numéros de comptes bancaires, des dates de naissance - il y a tout un éventail de renseignements de ce type dont les organisations sont dépositaires.

Donc l'organisation paie la rançon pour que ses systèmes soient débloqués, mais aussi pour les renseignements personnels qu'elle détient ne soient pas divulgués sur le Web caché. Les criminels qui procèdent à des attaques par rançongiciels exigent parfois d'être payés en cryptomonnaies.

Kunal aimerait peut-être parler de sa propre expérience en ce qui a trait aux attaques par rançongiciels. Je peux toutefois affirmer que nous avons constaté une augmentation spectaculaire des attaques par rançongiciel perpétrées contre les organisations.

Je peux toutefois compter sur les doigts d'une seule main les rares fois où les auteurs exigent d'être payés en cryptomonnaie. Dernièrement, j'ai certes constaté une augmentation de demandes de cryptomonnaies, mais il pourrait s'agir d'une goutte dans l'océan.

Balado sur l'état des cryptoactifs

Épisode 13

Kunal Bhasin:
Oui, c'est un bon point, Liezel. J'ajouterais que selon le rapport de Chainalysis, une bonne partie des cryptoactifs qui sont demandés par ces attaquants et acteurs illicites finit par passer par les bourses centralisées, les mixeurs et d'autres bourses B2B. Ultimement, les criminels ont besoin de convertir cette cryptomonnaie en monnaie fiduciaire.

Après avoir payé la rançon, les organisations visées embauchent des enquêteurs qui se pencheront sur les transactions au sein de la chaîne pour savoir où vont les fonds et être en mesure de les signaler aux autorités compétentes.

Dans de tels cas, il arrive que l'organisation veuille garder le secret et ne rien divulguer, mais dernièrement, nous constatons que les organisations déclarent qu'elles ont été piratées. Elles divulguent l'adresse du portefeuille choisi par les acteurs illicites pour que l'on sache que les cryptoactifs qui y transitent ont été acquis de façon illicite, de sorte qu'il devient beaucoup plus difficile pour ces acteurs de convertir ces cryptomonnaies en monnaie fiduciaire.

Liezel, vous avez constaté ça également?

Liezel Pistorius:
Tout à fait. Et on commence aussi à obliger les organisations à déclarer les attaques par rançongiciels, comme on le fait pour la divulgation de renseignements personnels.

Tout comme elles ont l'obligation de déclarer que des renseignements personnels ont été exfiltrés de leurs systèmes, les organisations ont aussi dans une certaine mesure l'obligation de déclarer les fonds illicites qui sont maintenant en train de passer par les bourses de cryptomonnaies pour ultimement intégrer le système.

Adam Rodricks:
C'est un excellent point, et je pense que c'est une façon parfaite de passer à la prochaine question. J'aimerais qu'on parle d'exposition directe et indirecte.

En général, comment les cryptoactifs et fournisseurs de services pourraient-ils être exposés indirectement à des crimes financiers?

Amrit Dev:
Et pour souligner ce que Liezel et Kunal disaient à propos des rançongiciels, une bonne partie des crimes financiers qui se produisent dans le monde des cryptoactifs est tout à fait semblable à ce qui se passe dans l'espace financier classique.

Nous observons donc habituellement des entités qui sont directement touchées en raison de manque de contrôles qui pourrait mener à une mauvaise gestion ou au vol de fonds, au blanchiment d'argent, à des opérations d'initié, etc.

Ce sont les types de crimes financiers que nous voyons en finance classique. Et nous continuons à nous attendre à voir le même type de crime dans le monde des cryptoactifs. Comme qui dirait, les fraudes sont les mêmes, seule la technologie a changé. Plus particulièrement, les fournisseurs de services de cryptoactifs pourraient être exposés indirectement à des crimes financiers par l'utilisation illicite de gains en cryptomonnaies et par le blanchiment de ces gains en cryptomonnaies.

Et comme Kunal l'a mentionné plus tôt, bon nombre de ces auteurs blanchissent des fonds en passant par bourses centralisées. Par exemple, un utilisateur peut déposer des jetons Ethereum obtenus illicitement sur une bourse centralisée, les échanger contre des bitcoins ou une autre cryptomonnaie, puis retirer ces fonds et les convertir en jetons différents et rompre la chaîne de possession. On appelle ça le saut de chaîne.

Et ce n'est qu'une des façons dont les fournisseurs de services de cryptoactifs pourraient être exposés indirectement à la criminalité financière.

Je sais que Liezel en a aussi de très bons exemples, je vais donc lui laisser la parole.

Liezel Pistorius:
Tout à fait. Encore une fois, je reviens au côté technologique en termes de rançongiciel. Et si nous poursuivons cette conversation pour parler cette fois de l'exposition indirecte, c'est vraiment là qu'un client, qu'il s'agisse d'un particulier ou d'une organisation, peut sans le savoir recevoir une partie de ces cryptoactifs obtenus illicitement.

Balado sur l'état des cryptoactifs

Épisode 13

Liezel Pistorius:
Revenons à l'exemple du rançongiciel : une organisation pourrait avoir payé une rançon en cryptomonnaie à un acteur illicite, qui finit par mettre en vente un jeton non fongible acheté avec le fruit de son geste illicite. Et par conséquent, cette personne, sans le savoir, finit par acheter une monnaie fiduciaire mise en circulation par le criminel à l'autre extrémité, sans vraiment comprendre l'origine de ce cryptoactif.

Kunal Bhasin:
Bon nombre de ces fournisseurs de services, en particulier ceux qui sont enregistrés auprès de leurs principaux organismes de réglementation, doivent tous s'inscrire en tant qu'entreprises de services monétaires, ou ESM.

Conformément aux règlements pertinents en matière de lutte contre le blanchiment d'argent et le financement des activités terroristes sur leur territoire, les ESM sont tenus de surveiller toute opération douteuse, d'enquêter sur cette opération et de la déclarer.

Dans le cadre de leurs responsabilités, elles ont elles aussi instauré des programmes de lutte contre le blanchiment d'argent. C'est ce qui leur a valu d'obtenir le permis. Ces programmes de lutte contre le blanchiment d'argent font l'objet d'une évaluation indépendante tous les deux ans. Les fournisseurs de services doivent mettre en œuvre de nombreuses procédures pour se conformer à la réglementation pertinente sur les crimes financiers.

Mais en fin de compte, la surveillance et le signalement des transactions douteuses représentent certains défis. Si un acteur illicite transfère à une bourse centralisée des cryptoactifs obtenus dans le cadre d'un piratage, la bourse centralisée signalerait la transaction pour qu'il y ait une enquête.

Bien sûr, il faut pour cela que la bourse en question ait mis en place les outils nécessaires. Le simple fait de signaler la transaction ne signifie pas qu'il y aura automatiquement une enquête ou que la transaction sera bloquée.

Si on prend en compte le nombre d'opérations qui se produisent sur une base quotidienne ou mensuelle dans toutes les bourses à volume élevé, il pourrait être plutôt compliqué d'enquête sur chacune.

De plus, ces fournisseurs de services ne disposent pas de suffisamment de ressources pour enquêter sur ces opérations illicites et soumettre des rapports en temps opportun. Parfois, la plupart du temps en fait, il est trop tard et l'acteur a déjà converti les cryptomonnaies obtenues de façon illicite et les a déposées auprès d'une bourse, soit en monnaie stable, puis les a transférées dans un portefeuille externe ou a effectué une autre transaction qui brouille les pistes.

C'est pourquoi il est difficile pour ces fournisseurs de services de rendre compte des transactions douteuses et de récupérer les fonds en temps opportun.

C'est une des choses que nous observons dans le monde des cryptoactifs. Et c'est là que ces fournisseurs sollicitent l'aide de sociétés comme la nôtre pour gérer leurs enquêtes quotidiennes et leurs rapports, entre autres parce qu'il y a très peu de professionnels qui peuvent enquêter sur les opérations en cryptomonnaie et déclarer ces transactions en temps opportun.

Mais cela ne concerne pas que les fournisseurs de services de cryptoactifs. J'irais jusqu'à dire que c'est également le cas pour les institutions financières et le monde de la finance classique. Ces acteurs facilitent les transactions vers des bourses où le risque est plus élevé.

Et quand je dis transaction, je pense à des opérations comme le transfert de monnaie fiduciaire vers des bourses à risque élevé. Quand ces transactions sont signalées, ou surveillées ou consignées, il est généralement trop tard.

Ainsi, même quand les banques classiques en font assez et s'assurent de respecter les règlements, elles doivent surveiller leur exposition aux cryptoactifs, particulièrement lors de transactions avec des bourses à risque élevé.

Adam Rodricks:
Super intéressant, Kunal, vous peignez un tableau très net, et je comprends beaucoup mieux l'ampleur du risque. Quel type de services d'enquête sur les cryptoactifs et de soutien en matière de crimes financiers KPMG au Canada offre-t-il?

Balado sur l'état des cryptoactifs

Épisode 13

Amrit Dev:
Une partie de la réponse se trouve dans la question. Notre équipe Juricomptabilité offre des services de recherche d'actifs et d'enquête. Nous mettons à la disposition du client une équipe multidisciplinaire composée de professionnels en juricomptabilité qui se consacrent à la juricomptabilité et aux services-conseils en règlement de différends.

Nous avons également des professionnels de notre groupe Cryptoactifs et chaîne de blocs et entreprise, qui est codirigé par Kunal et son équipe, qui fournissent les connaissances techniques en cryptomonnaie dans le cadre de ces enquêtes.

Nous sommes également appuyés par un réseau mondial de professionnels qui se spécialisent dans le renseignement d'affaires, la technologie juricomptable, l'analyse de données. Je vais laisser à Liezel le soin de décrire plus en détail nos offres de services en technologie juricomptable.

Liezel Pistorius:
Pour ce qui concerne les procédures de traçage et d'investigation, il y a toujours l'aspect technologique. C'est là que notre équipe de juricomptabilité, combinée à notre équipe d'intervention en cas de cyberincident, joue un rôle important.

Et je reviens un peu à votre première question Adam, sur les raisons qui me motivent à faire mon travail. Vraiment, je fais ça pour aider. Quand je vois le nombre d'organisations et de particuliers qui se retrouvent dans le pétrin sans être mesure de le comprendre assez rapidement, j'entre en jeu.

Ces entreprises ne savent pas par où commencer, à qui s'adresser. Du point de vue du traçage, nous comptons sur une équipe multidisciplinaire, comme l'a dit Amrit, mais il y a plus. C'est un service de soutien de bout en bout que nous offrons en tant que professionnels de KPMG.

Nous commençons par obtenir les preuves et recueillir les artefacts récupérés par les techniciens de la juricomptabilité, grâce à la technologie juricomptable, de chaque appareil qui a peut-être eu accès aux cryptomonnaies incriminées.

Cela inclut votre ordinateur, votre appareil mobile, tous les appareils IdO possibles, auxquels vous avez fourni une instruction pour exécuter une certaine transaction.

Nous ramenons tout cela dans nos bureaux et nous examinons à fond ces artefacts pour effectuer un traçage précis des transactions au moyen d'analyses avancées, qu'il s'agisse d'analyse de réseau ou d'analyse juricomptable du traitement des données, afin de comprendre les interactions avec les portefeuilles, les bourses, tout ce sur quoi l'utilisateur a pu cliquer, par exemple un courriel d'hameçonnage.

Cet examen nous aidera à vraiment comprendre d'où l'attaque provient, d'établir un calendrier d'événement pour être en mesure d'identifier et de suivre les cryptoactifs jusqu'au bout afin de récupérer vos cryptoactifs ou de vous aider à comprendre le risque pour que vous évitiez de répéter les mêmes erreurs en cliquant sur un courriel d'hameçonnage, par exemple. Ou en succombant à une attaque par rançongiciel sans avoir instauré les mesures de contrôle adéquat dans vos systèmes.

Nous ne nous contentons pas de récupérer vos cryptoactifs. Nous vous aidons également à combler certaines lacunes.

Kunal Bhasin:
Nous sommes un centre d'excellence en cryptoactifs et chaînes de blocs et nous travaillons avec des équipes multidisciplinaires à travers le Canada et le monde. Nous avons accès à plusieurs outils de cryptointelligence qui sont soit utilisés par divers cryptoactifs.

Ces fournisseurs sont des banques grand public, comme je l'ai dit plus tôt. Nous pouvons compter sur des professionnels qui sont certifiés dans ces enquêtes et dans la surveillance des transactions.

En fin de compte, si vous êtes une organisation qui traite en crypto et qui fournit des services boursiers ou de conservation de crypto, vous devez mettre en place un programme de lutte contre le blanchiment d'argent.

Il vous faut disposer de ressources pour pouvoir surveiller et signaler les opérations douteuses et faire enquête. Et comme je l'ai mentionné plus tôt, ce n'est pas toujours facile de faire ça en temps opportun.

Balado sur l'état des cryptoactifs

Épisode 13

Kunal Bhasin:
Il vous faut disposer de ressources pour pouvoir surveiller et signaler les opérations douteuses et faire enquête. Et comme je l'ai mentionné plus tôt, ce n'est pas toujours facile de faire ça en temps opportun.

C'est le genre de service que nous pouvons fournir. Nous effectuons des enquêtes quotidiennes, nous assurons un suivi quotidien des transactions. Nous fournissons toutes sortes de déclarations d'opérations douteuses ou de communications de soupçons. Nous pouvons vous aider si vous êtes novice dans ce domaine.

Si vous voulez de l'aide pour concevoir vos programmes de lutte contre le blanchiment d'argent pour que vous puissiez vous conformer aux règlements, non seulement pour cocher les cases d'une liste de contrôle, mais pour obtenir un soutien réel dans vos enquêtes sur des activités illicites ou sur la chaîne de blocs, nous pouvons vous aider à concevoir ces programmes et à les opérationnaliser.

À vrai dire, ces services n'ont rien de nouveau. Depuis des années, KPMG fournit ces services de lutte contre le crime financier classiques et aux services de lutte contre blanchiment d'argent. Nous y ajoutons une optique cryptographique en mettant à profit nos compétences, notre expérience et les outils auxquels nous avons accès.

Adam Rodricks:
Nous venons d'avoir une discussion très éclairante et j'essaie de prendre en note tous vos conseils. À vrai dire, chacune de vos réponses me donne envie d'approfondir le sujet. Mais étant donné que ma curiosité ne sera jamais assouvie, il est probablement préférable que nous mettions un terme à la discussion pour aujourd'hui.

Merci Amrit, Liezel et Kunal. Nous avons aujourd'hui une discussion très animée, merci beaucoup.

Liezel Pistorius:
Merci Adam. C'était passionnant.

Kunal Bhasin et Amrit Dev:
Merci de l'invitation.

Adam Rodricks:
Merci à nos remarquables auditeurs pour leur écoute. Ne manquez pas le prochain épisode de la série de balados de KPMG au Canada sur l'état des cryptoactifs. Bonjour à tous.