Andy Greenberg : "Le bitcoin est un piège dans lequel beaucoup de criminels sont tombés"

lexpansion.lexpress.fr/high-tech/andy-greenberg-le-bitcoin-est-un-piege-dans-lequel-beaucoup-de-criminels-sont-tombes_2183665.html

17 novembre 2022

La technicité des cryptomonnaies crée souvent d'énormes malentendus. Ces derniers jours, le crash brutal du géant des échanges crypto FTX rappelle en creux que les régulateurs peinent à comprendre et contrôler ce tumultueux secteur. Quelques mois plus tôt, le retournement brutal du marché crypto (en un an, le bitcoin a perdu 70%) prenait déjà de court nombre de petits porteurs qui pensaient détenir un ticket de loto gagnant.

Dans son passionnant nouveau livre *Les criminels de la cryptomonnaie. Traque au coeur du Dark Web* (éd. Saint-Simon), Andy Greenberg, journaliste d'investigation spécialiste de cybersécurité de Wired montre à quel point la sphère criminelle s'est, elle aussi, formidablement trompée au sujet des cryptomonnaies. Beaucoup de malfaiteurs ont ainsi cru que le bitcoin et ses cousins seraient une couverture parfaite à leurs activités clandestines. Mais des chercheurs et des experts curieux, vite suivis par les forces de l'ordre, ont trouvé ces dernières années des techniques redoutables pour faire parler les mystérieux "livres de comptes" crypto que sont les blockchains. Entretien.

L'Express : Dans votre livre, vous montrez que les cryptomonnaies constituent un outil à double tranchant pour la sphère criminelle. Les malfaiteurs se sont-ils mépris au sujet du bitcoin ?

Andy Greenberg : Lorsque le bitcoin a émergé, l'aspect anonyme du système a très vite intrigué. L'économie souterraine et le Dark Web tenaient-ils un nouveau type de cash intraçable ? Beaucoup de personnes -moi y compris - ont eu cette impression car la blockchain n'enregistre pas d'informations personnelles sur les individus réalisant des transactions crypto. Mais cette hypothèse était erronée : dans les années qui ont suivi, des experts ont établi des techniques permettant de tracer les transactions bitcoin de manière si précise qu'il devenait de plus en plus souvent possible d'identifier la personne derrière. Le bitcoin est un piège dans lequel beaucoup de criminels sont tombés. Ils pensaient tenir avec ça un outil derrière lequel se cacher, il les expose en réalité.

Comment s'y prend-on alors pour traquer des transactions crypto, notamment celles qu'on soupçonne liées à des activités illicites ?

Plus il y a de grand volume de données, plus il devient possible de dégager des schémas révélateurs. La chercheuse américaine Sarah Meiklejohn a été la première à proposer des techniques de traçage qui allaient bouleverser la connaissance qu'on peut avoir de la sphère crypto. L'étape préalable, c'est ce qu'on appelle le "clustering", c'est le fait de regrouper les adresses crypto d'une même personne ou d'une même entité dans une même liste. Ce n'est pas aisé : des adresses crypto, il y en a des millions, et à première vue, rien ne les rattache les unes aux autres. Mais certaines astuces permettent de repérer

celles qui proviennent d'une même personne. Par exemple, si des bitcoins situés sur des adresses différentes sont envoyés au même moment sur une adresse de réception commune, les adresses d'envoi appartiennent très probablement à une même entité.

Mais il y a d'autres techniques pour tracer ces flux d'argent. Souvent, les portefeuilles crypto fonctionnent comme une tirelire : si vous avez 5 bitcoins et voulez n'en dépenser qu'un seul, beaucoup de portefeuilles ne vous permettront pas de prendre le bitcoin désiré en laissant les 4 autres sur l'adresse initiale : ils enverront votre bitcoin vers l'adresse de votre choix et transféreront les 4 bitcoins restants vers une nouvelle adresse automatiquement créée. Si l'on se penche sur la date de création de ces adresses, il est cependant aisé de voir laquelle est votre nouvelle adresse : c'est la plus récente puisqu'elle vient d'être créée. Tout cela permet de suivre le circuit emprunté par l'argent d'une personne, d'une transaction à l'autre.

Une fois le circuit emprunté par l'argent établi, comment parvient-on à percer l'identité des personnes derrière ces transactions ?

En effet, après avoir regroupé toutes les adresses appartenant à de mêmes entités, il faut identifier celles-ci. La chercheuse Sarah Meiklejohn a commencé à déplacer de petites sommes d'argent sur tout un tas de services crypto et à faire de menus achats. Ce faisant, elle récupérait, pour chacune de ces entités, une de leurs nombreuses adresses. Elle la comparait ensuite à celle des grands clusters qu'elle avait établie au préalable.

Journaliste d'investigation spécialisé en cybersécurité, Andy Greenberg est l'auteur du livre "Les Criminels de la cryptomonnaie. Traque au coeur du Dark Web" (éd. Saint-Simon).
DR

De manière très schématique, le fait de réaliser un achat sur SilkRoad permet d'obtenir une adresse utilisée par la plateforme. Si, par ailleurs, cette adresse fait elle-même partie d'un groupe d'adresses bien plus vaste qu'on sait appartenir à une même entité, cela signifie que tout ce listing appartient en réalité à Silk Road. J'ai demandé à la chercheuse si elle pouvait tracer quelques achats crypto que j'avais moi-même faits pour des articles sur le bitcoin et elle les a très aisément remontés. Le fait de disposer des circuits de transactions d'entités suspectes est utile car en général, les criminels utilisent à un moment ou un autre un exchange (NDLR : une plateforme permettant d'acheter ou de vendre des crypto). Or ces plateformes disposent, elles, souvent d'informations sur leurs clients. La justice peut donc, à ce moment-là, leur ordonner de les transmettre aux autorités.

Le fait d'identifier les criminels qui utilisent des cryptomonnaies n'est toutefois pas toujours une garantie de succès. Parfois, la piste remonte à des zones où il sera impossible d'arrêter le coupable (Russie, Corée du Nord...). C'est le cas le plus étrange et le plus frustrant pour les autorités : être en mesure de suivre très précisément les flux d'argent des criminels... et ne pas pouvoir les condamner.

Les criminels n'ont-ils pas développé, eux aussi, de nouvelles techniques pour brouiller encore davantage les pistes lorsqu'ils utilisent des cryptomonnaies ?

Les criminels ont compris que le bitcoin n'était pas aussi intraçable qu'ils le pensaient au départ, mais beaucoup pensent qu'en faisant attention, ils parviendront à masquer leur identité. Ils utilisent diverses techniques pour protéger leur anonymat, mais celles-ci demeurent imparfaites. Les criminels utilisent par exemple ce qu'on appelle des "mixeurs de crypto", des services qui promettent de brouiller les pistes en mélangeant des fonds de diverses provenances, légales et illégales.

Sur de petites quantités, cela fonctionne, mais lorsque les fonds à blanchir sont importants, ce "mixage" ne suffit bien souvent pas à brouiller efficacement l'origine des flux. Plusieurs mélangeurs de crypto ont par ailleurs été fermés par les autorités qui ont, dès lors, pu plonger dans leurs dossiers. Ironie du sort, enfin, certaines plateformes de ce type très prisées des malfaiteurs sont parfois elles-mêmes des arnaques qui ne réalisent pas le brouillage promis.

Les cryptomonnaies sont donc un piège pour les criminels ?

Disons que le jeu du chat et de la souris n'est pas terminé. De nouvelles cryptomonnaies plus dures à traquer sont apparues. Mais les autorités affinent, elles aussi, leurs techniques. Et il faut bien voir que lorsqu'elles font une percée décisive, cela ne sert pas qu'aux enquêtes en cours ou à venir : elles appliquent leur trouvaille à tous les dossiers non résolus par le passé. Les criminels laissent donc sur la blockchain des empreintes qu'ils ne pourront jamais effacer.

Quels intérêts présentent les cryptomonnaies pour la sphère criminelle ?

Les cryptomonnaies ne sont pas aussi intraçables et anonymes que ce que l'on supposait au début. Mais elles présentent d'autres avantages qui les rendent attrayantes aux yeux des criminels, notamment le fait d'être "incensurables", ce qui signifie qu'un acteur, une autorité ou un Etat n'a pas le pouvoir de bloquer des transactions s'y déroulant. Et cela, c'est une caractéristique très intéressante pour des acteurs ayant des activités illicites.

"Les criminels de la cryptomonnaies. Traque au coeur du Dark Web", Editions Saint-Simon. Parution le 17 novembre 2022.
DR

Les criminels qui exploitent les cryptomonnaies ont-ils des profils différents de ceux qui utilisent des circuits plus traditionnels ?

Des figures criminelles atypiques ont en effet émergé dans la sphère crypto. Avec sa vision très nihiliste de la société et son profil *nerd*, Alexandre Cazes, le fondateur d'Alphabay (NDLR une énorme place de marché illégale) n'avait guère l'aspect d'un baron du crime classique. Idem pour Ross Ulbricht, ce trentenaire américain très inspiré par les courants

libertariens qui avait créé quelques années plus tôt la célèbre plateforme de vente de drogue SilkRoad. Aux yeux de Ross Ulbricht, personne ne devrait avoir le pouvoir d'interdire à d'autres individus de se droguer. Et toute sa plateforme était conçue de manière à ce qu'un internaute puisse trouver et commander aisément la substance de son choix. Mais il ne tolérait pas sur SilkRoad certaines activités plus violentes.

Quand Ross Ulbricht a été arrêté, d'autres criminels avec des profils plus "classiques" ont cependant pris sa suite, montant des plateformes similaires à SilkRoad, mais sans ces gardes fous. Les forces de l'ordre ont également été confrontées à des cas dramatiques, notamment celui de Welcome to video, un vaste réseau de diffusion de vidéos pédocriminelles. Là, c'est un tout autre niveau de noirceur... Les enquêteurs ont fait un travail remarquable qui a permis de secourir des douzaines d'enfants et d'arrêter 337 personnes dans le monde, notamment l'administrateur du site. Les ressorts de l'affaire sont extrêmement choquants. Les services qui ont permis de démanteler cette plateforme provenaient majoritairement de l'administration fiscale américaine et n'étaient pas des enquêteurs habitués à ce type d'affaires. Lors de mes échanges avec eux, j'ai mesuré à quel point ils étaient traumatisés par ce qu'ils avaient vu. Il est important de parler de ce cas. Les défenseurs de la vie privée sur internet s'inquiètent souvent de voir les questions de pédocriminalité instrumentalisées pour justifier la surveillance de masse. Et ils n'ont pas entièrement tort. Mais il est vital de garder en tête que ce sujet n'est pas non plus une vue de l'esprit : ces horreurs existent.

Les criminels se servent-ils fréquemment des cryptomonnaies ? En 2022, la firme Chainalysis révélait que seules 0,15% des transactions crypto étaient liées à des activités illicites.

Les cryptomonnaies intéressent un public de plus en plus vaste et le nombre de transactions crypto licites a grimpé en flèche. De ce fait, la part de transactions crypto liées à des activités criminelles a beaucoup baissé en proportion. Mais en volume, elles ont augmenté. Les criminels crypto sont plus actifs que jamais.