LA PLATEFORME DE FINANCE DÉCENTRALISÉE MANGO ESCROQUÉE DE 117 MILLIONS : PARTIE 1 - LES DAO SONT-ELLES RESPONSABLES DES CONTRATS INTELLIGENTS DE MALFAITEURS?

Publié le 18 octobre, 2022

Catégories: Perspectives, Publications

Le 12 octobre 2022, CoinDesk annonçait qu'un utilisateur mal intentionné avait dérobé plus de 116 millions de dollars américains de la plateforme de finance décentralisée Mango Markets (« **Mango** »)[1].

Mango permet de négocier des contrats à terme au comptant et perpétuels sur son interface de négociation à coût modique basée sur la chaîne de blocs Solana. Comme d'autres marchés décentralisés, elle emploie des contrats intelligents pour apparier des opérations d'utilisateurs de la finance décentralisée. Les contrats intelligents sont des programmes qui s'exécutent automatiquement lorsque certaines conditions sont réunies. Beaucoup trop souvent, ils sont recyclés et réutilisés. Avec suffisamment de ressources, des malfaiteurs peuvent exploiter des failles dans leur code avant que quiconque n'ait le temps d'intervenir pour bloquer l'attaque.

Celle dont a été victime Mango est décrite en détail ici. Selon CoinDesk, le malfaiteur a utilisé plus de 10 millions de dollars en jetons pour siphonner plus de 116 millions de dollars à Mango, en payant des frais modiques et « en faisant tout selon les paramètres établis par la plateforme »[2]. Le site spécialisé dans les cryptomonnaies affirme que, techniquement, Mango n'a pas été piratée. « [Le marché] a fonctionné exactement comme il le devait, et une personne avertie, mais mal intentionnée a réussi à le manipuler pour extraire un magot de ses jetons »[3].

L'attaque est survenue moins d'une semaine après que Binance (le plus grand marché de cryptomonnaies au monde) a subi une perte de 570 millions.

Après l'incident, les développeurs de Mango se sont empressés de défendre leur marché, soulignant que les fournisseurs de leur oracle de prix n'étaient pas fautifs. Mais si le code d'un contrat intelligent est déficient ou n'est pas assez robuste pour faire ce qu'il est censé faire, et qu'il est donc à risque d'être exploité par des escrocs, qui est en faute?

Devant la multiplication des attaques de plateformes de cryptomonnaies et les pertes de plus en plus substantielles qui en résultent, les utilisateurs exercent des pressions croissantes sur les organisations autonomes décentralisées (« **OAD** »), au sein desquelles ils interagissent, pour qu'elles les protègent contre les vulnérabilités de leurs contrats intelligents. Les OAD et leurs responsables en font-ils assez pour écarter les contrats intelligents inadéquats et pour éviter que leur code présente des vulnérabilités? Ces organisations peuvent-elles être tenues responsables d'avoir « permis » des attaques en employant un code de contrat intelligent recyclé ou faible? Quelles sont les normes de diligence applicables à la rédaction d'un code de contrat intelligent?

Des pressions grandissantes s'exercent aussi pour que les OAD remboursent les utilisateurs lésés. Dans le cas qui nous intéresse, Mango a promis de rembourser autant que possible les utilisateurs en utilisant sa trésorerie (sous réserve d'un vote) et les jetons qu'elle pourra récupérer[4]. Mango a demandé à l'auteur de l'attaque de la contacter à blockworks@protonmail.com pour recevoir une « prime à la faille détectée » en échange du retour des fonds. Qu'arrive-t-il cependant si le fraudeur refuse la prime? Quels sont les recours des OAD contre les malfaiteurs? Quels sont ceux des utilisateurs contre les OAD? Les attaques du genre sont fréquentes et elles soulèvent de sérieuses questions d'ordre juridique dont les tribunaux commencent à être saisis.

Au Canada, certaines de ces questions ont été soulevées dans une affaire, *Cicada 137 LLC c. Medjedovic,* où les auteurs du présent bulletin représentent le plaignant. Dans cette affaire, un pirate anonyme a volé pour plus de 15 millions de dollars d'actifs numériques à la plateforme de finance décentralisée Indexed Finance[5]. Il a utilisé une série de transactions exploitant des failles, comme le fraudeur de Mango, pour dévaloriser plusieurs fonds indiciels d'Indexed Finance et surévaluer artificiellement la cryptomonnaie qu'il a immédiatement acquise. La question de savoir si l'exploitation de failles de codes de contrats intelligents donne matière à des poursuites au civil ou peut être considérée comme une opération d'arbitrage formera le prochain chapitre de cette bataille judiciaire.

Si vous avez des questions sur les cas d'exploitation de failles traités dans le présent bulletin ou sur la manière dont les tribunaux canadiens commencent à évaluer l'argument selon lequel « le code fait la loi », n'hésitez pas à contacter les auteurs.

[1] Shaurya Malwa, « How Market Manipulation Led to a $100M Exploit on Solana DeFi Exchange Mango », 12 octobre 2022 : en ligne.
[2] Id.
[3] Id.
[4] Id.
[5] Christopher Beam, « The Math Prodigy Whose Hack Upended DeFi Won't Give Back His Millions », 19 mai 2022 : en ligne.

par Benjamin Bathgate, Reuben Rothstein et Madeline Klimek

Mise en garde