LA PLATEFORME DE FINANCE DÉCENTRALISÉE MANGO ESCROQUÉE DE 117 MILLIONS : PARTIE 2 – LE RÈGLEMENT AVEC LE MALFAITEUR EST-IL OPPOSABLE ET QUE SIGNIFIE-T-IL POUR LES OAD?

Publié le 21 novembre, 2022

Catégories: Perspectives, Publications

Dans la partie 1 de la présente série, nous relations une escroquerie récente du monde des cryptomonnaies dans laquelle un utilisateur mal intentionné avait dérobé plus de 116 millions de dollars américains de la plateforme de finance décentralisée Mango Markets (« **Mango** »). Nous notions que des pressions croissantes s'exercent sur les organisations autonomes décentralisées (« **OAD** ») pour qu'elles protègent les membres contre les vulnérabilités de leurs contrats intelligents. Peu après la publication de ce premier bulletin, les dirigeants de Mango ont commencé à négocier un règlement avec le malfaiteur, qu'on pense être Avraham Eisenberg.

Les négociations et leur dénouement soulèvent des questions pressantes sur la validité des règlements conclus dans l'univers des OAD et de la finance décentralisée.

La proposition d'Eisenberg

Peu de temps après la fraude, Eisenberg a présenté une proposition de règlement au forum de gouvernance de l'OAD de Mango. Il proposait de rendre à Mango pour 46 millions de dollars de jetons volés (MNGO, SOL et Marinade Staked SOL) en échange de deux choses : a) une prime de 70 millions de dollars en jetons; et b) la promesse de Mango de ne pas porter d'accusations criminelles contre lui ni de geler ses actifs[1].

Environ 100 millions de votes devaient être exprimés en faveur de la proposition pour qu'elle soit adoptée. Eisenberg a immédiatement voté pour sa propre proposition avec les jetons acquis lors de l'attaque, qui représentaient plus de 33 millions de votes[2]. Mais cela ne suffisait pas. Il lui fallait encore 66,7 millions de votes[3]. Le fait qu'Eisenberg ait utilisé le fruit de son méfait, les jetons volés, pour voter en faveur de sa propre proposition de règlement – censée, de surcroît, empêcher des poursuites criminelles – non seulement montre qu'il est culotté, mais soulève de sérieuses questions sur la capacité d'une proposition à une OAD de lier ses détenteurs de jetons en ce qui a trait à leurs pertes.

Si certains des dirigeants de Mango semblaient disposés à s'entendre avec Eisenberg (se disant prêts à « l'exonérer de toute faute » et à voir à ce qu'il réalise un « bon profit »), de nombreux détenteurs de jetons ont été outrés par son offre. Ils réclamaient que des poursuites sans merci soient intentées rapidement[4]. Cette dissension soulève encore plus de questions :

Qui parle au nom d'une OAD?

À qui revient-il de décider quelles propositions doivent être mises aux voix? Quelles conséquences exécutoires de tels scrutins peuvent-ils avoir?

Qui, en définitive, assume la responsabilité et le risque au sein des plateformes décentralisées?

Les dirigeants présentent leur propre proposition : Mango conclut un règlement avec Eisenberg

Après l'échec de la proposition d'Eisenberg, les dirigeants de Mango ont déposé leur propre proposition de gouvernance, qui contenait une contre-offre. Leur proposition était ainsi libellée :

[traduction] À [Avraham Eisenberg]...

Nous cherchons à ce que les utilisateurs soient rétablis dans leur situation antérieure dans la mesure du possible. Vous avez convenu de rendre le montant suivant :

[...]

La majeure partie de ces fonds se trouvent actuellement dans le portefeuille Solana yUJw et doivent être envoyés au portefeuille détenu par le Mango Upgrade Council : 9mM6NfXauEFviFY1S1thbo7HXYNiSWSvwZEhguJw26wY

Les 10 000 000 USDC peuvent être envoyés soit au portefeuille Solana de l'Upgrade Council, soit au portefeuille Ethereum qu'ont créé les développeurs : 0xa8e8729A6AAb10178FBac1E9D55A0c536ce3DCa8

Dans les 12 heures suivant l'ouverture de la proposition, vous devrez rendre les actifs autres que les actifs en USDC, en MSOL, en MNGO et en SOL pour montrer votre bonne foi. Les actifs restants devront être envoyés dans les 12 heures suivant la mise aux voix et l'adoption de la proposition.

Les fonds envoyés par vous et par la trésorerie de l'OAD de Mango serviront à couvrir toute mauvaise créance restante dans le protocole. Tous les déposants de Mango auront été rétablis dans leur situation antérieure. ***En votant en faveur de la présente proposition, les détenteurs de jetons de Mango conviennent de rembourser la mauvaise créance avec la trésorerie et renoncent à toute réclamation contre des comptes comportant de mauvaises créances, et ils conviennent de ne pas réclamer d'enquête criminelle ni de gel de fonds une fois que les jetons auront été remis comme décrit*** **ci-dessus**[5] [mise en relief ajoutée].

Quelques jours après l'ouverture de la proposition, la contre-offre des dirigeants de Mango a été adoptée. Une fois de plus, Eisenberg a voté pour en utilisant les jetons acquis lors de l'attaque[6]. Conformément au règlement conclu, il a rendu à Mango pour 67 millions de dollars de jetons volés. En échange, Mango a « permis » à Eisenberg de conserver une « prime à la faille détectée » de 47 millions de dollars en jetons volés et a « promis » de ne pas lancer d'enquête criminelle sur ses activités ni de geler ses actifs[7].

Selon des observateurs, la prime de 47 millions est de loin la plus élevée du genre jamais octroyée dans le secteur des cryptomonnaies. Elle dépasse largement celle souvent versée, d'environ 10 % du butin total[8].

Comme on s'y attendait, de nombreux détenteurs de jetons de Mango ont exprimé leur mécontentement. Leur indignation tenait surtout à la taille de la prime octroyée. Un votant a écrit sur Twitter : « [traduction] [...] une « prime au bogue » de 50 millions, c'est ridicule. Au mieux, le fraudeur devrait récupérer ses coûts (15 M$?) plus 10 M$. Une prime de 10 M$, c'est ce qui a été offert au chapeau blanc qui a dérobé 600 M$ à Wormhole. Mango peut négocier mieux que ça, d'autant plus que l'identité du fraudeur a pratiquement été révélée[9] ». Les détenteurs de jetons s'inquiétaient aussi de la « promesse » de Mango de renoncer à toute réclamation contre Eisenberg[10].

La défense d'Eisenberg : « le code fait la loi »

Le 29 octobre 2022, Eisenberg a accordé une entrevue à Laura Shin pour son balado bien connu, Unchained.

Pendant l'entrevue, il a insisté sur le fait qu'il avait « agi en toute légalité sur un marché ouvert » en suivant le protocole de Mango, même si son équipe de développement « n'avait pas prévu tout ce qui pourrait arriver quand elle a réglé les paramètres comme elle l'a fait »[11].

Bien sûr, la défense d'Eisenberg est très semblable à celles opposées dans d'autres affaires d'escroquerie d'envergure entourant les contrats intelligents et la finance décentralisée. La plus éloquente actuellement devant les tribunaux est celle du piratage allégué d'Indexed Finance par Andean Medjedovic, que relate Bloomberg dans son cahier Businessweek[12]. Les auteurs du présent bulletin représentent le plaignant dans cette affaire, *Cicada 137 LLC c.* *Medjedovic*, qui a déjà donné lieu à une ordonnance de saisie du portefeuille de stockage à froid du défendeur et à l'émission d'un mandat d'arrestation contre lui.

Eisenberg rejette aussi l'idée d'assimiler à une « prime » le fait qu'il conserve une partie considérable des fonds. Il note que les opérateurs prospères font souvent l'objet de critiques acerbes. Il cite l'exemple du milliardaire des cryptos Sam Bankman-Fried, le fondateur de FTX, célèbre pour avoir fait fortune en tirant profit d'occasions d'arbitrage[13].

Des questions pressantes

Le règlement intervenu entre Mango et Eisenberg vient allonger la liste des affaires où une personne exploite des contrats intelligents vulnérables d'une OAD, apparemment sans qu'il y ait possibilité de recours. Ces escroqueries soulèvent plusieurs questions pressantes au sujet du risque associé à la fraude dans l'univers des cryptomonnaies, de la responsabilité à l'égard des propositions de règlement qui s'ensuivent et de l'incidence que peuvent avoir ces affaires sur les droits conférés par la loi. Plus précisément :

Quelles sont les responsabilités des dirigeants d'OAD et des programmeurs à l'égard des codes de contrats intelligents vulnérables, et y a-t-il conflit d'intérêts si ces personnes participent à la rédaction de propositions de règlement quand tout part à la débandade?

Les propositions de règlement faites aux malfaiteurs (et les votes tenus subséquemment pour les valider) sont-elles valables? Sont-elles opposables? Lient-elles les détenteurs de jetons?

Ces « règlements » interdisent-ils aux détenteurs de jetons lésés d'exercer des recours au civil ou de déposer des plaintes au criminel, auprès des autorités policières?

Comment une proposition de règlement d'une OAD et un vote en sa faveur (comme dans le cas de Mango) peuvent-ils être justes et contraignants quand ceux qui subissent les pertes semblent perdre leur droit individuel de décider, et quand le malfaiteur lui-même peut se servir des fruits de l'attaque pour voter en faveur de la proposition?

Une partie (des dirigeants d'OAD ou des détenteurs de jetons) peut-elle « promettre » de ne pas porter d'accusations criminelles ou chercher à faire geler des actifs quand les tribunaux déclarent souvent nuls et non opposables des règlements contenant de tels accords (dissimulation/tentative d'empêcher des poursuites criminelles)

Le vote d'une OAD peut-il, à lui seul, lier un groupe de détenteurs de jetons aux intérêts disparates, dans un accord de règlement avec un fraudeur? Peut-il empêcher ces investisseurs de « faire cavalier seul »

Dans l'espoir d'aplanir les risques et les incertitudes qui pèsent sur leurs plateformes décentralisées et non réglementées, certaines OAD envisagent à présent de se restructurer pour adopter une forme plus classique; celle de la société à responsabilité limitée, par exemple.

Dans notre prochain bulletin consacré à l'affaire Mango Markets, il sera question de restructurations d'OAD. Nous verrons si cette solution peut procurer un bouclier juridique efficace dans le secteur vulnérable aux attaques de la finance décentralisée.

Si vous avez des questions sur les escroqueries traitées dans le présent bulletin ou sur les recours possibles

relativement à de telles affaires ou aux accords censés les régler, n'hésitez pas à contacter les auteurs.

[1] Jesse Coghlan, « Mango Markets exploiter said actions were 'legal', but were they? », 18 octobre 2022, *Cointelegraph*, en ligne.
[2] Sun, « Mango Markets hacker proposes steep settlement »; « Mango Markets looted of $117M, hacker demands massive bug bounty settlement », 13 octobre 2022, en ligne.
[3] « Mango Markets looted of $117M, hacker demands massive bug bounty settlement ».
[4] Repay bad debt discussion.
[5] Michael Bellusci et Sam Reynolds, « Mango Markets Community Counters Exploiter's Settlement Offer », 14 octobre 2022, *CoinDesk*, en ligne.
[6] Prajeet Nair, « Mango Markets Set to Pay $47M Bug Bounty to Hacker », 15 octobre 2022, Bank Info Security, en ligne.
[7] Michael Bellusci et Sam Reynolds, « Mango Markets Community Counters Exploiter's Settlement Offer », 14 octobre 2022, *CoinDesk*, en ligne.
[8] Martin Yong et Ali Martinez, « Mango Markets Community Conflicted Over Record $47M 'Bounty' », 15 octobre 2022, *BeInCrypto*, en ligne.
[9] Pereira, « Mango Market's DAO forum set to approve $47M settlement with hacker ».
[10] Sun, « Mango Markets hacker proposes steep settlement ».
[11] Nicholas Pongratz et Ali Martinez, « Mango Market Hacker Affirms He Isn't Sorry for Actions », 29 octobre 2022, en ligne.
[12] Christopher Beam, « The Math Prodigy Whose Hack Upended DeFi Won't Give Back His Millions », 19 mai 2022, en ligne.
[13] Voir dans le *Globe and Mail* la lettre d'opinion d'Adam Chisholm intitulée « Despite FTX implosion, overzealous crypto enforcement is not the answer».

par Benjamin Bathgate, Reuben Rothstein, Maddie Klimek

Mise en garde