Balado sur l'état des cryptoactifs

Épisode 12

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 preuve de réserve. Pour l'épisode d'aujourd'hui, je suis absolument ravi d'accueillir en studio pour la première fois Nic Carter, associé de Castle Island Ventures qui se joint à notre discussion.

Nic, merci beaucoup d'être ici, comment allez-vous aujourd'hui?

Nic Carter:
Je vais à merveille et je suis particulièrement ravi de participer à cet épisode. Merci de l'invitation.

Adam Rodricks:
Je partage votre enthousiasme, tout comme nos autres invités, nos collègues Kunal Bhasin et Kareem Sadek, qui après presque une douzaine d'épisodes font désormais partie des habitués de nos balados. D'abord et avant tout, bienvenue messieurs.

C'est un plaisir d'être de retour, Kunal, Kareem, comment allez-vous aujourd'hui?

Kunal Bhasin:
Très bien, Adam. C'est super d'être ici en votre compagnie et celle de Nic.

Kareem Sadek:
Bonjour Adam, ravi de discuter avec vous à nouveau. Et Nic, c'est un plaisir. J'ai bien hâte de vous entendre partager vos connaissances avec nous et notre auditoire.

Adam Rodricks:
Formidable! Puisque Nic est notre vedette du jour, il serait bien que nos auditeurs puissent le connaître un peu avant d'aller de l'avant. Pouvez-vous commencer par nous parler un peu de votre expérience dans le domaine, de la fondation de Coin Metrics à la direction des investissements en capital-risque à Castle Island?

Nic Carter:
Avec plaisir. J'ai mis sur pied Coin Metrics en tant qu'entreprise d'information sur les cryptoactifs axée sur les institutions autour de 2016 alors que j'étais aux études en affaires.

L'entreprise a été constituée en société en 2018. Je fais partie du conseil, mais je ne participe plus aux activités quotidiennes. En 2018, j'ai aussi lancé avec Matt Walsh Castle Island, un cabinet de capital-risque axé sur les cryptoactifs.

Nous investissons dans des entreprises en démarrage qui sont à l'étape du financement de série A. Nous venons de créer notre troisième fonds et avons environ 70 sociétés de portefeuille. Nous investissons dans tout l'écosystème.

Adam Rodricks:
70, c'est remarquable! Nous avons nettement fait appel à la bonne personne pour la discussion d'aujourd'hui. Nous sommes heureux de vous avoir parmi nous. Avant de poursuivre, peut-être direz-vous comme tout bon parent à qui on demande quel est son enfant préféré que vous les aimez tous de la même façon, mais avez-vous des investissements préférés parmi ceux que vous avez dirigés? Avez-vous des conseils pour nous?

Nic Carter:
J'ai de nombreux favoris. Et mes favoris sont bien entendu ceux qui performent le mieux, bien entendu! En fait, le cabinet a servi d'incubateur à Coin Metrics, et j'y suis particulièrement attaché. Nous n'avons pas encore d'investissements liés à la preuve de réserve et j'espère que je pourrais en ajouter à la liste. Talos est un des membres de notre portefeuille qui se distingue en proposant des outils de négociation qui permettent aux entreprises d'effectuer des transactions sur de nombreux sites différents en utilisant de nombreux dépositaires différents, entre autres. Ces deux investissements vont vraiment bien.

Adam Rodricks:
Intéressant. Au bénéfice des non-initiés, et sans entrer dans les détails, dites-nous en plus sur le processus. Beaucoup d'entre nous en ont entendu parler comme d'une équation, où la preuve de réserve ajoutée à la preuve de responsabilité égale la preuve de solvabilité. Mais pourriez-vous reculer d'un pas et nous expliquer en quoi consiste la preuve de réserve Nic?

Nic Carter:
Je dirais en fait qu'il y a un énorme problème de nomenclature.

Balado sur l'état des cryptoactifs

Épisode 12

Nic Carter (continué):
De nombreuses personnes aiment dire que la preuve de réserve ne constitue que la moitié de l'équation, mais à vrai dire, j'ai un peu de difficulté avec cette notion qui, à mon avis, remonte aux premières discussions à ce sujet dans la communauté des bitcoins, vers 2013, 2014.

À l'époque, la preuve de réserve était censée signifier qu'une entité assurait la garde des actifs des utilisateurs au nom de ces utilisateurs, en prouvant la propriété de ces actifs dans la chaîne, habituellement, et en démontrant en plus à leurs utilisateurs qu'ils faisaient partie des passifs.

Donc en gros, il fallait démontrer les deux côtés de l'équation et en faisant cela, attester aux clients que les fonds étaient entièrement provisionnés, ce qu'ils sont censés être. De nos jours, beaucoup de gens remettent en question cette nomenclature, ou pensent que la preuve de réserve ne concerne que le côté des actifs. À mon avis, elle concerne à la fois les actifs et les passifs, du moins les passifs qui font en quelque sorte partie du champ d'application.

C'est ce à quoi fait référence le terme « preuve de réserve » selon moi. Peut-être faudrait-il revoir la nomenclature, mais quand je parle de preuve de réserve, j'ai en tête à la fois les actifs et les passifs.

Kunal Bhasin:
Oui, je suis tout à fait d'accord avec vous, Nic. Quand nous utilisons le terme preuve de solvabilité, il y a bien d'autres facteurs à prendre en compte pour déterminer si une bourse est solvable ou non. Pour nous en tant que cabinet, quand nous parlons de preuve de réserve, nous nous assurons de tenir compte à la fois des actifs et des passifs, en particulier les passifs envers les clients de cette bourse bien précise.

Nic Carter:
Oui, je suis tout à fait d'accord avec vous, et c'est une des critiques à l'égard de la preuve de réserve. Il pourrait y avoir des passifs hors du champ d'application qui vous empêchent d'avoir une image complète de la solvabilité. Je suis d'accord. Une évaluation de la solvabilité d'une entité va toujours être plus large que la preuve de réserve, que je considère comme une procédure assez retreinte.

Kareem Sadek:
Je seconde. Quand on parle de preuve de réserve et de preuve de solvabilité, c'est plus large.

J'espère que nous y reviendrons un peu plus tard.

Nic Carter:
Et franchement, j'ai commis l'erreur au début d'opter pour la nomenclature de la preuve de solvabilité, mais je suis maintenant d'avis que vous ne pouvez pas prouver la solvabilité seulement par l'évaluation de la preuve de réserve. Et c'est là, bien sûr, qu'entrent en jeu la certification et la vérification classiques.

Kareem Sadek:
En effet.

Kunal Bhasin:
J'espère que la nomenclature sera bientôt clarifiée et qu'en tant que secteur, nous serons en mesure de nous mettre d'accord sur une la terminologie et de faire connaître les directives en tant que norme.

Adam Rodricks:
Intéressant en effet. Je repense à quelques-unes de nos discussions, Kunal et Kareem, et chaque fois que nous parlons de ce concept, cela revient presque toujours à la protection du consommateur.

Alors, Kunal, quels sont certains des avantages de la preuve de réserve pour les dépositaires et les bourses de cryptomonnaies et comment le processus protège-t-il les consommateurs?

Kunal Bhasin:
La preuve de réserve, c'est en fait un mécanisme qui est utilisé par les bourses de cryptomonnaies et les dépositaires pour fournir la transparence et vérifier les actifs qu'ils détiennent, en particulier au nom des clients. Cette façon de faire est de plus en plus populaire auprès de bon nombre d'entreprises de cryptoactifs comme moyen d'établir un climat de confiance avec leurs clients et avec la communauté en général. Quand nous parlons des avantages des bourses de cryptoactifs et des dépositaires, je commencerais par une transparence accrue qui permet aux clients de vérifier que la bourse ou le dépositaire détient et contrôle réellement les actifs qu'il prétend détenir au nom de ses clients. Cela offre aussi une meilleure sécurité, n'est-ce pas?

Balado sur l'état des cryptoactifs

Épisode 12

Kunal Bhasin (continué):
Les bourses de cryptoactifs peuvent ainsi démontrer qu'elles prennent des mesures pour protéger les actifs de leurs clients, et c'est particulièrement important pour les grandes bourses de cryptoactifs qui traitent avec différentes pratiques commerciales, y compris l'introduction de capitaux ainsi que d'autres occasions d'affaires potentielles. C'est également un meilleur outil de gestion des risques. Ainsi, les dépositaires et les bourses peuvent gérer le risque de manière plus efficace en fournissant une image plus précise de leurs actifs aux consommateurs, ainsi qu'à leurs investisseurs.

Enfin, je dirais que cela va devenir une norme dans le secteur; les organismes réglementation ont en effet commencé à inclure la preuve de réserve dans leurs directives et avis du personnel. Ainsi, dans de nombreux pays, nous avons constaté que les entreprises de cryptoactifs sont tenues de se conformer à des règlements sur la preuve de réserve. Elles s'exposent à des mesures disciplinaires si elles ne le font pas.

Peut-être souhaitez-vous ajouter quelque chose à cela Nic?

Nic Carter:
Nous sommes à un très intéressant tournant de l'histoire de la preuve de réserve. L'histoire s'est déroulée par vagues, au cours desquelles les bourses ont adopté la preuve de réserve, souvent en réaction après un effondrement. La première vague a eu lieu après la faillite de Mt. Gox. À l'époque, vers 2014-2015, plusieurs bourses ont commencé à exiger une preuve de réserve. Le mouvement a perdu son élan, mais il y a eu un regain d'intérêt après Quadriga. Et maintenant, bien sûr, après FTX, on constate le plus grand intérêt encore jamais manifesté pour cette procédure de même que l'émergence de nouvelles techniques, plus rafinées. Pour la première fois, il y a aussi une poussée de la part des organismes de réglementation. Ça vient à la fois de la base, c'est-à-dire les clients, et d'en haut, c'est-à-dire des contreparties qui la recherchent dans leurs contrôles diligents et ainsi que des organismes de réglementation. Il y a dorénavant une carotte et un bâton.

Je dirais que les grandes bourses et les dépositaires, s'ils ont la garde des actifs d'utilisateurs, devraient vraiment s'intéresser à la preuve de réserve et réfléchir à la façon de la mettre en place.

Kareem Sadek:
Parmi les avantages, après Mt. Gox, il en va aussi de la réputation de ce secteur.

La sécurité est l'un des principaux avantages, tout comme la confiance, non? Il faut continuer à bâtir cette confiance parce que c'est l'un des piliers clés d'une adoption croissante des cryptoactifs, pour que davantage d'institutions s'y intéressent.

La confiance est l'un des principaux avantages en tout.

Nic Carter:
Oui, et en tant qu'industrie, nous avons maintenant l'obligation de restaurer la confiance brisée après ce qui est arrivé en 2022, après la faillite de plusieurs entreprises. Jusqu'à maintenant, les bourses n'ont pas cherché à se faire concurrence en misant sur la crédibilité; elles ont plutôt vanté la liste de leurs actifs et la variété de leurs produits. Je trouve encourageant, et j'aimerais que cela se fasse dans des circonstances plus favorables, que les bourses commencent à rivaliser en misant sur leur crédibilité. Cela crée un environnement beaucoup plus favorable pour leurs clients.

Adam Rodricks:
Nic, vous avez mentionné la fin de l'année dernière et je sais que vous avez récemment écrit un article sur l'état de la preuve de réserve à la fin de 2022. Comment pensez-vous qu'une bourse peut démontrer sa preuve de réserve? Existe-t-il des pratiques exemplaires dans le secteur?

Nic Carter:
Collectivement, on commence à voir l'arrivée de nouvelles techniques mises en pratique par les bourses, mais à ce jour, je dirais que les preuves de réserve qui émergent sont très hétérogènes. J'aimerais qu'il y ait davantage d'uniformité.

Il y a un certain nombre d'axes sur lesquels ces procédures varient. Que vous montriez uniquement aux clients qu'ils sont inclus dans l'ensemble de passifs ou que vous montriez à un tiers qui n'est peut-être pas un client de la bourse la valeur globale de ces passifs, les bourses diffèrent le long de cet axe.

Balado sur l'état des cryptoactifs

Épisode 12

Nic Carter (continué):
Les bourses de cryptoactifs peuvent ainsi démontrer qu'elles Certaines bourses procèdent à une vérification cryptographique et obtiennent par des sources externes la preuve des actifs détenus dans la chaîne, et d'autres le font par l'entremise d'un cabinet de vérification de la sécurité ou d'un auditeur. Elles ne divulgueront peut-être pas leurs actifs dans la chaîne. En outre, il existe différents moyens techniques de démontrer le passif. La stratégie par défaut serait donc de créer un arbre de Merkle ou arbre de hachage, et nous constatons déjà là des différences techniques. Puis il y a de nouvelles approches du passif, qui impliquent les preuves à divulgation nulle de connaissance, qui en gros présentent un risque moindre de fuite de données sur les clients, et réduisent le risque de dévoiler de l'information sur les clients par inférence. Je dirais donc qu'il n'y a pas de norme à l'heure actuelle. Et bien sûr, même si certaines bourses font appel à des cabinets de vérification pour ratifier leurs preuves de réserve, il a aussi la fréquence de ces vérifications qui entre en jeu. Certaines bourses font des vérifications toutes les semaines ou toutes les quinzaines, alors que d'autres le font deux fois par année ou une fois par trimestre.

Nous avons vu plus de dix grandes bourses commencer à procéder à des vérifications, et je trouve cette augmentation de l'adoption plutôt encourageante. Mais encore, et pour résumer, il y a peu de normalisation jusqu'à maintenant dans le secteur. C'est une des choses pour lesquelles j'aimerais voir des améliorations dans les mois à venir.

Adam Rodricks:
Avez-vous des exemples à ce sujet?

Nic Carter:
Des exemples à quel égard?

Adam Rodricks:
Je pense tout particulièrement à une évaluation chiffrée de la preuve de réserve.

Nic Carter:
Je me suis dressé une liste de critères officieux pour évaluer la qualité de la preuve de réserve. Ce n'est pas censé être vu comme l'approbation d'une bourse ou l'autre, c'est seulement un outil personnel, où le meilleur candidat effectue une vérification cryptographique des actifs détenus. La preuve de réserve couvre la grande majorité de leurs actifs, sans toutefois atteindre la totalité de ces actifs, parce qu'arriver à une telle couverture peut s'avérer très difficile si les actifs sont de moindre taille.

Cette vérification cryptographique a lieu fréquemment et de façon continue, et ce détail est très important puisqu'il permet de déceler les situations de maquillage. Les utilisateurs peuvent vérifier leur inclusion dans l'ensemble de passifs, et idéalement, la vérification est faite par un tiers, même si peu de bourses procèdent ainsi. Et bien sûr, je recommande que des auditeurs soient inclus, même si c'est parfois délicat. Il y a aussi le fait de tenir compte du passif de tous les clients qui est important, mais c'est également compliqué si vous avez des choses comme des achats sur marge ou des dérivés. Cela devient beaucoup plus difficile parce qu'il ne s'agit pas simplement d'additionner les actifs pour les comparer aux passifs non réglés, mais de développer des techniques supplémentaires pour démontrer que le système d'établissement des marges du client est comptabilisé de façon crédible, ce qui est délicat dans certains cas.

Kunal Bhasin:
Je suis tout à fait d'accord avec vous. Nous constatons également que les organismes de réglementation souhaitent maintenant que les bourses séparent les actifs des clients de leurs propres actifs corporatifs. C'est en train de devenir une exigence, et nous verrons comme cela diffère d'une vérification financière. Toutefois, les organismes de réglementation demandent que cela fasse partie des états financiers vérifiés. Nous avons vu l'Autorité monétaire des Bermudes le faire récemment, et je crois que cela faisait aussi l'objet d'un des avis du personnel de la SEC au cours des deux derniers mois. Cela a aussi été demandé spécifiquement pour les bourses publiques.

Pour ce qui est de l'actif et du passif, je comprends que certaines bourses tentent de démontrer une preuve de réserve et appellent cela une « attestation » lorsqu'elles établissent cette preuve elles-mêmes. Ce terme d'attestation a toutefois un tout autre sens pour les auditeurs, surtout pour les cabinets comptables classiques. Une bourse pourrait demander à un auditeur de tierce partie comme nous de démontrer la preuve de réserve en leur nom.

Balado sur l'état des cryptoactifs

Épisode 12

Kunal Bhasin (continué):
Mais je peux vous dire que nous sommes encore loin de cela.

Nic Carter:
Oui, j'aimerais rappeler que vous êtes les vrais experts en comptabilité, alors que je ne le suis absolument pas, je ne suis qu'un participant enthousiaste. Je crois toutefois comprendre qu'une preuve de réserve est complémentaire à une vérification des états financiers, et non nécessairement un substitut. Les deux visent des objectifs différents. Il me semble qu'une vérification d'états financiers est une entreprise beaucoup plus vaste qui s'accompagne d'un niveau élevé d'assurance quant aux procédures générales que l'entité met en œuvre. Mais elle ne va pas nécessairement vous donner la même assurance que la preuve de réserve, qui peut, elle, être faite plus fréquemment et porter sur un aspect bien précis, soit le passif du client et les actifs détenus. Et en effet, si vous regardez certaines des bourses publiques, au moins aux États-Unis, historiquement, certaines vérifications d'états financiers ne couvrent pas nécessairement les actifs des clients ou les passifs en circulation dans les années précédentes. Je rappelle que je sors de mon champ de compétences pour ce qui est des questions de comptabilité, mais il me semble qu'il y a une méthode différente permettant de déterminer l'existence des actifs des utilisateurs. Il pourrait s'agir davantage de procéder par échantillonnage plutôt que de couvrir l'ensemble des actifs.

À mon avis, les procédures sont distinctes, elles portent sur des aspects différents. La preuve de réserve est plutôt étroite, ciblée, et vise un objectif restreint, tandis qu'une vérification des états financiers est plus large et complémentaire. Je ne les vois pas comme pouvant se substituer l'une à l'autre.

Kareem Sadek:
Oui, et je vais renchérir là-dessus Nic. La preuve de la réserve telle qu'elle se pratique en ce moment est très étroite, et je voulais seulement souligner qu'on entend beaucoup parler d'audit de la preuve de réserve. Or, de mon point de vue en tant que membre d'un cabinet comptable offrant des services professionnels, et Kunal en a glissé un mot, tout comme vous d'ailleurs, la nuance est très importante, car on voit malheureusement le mot employé dans un sens très différent. Il faut savoir que la preuve de réserve n'est pas un audit.

Ça regarde les actifs, les passifs auxquels ils correspondent, et c'est tout. Il n'y a pas d'audit en jeu. C'est pourquoi nous disons que c'est complémentaire. La vérification de la preuve de réserve peut faire partie des états financiers, d'un audit, ou autre, et c'est en gros un ensemble de procédures auxquelles vous acceptez de vous plier, sans qu'une attestation ou un audit y soit associé. Malheureusement, les termes ne sont pas utilisés de la bonne façon depuis un certain temps, et avec tout ce qui se produit maintenant, nous commençons à comprendre que la preuve de réserve est une mesure très étroite, à laquelle il convient d'ajouter autre chose.

Nic Carter:
Je n'ai pas le moindre contrôle sur le sujet, mais c'est regrettable que certains acteurs appellent ça un audit de la preuve de réserve. Cela a attiré beaucoup de critiques de la part de la communauté des CPA qui estime que les acteurs du monde des cryptoactifs exagèrent la nature des assurances associées à la preuve de réserve. Il y a même eu une lettre d'Elizabeth Warren et de certains de ses collègues concernant des cabinets de CPA aux États-Unis qui avaient supervisé les procédures de preuve de réserve, où elle disait qu'il s'agissait de vérifications bidon. La solution consiste peut-être à faire preuve d'une grande précision quant aux assurances qu'on peut obtenir sur la preuve de réserve. Et pourquoi pas, éviter d'utiliser des termes d'audit quand il est question de preuve de réserve.

Kareem Sadek:
Parfaitement d'accord, Nic.

Adam Rodricks:
Kareem, je sais que nous avons tous parlé d'histoires d'horreur ces derniers temps où les bourses ne démontrent pas la preuve de réserve. Me viennent en tête des exemples comme Quadriga, dont vous et moi avons déjà parlé, mais quelles sont certaines conséquences réelles du manque de preuves de réserve, et aurait-il été possible d'atténuer ces conséquences?

Kareem Sadek:
Oui, nul besoin de remonter très loin dans le temps, vous venez de mentionner un cas, mais je vais vous donner d'autres exemples.

Balado sur l'état des cryptoactifs

Épisode 12

Kareem Sadek (continué):
Il s'agit en gros d'un manque de transparence en général, mais aussi d'une absence de gouvernance. Je vais faire un parallèle entre les deux, même s'il s'agit de deux choses différentes. Vous avez parlé de Quadriga. Ça s'est passé au Canada, un peu plus récemment, et cela a mené à la perte de millions et de millions de dollars. Mais il y a aussi eu plus récemment FTX où la réserve ne correspondait plus du tout aux fonds des clients. Mais plus encore, on a vu là une mauvaise gestion, ou du point de vue de la gestion des risques, un manque de gouvernance. Mais il n'y a là rien de nouveau. Et on parle de quelque chose qui s'est produit en 2014!

On entend parler de preuve de réserve aujourd'hui en raison de FTX et d'affaires plus récentes, mais ces choses se produisent depuis un moment et la preuve de réserve est une discussion qui a lieu depuis le début. C'est très, très important de le souligner. Pour être honnête avec vous, il aurait été possible d'atténuer la portée de ces incidents. Je ne sais pas si je peux dire qu'ils auraient pu être évités, mais ils auraient pu être atténués dans une certaine mesure, en mettant en œuvre de robustes protocoles entourant la preuve de réserve. Ces protocoles à eux seuls auraient permis de donner l'alerte au moins, et de faire comprendre qu'il y avait anguille sous roche.

Et si le tout avait été assujetti à une solide gouvernance et des contrôles internes appropriés, alors là on pourrait davantage de prévention plutôt que d'atténuation. Honnêtement, des incidents comme ceux qui viennent de se produire ont un tel impact qu'ils ternissent la réputation du secteur des cryptomonnaies et minent la confiance. Ça ne fait qu'éloigner beaucoup de gens ou d'investisseurs potentiels.

La conséquence réelle est la perte de réputation causée par la perte de millions et de millions de dollars. Bien que la preuve de réserve en soi n'ait pas pu empêcher certaines choses, j'aurais vraiment aimé qu'on puisse atténuer l'impact de telles affaires et qu'on ait mis en place un système d'alerte qui aurait permis de conclure ici à une forme de détournement d'actifs, ou à quelque autre anomalie. Et j'insiste pour dire que je suis très favorable à de telles mesures. L'absence de mesures, c'est ce que nous avons avec vu Mt. Gox il y a longtemps, et maintenant avec Quadriga et FTX.

Nic Carter:
Je veux ajouter ici que je suis d'accord, et que je ne pense pas que la preuve de réserve puisse résoudre la situation. Il y a d'autres façons dont les bourses ou les dépositaires peuvent échouer même lorsqu'il y a une preuve de réserve. Il peut y avoir des risques liés aux personnes clés ou au piratage.

Il pourrait y avoir un siphonnage des fonds. Imaginez toutefois un monde où la preuve de réserve serait une pratique entièrement normalisée dans l'ensemble du secteur. Dans le cas de ces bourses, je ne pense qu'elles auraient même pas été en mesure d'obtenir une preuve de réserve par rapport à leurs activités. D'après ce que je comprends, Mt. Gox était insolvable depuis des années avant de finalement déclarer faillite en 2014. À moins d'avoir réformé sa structure et mis de l'ordre dans ses livres, l'entreprise n'aurait pas pu présenter de preuve de réserve.

Je crois qu'on peut dire la même chose de Quadriga : l'entreprise avait un problème de longue date avant sa chute. En ce qui a trait à FTX, nous ne connaissons pas encore tous les détails.

En gros, si tout le monde présentait une preuve de réserve, il y aurait eu d'énormes drapeaux rouges autour de ces bourses qui sont incapables ou refusent de fournir une preuve de réserve. Les bourses réglementées ou mieux organisées font la preuve de réserve. Lorsqu'on est un client potentiel d'une bourse qui n'est pas en mesure de fournir une preuve de réserve ou qui refuse de le faire, cela envoie des signaux très forts.

C'est pourquoi j'estime qu'il est si important que la preuve de réserve soit normalisée dans tout le secteur pour que ce signal devienne beaucoup plus fort s'il n'y a qu'une petite poignée de bourses qui ne le font pas.

Kunal Bhasin:
Dans la plupart de mes conversations après FTX, et je suis persuadé qu'il en va de même pour vous Nic et Kareem, les gens qui avaient déjà des réserves envers les cryptoactifs disaient avoir encore plus de raisons de s'en méfier.

Balado sur l'état des cryptoactifs

Épisode 12

Kunal Bhasin (continué):
C'est une conséquence importante dans le monde réel qui a fait prendre quelques années de recul au secteur. S'il y avait eu une preuve de réserve adéquate ou des procédures similaires pour identifier ou atténuer la fraude, on aurait pu déceler le problème beaucoup plus tôt et il y aurait eu beaucoup moins de pertes. Mais les réserves ne sont pas seulement une question de passifs adossés sur des actifs; il s'agit aussi de connaître certains des contrôles internes, par exemple de connaître les risques posés par les personnes clés comme l'a dit Nic. Par exemple, on ne devrait pas permettre à une personne seule ou encore à deux personnes qui sont d'excellents amis d'être cosignataires pour un ensemble de cryptoactifs, de bourses de cryptomonnaies ou d'actifs.

Il faut établir des procédures. Il faut documenter les risques pour pouvoir correctement les atténuer.

Et en tant que secteur, et nous le faisons en tant que cabinet, nous devons pouvoir discerner les pratiques exemplaires parmi ces procédures et les mettre en valeur. Je ne pense pas qu'on puisse se permettre d'attendre que ce soient les organismes de réglementation ou encore les organismes de réglementation de cabinets comme le nôtre qui établissent les procédures.

En tant que secteur d'activité, nous devons identifier les procédures, respecter les pratiques exemplaires et informer tout le monde à leur sujet, expliquer comment nous gérons le risque plutôt que chercher à éviter complètement le risque en refusant de travailler avec les cryptoactifs.

Kareem Sadek:
J'aime la discussion, parce qu'on est en train de délimiter la preuve de réserve et de la compléter avec d'autres procédures d'audit. Êtes-vous d'accord avec moi pour dire qu'une preuve de réserve en l'état actuel ne garantit aucunement la qualité de la bourse? J'aimerais que les auditeurs comprennent cela.

La preuve de réserve ne vous permettra en aucun cas d'obtenir des informations sur la qualité de la bourse ou par exemple sur la possibilité qu'une bourse en particulier soit susceptible d'être piratée.

Ces questions ne font pas partie de la preuve de réserve; la preuve de réserve ne dit rien sur la solvabilité ou sur l'avenir d'une bourse. Cela ne peut avoir lieu avec l'état actuel de la preuve de réserve.

C'est très important, à mon avis. Encore une fois, je répète des choses que nous avons déjà dites, mais la preuve de réserve à elle seule ne garantira pas la qualité d'une bourse. Est-ce que ce commentaire vous paraît juste?

Nic Carter:
Oui, je suis d'accord. Je dirais que les bourses qui ont fait la preuve de leur réserve et qui le font à un niveau élevé donnent une indication qu'elles se portent bien. Mais ce n'est certainement pas une panacée en soi.

Kunal Bhasin:
Oui, je suis tout à fait d'accord. Et j'ajouterais le point suivant : la fréquence à laquelle la bourse refait sa preuve de réserve compte pour beaucoup. Il peut se passer bien des choses au sein de la chaîne en six mois, alors si la preuve de réserve n'a lieu qu'une fois par semestre, ce n'est pas très utile.

Nic Carter:
En effet, et il faudrait régler cette situation. Le terme « habillage » s'applique probablement, mais vous me le direz s'il en existe un meilleur. À la base, les critiques de la preuve de réserve soutiennent que les bourses pourraient simplement emprunter à court terme à la fin d'un trimestre ou à une autre fréquence pour trouver suffisamment d'actifs pour honorer leurs engagements si leur réserve n'est pas suffisante. Et la fréquence de la preuve aide à résoudre ce problème.

Je dirais que si vous faites plus souvent la preuve de réserve, comme certaines bourses qui le font tous les jours, ça devient illogique d'emprunter des fonds littéralement tous les jours.

Il faut dire aussi que ces mouvements seraient observables dans la chaîne, et c'est ici que la transparence entre en jeu. Dans l'ancien paradigme, personne ne pouvait observer les fonds qui entrent et sortent d'une banque, par exemple, ou d'un dépositaire d'autres types d'actifs.

Balado sur l'état des cryptoactifs

Épisode 12

Nic Carter (continué):
Ici, dans de nombreux cas, les bourses divulguent leur stockage hors ligne, leurs grappes de portefeuilles au sein de la chaîne; il y aurait donc ici une certaine forme de vérification par les utilisateurs, où il serait possible de voir s'il y a eu des entrées et des sorties de fonds massives au moment où la preuve de réserve a été évaluée.

Cela nous donnerait un indice pour déterminer s'il y a eu ou non une tentative de camouflage.

Kunal Bhasin:
La transparence de la chaîne est en effet l'un des arguments de vente propre aux cryptoactifs et à ce secteur dans l'ensemble. Nous devrions reconnaître cet avantage.

Nic Carter:
Et j'ajouterai que les gens ordinaires sur Internet qui regardent les portefeuilles de FTX ont rappelé leur portefeuille après les révélations du pupitre Corn Desk. C'était l'une des façons dont nous avons appris que quelque chose clochait vraiment.

La cryptomonnaie est vraiment à nulle autre pareille à cet égard, et il y a un niveau latent de transparence qui peut être exploité pour déterminer si une bourse agit de façon malhonnête.

Une preuve de réserve normalisée faciliterait largement la tâche des gens ordinaires pour qu'ils puissent vraiment faire une évaluation.

Adam Rodricks:
Bon Nic, êtes-vous prêt à répondre à une question épineuse?

Nic Carter:
Allez-y, je suis prêt!

Adam Rodricks:
J'aimerais que vous glissiez un mot sur le concept de preuves à divulgation nulle de connaissance et que vous expliquiez à nos auditeurs de quoi il s'agit. Votre réponse fera parfaitement la transition pour que nous commencions à parler de certains des enjeux de la mise en œuvre et du maintien d'une preuve de réserve. Nous aurons peut-être le temps de parler des solutions novatrices dont vous avez pris connaissance qui permettent de traiter cet enjeu.

Nic Carter:
Je dirais que l'un des développements les plus passionnants, à la fois pour ce qui est de la preuve de réserve et dans le secteur des cryptos en général, c'est l'émergence à grande échelle de preuves à divulgation nulle de connaissance. Ce n'est que relativement récemment que des bourses de cryptoactifs ont introduit ce type de preuve. Essentiellement, il s'agit de donner à un tiers la preuve qu'un fait ou une donnée est connu sans nécessairement révéler d'information sur les données sous-jacentes.

L'exemple qu'on donne généralement est celui où quelqu'un entrerait dans un bar en prouvant qu'il a 21 ans, mais sans dévoiler sa date de naissance.
Je ne peux pas vous donner plus de détails sur le plan cryptographique, mais en matière de preuve de réserve, c'est très important parce que traditionnellement, la façon dont les bourses divulguent l'information sur leurs passifs consiste essentiellement à bâtir un arbre de Merkle.

En gros, il s'agit d'établir une liste de passifs en procédant à une certaine anonymisation, sans laisser couler l'information, en indiquant par exemple que le client un possède deux bitcoins, voici son adresse électronique, en bref, ce genre d'anonymisation.

Mais en procédant ainsi, on divulgue encore une quantité importante de données, tel que le montant total des soldes des clients en bourse, la distribution des actifs dans cette bourse, et potentiellement, selon la mise en œuvre, il pourrait également y avoir des fuites de données sur la variation des soldes du client au fil du temps. Et les clients ne souhaitent pas toujours divulguer ce genre d'information. Par exemple, si vous investissez dans des fonds de couverture, vous négociez sur une bourse, vous avez des garanties sur la bourse, voulez-vous vraiment que quelqu'un puisse voir que vous êtes passé d'un actif à un autre au cours de la période où la preuve de réserve était faite? Ce n'est pas souhaitable.

Nous observons aujourd'hui de nouvelles techniques de divulgation du passif, où, au lieu de simplement publier une liste de soldes, vous fournissez seulement aux clients un reçu cryptographique montrant qu'ils sont inclus dans l'ensemble des passifs, et ce passif s'ajoute à un certain montant, qui est égal aux actifs de la chaîne. Mais vous ne divulguez pas beaucoup d'autres données.

Balado sur l'état des cryptoactifs

Épisode 12

Nic Carter (continué):
Vous ne divulguez pas la répartition des soldes. C'est vraiment à vous de décider ce que vous voulez divulguer.

Vous pouvez donc être plus sélectif avec les données qui sont divulguées. Depuis toujours, c'est une des principales raisons avancées par les bourses qui refusent d'établir une preuve de réserve. Elles refusent de le faire, parce que ça les oblige à divulguer trop d'information sur des centaines de millions de clients.

Si elles ont 100 millions de clients, elles ne veulent tout simplement pas courir le risque de divulguer une grande quantité de données. Donc la preuve à divulgation nulle de connaissance est une innovation réellement positive, puisqu'elle signifie qu'on peut désormais établir la preuve de réserve d'une façon très raffinée. On obtient le même niveau d'assurance, mais sans dévoiler inutilement certaines données qui pourraient être utilisées contre la bourse ou ses clients.

Kareem Sadek:
Oui, c'est la question de la vie privée, non? Qu'il s'agisse d'une critique ou d'un facteur qui fait hésiter, cela revient toujours à une question de protection de la vie privée. Quand on divulgue de l'information sur un passif ou sur tout un ensemble des passifs, il s'agit d'une exposition importante sur le plan de la vie privée, et il me semble que la preuve à divulgation nulle de connaissance vient régler ou atténuer ce problème dans une certaine mesure.

Nic Carter:
C'est ce que je crois en effet. Honnêtement, il s'agit d'une préoccupation légitime à mon avis. La meilleure façon de faire une réserve de preuve consiste essentiellement à communiquer au grand public la comptabilité complète des soldes.

Mais bien sûr, cela pourrait entraîner la divulgation d'une énorme quantité de données. Chaque fois que vous publiez un grand ensemble de données, plus de gens peuvent faire des inférences et découvrir de l'information sur la bourse et ses clients et des choses du genre.

Le problème ici est que la preuve à divulgation nulle de connaissance fait un peu penser à une boîte noire; ce n'est pas aussi explicite qu'un arbre de Merkle, une technique fort simple et très bien comprise.

Il y a donc un compromis, mais c'est généralement la direction que nous prenons et c'est une technologie cryptographique plus raffinée. J'y vois vraiment un progrès.

Adam Rodricks:
D'après notre discussion jusqu'à présent, il semble que nous ayons un consensus parmi nos invités sur la nécessité de normes supplémentaires.

Nic, vous avez écrit un article convaincant contenant des observations sur la preuve de réserve à l'intention des décideurs, et je veux aborder ce sujet. Quel devrait être le rôle de la réglementation et du gouvernement dans l'application des exigences relatives à la preuve de réserve?

Nic Carter:
Je vais probablement me faire renier par mes collègues du secteur des cryptos, et on va probablement m'accuser d'être étatiste, mais même si je suis très impressionné et encouragé par l'adoption de la preuve de réserve par les bourses de cryptoactifs, ce n'est pas une solution complète. J'ai fait une comptabilité de la couverture où j'ai constaté une preuve de réserve pour les actifs des clients à la fin de l'exercice 2022, et j'ai trouvé 33 milliards d'actifs sécurisés, mais bien sûr il y a beaucoup, beaucoup plus actifs détenus en dépôt avec ces bourses et dépositaires.

Je dirais probablement plus de mille milliards, ou plus probablement des centaines de milliards au moins. Il reste donc que la preuve de réserve vise une minorité de tous les cryptoactifs. Des règles sont nécessaires, mais aussi il faut davantage d'incitatifs. Je ne blâme pas les décideurs de vouloir commencer à incorporer cela dans la législation.

C'est une demande raisonnable, et toute bourse crédible devrait être capable d'y répondre. Et technologiquement, c'est maintenant faisable. Je ne pense pas que ce soit trop demander.

C'est même déjà en train d'avoir lieu. La question a été soulevée dans le Wyoming, vous me disiez qu'on parle maintenant de preuve de réserve au Canada.

Balado sur l'état des cryptoactifs

Épisode 12

Nic Carter (continué):
Et il y a même un projet de loi au Texas où l'on demande aux bourses qui détiennent plus de 50 millions de dollars d'actifs appartenant aux clients de faire une preuve de réserve, tous les trimestres, il me semble.

Je pense que c'est tout à fait sensé et que les bourses et les dépositaires devraient commencer à comprendre que les organismes de réglementation auront cette exigence. Et c'est d'après moi un développement positif.

Adam Rodricks:
Kunal, plus tôt dans la conversation, vous avez mentionné les vérifications financières classiques. J'aimerais savoir comment la preuve de réserve se compare aux vérifications financières classiques? Y a-t-il des différences qui devraient attirer l'attention de nos auditeurs?

Kunal Bhasin:
Oui, d'abord, chaque vérification commence par des assertions. Nous examinons donc certaines assertions portant entre autres l'exactitude de l'évaluation, l'existence, l'exhaustivité, les droits et obligations, ainsi que la présentation des informations à fournir. Nous examinons chaque poste des états financiers.

Quand on parle de preuve de réserve, on parle d'éléments très précis. Nous ne parlons pas d'opérations entre parties liées. Nous ne parlons pas du déroulement des activités de la bourse ou de l'entreprise.

Les preuves de réserve sont très étroites, c'est leur nature. Tout ce que nous faisons, c'est de nous assurer que la bourse est en mesure, au bout du compte, d'atteindre les passifs de ses clients.

Pour faire cela, et une partie du secteur pense que notre travail s'arrête là, il faut vérifier les soldes des portefeuilles au sein de la chaîne et la maîtrise de la réserve que la bourse prétend avoir. Ensuite, nous vérifions et additionnons les soldes de ces portefeuilles pour nous assurer qu'ils sont égaux ou supérieurs aux passifs des clients.

Mais là encore, nous devons mettre en œuvre d'autres procédures pour faire la preuve de réserve. Nous devons nous assurer de l'ensemble des passifs du client.

Nous devons vérifier les assertions sur les droits et les obligations. Par exemple, on peut se demander si la bourse détient les clés privées des portefeuilles.

Y a-t-il d'autres bourses ou d'autres contreparties qui détiennent ces clés privées et qui pourraient prendre le contrôle de ces portefeuilles?

Nous examinons aussi l'exactitude des rapports. C'est pourquoi je ne pense pas que la preuve de réserve soit une solution complète. Par contre, une preuve de réserve assortie d'un audit financier, où nous examinons le portrait dans son ensemble ainsi que toutes les assertions, est beaucoup plus rassurante pour toutes les parties concernées, qu'il s'agisse du client, des investisseurs, des organismes de réglementation et même des institutions.

Tous ces gens veulent être en mesure de dire que les opérations commerciales d'une bourse ou d'un dépositaire sont en ordre, qu'il est démontré en toute transparence que les actifs de l'entreprise sont séparés des actifs des clients.

Et il est assez facile de surveiller au sein de la chaîne ce que les bourses et les dépositaires font avec les actifs des clients. La vérification financière est donc beaucoup plus large, ce qui nous donne beaucoup plus d'assurance, alors qu'il n'existe pas encore de norme particulière pour la preuve de réserve.

Nous avons toutefois des pratiques exemplaires qui, je crois, finiront par devenir des normes.

Nic, Kareem, vous avez quelque chose à ajouter?

Kareem Sadek:
J'ajouterais ceci : en deux mots, ce sont des procédés différents.

Comme pour les audits d'ailleurs, il en existe différents types. Les vérifications des états financiers mentionnées par Kunal sont en général plus larges. Il y a aussi des nuances à faire.

La vérification des états financiers peut-elle remplacer la preuve de réserve?

Balado sur l'état des cryptoactifs

Épisode 12

Kareem Sadek (continué):
Personnellement, je ne le crois pas. Pensons seulement à la façon dont se déroule la vérification des états financiers.

Que vous fassiez des états financiers de qualité et ensuite des états financiers annuels, le temps écoulé ne rassure pas les parties prenantes ou les clients sur ce qui se passe avec les réserves, n'est-ce pas? Les vérifications des états financiers sont si détaillées et exigent tellement de temps qu'il faut les compléter par une preuve de réserve.

Si la preuve de réserve est correctement faite et si elle est faite fréquemment, et qu'elle s'ajoute aux états financiers, elle peut apporter une certaine tranquillité d'esprit.

On peut se demander en quoi les preuves de réserve sont différentes des audits classiques. Quand on parle des cas d'insolvabilité, on peut se demander ce qui arriverait aux actifs des clients? Est-ce qu'on leur accorde la priorité? Ou non? Cet aspect n'est pas visé par la preuve de réserve, peut-être pas non plus par un audit des états financiers. Il se pourrait qu'une évaluation juridique ou quelque chose du genre soit nécessaire.

Il y a donc plusieurs choses à faire conjointement pour qu'au bout du compte les clients soient rassurés sur la solvabilité. Je le redis : ce sont deux choses très différentes. Et le temps requis pour accomplir les deux n'est pas du tout le même. Les deux devraient se compléter.

Nic Carter:
J'aimerais ajouter une chose. Une grande partie de la critique autour de la preuve de réserve se concentre essentiellement sur le fait que toutes les assurances qu'un client pourrait chercher à obtenir d'une bourse ne peuvent pas être produites cryptographiquement ou mathématiquement.

Comme vous le dites, il faut un contexte juridique et contractuel supplémentaire pour qu'un déposant ait suffisamment l'assurance que ses actifs restent légalement les siens, et qu'il n'est pas en train d'agir comme créancier non garanti pour la bourse. Les déposants veulent savoir que leurs actifs seront privilégiés en cas de liquidation ou de faillite, comme ce devrait être le cas.

Il n'y a pas de certitude quant au fait que, par défaut, leurs actifs sont séparés du capital d'exploitation de la bourse. Il faut donc mettre en place des processus contractuels supplémentaires.

La preuve de réserve est une tentative de réduire le processus d'assurance à quelque chose d'assez mathématique, mais on doit quand même convenir qu'elle ne fait pas tout.

La réaction contre la preuve de réserve vient de ce que les gens ne réalisent pas que la preuve de réserve n'a pas réponse à tout.

Et une fois que nous comprenons ses limites, il devient plus simple de raisonner la chose.

Adam Rodricks:
Nic, vous êtes sur la sellette depuis le début et vous vous en sortez vraiment très bien. Mais nous manquerions à notre devoir si nous ne vous proposions pas de changer de rôle et de poser des questions à votre tour. Y a-t-il des questions que vous aimeriez poser, des commentaires à formuler aux représentants de KPMG?

Nic Carter:
J'observe ce qui se passe en matière de preuve de réserve, et je suis ravi de voir les décideurs l'adopter tant au Canada qu'aux États-Unis. Mais je m'inquiète du fait qu'il n'y ait pas assez de couverture des cabinets de CPA pour surveiller la procédure, et je pense que c'est souvent parce que les bourses qui sont vraiment intéressées à faire la preuve de réserve proviennent d'endroits où les institutions n'inspirent pas la confiance. Elles essayent d'établir cette confiance par des moyens cryptographiques.

C'est beaucoup plus difficile de les convaincre de devenir des clients.

Et bien sûr, il y a beaucoup de discussions sur les cabinets d'audit qui ont en fait quitté le domaine de la preuve de réserve. Quand on observe les missions de procédures convenues proposées aux cabinets qui font la preuve de réserve, on voit qu'un bon nombre de cabinets ont quitté ce marché aujourd'hui.

Balado sur l'état des cryptoactifs

Épisode 12

Nic Carter (continué):
Ils font parfois l'objet de critiques, ils ont peut-être été aux prises avec l'effondrement de diverses bourses… Donc j'aimerais que vous me disiez s'il y a des chances que les cabinets comptables, en particulier les plus grands, reviennent sur ce marché, et à quel point les bourses devraient s'inquiéter si des cabinets comptables reçoivent le mandat de faire la preuve de réserve.

Quels sont les obstacles qui les empêchent de faire appel à un CPA dès le départ pour ratifier la procédure?

Kunal Bhasin:
Je peux dire un mot là-dessus. Nous savons tous que certains cabinets comptables ont quitté le domaine des cryptos, mais ici au Canada et ailleurs dans le monde, KPMG continue de bâtir son groupe sur les cryptomonnaies et cherche des façons d'offrir une preuve de réserve. Nous avons des procédés d'acceptation des clients et de gestion des risques à respecter et l'une des premières choses que nous ferions avant d'accepter un client consisterait à obtenir l'identité complète de l'organisation et sa structure organisationnelle. Et nous le faisons précisément parce que le secteur des cryptos est considéré comme un secteur à plus haut risque pour nous en tant que cabinet comptable classique.

Nous devons donc mettre en œuvre des procédures améliorées de connaissance du client à l'égard des principaux actionnaires et comprendre à quoi ressemblent la structure organisationnelle et l'évaluation préliminaire des risques (inaudible), pas seulement à un niveau inférieur, mais au niveau de l'entité mère. Selon mon expérience (et Kareem peut probablement renchérir), nous ne sommes pas toujours en mesure d'obtenir le niveau d'information dont nous avons besoin de la part de certaines bourses qui nous demandent de faire la preuve de réserve. Donc il n'est pas seulement question d'être en mesure de faire la preuve de réserve.

Nous ne pourrons accomplir aucun travail pour des clients que nous ne pouvons accepter faute de transparence de leur structure organisationnelle dans son ensemble. C'est un important obstacle à surmonter, et je serais heureux de discuter avec quiconque souhaite faire une preuve de réserve adéquate, mais qui ne veut pas partager sa structure, son lieu de constitution, etc.

C'est un important enjeu pour nous.

La deuxième, et nous en avons parlé, est le manque de directives ou de normalisation de la part d'AICPA, de CPA Canada ou d'autres organismes de réglementation du secteur comme le PCAOB.

Nous devons pouvoir être rassurés à l'égard des procédures que nous avons documentées et qui sont fondées sur nos compétences et notre expertise, et sur ce que nous observons dans le secteur.

Chaque fois que nous créons un programme d'audit, nous nous assurons qu'il répond à des normes précises et respecte des exigences de qualité.

À l'heure actuelle, nous ne sommes pas en mesure de proposer des procédures que nous aurions conçues et de demander au client de nous donner son accord. Nous ne pouvons lui demander d'accepter des procédures non standards et lui garantir que nous ne serons pas blâmés après coup pour avoir exécuté ces audits.

Avec un peu plus de collaboration et d'éducation, nous devrions nous adresser aux organismes de réglementation en tant que secteur, aux associations de CPA et les aider à comprendre quels sont les risques et quelles sont les stratégies d'atténuation fondées sur les pratiques exemplaires. L'audit n'est pas une attestation - nous ne fournissons pas d'assurance absolue.

Nous fournissons une assurance raisonnable, ce qui signifie que nous essayons d'atténuer et de gérer les risques plutôt que d'éviter les risques dans leur ensemble.

Voilà ce que j'avais à dire sur la question.

Kareem Sadek:
Bien dit Kunal, surtout à la toute fin.

Vous avez bien résumé la situation. Si nous ne pouvons pas vous accepter comme client, si nous ne pouvons pas obtenir toute la transparence requise, nous ne pouvons pas gérer le risque.

Balado sur l'état des cryptoactifs

Épisode 12

Kareem Sadek (continué):
Si nous n'obtenons pas cette transparence dès le début d'un processus d'orientation et de connaissance du client parce que ce dernier refuse de partager l'information, nous arrêtons tout et refusons d'aller plus loin.

Et j'espère que ça va changer. Et j'espère que ça changera rapidement. Nous avons d'ailleurs parlé des directives et des règlements à venir.

Vous avez parlé du Texas, nous avons parlé de ce qui est arrivé au Canada. Les choses vont changer, et très honnêtement, nous attendons ce changement avec impatience.

Ce n'est pas par manque d'expertise, et je ne peux parler que de KPMG au Canada et à l'échelle mondiale. Nous avons l'expertise; nous savons comment nous y prendre, mais nous devons nous assurer de bien faire les choses et d'obtenir les directives adéquates avant de plonger dans le vif du sujet.

Adam Rodricks:
Impressionnant. Nic, nos auditeurs ont sûrement des questions pour vous, et un des auditeurs de PodBytes vous pose en fait la question suivante.

Il s'interroge sur l'une des sociétés de portefeuille de Castle Island, Hidden Road, qui adopte une approche unique pour gérer le risque de contrepartie avec des bourses centralisées. Que pouvez-vous nous dire à ce sujet?

Nic Carter:
Il s'agit en fait d'un développement structurel très intéressant dans le secteur des cryptoactifs.
Hidden Road est en fait une sorte de courtier de premier ordre, et son objectif est de permettre aux sociétés d'investissement de négocier en bourse sans exposition directe à ces bourses, sans obligation de garantir des fonds sur ces bourses. Cela finit par refléter la manière traditionnelle dont fonctionne le marché boursier, où la garde et la compensation et ensuite la concordance des ordres sont des fonctions distinctes.

Elles bénéficient donc de la dissociation des bourses. Depuis le départ, vous savez sans doute que les bourses de cryptoactifs sont intégrées verticalement.

Ce qui se passe maintenant, particulièrement en ce qui concerne les règles sur les dépositaires proposées par la SEC, c'est l'arrivée de règles qui visent à dissocier la fonction de dépositaire de la fonction d'opérateur de bourse.

C'est à mon avis un excellent développement, parce que les bourses ne sont pas nécessairement de bons dépositaires. Pensez simplement à notre discussion d'aujourd'hui. L'établissement de procédés adéquats visant à protéger les actifs des clients diffère très largement de l'établissement de procédés qui rendront très performants une bourse, sa fonction de concordance des ordres ou d'établissement de marges. La pertinence de la preuve de réserve est qu'il y aura maintenant des dépositaires où la bourse sera un client du dépositaire, et où les clients des bourses seront des clients du dépositaire par le biais de ce mécanisme de transmission. Nous assisterons à des preuves de réserve récursives sur la durée de l'exercice. Le dépositaire fait une preuve de réserve, qui est fournie à la bourse, qui la fournit à son tour aux clients.

C'est un développement positif. Tous les principaux dépositaires de ces bourses devraient selon moi examiner des preuves de réserve et en tenir compte dans la dynamique de la preuve de réserve. Il s'agit d'une révolution prometteuse de la structure de marché.

Je pense que c'est pour le mieux et que c'est justifié, mais ça veut aussi dire que nous allons devoir devenir un peu plus rigoureux pour permettre à ces preuves de réserves d'arriver jusqu'au client final.

Kunal Bhasin:
Et c'est aussi en ce sens que s'oriente le secteur. Récemment, les Autorités canadiennes en valeurs mobilières ont souligné dans un de leurs avis du personnel la définition de « dépositaire tiers acceptable » et donné des règles précises que doivent respecter les dépositaires sur le plan de la conservation officielle des fonds et de la ségrégation des actifs.

Je donc suis entièrement d'accord. C'est un excellent produit.

Balado sur l'état des cryptoactifs

Épisode 12

Nic Carter:
C'est malheureux que les bourses aient pris l'initiative d'instaurer leurs propres solutions de conservation des actifs, surtout si elles étaient légèrement réglementées. Mais cela s'explique par le fait que les bourses étaient en concurrence sur la base d'inscriptions d'actifs et du nombre de chaînes de bloc prises en charge, entre autres choses.

Pour demeurer dynamiques et agir rapidement, elles ont dû devenir leur propre dépositaire, c'est du moins ce qu'elles m'ont dit.

Les choses sont un peu différentes aujourd'hui. Les bourses se font concurrence sur la base de la crédibilité, et leurs clients souhaitent négocier avec elles, sans avoir à faire une diligence complète ou à s'exposer en matière de contreparties.

Il n'est pas non plus efficace de garantir l'intégrité de 20 bourses différentes en tant que société d'investissement. Par conséquent, les pressions structurelles dans le secteur poussent maintenant les bourses à délaisser la conservation comme produit de base pour considérer les fonds des clients sur la plateforme comme un passif qu'elles veulent peut-être minimiser.

C'est un peu le nouvel état d'esprit, et il me semble que c'est plutôt positif pour le secteur. Le fardeau de la preuve de réserve pourrait éventuellement passer des bourses aux dépositaires qui en viendront peut-être à servir plusieurs bourses.

Adam Rodricks:
Messieurs, nous venons d'avoir une discussion très éclairante, et honnêtement, chacune de vos réponses soulève de nouvelles questions de ma part. J'aimerais pouvoir poursuivre cet entretien, mais nous devons clore la discussion pour aujourd'hui.

Comme toujours, merci à Kareem et à Kunal de leur présence. C'est toujours un plaisir d'apprendre en votre compagnie.

Kunal Bhasin:
Merci Adam.

Kareem Sadek:
Merci de l'invitation Adam.

Adam Rodricks:
Et j'adresse des remerciements particuliers à Nic.

C'était vraiment stimulant d'entendre vos commentaires sur des questions qui devraient certainement être au cœur des préoccupations tous ceux qui s'intéressent au monde des cryptoactifs. Merci de votre présence parmi nous.

Nic Carter:
C'est un sujet d'une grande importance, et je suis particulièrement ravi d'avoir participé à cet épisode.

Adam Rodricks:
À nos remarquables auditeurs: merci beaucoup de votre écoute. Je suis votre hôte, Adam Rodricks, et ne manquez pas de vous joindre à nous lors du prochain épisode des balados de KPMG au Canada sur l'état des cryptoactifs. Bonjour à tous.