LES CAHIERS DU CEIFAC

CEIFAC

Collège Européen des
Investigations Financières et
Analyse financière Criminelle

ACTES DE COLLOQUE
CRYPTOMONNAIES ET BLOCKCHAIN : QUELLES PERSPECTIVES ?

Université de Strasbourg (France)
24 octobre 2019

N°4 - 2020 Parution - Gratuite - ISSN 2272-981X

Éditorial

SÉBASTIEN DUPENT

PROFESSEUR ÉCONOMIE GESTION OPTION INFORMATIQUE ET SYSTÈME D'INFORMATION
CONSUTANT INGÈNIEUR DE RECHERCHE AU CEIFAC
SPÉCIALISTE CYBERSÉCURITÉ - CYBERCRIMINALITÉ

Les monnaies virtuelles ou cryptomonnaies dont le concept a vu le jour en 1989 par la création d'un protocole de paiement anonyme basé sur la cryptographie par la *société DigiCash Inc.* fondé par David Chaum, connaît actuellement un boum sans précédent à la fois dans leur utilisation et dans leur nombre.

Ainsi, depuis 2009, date de naissance de la monnaie virtuelle la plus connue, le Bitcoin, plus de 2500 monnaies virtuelles sont nées et ont essayée de trouver une place dans le domaine du paiement numérique et anonyme[1]. De plus, tout comme le Bitcoin, qui a connu son plus haut niveau en dépassant les 19000 $ en fin d'année 2017 et qui fluctue depuis entre 7000 et 11000 $, certaines voient leur cours atteindre des sommets du fait d'annonces politiques ou commerciales[2].

Les monnaies virtuelles sont généralement mises en place pour répondre à un certain nombre de demandes légitimes et bénéfiques. Par exemple, la réalisation de transactions peu coûteuses, rapides et nécessaires dans l'économie 4.0 ou tout un chacun peut effectuer des achats à l'autre bout du monde ou encore offrir des services financiers dans les régions en voie de développement où l'accès aux banques est souvent inexitant.

Au demeurant, *l'a priori* négatif exprimé par le grand public peut aisément trouver une explication au regard des publications dans la presse, ou de la position de certains gouvernements qui n'hésitent pas à mettre en avant l'utilisation de ces monnaies à des fins criminelles, particulièrement dans le cadre du blanchiment d'argent sale.

Bien au contraire, penser de la sorte, c'est oublier que le taux de change des monnaies virtuelles par rapport aux monnaies fiduciaires est très variable. De plus, il est à relever que, malgré leurs réputations de monnaies anonymes, un bon nombre d'entre-elles ont perdu cette qualité.

Ainsi, les enquêteurs disposent maintenant d'outils d'investigation de plus en plus performants pour à des fins d'analyse et de poursuite des flux suspects, tel que, en matière de Bitcoin, l'utilisation d'une blockchain[3] ouverte, permettant de suivre les transactions de bout à bout.

Cette combinaison d'éléments mêlant avancées technologiques et évolution des risques liés au phénomène de la criminalité financière transnationale constituent un réel défi qu'a tenté de relever l'Union européenne.

En 2018, la mise en place de la cinquième directive anti-blanchiment d'argent[4], applicable depuis le 10 janvier 2020 dans l'ensemble des États membres, pose un cadre réglementaire destiné à réguler les échanges des monnaies virtuelles.

Le CEIFAC s'est lui aussi intéressé à cette problématique lors du colloque « Cryptomonnaies et blockchain : quelles perspectives ? », organisé en octobre 2019.

En donnant la parole à des universitaires, mais également à des spécialistes des enquêtes dans le domaine des monnaies virtuelles, le colloque a eu pour but de faire état des obstacles et des menaces gangrénant la matière.

Vous trouverez dans ce cahier le détail des présentations effectuées lors de cette conférence.

Notes :

1. Parmi lesquelles on peut citer *l'Ethereum, le Ripple, le Bitcoin Cash, le Litecoin, le NEO et le Monero*
2. L'annonce de la création par Facebook d'une monnaie virtuelle du nom de Libra a fait croitre de plus de 20 % le cours des principales monnaies virtuelles.
3. Système qui peut être comparé à un grand livre
4. https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32018L0843

Sommaire

SÉMINAIRE DE RESTITUTION DU PROGRAMME DE RECHERCHE-ACTION DU CEIFAC

PROPOS INTRODUCTIFS

Par Emilie EHRENGARTH, Docteure en droit
Chercheur associé à l'université de Strasbourg

Chaque année, l'Union européenne organise une « journée du Numérique » (le 10 avril) au cours de laquelle les États membres sont encouragés à prendre des engagements communs. La première journée, organisée en 2017 à Rome, avait été marquée par la signature d'une déclaration en faveur d'une coopération européenne accélérée en matière de superordinateurs

En 2019, la Commission européenne et la présidence du Conseil de l'Union européenne encouragent la coopération en matière d'Intelligence Artificielle – IA, de cybersanté, et de blockchain. Cette technologie nouvelle consiste à stocker des blocs d'informations de façon à les distribuer sur le réseau et est à la base de la monnaie virtuelle, le Bitcoin.

La Commission entend alors « établir les bases de la création d'un partenariat européen de la blockchain afin de promouvoir des infrastructures interopérables qui renforceront » la confiance des opérateurs et des consommateurs pour « garantir la sécurité et la vie privée ».

En 2017, dans un rapport, *Transparency International* affirmait que le blanchiment d'argent sale traversait les centres financiers européens et relevait qu'il était très difficile pour les autorités d'identifier les bénéficiaires effectifs des sociétés-écrans et des trusts (particulièrement en République tchèque, en Italie, au Luxembourg, aux Pays-Bas, au Portugal et en Slovénie). Plusieurs secteurs, et particulièrement la monnaie virtuelle, ont été reconnus comme extrêmement vulnérables favorisant la criminalité transfrontalière.

Très récemment, dans un rapport conjoint (5 juin 2019), Eurojust et Europol ont fait état d'un problème de localisation physique des criminels qui usent largement d'outils de cryptage et d'anonymisation tout en ayant recours aux monnaies virtuelles ; le rapport, d'ajouter, que l'ensemble de ces obstacles est renforcé par le manque d'harmonisation des cadres juridiques nationaux, empêchant une coopération européenne et internationale efficace.

Sur la base de ce rapport, le colloque propose d'évaluer l'impact des Bitcoin sur la criminalité transfrontière et de déterminer les moyens de lutte et les défis présents et futurs, le tout dans l'optique d'une coopération européenne renforcée.

Seront étudiées les différentes évolutions de ces cryptomonnaies et leur «reconnaissance» par des États, notamment par de grandes compagnies (ex : lancement possible d'une cryptomonnaie *Libra par Facebook*), les moyens dont disposent les enquêteurs au niveau de l'analyse, du suivi, de l'identification et de la saisie de ces biens immatériels, … Présentation de cette thématique par Monsieur Robby HOUBEN (professeur à l'Université d'Anvers, spécialiste de la cryptomonnaie).

Quant aux blockchains, bases de données publiques décentralisées, qui contiennent toutes les transactions de certaines monnaies cryptées (par exemple : *Bitcoin, Ethereum, VeChain*), cette information publique, offrira aux enquêteurs des pistes des possibilités existantes pouvant les aider dans le cadre de leurs enquêtes financières. Pour ce faire, un regard technique sera apporté par l'enquêteur Christophe LANDRIES qui se propose de présenter les moyens et outils mis à disposition des autorités de poursuites.

TABLE RONDE N° 1:
ETAT DES LIEUX
PAR ROBBIE HOUBEN

Propos retranscrits par Elena Pelliser, docteure en droit, Université de Strasbourg.

Professeur en entreprise et marchés des capitaux à l'Université d'Anvers, Robby Houben, à la demande du Parlement européen en 2017, a effectué une étude sur les cryptomonnaies et la cybercriminalité.

En matière de cryptomonnaies et de blanchiment de ces dernières, mais aussi de blockchain, le maillon technologique qui sous-tend les cryptomonnaies, la technologie et les techniques évoluent rapidement. Le phénomène « crypto » est énorme : les 100 cryptos les plus présentes constituent une capitalisation mondiale supérieure à 330 milliards d'euros. Mais selon Christine Lagarde, il n'y a pas lieu de s'inquiéter concernant la régulation, le phénomène étant jugé comme marginal, même si l'avènement de la Libra – la cryptomonnaie de Facebook – pourrait changer la donne. En effet, avec des milliards d'utilisateurs potentiels, cette dernière pourrait avoir un impact non négligeable en termes de politique monétaire.

En revanche, l'impact peut être considérable pour des petits investisseurs confrontés à une extrême volatilité de ces supports. Le phénomène n'est pas non plus marginal pour les services de lutte contre la fraude, le blanchiment et le financement du terrorisme. Pour preuve, en 2018, 7 milliards d'euros de cryptomonnaies auraient été utilisés à des fins illicites.

Les cryptomonnaies sont définies comme une représentation numérique d'une valeur (autrement dit non physique) ayant vocation à être utilisées en peer-to-peer en tant qu'alternative à la monnaie fiduciaire émise par les Etats. Elles sont hors système étatique et ne sont pas contrôlées par les Etats. Elles servent de moyen général d'échange et sont conçues d'emblée comme des moyens de paiement, même si elles sont utilisées essentiellement à des fins spéculatives. Indépendantes des banques centrales et sécurisées au moyen d'un mécanisme de cryptographie, elles peuvent être converties en monnaies fiduciaires et réciproquement.

Les cryptomonnaies se distinguent des « jetons », qui sont conçus pour lever des fonds et non comme moyens de paiement, même si ces deux supports ont en commun d'avoir une valeur et de pouvoir servir à du blanchiment.

Elles dépendent d'une technologie dite distribuée, par exemple, la blockchain. Pour autant, accuser cette technologie d'être un vecteur de blanchiment serait un peu brutal. Il vaudrait mieux se concentrer sur les utilisations illicites de la technologie, ce qui est également l'approche adoptée par l'Union européenne (UE).

Pour comprendre le contexte réglementaire entourant les cryptoactifs, analysons les grands acteurs et en premier lieu les utilisateurs, suivis des « mineurs » de cryptoactifs qui valident les transactions.

Les risques associés à l'activité des mineurs de cryptoactifs ont été sous-estimés, du fait de l'anonymat relatif des personnes et des lieux utilisés pour cette activité. Les places de change sont également des intervenants importants. Pour les acteurs du marché, ces plateformes ouvrent des possibilités de trouver des contreparties pour leurs opérations. Pour finir, citons comme acteurs, les fournisseurs de portefeuilles numériques de cryptoactifs, puis les dépositaires de clés cryptées et enfin les créateurs de cryptoactifs.

Les principaux défis de lutte contre blanchiment en matière de cryptoactifs.

L'identification des défis posés par la lutte contre le blanchiment est une question prioritaire, au premier rang desquels, celle de l'anonymat des individus (anonymat total ou pseudo-anonymat). Dans le cas d'un pseudo-anonymat, maîtriser les techniques de levée de l'anonymat permet de savoir qui utilise les cryptoactifs, or, pour certains bitcoins tels Monero ou Dash, l'opération est impossible. L'anonymat permet de faire des opérations en-dehors du contrôle des autorités, ce qui est particulièrement intéressant pour les organisations criminelles.

Face au défi de l'anonymat de l'opérateur, la cryptomonnaie et la blockchain pourraient constituer de nouvelles armes pour lutter contre le crime organisé, la corruption ou autres infractions telles que les rançongiciels, actes par lesquels des criminels prennent le contrôle d'un ordinateur et demandent le versement d'une rançon pour recouvrer l'accès aux données. Elles pourraient empêcher ces types de crime par la décentralisation des données, permettant alors leur sécurisation (par exemple, à Shenzen en Chine, les blockchains sont utilisées pour lutter contre la fraude fiscale). Si les blockchains enregistrent toutes les données, elles pourraient, à l'avenir, enregistrer bien d'autres données, facilitant alors le travail des professionnels de la sécurité. Cette possibilité, utile au demeurant, se heurtera à l'épineux sujet de la protection des données personnelles et plus largement de la cybersécurité. En l'espèce, un équilibre délicat est à trouver. Mais, en tout état de cause, les risques liés à une utilisation illégitime des dispositifs de lutte contre les infractions susnommées peuvent justifier que les besoins de la société priment sur la garantie d'anonymat de l'acteur.

Une deuxième difficulté réside dans la nature transfrontalière de ces défis, ce qui exige une réponse internationale coordonnée.

Enfin, une troisième difficulté consiste en l'absence d'intermédiaire central. Pour utiliser les moyens proposés dans la loi, il faut une personne contre qui se retourner, faute de quoi cela devient très difficile. Imposer un intermédiaire

permettrait d'actionner les leviers du droit.

Le rôle des instances internationales et européennes.

Il faut relever l'existence de plusieurs organismes internationaux. Que ce soit le Fonds monétaire international (FMI), la Banque mondiale, le G20 ou encore le G7, il est légitime de se demander si le cadre réglementaire de l'UE est suffisant face à ces défis lorsqu'il s'agit de lutter efficacement contre l'anonymat dans le champ des monnaies virtuelles et l'utilisation des sites de ces dernières.

En l'état actuel des législations, il n'y a rien. La « 4e directive »[1] est silencieuse, et la « 5e directive », entrée en vigueur en janvier 2020[2], ne traite que de deux des acteurs de la cryptomonnaie, à savoir, les places de change de cryptomonnaies et les prestataires qui conservent les portefeuilles numériques de cryptomonnaies. Ces deux acteurs sont définis comme des entités soumises à obligation qui doivent réaliser les contrôles de diligence de leurs clients et déclarer les opérations suspectes, ce qui marque un net progrès. Ce ne sont toutefois que deux des acteurs du secteur des cryptomonnaies alors que pas moins de sept acteurs devraient être concernés par les dispositifs légaux. Il demeure donc encore un grand nombre d'angles morts et on peut s'attendre à ce qu'ils soient exploités par des criminels. Il serait naïf de considérer que de telles lacunes ne deviennent pas le terrain de jeu privilégié des organisations criminelles internationales.

A l'occasion des travaux préparatoires du Parlement européen, la Commission avait suggéré d'introduire une sorte de registre d'utilisateurs. Cette suggestion n'a pas été adoptée. Au contraire, la Commission a pris le faible engagement d'examiner la faisabilité d'un enregistrement volontaire futur. Il est fort à parier que les organisations criminelles ne s'exécuteront pas. Si l'enregistrement était obligatoire, il devrait être sélectif, déclenché, par exemple, par un seuil. Et même dans ce cas, les réseaux criminels risquent certainement de ne pas s'enregistrer. En revanche, un tel registre constituerait un outil supplémentaire de sanction.

Les réglementations ne seront toutefois pas suffisantes. Il faut les combiner avec des techniques d'investigation pour savoir ce qui se passe précisément sur le terrain et dans l'éventuelle découverte d'infractions, des outils de sanction adaptés doivent exister. A l'évidence, la « 5e Directive » n'envisage pas de traiter les crypto-acteurs comme les banques.

Notons, par ailleurs, que des initiatives ont déjà été prises. Dès 2015, le Groupe d'Action Financière (GAFI) a lancé des activités sur les cryptomonnaies, puis, a élargi la portée des recommandations en 2018 afin qu'elles couvrent les actifs virtuels et les prestataires de services concernant lesdits actifs, dont les acteurs purs de change, ce que ne fait pas l'UE[3].

Au début de l'été 2019, le GAFI a même renforcé son action en demandant aux Etats membres, dont l'UE, de mettre en œuvre les recommandations ainsi formulées d'ici juin 2020. Un exercice de monitoring à cet égard sera mené en juin 2020 en vue, d'une part, d'élaborer un cadre de sanctions adéquat en matière d'affaires traitant d'utilisations illégales d'actifs virtuels par des prestataires de services, et d'autre part, faire que les acteurs du secteur ne contournent pas les dispositions par une autorégulation. Le contrôle et la surveillance doivent être mis en place par un organe étatique.

Aux vues du caractère transfrontalier des cryptoactifs, le niveau d'action européen semble bien mieux adapté que le niveau national. Cependant, force est de constater que, si l'Union européenne demeure inactive, ce sera aux Etats de répondre aux défis soulevés.

Il faut relever que même si le GAFI a mis à jour en octobre 2018 ses recommandations en la matière, leur mise en œuvre reste problématique. Face à une question qui intéresse tant les professionnels du secteur public, que ceux du secteur public, ou encore le citoyen lambda, il faut rappeler l'extrême volatilité de ces cryptomonnaies, qui ne sont pas couvertes explicitement par les règles de protection des investissements, alors que les avertissements et appels à la prudence sont nombreux.

Evoquons, par exemple, le prospectus d'une société londonienne spécialisée dans le transfert de devises à moindre frais. Ce document précise que la Libra répond à un problème de transfert de monnaies entre différents pays : le coût des transferts notamment est assez onéreux. La technologie pourrait apporter des solutions par la rapidité des opérations. Or, la Libra ne serait qu'une cryptomonnaie de plus. Le fait qu'elle soit créée par Facebook lui donne une envergure et un impact considérables et comme elle est soutenue par Visa, Paypal et d'autres moyens de paiement lui donne encore plus de puissance. Sa force vient du fait qu'elle s'appuie sur une monnaie sous-jacente, et ne varie pas simplement selon l'offre et la demande. La Libra sera introduite par Calibra, une filiale de Facebook, ce qui donnera à ce dernier l'accès à des masses de données d'utilisateurs. Même si Facebook se défend de vouloir le faire, il pourrait personnaliser les profils en fonction des dépenses et cibler plus facilement la publicité.

Les entités privées ne sont pas seules à envisager la création de monnaies virtuelles. Certains pays, comme la Suède qui avait en projet la e-krona resté sans effet à ce jour, explorent cette piste. En revanche, des projets visant à numériser la monnaie fiduciaire d'un pays, très différents des bitcoins et autres cryptomonnaies, sont également à l'étude, sous le contrôle des banques centrales et des Etats. Un nombre conséquent de banques centrales explorent cette piste, mais à l'évidence, nous sommes à l'opposé de l'idée de décentralisation. Parmi les cas connus, au Venezuela, le Petro n'est pas réellement une réussite, il s'agit d'éviter des sanctions internationales et cela laisse à penser qu'un petit groupes d'îles du Pacifique vont tenter d'adopter des cryptomonnaies en tant que monnaie nationale. Pour l'instant, rien n'est envisagé à grande échelle, mais seul l'avenir nous le dira.

Ajoutons enfin, que pour mettre en place un système de monnaies virtuelles, il

faut disposer de la technologie et des connaissances suffisantes. Par exemple, pour générer des bitcoins, il faut beaucoup de puissance informatique, et donc beaucoup d'électricité. Certains pays ne disposent pas de la capacité matérielle ou financière, et, avant d'envisager la mise en place d'un dispositif régalien destiner à encadrer et à lutter contre tout risque de corruption, de blanchiment ou encore de financement du terrorisme via l'usage des cryptomonnaies, le premier défi qui se posera à ces Etats sera celui de l'avancée technologique et technique des moyens pratiques de mise en œuvre de tels supports de paiement.

1. Notes

2. Directive (UE) 2015/849 du Parlement Européen et du Conseil du 20 mai 20+15 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission (Texte présentant de l'intérêt pour l'EEE), OJ L 141, 5.6.2015, p. 73–117.

3. Directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les directives 2009/138/CE et 2013/36/UE (Texte présentant de l'intérêt pour l'EEE) PE/72/2017/REV/1, OJ L 156, 19.6.2018, p. 43–74.

4. http://www.fatf-gafi.org/fr/themes/recommandationsgafi/documents/recommandations-gafi.html?hf=10&b=0&s=desc(fatf_releasedate).

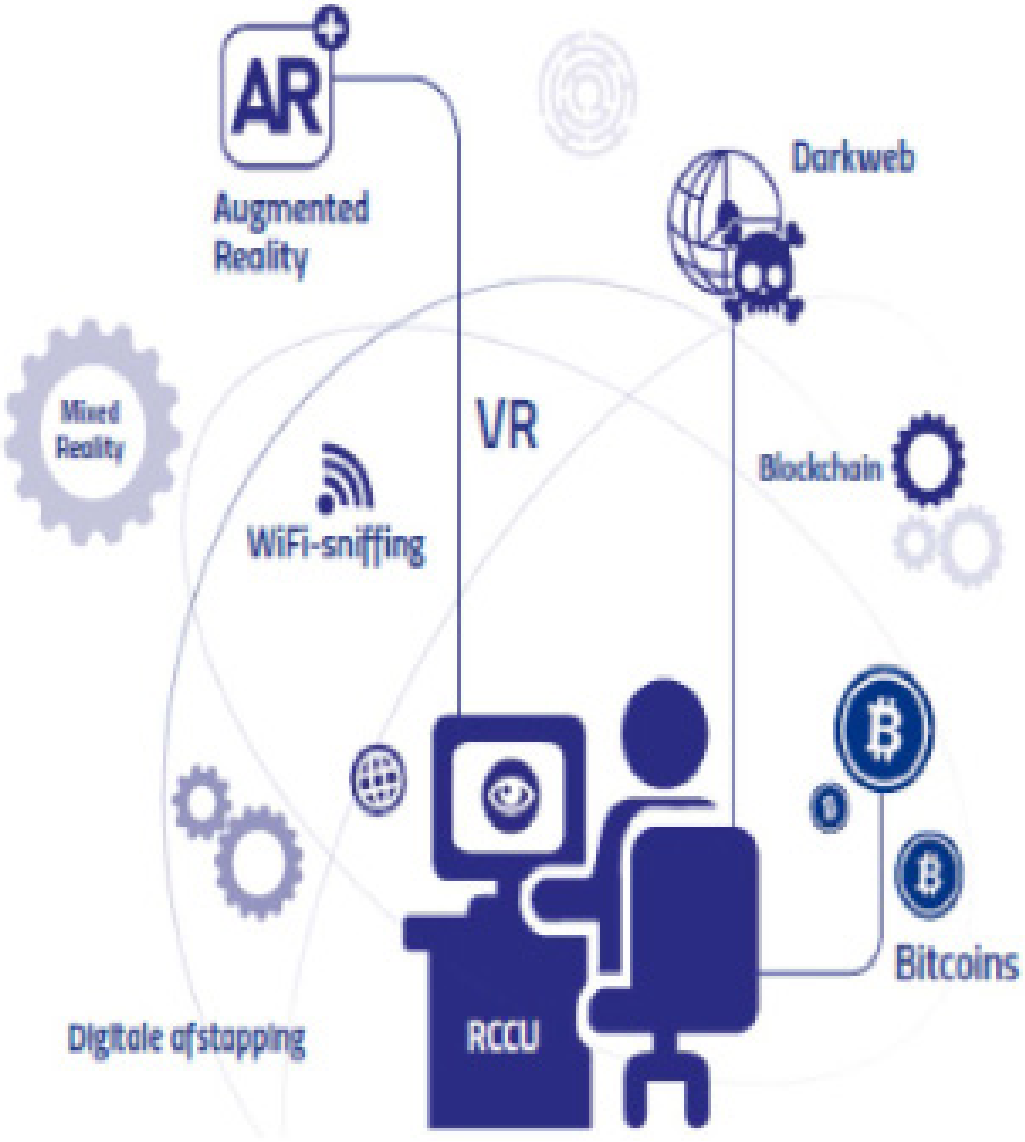


TABLE RONDE N° 2:
ENQUETES EN MATIERES DE CRYPTOMONNAIES : QUELS DEFIS ?
PAR CHRISTOPHE LANDRIES

(Propos retranscrits par Elena Pelliser, docteure en droit, Université de Strasbourg).

Enquêteur depuis plus de vingt ans, affecté à l'équipe R&D de l'Unité fédérale belge de lutte contre la criminalité informatique, Christophe Landries travaille sur les questions de cybercriminalité depuis plus de onze années. Il est spécialisé dans la problématique du DarkWeb ou encore des cryptomonnaies. Actuellement, il est à la tête d'un projet international EMPACT et donne intervient auprès du CEPOL, au Conseil de l'Europe et à Interpol.

La thématique de la formation contre la cybercriminalité est un sujet très sensible.

A ce jour, sont recensées 3 028 cryptomonnaies, et, on peut aisément annoncer que chaque jour de nouvelles sont mises sur le marché.

On estime qu'elles représentent 204 milliards de dollars de capitalisation. Parmi cette somme, 66% se matérialisent en Bitcoin, monnaie pseudo-anonyme, ou encore sous la forme de Monero, Euthereum ou encore Zcash sont, elles, sont anonymes.

Le commerce des monnaies virtuelles.

Les monnaies virtuelles ou cryptomonnaies sont numérique.

Elles ne sont pas sous contrôle étatique, donc non réglementées.

Elles ne dépendent pas d'une autorité centrale et sont par conséquent décentralisées.

Elles peuvent être pseudo-anonymes (en partie privées, en partie transparentes) ou totalement anonymes.

Elles sont immuables, disponibles en offre limitée et se jouent des frontières terrestres, maritimes ou étatiques.

Toutes les transactions sont recensées dans un grand livre public qui se réalise via la technologie des chaînes de blocs ou blockchain en anglais. En somme, il est possible de connaître la transaction mais il est impossible de savoir qui a effectué ladite transaction.

Les cryptomonnaies constituent un sous-ensemble des monnaies virtuelles. Elles utilisent un système de clés publiques et privées. Pour leur part, les bitcoins peuvent être utilisées de bien des manières pour la réalisation d'objectifs criminels comme, par exemple, en matière d'extorsion (rançongiciels ou sextorsions), du cryptojacking, dans le commerce de biens et des services illégaux (mise en place de marchés sur le darknet), celui du blanchiment d'argent sale, du transfert de ressources dans le but de dissimuler ces fonds, du financement du terrorisme, ou encore de cyber-attaques à l'encontre des sociétés ou des utilisateurs de cryptomonnaies.

Par ailleurs, le secteur des cryptomonnaies donne lieu à un nombre important d'arnaques.

Citons, par exemple, l'utilisation d'un rançongiciel utilisé pour crypter les données de la victime et qui ne seront décryptées qu'en échange de l'achat d'une clé de décryptage. Les services répressifs sont confrontés à une forme émergente de criminalité : la « RaaS » (Ransomware-as-a-Service).

Dans cette forme de criminalité, les criminels vendent ou offrent une suite logicielle (abonnement mensuel ou annuel) et se rémunèrent sur les rançons versées par les victimes pour récupérer leurs données. Les criminels proposent toute une série de services (helpdesk, C&C etc.). Les rançongiciels sont livrés prêts à l'emploi. Le chiffre d'affaires est très important et le niveau de connaissances est peu élevé. Les bénéfices sont réinvestis dans d'autres activités, légales. Un projet international a été lancé sous l'égide d'Europol : le projet « NoMoreRansom »[1]. La plateforme mise à disposition s'avère importante et utile tant pour les services répressifs que pour les victimes de ces agissements.

Enfin, des sites de commerce illicite sur le Darkweb utilisant les paiements en bitcoins sont fermés régulièrement par les forces de l'ordre (Alpha Bay par exemple). Les bitcoins sont utilisés pour commercer, par des fournisseurs de cartes de débit prépayées, qu'elles soient tangibles ou virtuelles, pour le minage ou encore par des fournisseurs de services de DAB. L'importance de la surveillance et de règlementation de l'ensemble de ces secteurs ou activités se justifie pleinement car ce sont des points d'entrée pour la cybercriminalité organisée.

Afin de s'en prémunir, en cas de transactions en cryptomonnaies, il est indispensable d'adopter des mesures de connaissance client, dites « KYC », et notamment, obtenir des justificatifs d'identité et de résidence telle une photo pour prouver l'identité de l'intéressé et des justificatifs de résidence réelle comme la production de facture d'électricité ou de gaz. Il faut également recueillir les numéros de téléphone et adresses électroniques du bénéficiaire ainsi que ses informations bancaires complètes, actualisées et exactes. Toutes les transactions effectuées en bitcoins sont enregistrées et peuvent être téléchargées. Pour ce faire, passer par un moteur de recherche permet d'interroger la blockchain qui contient beaucoup d'informations utiles à l'enquête. Citons ici, quelques sites utiles :

http://blockchain.info

https://www.blocktrail.com/BTC

http://bit.ly/blockexplorers (alternatives- sur Reddit)

http://www.walletexplorer.com

Comment acheter des cryptomonnaies ?

L'achat de tels moyens de paiement s'effectue auprès d'un distributeur automatique de bitcoins (par exemple, le site coinatmradar.com indique la location des DAB proposant de telles opérations), sur des bourses spécialisées, ou encore, par en ayant recours à la vente

de biens ou de services.

Dans le cadre de leurs investigations, les services répressifs sont en mesure de vérifier si une transaction a bien été enregistrée dans le registre blockchain. Si l'enregistrement d'une telle transaction fait défaut, il ne sera pas possible d'enquêter sur la destination de la rançon versée pour récupérer ses données. Le cas le plus fréquemment rencontré au cours d'enquêtes pénales est celui d'une transaction ou deux transactions en sortie, démontrant que l'adresse a changé et que la rançon a été déplacée ou que le pourcentage criminel a été récupérée. Pour mener l'enquête, l'officier devra relier les adresses les unes aux autres dans le but de faire émerger le réseau criminel bénéficiaire de cette opération illégale.

De plus, l'interrogation du registre de blockchain permet de vérifier les honoraires des mineurs et les frais de transactions. Initialement, il était possible de miner des bitcoins à partir de son ordinateur personnel ; actuellement, le recours à des infrastructures lourdes et coûteuses est incontournable. Les mineurs se rassemblent alors autour d'une série d'ordinateurs.

Par ailleurs, rappelons ici que la blockchain est une technique qui permet l'accès public aux transactions regroupées en blocs ordonnés, dans un registre décentralisé et public. Une blockchain contient plusieurs blocs (le premier block est 0. Chaque bloc contient plusieurs transactions (un millier), chaque transaction a une valeur de hachage, et le tout est sécurisé.

Comment enquêter sur des cryptomonnaies ?

En la matière, plusieurs possibilités s'offrent aux services spécialisés. Ils peuvent notamment suivre la piste de l'argent, rechercher des renseignements en source ouverte (OSINT), analyser et suivre des blockchains et s'attacher en particulier au clustering (multiplicité d'entrées, changements) ou à l'attribution, utiliser des outils en source ouverte ou commercialisés, ou encore, utiliser le potentiel des informations de KYC.

Les enquêtes portent principalement sur le Bitcoin. On assiste peut-être à un basculement vers des cryptomonnaies garantissant l'anonymat (*Monero, Verge, Zcash*, par exemple). Tous les Bitcoins ne sont pas utilisés à des fins criminelles. Même en cas d'utilisation des cryptomonnaies anonymisées, par des renseignements en source ouverte, il est tout à fait possible de décoder l'adresse de destination. Concernant l'analyse et le suivi d'une blockchain, l'enquêteur peut vérifier le solde d'une blockchain grâce à un moteur de recherche de type blockchain.com et étudier l'historique des transactions. Il existe pour cela des outils disponibles en source ouverte ou sous la forme de logiciels commercialisés. Il convient de faire attention aux transactions qui se scindent, par exemple en *« Bitcoin Cash » (BCH) et « Bitcoin Gold » (BTG)*. Même dans ce cas de figure, Il existe des outils permettant un suivi des transactions.

Certaines techniques permettent de lever l'anonymat des transactions. Par exemple, l'enquêteur a recours au groupage (adresses d'entrée multiples/adresses de changement), à l'attribution (mettre des tags ou attributs), aux bourses et autres places formant un écosystème de transaction, et étudie les points d'entrée et de sortie (monnaie fiduciaire/BTC).

Quelles sont les difficultés auxquelles se heurte l'enquête sur des cryptomonnaies ?

Dans la lutte contre le blanchiment d'argent sale ou le financement du terrorisme, il existe des techniques spéciales permettant de camoufler les opérations telles que le mixing, le tumbling ou le laundering. Ces techniques rompent les liens et en empêchant la traçabilité des opérations. Il est également possible pour le criminel de regrouper des transactions individuelles en lot, ce qui aura pour effet d'empêcher le suivi d'une des traces. En matière de Bitcoin, l'anonymat reste relatif.

Face à un processus de mixing, tumbling et laundering, il est important pour l'enquête d'identifier celui qui procède réellement aux opérations. Or, certains wallets ont une fonction « CoinJoin intégrée » qui regroupe des transactions en une opération unique pour garantir une plus grande protection de l'anonymat, et certaines cybermonnaies alternatives (altcoins) ont des caractéristiques de mixage. La question de la protection de l'anonymat est de plus en plus importante sur les places de marché du Dark-Net.

Comment les cryptomonnaies favorisent le blanchiment d'argent ?

Le GAFI s'efforce de faire sortir les criminels du secteur des cryptomonnaies anonymes.

Il est légitime de demande s'interroger sur l'opportunité de se doter au niveau européen d'une base de données pour les services de police regroupant toutes ces informations, sur le modèle américain de ICECRIM, qui permet de recenser la plupart des sites illégaux et est accessible à toutes les forces de l'ordre. Notons, qu'en la matière, l'échange et le recueil d'information accrus ainsi que la formation vont dans le bon sens. On ne peut que saluer cela et appuyer toute initiative permettant l'expansion des outils de lutte contre ces formes de criminalités organisées.

L'échange des informations, la coopération entre les services européens, et le partage des techniques d'analyse, donnent de plus en plus de résultats.

En revanche, il faut relever que les cryptomonnaies reposant sur l'anonymat total sont un réel souci pour les représentants de l'ordre public, mais rien n'est impossible, et, il est important de noter que certains bureaux de change n'acceptent plus certaines cryptomonnaies comme *Monero*. Si plus aucun acteur n'accepte ces cryptomonnaies, l'enquête n'en sera que plus simplifiée et la lutte contre la cybercriminalité plus efficace. Pour résoudre le défi soulevé par l'anonymat garanti par Monero, le rétro-engineering permettrait peut-être de récupérer l'adresse de sortie de

l'opération. Par exemple, les forces de l'ordre suédoises opèrent une comparaison entre les achats et les ventes en monnaies virtuelles pour identifier les transactions aberrantes.

Enfin, il faut relever que ces monnaies virtuelles ne sont pas intraçables, ce n'est que momentané car tout laisse une trace sur Internet. Les avancées en matière d'intelligence artificielle et la mise en œuvre de l'ordinateur quantique participeront à n'en pas douter à l'amélioration des dispositifs de lutte contre le détournement de l'usage des cryptomonnaies.

Notes

1. https://www.europol.europa.eu/newsroom/news/no-more-ransom-108-million-reasons-to-celebrate-its-third-anniversary.

LES CAHIERS DU CEIFAC

Numéro ISSN : 2272-981X
Université de Strasbourg, UMR-DRES 7354
11, rue du Maréchal Juin - BP 68 - 67046 STRASBOURG CEDEX
Site internet : www.ceifac.eu
Adresse mail : contact@ceifac.eu
Directrice du CEIFAC : Chantal CUTAJAR
Rédacteur en chef : Sébastien DUPENT
Conception : Manuela TANE

TABLE RONDE N° 3:
LA PREVENTION DES RISQUES LIES AUX CRYPTOMONNAIES
PAR MICHELLE ABRAHAM

Avocate d'affaires au Barreau de Paris, chargée de cours à l'université d'Évry.

Ancienne collaboratrice de la Délégation des Barreaux de France à Bruxelles, elle travaille depuis 2014 sur les cryptomonnaies, les blockchains et le défi réglementaire que leur développement implique.

A ce titre, elle écrit régulièrement des articles sur le site bitcoin.fr.

Michelle Abraham est également membre du Cercle du Coin (association spécialisée dans les cryptomonnaies) et participe à la commission Blockchain de l'AFNOR qui représente la France à l'ISO.

Les criminels ont très tôt vu les avantages d'utiliser bitcoin pour acheter et vendre des produits illicites sur le darknet. Les sites Silk Road, Silk Road 2 et plus récemment Alpha Bay et Hansa sont des exemples notoires fermés par le FBI pour avoir vendu des milliers de produits illicites contre des bitcoins.

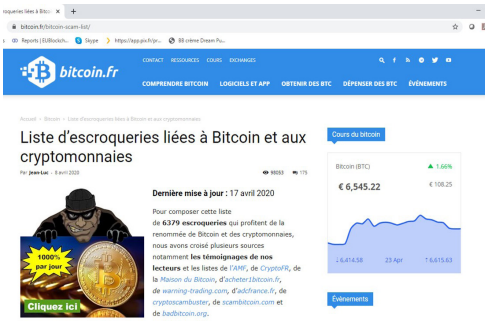
Or, les cas d'utilisation des cryptomonnaies (achat et vente de produits et de services, plateformes de change, portefeuilles de cryptomonnaies, minage, fonds d'investissement en cryptomonnaies et autres prestataires de services sur actifs numériques, etc.) sont très majoritairement licites.

Selon la société Chainalysis seulement 1,1% du volume de l'ensemble des cryptomonnaies serait utilisé à des fins illicites[1].

Les cryptomonnaies, comme les crypto-actifs de manière générale, ne sont qu'un outil technologique.

Certaines caractéristiques des cryptomonnaies peuvent malheureusement être utilisées à des fins illégales.

Des criminels détournent les investissements en cryptomonnaies pour appâter le public par des faux investissements dans des cryptomonnaies qu'ils n'ont même pas.



https://bitcoin.fr/bitcoin-scam-list/

De même, alors que des entreprises dépensent des fortunes en électricité, en achats d'ordinateurs surpuissants, en locaux et en sécurité pour effectuer légalement leur activité de minage des cryptomonnaies, les cybercrimels détournent la puissance de calcul et les ordinateurs de tiers pour miner à leur insu des cryptomonnaies.

Les victimes sont souvent des personnes ou des entreprises qui n'avaient jamais entendu parler de cryptomonnaies avant les faits. Lorsqu'elles découvrent les escroqueries ou les atteintes à leur système de traitement automatisées de leurs données (ordinateurs, périphériques), ces victimes se trouvent souvent démunies et ne savent pas à qui s'adresser.

Afin de limiter ces méfaits, il est important de s'attacher à prévenir les risques liés aux cryptomonnaies.

Cette prévention passe par la compréhension des caractéristiques des cryptomonnaies et de leur détournement possible, ce qui permettra de développer de bonnes pratiques et une coopération entre les différents acteurs du secteur.

COMPRENDRE LES CARACTERISTIQUES DES CRYPTOMONNAIES ET DE LEURS DETOURNEMENTS

Les criminels choisissent souvent leurs victimes parmi le grand public où les personnes sont généralement peu averties des particularités des cryptomonnaies.

Pour lutter contre ces agissements, il est essentiel de former ces populations et de les avertir des menaces.

A. CONNAITRE LES CRYPTOMONNAIES : QUELLES SONT LES CARACTERISTIQUES DE BITCOIN ET DES AUTRES CRYPTOMONNAIES ?

1. Qu'est-ce que bitcoin ?

A la création d'Internet, la question d'envoyer de l'argent par ce biais s'est rapidement posée. Néanmoins, lorsqu'un document est envoyé par courriel, l'envoyeur en reste propriétaire et peut l'envoyer à une ou des milliers de personnes à la fois. Or, cette solution n'est pas acceptable en ce qui concerne un moyen de paiement.

Bitcoin[2] est la première cryptomonnaie qui relève avec succès le problème de la double dépense. Dans ce système décentralisé et open source, les transactions sont inscrites sur la blockchain par les « mineurs », des ordinateurs extrêmement puissants et très chers (actuellement on ne peut plus miner des bitcoins avec un ordinateur ordinaire car il n'est pas assez puissant pour obtenir des bitcoins), qui vérifient au préalable que :

la personne qui envoie des bitcoins les détient réellement (il n'y a pas de crédit dans la blockchain bitcoin : on ne peut dépenser que l'argent que l'on possède),

le propriétaire n'envoie qu'une seule fois ses bitcoins (pas de double dépense).

Une fois validée, la transaction ne peut être annulée. Les bitcoins sont transférés de manière irréversibles du portefeuille de l'envoyeur (qui ne les possède plus) à celui du receveur. La transaction

peut être consultée sur la blockchain à partir de moteurs de recherche spécialisés librement accessibles[3]. Le mineur reçoit, en récompense pour ses services, une portion de nouveaux bitcoins créés directement par l'algorithme[4]. Le nouveau propriétaire des bitcoins se voit attribuer une clé privée (équivalent à un code pin bancaire) et une clé publique (équivalent à un numéro de compte bancaire). Dans les affaires liées aux investissements factices, la victime ne se voit jamais attribuer ces clés.

2. Qu'est-ce que les autres cryptomonnaies (ou altcoins) ?

D'autres cryptomonnaies sont apparues, à la suite de la création du bitcoin. Ces monnaies virtuelles, dont certaines peuvent être très éloignées du modèle bitcoin, sont dénommées altcoins (pour l'expression anglaise « Alternative coins »).

Il existe actuellement plus de 5.000[5] cryptomonnaies différentes vendues sur plus de 300 plateformes de change qui regroupent ensemble plus 21.000 combinaisons d'offres. Chacune de ces monnaies virtuelles a des caractéristiques propres. Certaines ont été faites sur le modèle de bitcoin comme litecoin, d'autres sont faites pour être aussi anonymes que des espèces c'est le cas de monero et de zcash. Il convient de noter que pour miner du monero, il n'est pas nécessaire d'avoir des ordinateurs aussi puissants que pour bitcoin. On peut miner cet « altcoin » avec un simple ordinateur portable.

Dans la mesure où la création de cryptomonnaies est libre, toute personne peut en créer. Les détournements peuvent donc être potentiellement nombreux. La force d'une monnaie virtuelle va dépendre de sa diffusion, de son utilisation, du protocole de registre distribué utilisé, ainsi que de la communauté de développeurs et d'utilisateurs qui la soutiennent.

B. CONNAITRE LES MODES OPERATOIRES DES CRIMINELS EN MATIERE DE CRYPTOMONNAIES

De nombreuses fraudes existent en la matière, mais pour les besoins du présent article seules seront analysées celles qui sont peu connues du grand public : l'investissement factice dans des cryptomonnaies et le « cryptojacking ».

1. Les escroqueries aux cryptomonnaies sans cryptomonnaies

Le 14 avril 2020, 6.375 escroqueries[6] exploitant la renommée de bitcoin et des cryptomonnaies ont été répertoriées le site bitcoin.fr. Beaucoup de ces fraudes concernent des investissements factices en cryptomonnaies mis en place par des bandes organisées.

Dans un communiqué de presse du 17 septembre 2019, le Parquet de Paris, l'Autorité des Marchés Financiers (AMF) et l'Autorité de contrôle prudentiel et de résolution (ACPR) lançaient une alerte sur l'industrialisation du phénomène.

Le mode opératoire est le suivant : « des placements sur (…) le bitcoin (…) peuvent être proposés par des sites particulièrement bien documentés et présentant une apparence de sérieux. (…) Ces propositions proviennent d'interlocuteurs avec lesquels toutes les démarches sont effectuées en ligne, par internet et par messagerie, puis par téléphone sur un numéro français (ou apparemment français), sans rencontre physique. (…) La victime est mise en relation avec un faux conseiller dont le discours [est] manipulatoire (…). Incitée à effectuer un premier versement et rassurée sur la rentabilité et la réalité de son investissement, la victime investira des sommes plus importantes qu'elle ne pourra récupérer. (…) Les sommes sont versées sur des comptes bancaires étrangers situés dans des pays proches de la France et appartenant même parfois à la zone euro, avant d'être systématiquement virées de nouveau vers d'autres pays beaucoup moins coopératifs sur le plan judiciaire. »

La criminalité organisée leurre, par ce biais, ses victimes en leur faisant croire qu'ils achètent des cryptomonnaies, comme avant elles leur faisait croire qu'ils achetaient des diamants. Alors qu'en réalité, il n'y a jamais eu ni cryptomonnaies ni diamants ! La difficulté est qu'ils se présentent de manière très professionnelle (usurpant si besoin l'identité de personnes ou de sociétés) et font des pressions psychologiques sur leurs victimes.

Par ailleurs, comme il n'y a pas de petit profit ces escroqueries se doublent souvent d'une arnaque dite de la « recovery room »[7]. Les victimes sont recontactées par les criminels (qui changent d'identité ou transfèrent les données de leurs victimes à d'autres criminels) qui leur proposent, en se présentant sous de fausses identités professionnels (avocat, analyste financier, comptable, conseiller financier)[8], de les aider à récupérer les fonds qu'ils ont perdus. Bien entendu, une fois encore les victimes devront payer mais ne recouvrons pas leur argent !

https://www.titanium-project.eu/

Selon l'AMF, les plus de 50 ans représentent plus de 65 % des victimes et 81 % de l'ensemble des sommes perdues, la tranche d'âge la plus impactée étant celle des 60-69 ans. Pourtant, les statistiques montrent qu'aucune tranche d'âge n'est à l'abri. Si les retraités sont les plus touchés (48,2 % des montants investis), toutes les catégories socio-professionnelles sont concernées. Le territoire français est touché dans son ensemble. Toutefois, la région Provence Alpes Cotes d'Azur apparait comme la première région visée par les escroqueries (17,3 % des montants investis), suivie par l'Auvergne-Rhône-Alpes, l'Occitanie, puis l'Ile de France.

Les escrocs s'adaptent très rapidement aux évolutions du marché et aux opportunités qu'ils peuvent saisir.

Le prochain halving[9] de bitcoin laisse à penser que l'on va assister à une nouvelle envolée du cours. Les escrocs risquent

de saisir cette nouvelle occasion pour sévir.

L'AMF a ainsi répertorié depuis peu une recrudescence de nouveaux sites internet proposant de manière illicites des cryptomonnaies. Le 3 avril 2020, l'AMF et l'ACPR ont lancé une alerte mettant en garde le public contre les activités de plusieurs acteurs proposant en France, sans y être autorisés, par la voie de leur site internet, des investissements sur des produits dérivés sur crypto-actifs[10].

2. Les attaques à coût réduit pour les cyberattaquants : le « cryptojacking »

Le « cryptojacking » est une technique qui vise à utiliser les ordinateurs de tiers pour miner sans permission des cryptomonnaies. Les cybercriminels subtilisent la puissance de calcul des ordinateurs qu'ils infectent : ce qui augmente les coûts énergétiques pour le véritable propriétaire et use plus rapidement le matériel qui est plus lent et a beaucoup de « bugs ».

De nos jours, le « cryptojacking » vise principalement le minage de moneros.

Deux techniques sont employées :

- infecter la page d'un site légitime (en général un site très fréquenté afin que cela soit rentable), en y insérant un code malveillant, afin que les ordinateurs des utilisateurs qui se connectent à cette page minent, à l'insu, du monero tant qu'ils naviguent sur cette page,

- infecter directement un ou plusieurs ordinateurs cibles.

La société Bitdefender, spécialisée en sécurité informatique, a relevé, qu'entre septembre 2017 et janvier 2018, le nombre de logiciels malveillants de minage avait augmenté de 130,10% !

En février 2018, le site « the Hackernews », annonçait que plus de 4.000 sites auraient été infectés. Les victimes se trouvaient dans le monde entier et un certain nombre de sites officiels étaient atteints : la National Health Service (système de santé britannique), l'Information Commissioner's Office (équivalent britannique de la CNIL), ou le portail d'information judiciaire... américain.

Interrogé sur ce phénomène, M. Vincent Meysonnet[11], représentant technique en France de Bitdefender indiquait que les cybercriminels pouvaient générer 0,25 dollar de monero par jour et par machine, ce qui représentait pour 2.000 ordinateurs infectés un montant de 500 dollars par jour.

Le site de silicon.fr [12], s'appuyant sur un rapport de la société de sécurité informatique Symantec, indiquait que « La France, à elle seule, concentre 5,9% du volume total d'attaques de type cryptojacking. L'Hexagone se positionne ainsi au 4e rang mondial et au 2e rang européen ».

En août 2019, la gendarmerie nationale[13] a démantelé un réseau situé en Ile de France qui avait infecté 850.000 ordinateurs à travers le monde et dont une grande majorité se situaient en Amérique centrale et en Amérique du Sud.

Pour lutter contre cette criminalité, il apparaît essentiel de mettre en place des mesures de prévention efficaces.

DEVELOPPER DES BONNES PRATIQUES ET LA COOPERATION POUR FACILITER LA PREVENTION

La prévention ne pourra se développer qu'en passant par la mise en place de bonnes pratiques et une coopération entre les différents acteurs de l'écosystème et les forces de l'ordre et entre les différents pays.

A. SUIVRE DES BONNES PRATIQUES :

Différentes organisations[14] ont proposé un certain nombre de principes pour se prémunir contre l'utilisation criminelle des cryptomonnaies. Ces conseils peuvent en substance être regroupés en deux catégories : les bonnes pratiques applicables aux particuliers et celles applicables aux entreprises.

1. Les bonnes pratiques pour les particuliers

i) Face à l'offre de tiers ou d'un ami : les entreprises sérieuses dans le domaine des cryptomonnaies ne font pas du démarchage agressif et ne font en général aucune promesse de rendement excessif. Il est important de ne répondre pas aux démarchages téléphoniques. Si un ami ou un proche vous parle d'un investissement dans les cryptomonnaies, se rappeler du principe que la confiance n'empêche pas le contrôle. Des vérifications concernant les sociétés et leur dirigeant s'imposent par des recherches sur les réseaux sociaux et sur Who.is (pour avoir des informations sur le site). Dans la mesure où les criminelles visent à l'économie et reproduisent illégalement des photos ou des textes déjà publiés sur internet, il est intéressant de rechercher les images ou les textes sur google afin de voir s'ils ne proviennent pas d'autres sites,

ii) Consulter dans tous les cas les listes noires de l'AMF, ainsi que les listes de sites spécialisés (bitcoin.fr, cryptofr.com,...) qui sont en générale beaucoup plus fournies et importantes[15]. Il est également très intéressant de consulter les escroqueries répertoriées sur le site de l'Association de Défense des consommateurs de France (« ADC France »), qui est la première association française à enquêter en la matière,

iii) Si vous souhaitez investir : ne jamais investir plus que ce que l'on est prêt à perdre, résister à la tentation d'un gain important et rapide. Il est essentiel de prendre le temps de se former et de se renseigner sur les cryptomonnaies auprès de tiers avant d'investir des sommes importantes,

iv) Investissez de préférence sur des plateformes situées en France[16] et prêter une attention particulière à la présence ou pas des mentions légales obligatoires. Consulter le site mis en place par l'AMF afin d'alerter et protéger les épargnants des fraudes éventuelles (la section « Suis-je victime d'une arnaque ? » https://protectepargne.amf-france.org/),

v) Si vous êtes malheureusement victime : se rappeler que tout le monde peut être victime de cybercriminels,

qui sont de plus en plus inventifs pour montrer une apparence de sérieux et de professionnalisme, même les personnes les plus aguerries peuvent tombées dans leurs pièges. Il n'y a rien de honteux à cela. Demander de l'aide auprès de professionnels dont vous avez pu vérifier les références (faites en particulier attention aux « recovery room »).

vi) Porter plainte : l'ADC France rapporte la difficulté d'un certain nombre de consommateurs à déposer plainte : certains services refusent de prendre les plaintes. En cas de difficultés ou de classement sans suite de votre plainte, ne pas hésiter à faire appel à des professionnels du droit afin de vous assister et à déposer une plainte avec constitution de partie civile.

2. Les bonnes pratiques pour les entreprises

i) Principes généraux liés à la cybersécurité : garder tous les systèmes à jour, utiliser un anti-virus et d'autres logiciels protégeant votre ordinateur et votre navigation, conserver plusieurs types de sauvegardes,

ii) Principes à avoir à l'esprit concernant les cryptomonnaies : surveiller le réseau du trafic et les activités anormales de son ordinateur, former les utilisateurs d'internet sur ces questions, faire appel à des entreprises spécialisées pour détecter les logiciels de minage et détruire les scripts.

iii) Porter plainte afin de permettre aux forces de l'ordre d'agir. Dans ces derniers rapports sur la cybercriminalité, Europol déclarait que même si ces cas de « cryptojacking » étaient publiés dans la presse peu d'entre eux étaient officiellement signalés.

B. LA COOPERATION EST L'UNE DES PIERRES ANGULAIRES DE LA PREVENTION

1. Développement d'une coopération en France entre les victimes, les acteurs du secteur des cryptomonnaies, les associations et les forces de l'ordre et la justice

Le monde des cryptomonnaies est complexe tant par sa technicité que par son caractère international. Ce qui nécessiterait une collaboration étroite entre les victimes, les associations et les conseils qui les représentent, les sociétés spécialisées en matière de crypto-actifs, les forces de l'ordre et la justice. Pour cela, il faut des moyens et du temps.

Interrogé sur le sujet, M. Guy Grandgirard, président d'ADC France regrette que nombre de consommateurs victimes de fraude à l'investissement de cryptoactifs subissent une double peine : celle d'être déconsidérés par les instances qu'ils rencontrent pour avoir cru à des rendements de 250% pour l'achat de monnaies virtuelles. Il précise que bon nombre des victimes ne voulaient que placer leur patrimoine issus d'héritage, d'assurance-vie ou autre à un moment où les taux d'intérêts proposés par les banques étaient devenus dérisoires et que les médias et la télévision ne cessaient de parler de l'évolution du cours du bitcoin passé en quelques mois de 3.000 euros à 20.000 euros.

Il rappelle que parmi l'ensemble des escroqueries liées au forex, diamants, vins rares et autres, celles concernant les cryptomonnaies représentent les montants dérobés les plus importants : de 500 euros à 3.000.000 d'euros, soit une moyenne de 50.000 euros par victime.

Il souhaiterait voir la création d'une instance nationale qui pourraient centraliser tous les cas liés à ces affaires et avoir ainsi une efficacité accrue en ayant une vision plus globale.

Il est aussi essentiel de créer des ponts entre les communautés de cryptomonnaies, les forces de l'ordre et les acteurs institutionnels.

Les meilleurs spécialistes des cryptomonnaies sont les membres de la communauté des cryptomonnaies eux-mêmes, ainsi que les sociétés spécialisées en cybersécurité. Face aux escroqueries, ils sont mieux armés que le grand public pour éviter les dangers.

De nombreuses informations sur des fraudes sont régulièrement publiées par l'écosystème. Elles se trouvent facilement en ligne, notamment sur les sites suivants : bitcoin.fr, journalducoin.com, cryptofr.com, cryptonaute.fr, cryptoast.fr, thecointribune.com, fr.cryptonews.com.

D'autres associations spécialisées dans le secteur des cryptomonnaies et autres cryptoactifs peuvent être consultées : le Cercle du coin, Asseth, Association pour le Développement des Actifs numériques (ADAN)...

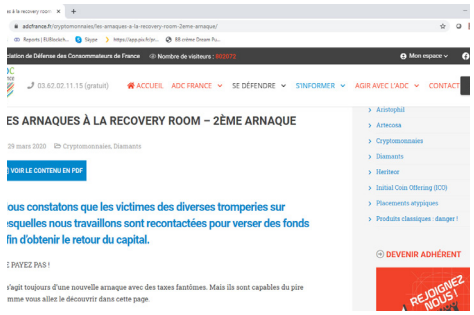
L'écosystème des cryptomonnaies s'est d'ailleurs adapté et certaines sociétés, comme Chainalysis[17] ou Scorechain[18] se sont spécialisées dans la détection de transactions douteuses sur la blockchain. Chainalysis a d'ailleurs participé à des opérations menées avec succès avec Europol.

2. Développement d'une coopération internationale

Les cybercriminels opérant au niveau international, la coopération entre les Etats est un élément essentiel. Les victimes se retrouvent souvent découragées et dans l'incompréhension lorsqu'on leur explique que dans la mesure où leurs fonds sont sortis du territoire national et ont fait l'objet d'un transfert dans un, voire plusieurs pays peu coopératifs en matière pénale, elles ont peu de chance de recouvrer leurs avoirs. Un Etat seul ne peut lutter contre des fraudes de dimension internationale concernant des pays dans le monde entier. Il apparaît essentiel de faire appel à organisations comme Europol ou Interpol.
Europol est un acteur très actif dans le cadre de la coopération judiciaire internationale concernant les affaires ayant un rapport avec les cryptomonnaies. Europol a également la particularité d'avoir très tôt fait la distinction entre les entreprises de cryptomonnaies ayant une activité licite et les cybercriminels utilisant de manière illicite les cryptomonnaies[19]. Néanmoins, cet organisme ne peut agir que s'il est saisi par les Etats membres et si un nombre important de victimes est répertorié et qu'elles portent plainte.

Interpol participe pour sa part au projet européen TITANIUM[20] (pour "Tools for

the Investigation of Transactions in Underground Markets").



https://www.adcfrance.fr/cryptomonnaies/les-arnaques-a-la-recovery-room-2eme-arnaque/

TITANIUM est une initiative intéressante, même si elle ne concerne pas à proprement parler les investissements factices en cryptomonnaies. Ce projet a été mis en place afin de rechercher, développer et valider de nouvelles techniques et solutions axées sur les données conçues pour aider les forces de l'ordre chargées d'enquêter sur les activités criminelles ou terroristes impliquant des monnaies virtuelles et / ou des marchés clandestins dans le darknet.

Les outils[21] créés par le projet TITANIUM recouvrent les trois missions suivantes : i) surveiller les tendances des écosystèmes du marché des monnaies virtuelles et du darknet ; ii) analyser les transactions sur différents portefeuilles de devises virtuelles iii) produire des rapports pouvant être présentés comme preuve devant les tribunaux. Il s'agit de premiers pas.

L'association ADC France ne connaît actuellement pas d'équivalent en France et en Europe. Elle reçoit des demandes de ressortissants Belges, Suisses, Espagnols et Portugais qui ne savent pas vers qui se tourner dans leur pays et la sollicitent. Cet exemple montre que malgré des initiatives ponctuelles, des efforts restent à faire et tous les pays sont concernés.

Notes

1. Rapport de Chainalysis « The 2020 state of crypto crimes », Janvier 2020, https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf,

2. Pour plus d'information sur le sujet, voir « Bitcoin et altcoins : des questions juridiques ... et comptables », Michelle Abraham, RF Comptable, Février 2018 n°457

3. https://www.blockchain.com/explorer,

4. Le nombre de bitcoins (BTC) devant être produits au total est de 21 millions. Ils sont émis par portion toutes les 10 minutes, jusqu'en 2140. Les portions de bitcoins sont divisées par deux tous les quatre ans : c'est ce que l'on appelle le « halving ». A sa création, 50 BTC étaient émis par transaction validée, puis ce chiffre a été de 25 BTC, actuellement il est de 12,5 BTC et sera de 6,25 BTC lors du prochain halving attendu vers le 12 mai 2020 (pour plus d'information lire : https://fr.cryptonews.com/news/le-troisieme-halving-de-bitcoin-c-est-dans-moins-d-un-mois-6157.htm),

5. Selon le site coinmarketcapt.com au 12 avril 2020

6. https://bitcoin.fr/bitcoin-scam-list/

7. Voir la définition très intéressante donnée par l'Autorité des Marchés financiers belge de la « recovery room » : https://www.fsma.be/fr/recovery-room, consulter également le site de l'Association de Défense des consommateurs de France qui donne des exemples de « recovery room » https://www.adcfrance.fr/

8. https://www.adcfrance.fr/

9. Voir la note iv ci-dessus

10. https://www.amf-france.org/fr/actualites-publications/communiques/communiques-de-lamf/lamf-et-lacpr-mettent-en-garde-le-public-contre-les-activites-de-plusieurs-acteurs-qui-proposent-en

11. https://www.youtube.com/watch?v=q-tUN4kvKL7A

12. https://www.silicon.fr/cryptojacking-france-4e-rang-mondial-204337.html,

13. https://www.lemonde.fr/pixels/article/2019/08/28/la-gendarmerie-a-neutralise-un-reseau-de-850-000-ordinateurs-infectes-par-le-meme-virus_5503771_4408996.html, https://decoded.avast.io/janvojtesek/putting-an-end-to-retadup-a-malicious-worm-that-infected-hundreds-of-thousands/

14. Telles que l'Autorité des marchés financiers, la Security Exchange Commission américaine, l'Autorité des Marchés financiers belge, l'ADC France,

15. 95% d'escroqueries sont répertoriées en plus sur ces sites,

16. L'absence de listes blanches créées par des institutions a longtemps été un facteur de risque. L'AMF a commencé à établir une liste blanche des prestataires sur actifs numériques et notamment des plateformes de change en cryptoactifs. Pour l'instant, il n'y a qu'une société (Coinhouse) qui a obtenu le précieux sésame. Les critères de fonds propres demandés par l'AMF sont souvent en pratique des freins aux sociétés françaises licites du secteur qui étant de petites tailles et ne pouvant s'aligner préfèrent s'établir à l'étranger et laissent ainsi une place libre que les criminels s'empressent de combler,

17. https://www.chainalysis.com/,

18. https://www.scorechain.com/

19. https://bitcoin.fr/les-gendarmes-et-les-voleurs-et-bitcoin/

20. https://www.titanium-project.eu/

21. Pour plus de détails sur ces outils consulter le site de Titanium et voir la vidéo « Seven Steps to Combat Cybercrime » également présente sur le site.

LES PARTENAIRES DU CEIFAC

Dans le cadre du programme « Prevention and fight against crime » initié par la Commission européenne (CE) (DG Home Affairs – Action grant 2012-FINEC Financial and economic crime), le CEIFAC a été financé de 2013 0 2015 par la CE à 90% du montant total du projet et le complément a été apporté par les collectivités locales et territoriales (Eurométropole et ville de STRASBOURG et Conseil régional d'ALSACE), l'Université de STRASBOURG et la Gendarmerie Nationale.

Les partenaires financiers

FSI Fonds Sécurité Intérieure
Union européenne
l'Europe se mobilise

Strasbourg.eu
eurometropole

Grand Est
ALSACE CHAMPAGNE-ARDENNE LORRAINE

Gendarmerie nationale

Les partenaires institutionnels

Douanes & Droits Indirects

Police
Police judiciaire fédérale

EUROPOL

EUROJUST

Oficina Antifrau de Catalunya

Police Nationale – Direction Centrale de la Police Judiciaire

UNIL | Université de Lausanne