Communiqué du Cercle du Coin sur l'attaque de la DAO

Vendredi 17 Juin 2016, 17 heures

TheDAO, première organisation autonome décentralisée sur la blockchain Ethereum, est depuis ce vendredi matin la cible d'une puissante attaque qui visait à siphonner progressivement les 11 millions d'ethers investis dans le projet. Près de 3,6 millions d'ethers ont ainsi été détournés, soit plus de 30% des fonds de la DAO. C'est un événement majeur dans la jeune histoire de l'économie décentralisée.

Si le problème a vite été identifié, il n'a pas pu être contré dans l'instant même autrement que par un procédé visant à ralentir l'attaque. Un *smart contract* est une chose autonome que la volonté humaine n'arrête point.

Les médias ne vont pas manquer de se saisir de ce sujet, qui pose évidemment de vraies questions, mais risque de les mener à des conclusions hâtives. Il a paru nécessaire, au Cercle du Coin, de fournir des explications à ceux qui souhaitent comprendre, avant de donner lui-même son opinion sur ce sujet.

Les faits

L'attaque utilise une fonction récursive après un appel "split" de payout, permet de collecter des ethers. Des vérifications insuffisantes lors d'erreurs dans l'exécution de transactions dans le protocole Ethereum sont mises en pratique par l'attaquant pour débloquer des fonds.
Cependant, le fonctionnement normal de la DAO fait que l'attaquant ne peut récupérer les éthers volés avant un délai de 27 jours, le temps d'initier la sortie des éthers immobilisés sur le "smart contract " de la DAO. Sans action extérieure, le pirate ne pourra donc pas retirer les fonds avant 27 jours minimum. Le pirate informatique a simplement bougé les fonds vers une proposition qu'il contrôle. Les tokens ne sont donc pas véritablement sortis de TheDAO.

En première réaction, la communauté Ethereum et TheDAO (ou ce qu'il faut bien désigner comme des "responsables" de cette organisation) a proposé un *"soft fork"* qui empêcherait

toute transaction réduisant le compte de la DAO, et ceci dès le bloc 1.760.000, en empêchant les ethers d'être retirés par l'attaquant après le délai de 27 jours (et en basculant de fait TheDAO dans une nouvelle structure). Ce soft fork serait éventuellement suivi par un "*hard fork*" donnant aux détenteurs de tokens de la DAO la possibilité de récupérer leurs éthers en annulant les transactions. Afin que ces deux propositions respectives soient effectivement appliquées, il est désormais nécessaire qu'une majorité des participants au réseau Ethereum applique les modifications inscrites au sein de la nouvelle version patchée du client Ethereum qui vient d'être mise à disposition de tous, de manière à approuver implicitement ces deux choix en accord avec la philosophie de consensus décentralisé à l'origine des crypto-monnaies.

Le blog Ethereum a aussi saisi cette occasion dramatique pour rappeler certaines règles de prudence : "*Les utilisateurs de smart-contracts doivent être très vigilants sur les risques des fonctions récursives, et prendre l'avis de la communauté des programmeurs Ethereum. Cette communauté résoudra probablement ces problèmes dans les prochaines semaines. Il est d'autre part déconseillé de créer de nouveaux contrats qui concerneraient plus de 10 millions de dollars d'investissement, à l'exception des contrats de tokens dérivés et des autres systèmes dont la valeur serait elle-même définie par un consensus exprimé en dehors de la plateforme Ethereum et qui pourrait aisément faire l'objet d'un hard-fork par un consensus de la communauté si un nouveau problème surgit (ex. MKR) et cela au moins jusqu'à ce que les développeurs acquièrent plus d'expérience sur la résolution des bugs et/ou de meilleurs outils soient développés."*

Les réactions

Cette réponse par *hard-fork*, envisagée certes dans l'urgence, mais qui revient à ré-écrire l'histoire et à reprendre en main le système, s'avère cependant assez décriée dans la communauté des crypto-monnaies et donne matière à s'interroger.

La décentralisation et l'autonomie d'un système serait remise en cause de façon assez radicale avec ce choix de hardfork. Les opposants au hardfork pensent qu'un système autonome et décentralisé devrait le rester. Il faut avouer qu'il y a un problème réel si une personne peut modifier le livre des compte ou les contrats qui sont normalement infalsifiables. Le site Ethereum expliquait il y a peu de temps encore : *construisez des applications que nul ne pourra arrêter. Les applications s'exécutent exactement comme programmées, sans possibilité d'arrêt, de censure, de fraude, ni d'interférence par une tierce partie.* La solution envisagée par les dirigeants du projet vient contredire de manière frontale ce discours prometteur. "Ce qui pose un second problème, car en #reprenant la main# (RW: proposant de telles modifications) sur les contrats, l'organisation ne serait-elle pas contrainte d'assumer la responsabilité juridique de leur application ? Sur quels critères seraient désormais décidé ces interventions humaines?

Eric Larcheveque, dirigeant de Ledger, société membre du Cercle du Coin, rappelle sur ce propos que *"le contract a été exécuté de façon légale puisque le code source faisait force de loi lors de la période de création. Ethereum montre que finalement ce projet n'est pas si décentralisé que cela, et que le "Code is Law" s'arrête là ou commence la loi des développeurs d'Ethereum".*

A l'heure ou nous écrivons ces lignes, les dirigeants de l'organisation Ethereum et TheDAO semblent revenir en arrière sur cette option de *hard-fork*, ce qui poserait alors la question des dégâts du vol et de l'avenir du projet de TheDAO.

Notre avis

Des voix respectées dans la communauté rappellent que le Bitcoin, malgré les problèmes d'implémentation déjà rencontrés au fil de son histoire n'a jamais envisagé de telles méthodes. Après tant de critiques malintentionnées sur la gouvernance du bitcoin, et tant d'assurance dans les vertus des blockchains les plus diverses, l'événement de ce vendredi impose un bilan d'étape.

L'Association **Le Cercle du Coin** a publié depuis des mois qu'il n'y aurait "***pas de révolution Blockchain sans Bitcoin***". Or on observe depuis lors que le Bitcoin, souvent décrié par les institutions comme par les médias, bénéficie cependant de façon manifeste tant du développement de l'économie décentralisée que de l'évidence de ses qualités comme monnaie pivot de ces échanges et réserve de valeur. Ceux qui ont suivi pour eux-mêmes le conseil qu'ils donnaient aux autres "d'oublier Bitcoin" doivent en éprouver une certaine amertume.

L'engouement systématique pour toutes les alternatives au Bitcoin, sans discrimination, est souvent le fait de personnes mal informées ou défavorables par principe au Bitcoin. En effet , les spécialistes sont encore dubitatifs sur la solidité et la viabilité d'une blockchain en Turing-Complete car les boucles peuvent être utilisées de manière malintentionnée. C'est une critique importante envers Ethereum et l'on voit qu'elle est encore d'actualité.

Alors que l'implémentation du Bitcoin tourne depuis 8 ans et sécurise aujourd'hui dix milliards d'euros, des projets plus jeunes et exécutés précipitamment avec un manque d'attention peuvent mettre en péril des systèmes financiers. Et il convient aussi de rappeler aux politiques, aux régulateurs et aux professionnels de la finance, que ce qui fait la solidité financière du Bitcoin n'est autre que la solidité technologique de sa blockchain, se basant sur un agencement particulièrement performant dont le token monétaire Bitcoin est un élément crucial.

Le Cercle du Coin saisit cette occasion pour rappeler aux développeurs qu'ils doivent garder une grande vigilance dans leurs projets. Et tout particulièrement, lorsque ces projets concernent des transferts de valeur ou des investissements financiers. La sécurité informatique des blockchains demande des compétences pointues. Des erreurs d'implémentation dans le code ont parfois des conséquences désastreuses.