Cryptomonnaies, blockchains: problèmes pénaux choisis


DR

Marco Traglia,
avocat


DR

Thierry Godel,
Dr en droit

L'anonymat et la traçabilité limitée des transactions au moyen de cryptomonnaies attisent les convoitises des esprits criminels. Or, les caractéristiques des monnaies virtuelles et de la blockchain rendent malaisée l'incrimination de certains comportements au regard du droit pénal en vigueur, sans toutefois les soustraire à toute répression.

1. Généralités

Les marchés frémissants et attractifs des cryptomonnaies génèrent une forme de criminalité sophistiquée contre des individus, des entreprises, des administrations ou des plateformes d'échange: des *maliciels* cherchant à dérober aux utilisateurs des cryptoactifs dans leur porte-monnaie (*wallet*[1]) ou utilisant la puissance de calcul de leur appareil à des fins de minage (*cryptojacking*), des vols de clés privées (*private key*[2]) par hameçonnage (*phishing*), des *rançongiciels*, etc. Ces attaques peuvent être menées lors de la confection d'une monnaie électronique, de sa mise en circulation (par exemple par *initial coin offering*) ou de son utilisation. Les risques concrets de blanchiment d'argent et de financement du terrorisme, par des investissements ou des recherches de fonds en cryptomonnaies, sont déjà reconnus[3]. Elles sont utilisées, sur le *darknet* ou dans la réalité tangible, pour le commerce de drogues, de pornographie illégale, de cartes de crédit volées, de marchandises falsifiées, d'armes et d'autres produits illégaux. Des rançons sous forme de monnaies virtuelles ont déjà été demandées dans des affaires d'enlèvement de mineurs.

La forte évolution des cryptomonnaies ainsi que l'anonymat et la traçabilité limitée qui caractérisent leurs transactions attisent les convoitises des organisations criminelles[4]. Par exemple, une étude estime à environ 76 milliards de dollars par an les activités illégales impliquant du *bitcoin* (soit 46% des transactions en *bitcoins*)[5]. Une majorité d'actes criminels n'est vraisemblablement pas identifiée en raison des caractéristiques inhérentes au système.

2. La traçabilité limitée des transactions

Le système des cryptomonnaies fonctionne avec la *blockchain*, une technologie de stockage et d'échanges codés[6]. Elle peut être décrite comme un grand livre comptable, complet et inaltérable, d'échanges entérinés au sein d'une communauté virtuelle[7], sans organe de contrôle centralisé. Ce système repose sur la confiance des consommateurs dans le code, via un réseau informatique *peer to peer*. Le registre virtuel est conservé au sein des nœuds du réseau (*nodes*), formés par les milliers de supports informatiques connectés entre eux (ordinateurs ou *smartphones*) qui forment la communauté.

Une *blockchain* est unique[8]. Elle est généralement publique, de sorte que quiconque rejoint la communauté virtuelle a accès au registre et peut procéder à une nouvelle opération. Elle peut être privatisée en restreignant l'accès au réseau à quelques membres identifiés[9]. Pour autant qu'ils soient connectés et respectent les règles prédéfinies par la communauté virtuelle, ses utilisateurs peuvent échanger sans obligation de dévoiler leur identité. L'anonymat dépend de la protection des données personnelles liées à l'*account* utilisé[10]. Par exemple, lorsqu'une personne physique ou morale obtient une adresse *bitcoin*, une pseudo-identité lui est attribuée. Chaque utilisateur peut créer un nombre illimité de comptes et lui seul détient le contrôle sur ses cryptoactifs (*private key/public key*)[11].

Si le concept de *blockchain* publique tend à assurer la transparence des opérations effectuées, la traçabilité des utilisa-

iStock

Selon une étude, 46% des transactions en bitcoins seraient illégales.

teurs de cryptonymes est relative: tout au plus est-il possible d'obtenir les adresses émettrices et réceptrices. Des études[12] ont démontré que, avec des moyens technologiques avancés, il était possible de démasquer les identités sous-jacentes en utilisant les données des fournisseurs de services des autres écosystèmes *bitcoin*, supprimant la confidentialité des transactions passées et futures associées à l'adresse de l'utilisateur démasqué. Ainsi, n'importe quel *hacker* pourrait effectuer ce type de «désanonymisation»[13]. Pour parer à ces risques, de nouvelles cryptomonnaies intraçables[14] sont apparues: Zerocoin (fin 2013), Monero (courant 2014), etc. Certes, elles renforcent la protection des données, mais elles constituent des obstacles à la poursuite pénale.

3. Problématiques d'application de la loi pénale et dilution des responsabilités

L'infraction consommée est commise au lieu de l'action délictueuse et, si l'énoncé de fait légal le prévoit, au lieu du résultat (art. 8 CP). Par exemple, le droit pénal suisse est applicable aux actes qui concrétisent la soustraction de monnaies virtuelles (art. 143 CP), la violation du domicile informatique (l'endroit où se trouve le serveur[15]) ou l'usage indu de moyens informatiques à des fins de minage (art. 143bis CP), la collecte ou le transfert de cryptoactifs au profit d'un organisme terroriste (art. 260^{quinquies} CP), la conversion d'argent de provenance criminelle en monnaies électroniques (art. 305bis CP), etc., s'ils sont localisés en Suisse (art. 3 CP).

Le fonctionnement de la *blockchain* et la portée universelle des transactions sur internet rendent complexe la détermination du droit applicable. Par exemple, en cas de détournement de cryptoactifs au moyen de *maliciels* ou d'usage criminel d'une puissance informatique à des fins de minage, l'infraction est susceptible d'être localisée partout dans le monde. Pour parer aux barrières procédurales et aux conflits positifs de compétences que créerait la reconnaissance d'une compétence universelle, les infractions sur internet sont notamment localisées au lieu où la transmission, le téléchargement ou le

[1] Les *wallets* sont créés via des logiciels disponibles sur le marché.
[2] Un utilisateur dispose d'un porte-monnaie sous forme d'une paire de clés cryptographiques asymétriques: la clé publique (*public key*) est assimilée au numéro de compte vers lequel les cryptomonnaies peuvent être transférées, alors que la clé privée (*private key*) permet de signer le paiement. Pascal de Preux, Daniel Trajilovic, Blockchain et lutte contre le blanchiment d'argent – le nouveau paradoxe?, Expert Focus 1-2, 2018, pp. 65 s.
[3] National Risk Assessment (NRA): Le risque de blanchiment d'argent et de financement du terrorisme par les *crypto-assets* et le *crowdfunding* – Rapport du groupe interdépartemental de coordination sur la lutte contre le blanchiment d'argent et le financement du terrorisme (GCBF) octobre 2018; Conseil fédéral (CF), Bases juridiques pour la *distributed ledger technology* et la *blockchain* en Suisse, Etat des lieux avec un accent sur le secteur financier, rapport du 14.12.2018.
[4] Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), Rapport semestriel 2017/II, ch. 5.4.3, rapport semestriel 2018/II, ch. 5.3.2.
[5] Sean Foley, Jonathan R. Karlsen et *alii, Sex, drugs and bitcoin: How much illegal activity is financed through cryptocurrencies?*, Review of Financial Studies, Forthcoming (>https://papers.ssrn.com/ sol3/ papers.cfm?abstract_id=3102645, consulté le 31.5.2019).
[6] Enée Bussac, Bitcoin, ether & Cie – Guide pratique pour comprendre, anticiper et investir 2019, Malakoff 2018, p. 32.
[7] Pascal Ronc, Benedikt Schuppli, Kryptowährungen im Lichte des Schweizerischen Geldwäscherei- gesetzgebung, Forumpoenale 6/2018, pp. 529-535.
[8] Bussac, p. 33.
[9] De Preux,Trajilovic, p. 65.
[10] Elfriede Sixt, Bitcoins und andere dezentrale Transaktionssysteme – Blockchains als Basis einer Kryptoökonomie, Wiesbaden 2017, p. 33; Bussac, p. 41.
[11] Sixt, p. 33.
[12] Fergal Reid, Martin Harrigan, An Analysis of Anonymity in the Bitcoin System, (>https://arxiv.org/pdf/1107.4524.pdf, consulté le 31.5.2019).
[13] Sixt, p. 33.
[14] CF, Bases juridiques, p. 27.
[15] TPF BG.2012.37 du 24.1.2013 c. 2.1.

stockage des données a été ordonné (lieu de la donnée d'ordre[16]). La localisation de tous les serveurs par lesquels les données ont été diffusées ou ont transité n'est donc pas déterminante. Pour certaines infractions, des éléments spécifiques de l'énoncé de fait légal, parfois non écrits, sont considérés pour établir la compétence de la Suisse: le lieu de l'atteinte aux intérêts pécuniaires[17], la localisation de l'acte qui concrétise l'enrichissement illégitime[18], etc. Partant que les cryptomonnaies suivent généralement leur détenteur, ces critères doivent être appliqués avec prudence, au risque de reconnaître une compétence universelle par un autre chemin.

Avant d'être enregistrée sur la *blockchain*, chaque transaction est validée par les mineurs (*miners*), qui s'assurent que le donneur d'ordre détient les avoirs ou les données qu'il prétend transmettre. Cette opération de minage assure le cryptage des transactions de la *blockchain* par la résolution de problèmes mathématiques complexes (au moyen de techniques cryptographiques): concrètement, les *miners* exécutent le code et vérifient les données entrantes sur le registre, afin de valider un nouveau bloc de transactions et les transactions chiffrées des blocs existants[19]. La sécurité de la *blockchain* est garantie par cette méthode de validation dite «consensus de preuve de travail» (*proof of work*), qui impose aux *miners* du réseau (qui sont autorisés à intervenir) des calculs coûteux en énergie et en temps. Ce procédé rend difficile le piratage (devenir la première puissance de calcul est extrêmement coûteux et suppose des connaissances accrues en cryptographie) et évite que les envois massifs de *spams* engendrent une surcharge du réseau. Vu la puissance informatique nécessaire au minage, il est courant que ces opérations soient accomplies par des équipes ou des sociétés de *mining*.

Malgré la complexité de la *blockchain*, des défaillances sécuritaires ou informatiques peuvent se produire, causant la perte définitive de cryptoactifs. En cas d'exécution parfaite des cocontractants, les fautes peuvent être difficiles à démontrer, puisque le fonctionnement du système par fragmentation du code tend à diluer la responsabilité pénale des négociants, des membres de la communauté virtuelle et des *miners*. D'ailleurs, on peut s'interroger si les actes de piratage et certaines défaillances informatiques imprévisibles ne devraient pas être considérés comme des actes fortuits pour lesquels nul ne saurait être tenu pour responsable.

Les plateformes d'échanges et les utilisateurs peuvent aussi être soumis à une réglementation ou à des obligations de *due diligence* nationales, disparates d'un pays à un autre, qui peuvent intéresser l'autorité pénale au moment d'établir la violation d'un devoir de prudence. L'analyse du droit applicable et des responsabilités est d'autant plus ardue que les cryptomonnaies sont encore peu réglementées.

4. Les infractions contre les monnaies ayant cours légal

Dans un arrêt récent, le Tribunal fédéral[20] s'est penché pour la première fois sur la qualification juridique des monnaies virtuelles, indiquant qu'elles devaient être considérées comme des monnaies privées parallèles et non des moyens de paiements légaux au sens de l'art. 2 LUMMP. La position des juges fédéraux s'explique par le fait que ces monnaies, qui n'ont pas cours légal, ne servent de moyens d'échange[21] que si le créancier les accepte. Il n'existe aucune obligation d'accepter les cryptomonnaies comme moyens de paiement et elles ne sont pas soumises à la surveillance de la BNS[22] ou à celle d'un exploitant du système.

Les art. 244 à 247 et 249 s CP et l'art. 11 LUMMP, qui protègent les monnaies ayant cours légal[23], ne sont pas applicables aux monnaies virtuelles, de sorte que la création de cryptomonnaies par *minage* est une activité légale[24]. De plus, l'émission de cryptomonnaies ne constitue pas une infraction au sens de l'art. 178bis CP, partant que ces moyens de paiement ne sont pas destinés à circuler dans le public.

Le faux dans les titres (art. 251 CP) n'est également pas applicable aux cryptomonnaies dont la valeur et l'usage ne sont pas garantis[25]. La contrefaçon de certains types de *token* (par exemple *les jetons à support d'actifs* qui endossent un ou plusieurs actifs hors de la *blockchain*) pourrait néanmoins tomber sous le coup de l'art. 155 CP (falsification de marchandise), considérant que, à l'instar des pièces de monnaie qui n'ont pas ou plus cours légal, ils sont des biens corporels mobiliers susceptibles d'être introduits dans le commerce et d'exprimer une valeur de marché fluctuante[26]. Tel n'est pas le cas de la monnaie à l'état virtuel[27].

5. Les infractions contre le patrimoine et à la propriété

Les monnaies virtuelles n'ont pas de statut juridique spécifique en droit suisse. Elles peuvent être abordées comme des «programmes informatiques dont les unités se créent au fur et à mesure et s'échangent contre des biens et des services ou s'achètent et se vendent sur des plateformes internet connues à cet effet, en

obéissant exclusivement à la loi de l'offre et de la demande, le tout sans aucune garantie de préservation de valeur ni d'échange et de récupération de la valeur investie»[28].

Une cryptomonnaie se caractérise par sa valeur patrimoniale, comme d'autres valeurs incorporelles telles que les créances, de sorte que les infractions d'abus de confiance (art. 138 CP), l'escroquerie (art. 146 CP) ou l'utilisation sans droit de valeurs patrimoniales (art. 141[bis] CP) peuvent être retenues. En revanche, le vol (139 CP), l'appropriation illégitime (art. 137 CP), le brigandage (art. 140 CP) ou la soustraction d'une chose mobilière (art. 141 CP) ne s'appliquent pas aux monnaies électroniques en tant que données (valeurs incorporelles) contenues dans un portefeuille numérique (*wallet*). Ces normes ne sont envisageables que pour les supports (*hardware wallet* prenant la forme de disques durs ou de clés USB, CD-ROM, *token*, etc.)[29] sur lesquels les logiciels de cryptomonnaies seraient enregistrés.

S'agissant du dommage considéré au moment d'établir la culpabilité de l'auteur (atteintes aux intérêts pécuniaires ou à la propriété), il faut tenir compte du caractère particulièrement fluctuant des cryptomonnaies qui fait que le gain espéré (préjudice envisagé) se distingue généralement du gain réalisé (préjudice causé). Notre propos vaut spécialement pour les «cyberattaques à retardement» (par exemple par infection du réseau au moyen de *maliciels*).

6. Le piratage informatique

Le *cryptojacking* consiste à utiliser la puissance des ordinateurs ou des *smartphones* de tiers, infectés par un *malware* (appelés *botnets*), pour accomplir une opération de minage. Des scripts sont installés à l'insu du détenteur pour effectuer une activité de minage cachée via des navigateurs[30]. Ces attaques sont aussi commises contre des processeurs particulièrement puissants. En février 2018, des scientifiques du Centre fédéral nucléaire russe de Sarov ont été arrêtés par le FSB au moment où ils s'apprêtaient à connecter à internet le système informatique du centre, qui est l'un des ordinateurs les plus puissants du monde, pour effectuer des opérations de minage de *bitcoin*[31].

Le piratage peut également concerner des *smart contracts* (*contrats intelligents*), des programmes autonomes qui exécutent automatiquement une opération prédéfinie et inscrite dans la *blockchain*. La collecte des données nécessaires à l'exécution du contrat est automatisée, de sorte qu'il est possible de vérifier que chaque partie a rempli ses obligations, avant d'enclencher les actions correspondantes[32]. Ces contrats, qui permettent à deux personnes d'interagir sans que la transaction repose sur le principe de la confiance mutuelle[33], peuvent gouverner tout événement vérifiable de manière informatisée: le paiement automatique d'un colis au moment de la livraison, le versement des gains au vainqueur d'un pari sportif dès le match terminé, ou encore l'indemnisation de passagers en cas de vol en retard en fonction de la base de données de l'aéroport[34], etc. De par leur nature, ces contrats sont tributaires du développement des technologies et de la fiabilité du codage des informations transmises[35].

Dans la blockchain, les cryptomonnaies sont des données enregistrées et transmises électroniquement[36]. En cas de piratage informatique ou de diffusion

[16] TF 8G.43/1999 du 11.8.1999, Medialex 1999 235; TPF SK.2007.4 c. 1.1.2 du 21.6.2007 et réf. cit. Christian Schwarzenegger, Der räumliche Geltungsbereich des Strafrechts im Internet, RPS 118 [2000], pp. 109 ss., p. 117.

[17] P.ex. art. 138 et 141bis CP. Cf. ATF 124 IV 241 c. 4d; TF 6P.46/2004, 6S.141.2004 c. 3.2; ATF 111 IV 19 c. 5, JdT 1985 IV 141; Marcel A. Niggli, Christof Riedo in: Basler Kommentar Strafrecht II, M.A. Niggli – H. Wiprächtiger, 4e éd., Bâle 2018, *ad* art. 138 N. 109 et réf. cit.; Marcel A. Niggli, Basler Kommentar II, *ad* art. 141bis N. 31.

[18] P.ex. art. 138, 139 et 143 CP. Michel Dubuis, Bernard Geller et *alii*, Petit Commentaire du Code pénal, 2e éd., Bâle 2017, *ad* art. 8, N. 13 et réf. cit.

[19] CF, Monnaies virtuelles, p. 8; NRA, pp. 7 et 13.

[20] TF 6B_99/2019 et 6B_148/2019 du 18.4.2019 c. 2.3.2. Vincent Mignon, Le «[B]itcoin», un nouveau défi pour le juriste suisse?, Jusletter du 4.5.2015, pp. 1-49, p. 43 décrit le bitcoin de «*monnaie conventionnelle*» qu'un créancier n'est pas obligé d'accepter.

[21] Jeremy Bacharach, Blockchain: Le Tribunal fédéral se penche sur les cryptomonnaies, (>https://www.cdbf.ch/1065/, consulté le 31.5.2019). Selon l'auteur, le paiement en cryptomonnaie est soumis aux règles du contrat d'échange (art. 237 ss. CO).

[22] Mignon, p. 19.

[23] Il s'agit de la «monnaie qu'a frappé ou fait frapper pour son propre compte un Etat qui l'a adoptée comme moyen de paiement, en imposant l'obligation de l'accepter pour la valeur qui lui est attribuée par la loi» (ATF 82 IV 198 c. 1, JdT 1957 IV 68; ATF 78 I 225 c. 3, JdT 1953 I 181).

[24] Jean-Daniel Schmid, Alexander Schmid, Bitcoin – eine Einführung in die Funktionsweise sowie eine Auslegeordnung und erste Analyse möglicher rechtlicher Fragestellungen, Jusletter du 4.6.2012, p. 9; Mignon, p. 43.

[25] Schmid, Schmid, p. 9 s; Stoll, p. 9. Les cryptomonnaies n'entrent pas dans la définition des titres de l'art. 110 al. 4 CP.

[26] ATF 101 IV 36 c. 3, JdT 1977 IV 11.

[27] Mignon, p. 44 s; Schmid, Schmid, p. 9.

[28] Daniel Stoll, Le bitcoin et les aspects pénaux des monnaies virtuelles, forumpoenale 2/2015, pp. 99-108, p. 99.

[29] Stoll, p. 98 s; Mignon, p. 44 donne l'exemple du papier sur lequel les clés numériques sont notées.

[30] MELANI, Rapport semestriel 2017/II, p. 40.

[31] NRA, p. 23.

[32] Bussac, p. 53.

[33] CF, Bases juridiques, p. 23.

[34] De Preux,Trajilovic, Blockchain, p. 66.

[35] Bussac, p. 52.

d'un logiciel malveillant, la soustraction de données (143 CP), la détérioration de données (art. 144bis CP) ou l'utilisation frauduleuse d'un ordinateur (art. 147 CP) est généralement réalisée[37]. D'autres infractions peuvent être envisagées si le *hacker* a préalablement brisé les sécurités pour détourner gratuitement une puissance informatique payante ou en cas de mise en circulation d'un programme de piratage (art. 143bis CP).

7. Le blanchiment d'argent

L'infraction de blanchiment d'argent (art. 305bis CP) peut être réalisée par n'importe quel acte propre à entraver l'établissement d'un lien entre le crime préalable et la valeur patrimoniale qui en provient, ou à faire échapper la mainmise sur ces valeurs par les autorités. Cet acte doit être propre à introduire la valeur patrimoniale dans l'économie légale[38].

La conversion de fonds criminels en cryptomonnaie peut en être un exemple, puisque cette opération rompt le *paper trail*[39]. Une fois une transaction effectuée et enregistrée, la traçabilité des avoirs devient compliquée, puisque le système permet aux membres d'interagir anonymement – contrairement aux opérations bancaires – et n'identifie pas la provenance criminelle des fonds ou les adresses IP utilisées[40]. La nature criminelle d'une acquisition de cryptomonnaies est d'autant plus ardue à démontrer, lorsque les utilisateurs recourent à des moyens autorisés par le système, tels que les attaques des 51%, traitées plus bas, ou les *smart contracts*[41].

Le blanchiment d'argent est principalement effectué par conversion de monnaies officielles en cryptomonnaies ou par *phishing*[42]. La première méthode consiste à convertir des fonds en cryptoactifs pour en dissimuler la provenance criminelle. Cette problématique est d'autant plus réelle que les marchés des biens s'ouvrent de plus en plus aux monnaies virtuelles comme moyens de paiement. En cas de revente ultérieure des biens acquis par ce biais, les chances d'établir un lien direct avec l'origine criminelle des fonds sont quasi nulles. La seconde méthode, celle de l'hameçonnage (ou *phishing*), est une technique frauduleuse utilisée pour obtenir les informations d'accès aux comptes bancaires des utilisateurs d'internet. En pratique, un acheteur et un vendeur s'accordent sur une transaction en monnaie virtuelle. Le paiement présumé de l'acheteur est crédité au compte du vendeur. Après la confirmation de la réception de l'argent, les cryptoactifs sont débloqués et transférés au vendeur. Lorsque la banque du vendeur est informée que le paiement a été déclenché par la méthode du *phishing* et utilisé pour le paiement sans que le titulaire du compte en ait eu connaissance, le paiement est bloqué. Avec l'accord du vendeur, l'argent est reversé à la victime. Toutefois, la transaction en monnaie virtuelle étant irréversible, les cryptoactifs ne peuvent pas être récupérés.

8. Le financement du terrorisme et le soutien aux organisations criminelles

L'attrait pour les cryptomonnaies est grandissant sur les plateformes de négoce du *darknet*[43]. Le *Monero*, qui garantit l'intraçabilité des transactions, semble avoir remplacé le *bitcoin*[44].

Il arrive que des transactions suspectes soient effectuées depuis des plateformes de services en *crypto-assets* qui ne sont pas enregistrées en Suisse. Dans de telles situations, les autorités de poursuite sont démunies et espèrent que le criminel présumé commette une erreur permettant de percer son anonymat ou que les échanges d'informations policières et judiciaires avec leurs homologues étrangers se révèlent productifs. Bien que la voie de l'entraide internationale constitue certainement l'un des instruments de lutte les plus efficaces de la répression de la criminalité en cryptomonnaies, elle est cependant souvent dépassée par la rapidité des transactions d'une juridiction à l'autre[45].

L'organisation de lutte contre le terrorisme, *Ghost Security Group*, a indiqué que des *wallets* de *bitcoins* avaient contribué au financement des attentats terroristes commis en France et en Indonésie et que l'Etat islamique détenait des *wallets* contenant l'équivalent de plusieurs millions de dollars. Des appels aux donations en cryptomonnaies auraient été émis par la même organisation terroriste. Dans ces conditions, le *crowdfunding* de *token* et les ICO pourraient représenter un instrument de levée de fonds discret et efficace pour financer des activités terroristes[46].

Le soutien aux organisations criminelles (art. 260ter CP), à savoir aux organismes d'au moins trois membres qui poursuivent le but de commettre des actes de violence criminels ou de se procurer des revenus par des moyens criminels et dont la structure et leur effectif restent secrets, est répréhensible. La réunion ou la mise à disposition de fonds dans le but de soutenir des actions violentes visant «à intimider une population ou à contraindre un Etat ou une or-

ganisation internationale à accomplir ou à s'abstenir d'accomplir un acte quelconque», tombent sous le coup de l'art. 260^{quinquies} CP. Le nouvel art. 260^{sexies} CP[47], qui devrait entrer en vigueur courant 2019, réprimera spécifiquement le soutien financier aux actions de recrutement, d'entraînement ou de voyage à des fins terroristes.

L'application de ces normes demeure limitée, les soupçons de soutien ou de financement du terrorisme étant généralement ardus à étayer lorsque l'argent a été transféré hors du pays. La tentative est presque vaine pour les transactions en monnaie virtuelle qui peuvent passer instantanément d'un portefeuille à un autre et dont la traçabilité est parfois inexistante. Ce constat ne porte pas à conséquence pour le moment, puisque la place financière suisse ne joue pas un rôle central dans le financement du terrorisme. On dénombre néanmoins une augmentation des transactions, en Suisse ou à partir de la Suisse, soupçonnées de financer des activités djihadistes[48]. Quoi qu'il en soit, le cadre légal renforce la répression des cyberattaques par des organisations criminelles, en sus des dispositions qui protègent les données.

9. La manipulation de cours de monnaies virtuelles et les ICO

La monnaie virtuelle n'étant pas une valeur mobilière au sens de la LBVM[49] ou de la LIMF, les vendeurs de cryptomonnaies (en tant que négociants en valeurs mobilières) et les exploitants de plateformes d'achat et de vente de ces monnaies (en tant que bourses) ne sont en principe pas soumis à ces lois. L'exploitation d'informations d'initiés (art. 154 LIMF) et la manipulation de cours (art. 155 LIMF) ne sont donc pas envisageables comme des bourses.

La règle a changé avec l'ICO (*initial coin offering*), un mécanisme de levée de fonds utilisant des *tokens* qui précède la mise en circulation d'une monnaie virtuelle. Sorte d'introduction en bourse version cryptomonnaie, ce protocole permet notamment aux *start-up* d'amasser des fonds sans encombrement administratif ou réglementaire[50]. Concrètement, des jetons sont émis par la société qui développe son projet. Des investisseurs virent les fonds au promoteur de l'ICO en échange de jetons dont la valeur initiale est spéculée en fonction du succès futur de la cryptomonnaie.

Avant l'apparition des ICO, les fonds étaient déjà collectés sur internet par l'intermédiaire de plateformes de *crowdfunding*. Le *crowdfunding* consiste en un financement d'un projet par une multitude de bailleurs de fonds. Dans le *crowdfunding* classique, il existe généralement une plateforme (intermédiaire) entre les bailleurs de fonds et les emprunteurs et les fonds sont transférés en monnaie-fiat, ce qui n'est pas le cas pour la plupart des ICO. Autrement dit, l'ICO est une forme de *crowdfunding* sans plateforme intermédiaire. En outre, le montant est souvent (mais pas systématiquement) perçu en cryptomonnaies[51].

Il n'existe pas de classification universellement reconnue des ICO et des jetons[52] émis. L'émission de *tokens* comme moyens de paiement (*payment tokens*) pour l'achat de produits ou de services, ou le transfert d'argent ou de valeurs patrimoniales est une opération soumise aux obligations de diligence de la LBA (art. 2 al. 3 let. b LBA *cum* art. 4 al. 1 let. b OBA)[53], ainsi qu'à l'obligation de

[36] Une donnée est une information relative à un état de fait, représentée sous forme de lettres, de nombres, de signes, de dessins, etc. qui est transmise, traitée ou conservée en vue d'une utilisation ultérieure (FF 1991 II 933, p. 951).
[37] Mignon, pp. 43 ss.; Stoll, pp. 99 ss.
[38] ATF 119 IV 59 c. 2, JdT 1995 IV 43.
[39] De Preux, Trajilovic, p. 67.
[40] NRA, p. 35
[41] NRA, pp. 26 s.
[42] CF, Monnaies virtuelles, p. 22.
[43] Sur le *darknet*, la technologie TOR recourt à des relais qui opèrent des changements indéfinis d'adresses IP, de sorte qu'il devient extrêmement difficile d'identifier l'adresse IP réelle de l'utilisateur. NRA, p. 29.
[44] CF, Monnaies virtuelles, p. 20; NRA, p. 29.
[45] NRA, p. 35.
[46] NRA, p. 28.
[47] FF 2018 6557.
[48] Service de renseignement de la Confédération (SRC), Rapport de situation, La Sécurité de la Suisse 2018, p. 47.
[49] CF, Monnaies virtuelles, p. 14.
[50] Bussac, p. 118 s.
[51] NRA, pp. 14 et 44.
[52] Finma, Guide pratique pour les questions d'assujettissement concernant les *Initial coin offerings (ICO)* du 16.2.2018. La Finma classifie les jetons selon leur fonction économique: *payment tokens* (jetons acceptés comme moyen de paiement), *utility tokens* (jetons donnant accès à un usage ou à un service numérique de la blockchain) et *asset tokens* (jetons d'investissement qui représentent des valeurs patrimoniales).
[53] NRA, p. 37.

s'affilier à un OAR (organisme d'autorégulation, telle que la Finma) ou de se soumettre à la surveillance de la Finma[54]. Les jetons de paiement ne sont pas considérés comme des valeurs mobilières par la Finma[55].

Les jetons d'investissement (*asset tokens*) sont des valeurs mobilières dans le sens de l'art. 2 let. b LIMF s'ils représentent un droit-valeur et que les jetons sont standardisés et susceptibles d'être diffusés en grand nombre sur le marché[56]. L'art. 2 al. 1 OIMF précise que ce sont des papiers-valeurs, des droits-valeurs, des dérivés et des titres intermédiés qui sont standardisés et susceptibles d'être diffusés en grand nombre sur le marché, c'est-à-dire structurés et fractionnés de la même façon et offerts au public ou vendus à plus de 20 participants, pour autant que ces valeurs ne soient pas créées spécialement pour certaines contreparties. Pour qu'un droit-valeur soit créé, il doit être inscrit au journal des droits-valeurs tenu par le débiteur (art. 973c al. 3 CO). Celui-ci peut être géré sous forme numérique sur une *blockchain*. Ainsi, le promoteur d'une ICO qui veut émettre des *asset tokens* doit obtenir une autorisation de négociant en valeur mobilière.

Les jetons d'utilité (*utility tokens*) ne sont pas considérés comme valeurs mobilières, lorsqu'ils confèrent uniquement un droit d'accès à un usage ou à un service numérique et que le jeton d'utilité est utilisable dans ce sens à la date d'émission[57].

Le promoteur d'une ICO peut choisir les investisseurs visés, géographiquement ou selon les différentes juridictions, pour ne pas tomber dans le viseur de la SEC (*Securities and Exchange Commission*[58]). Il est courant que de nombreuses ICO internationales ne soient pas adressées aux investisseurs américains ou que ceux-ci ne puissent pas acheter de jetons (par blocage de l'adresse IP de l'utilisateur). Cette pratique s'explique par le fait que la SEC qualifie la plupart des *tokens* comme des *securities* (jetons d'investissement), imposant l'enregistrement préalable de l'ICO au sens de la *Securities Law* pour qu'elle ne soit pas illégale[59].

Les ICO comportent certains risques de fraude ou de piratage. La valeur des jetons peut fluctuer drastiquement au point que trouver un acheteur peut devenir presque impossible. Partant que les marchés des cryptomonnaies se caractérisent par le haut degré de rendement et de volatilité de ces monnaies, des reproches de mauvaise gestion sont difficilement envisageables. Selon certaines études récentes, plus de la moitié des projets lancés par les *start-up* financées par ICO n'ont pas abouti, laissant les investisseurs avec des jetons d'utilité donnant accès à un service médiocre ou incomplet ou des jetons d'investissement de faible valeur[60].

10. Conclusion

La cryptomonnaie crée de nombreuses difficultés sur le plan pénal. Le fonctionnement du système de la *blockchain* est un sérieux frein à la poursuite pénale, favorisant l'impunité des criminels et exposant les lésés à des dommages irréversibles. La Suisse n'est pas épargnée par ce phénomène, même si la criminalité connue est encore limitée[61] en raison des moyens financiers, de la puissance informatique et des connaissances en cryptographie, en mathématiques et en codage informatique que requière ce type de cyberattaques.

On ne saurait toutefois éluder le fait que les technologies liées aux cryptomonnaies sont complexes et en constante évolution, laissant les autorités à un (si ce n'est à deux) temps de retard. A notre avis, les autorités judiciaires (et administratives) ne disposent pas d'instruments procéduraux permettant la mainmise de l'Etat sur ces monnaies au rendement aussi élevé que leur degré de volatilité[62]. En cas de saisie, de séquestre, de confiscation, etc., les risques liés aux fortes fluctuations sont significatifs[63], les marchés décentralisés des cryptomonnaies ne profitant pas de la stabilité du système financier étatisé. De plus, étant donné que seul le détenteur du portefeuille a accès à ses cryptoactifs, de telles mesures peuvent s'avérer inapplicables sans son concours.

Même si le Conseil fédéral considère que les monnaies virtuelles ne sont qu'un phénomène marginal et que les transactions n'évoluent pas dans un vide juridique[64], nous rejoignons l'avis de certains auteurs[65] qui estiment que les gouvernements, les autorités judiciaires et administratives ne disposent pas des armes légales pour faire face à ces technologies modernes. A l'instar de toute nouvelle technologie, la réglementation s'y rapportant est parfois lacunaire et les risques pour le consommateur laïc sont réels. Dans un avenir assurément proche, il sera possible de constater si des failles technologiques ou législatives ont déjà été mises à profit.

Récemment, les sept Sages ont reconnu la nécessité d'adapter le droit fédéral[66] existant aux développements de ces nouvelles technologies numériques, rejetant néanmoins l'idée d'une lex *blockchain*. L'insertion d'une norme pénale spécifique n'est également pas à l'ordre du jour, le projet en consultation n'arborant, au demeurant, aucune modification de la loi pénale.

[54] *Ibid*. Selon la pratique de la Finma, cette obligation est respectée quand les fonds sont reçus par un intermédiaire financier soumis à la LBA en Suisse et que celui-ci honore les obligations de diligence.
[55] Finma, p. 4.
[56] *Ibid*.
[57] *Ibid*.
[58] L'organisme fédéral américain de réglementation et de contrôle des marchés financiers.
[59] Luca Brunoni, Louise Bonadio, Initial coin offering (ICO) e criptovalute: investire e raccogliere fondi grazie alla blockchain, NF 2018, pp. 477-482, p. 481.
[60] Brunoni, Bonadio, p. 479.
[61] MELANI (n. 5), Rapport semestriel 2014/I, ch. 4.10.
[62] Giovanni Merlini, L'evoluzione regolamentare della lotta al riciclaggio. Necessità di nuovi interventi legislativi?, NF 2018, pp. 104-108, p. 107.
[63] P.ex. le bitcoin a perdu 75% de sa valeur entre octobre et décembre 2017.
[64] CF, Monnaies virtuelles, p. 28.
[65] Micaela Pizolli, Antiriciclaggio e sistema finanziario, NF 2018, pp. 95-102.
[66] Département fédéral des finances (DFF), Rapport explicatif relatif au projet de loi fédérale sur l'adaptation du droit fédéral aux développements de la technologie des registres électroniques distribués du 22.3.2019.