Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Octobre 2018

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)

Table des matières

Résumé analytique

Les autorités suisses n'ont répertorié jusqu'à ce jour aucun cas de financement du terrorisme par le recours aux crypto-assets ou au crowdfunding online et elles n'ont recensé que de rares cas de blanchiment d'argent par l'utilisation de ces nouvelles technologies. Un tel état de fait ne permet en conséquence pas d'évaluer précisément le risque réel qu'elles représentent du point de vue du blanchiment d'argent et du financement du terrorisme, mais le présent rapport établit que la menace qu'elles constituent, de même que les vulnérabilités de la Suisse à leur égard, sont considérables, même si elles caractérisent également toutes les juridictions et pas uniquement la Suisse.

La menace associée aux crypto-assets est constituée par l'anonymat qui entoure les transactions en tokens, avant tout relative à l'ayant droit économique des valeurs en jeu, et par le fait qu'une large partie des transactions s'effectuent de pair à pair, sans recours à un intermédiaire financier, de sorte qu'elles échappent à tout contrôle. Elle se traduit à la fois par l'exploitation criminelle de failles de conception des crypto-monnaies, par des escroqueries aux investisseurs, notamment dans le cadre d'ICOs, et par l'utilisation de crypto-monnaies pour les paiements de *ransomwares*. En outre, la menace représentée par les crypto-monnaies s'exprime aussi par leur utilisation à des fins illégales dans des schémas criminels qui existent par ailleurs: financement du terrorisme, blanchiment d'argent issus de la vente de produits et de services illégaux, d'escroquerie sur Internet de type *phishing*, de trafic de stupéfiants, notamment en mains d'organisations criminelles. En raison de leur anonymat, les crypto-monnaies se prêtent particulièrement bien au blanchiment d'argent.

Comme les autres pays, la Suisse est vulnérable à cette menace parce que l'identification des ayants droit économiques des avoirs en jeu est compliquée pour les intermédiaires financiers comme pour les autorités de poursuite pénale. Dans la majorité des cas, l'impossibilité d'établir cette identité est la conséquence de la technologie sous-jacente aux crypto-assets. Les seules transactions en crypto-assets qui permettent avec certitude l'identification de l'ayant droit économique des valeurs en jeu sont leur acquisition et leur vente contre des monnaies-fiat. Cela ne garantit cependant pas entièrement contre les fraudes les bureaux de change online qui les effectuent. Ils n'ont en effet aucun moyen de vérifier l'identité de l'ayant droit économique des portefeuilles électroniques qu'ils créditent sur ordre de leurs clients. Par ailleurs, l'origine criminelle d'avoirs impliqués dans une transaction en crypto-assets est extrêmement difficile à établir.

Cette nouvelle technologie pose aussi un grand défi pour les autorités de poursuite pénale. Outre les difficultés à identifier les ayants droit économiques de crypto-assets et l'origine criminelle d'une transaction qui y fait recours, elles sont confrontées à l'impossibilité technique de séquestrer les valeurs déposées sur un *wallet* électronique lorsqu'elles n'en détiennent pas la clef cryptographique privée. Par ailleurs, la nature généralement transfrontalière des transactions en crypto-assets réclame de recourir à des demandes d'entraide judiciaires internationales ou à la collaboration policière internationale pour réprimer la criminalité économique qui y fait recours, de sorte que les autorités de poursuite pénale sont souvent dépassées par la rapidité et la mobilité des transactions en crypto-assets, et que des problèmes de for juridique surviennent souvent.

Il convient toutefois de souligner que l'entraide policière et judiciaire internationale est à ce jour l'instrument le plus efficace pour lutter contre le blanchiment d'argent et le financement du terrorisme par les crypto-assets: c'est grâce à elle que les plus beaux succès en matière de répression de la criminalité économique par les crypto-monnaies ont été cueillis. Cela illustre la nécessité d'une réponse élaborée à l'échelle internationale pour contrer cette menace par nature transnationale.

À cet égard, l'engagement de la Suisse au sein du GAFI en faveur d'une plus grande harmonisation des réglementations nationales en matière de lutte contre le blanchiment d'argent et le financement du terrorisme par les crypto-assets constitue une réponse adéquate. Elle est complétée par les efforts développés en matière de formation des autorités de poursuite pénale en matière de cybercriminalité

économique et par la création, à l'été 2018, d'une plateforme nationale de coopération judiciaire et policière, le Cyberboard, spécialisée dans ce type de criminalité économique.

Par ailleurs, en Suisse, la LBA s'applique à un éventail particulièrement large de services actifs dans le commerce et les transactions en crypto-assets, même si de possibles précisions quant à son champ d'application sont actuellement envisagées[1].

Grâce à ces différentes mesures, le rapport conclut que la Suisse a su développer le meilleur dispositif réglementaire possible pour contrer la menace considérable que représentent les crypto-assets, même s'il ne comble pas les vulnérabilités également considérables à cette menace, que seule une réponse internationale pourrait diminuer significativement.

En ce qui concerne le crowdfunding, la principale menace associée à cette nouvelle technique de levée de fonds est une menace de financement du terrorisme, bien qu'aucun cas n'en ait été répertorié en Suisse. Cette menace est le résultat de l'anonymat de donateurs, mais aussi de la non-soumission de certaines catégories de plateforme de crowdfunding online à la LBA. Pour diminuer ce risque, le rapport recommande d'examiner l'opportunité d'introduire une mention de telles plateformes dans l'ordonnance du 11 novembre 2015 du Conseil fédéral sur la lutte contre le blanchiment d'argent et le financement du terrorisme dans le secteur financier (OBA; RS 955.01).

[1] Voir les recommandations dans le rapport du Conseil fédéral «Bases juridiques pour la *distributed ledger technology* et la *blockchain* en Suisse», 7 décembre 2018.

Liste des abréviations

CCDJP: Conférence des directrices et directeurs des départements cantonaux de justice et police

CCPCS: Conférence des commandants des polices cantonales de Suisse

CFMJ: Commission fédérale des maisons de jeu

CPS: Conférence des procureurs suisses

DLT : Distributed Ledger Technology

FINMA: Autorité fédérale de surveillance des marchés financiers

GAFI/FATF: Groupe d'action financière/Financial Action Task Force

GCBF: Groupe interdépartemental de coordination sur la lutte contre le blanchiment d'argent et le financement du terrorisme

ICO: Initial Coin Offering

LBA: loi fédérale du 10 octobre 1997 concernant le blanchiment d'argent et le financement du terrorisme

MELANI: Centrale d'enregistrement et d'analyse pour la sûreté de l'information

MPC: Ministère public de la Confédération

MROS: Money Laundering Reporting Office of Switzerland

NRA: National Risk Assessment

OFJ: Office fédéral de la Justice

PSC: Prévention suisse de la criminalité

RNS: Réseau national de sécurité

SFI: Secrétariat d'État aux questions financières internationales

SRC: Service de renseignement de la Confédération

UPIC: Unité de pilotage informatique de la Confédération

Index

Bitcoin: le bitcoin est la plus ancienne et la plus populaire des crypto-monnaies, créée en 2009 en réponse à la crise financière de l'année précédente.

Blockchain: la blockchain est une technologie informatique de stockage et de transmission de données sans organe de contrôle centralisé. Par extension, le terme désigne également la base de données qui contient l'historique de toutes les transmissions effectuées par le recours à cette technologie. La blockchain est particulièrement utilisée dans le domaine des crypto-assets. Elle constitue le support de nombreux d'entre eux, par exemple le bitcoin ou l'ether, dont elle permet la lisibilité de toutes les transactions. Pour être enregistrées sur la blockchain, plusieurs transactions sont regroupées chronologiquement en un bloc, qui est rattaché au bloc précédent après que les transactions ont été validées par les mineurs, qui vérifient que l'individu qui ordonne une transaction détient bien les avoirs ou les données qu'il prétend transmettre. Une telle opération de validation est effectuée grâce à la résolution de problèmes mathématiques. Une fois enregistrées sur la blockchain, les transactions ne peuvent être effacées que par une personne ou un ensemble de personnes qui détient plus de 51 % de la puissance de calcul nécessaire à la validation des transactions sur l'ensemble de la blockchain.

Crypto-asset: les crypto-assets sont une représentation digitale d'une valeur qui peut être échangée de manière numérique sur une blockchain et employée à des fins de paiement (fonction de paiement), d'utilisation (fonction d'utilisation) ou d'investissement (fonction d'investissement).

Cryptographie asymétrique: la cryptographie asymétrique est une technique de chiffrement qui établit une distinction entre les données de chiffrement publiques et les données de chiffrement privées, ces dernières étant en réalité des données de déchiffrement. Cette technique est utilisée dans le domaine des crypto-assets pour effectuer des transactions sécurisées entre deux *wallets*. Chaque *wallet* dispose de données de chiffrement publiques, la clef publique, et des données de chiffrement privées, la clef privée. Pour effectuer une transaction en faveur d'un *wallet*, la personne qui ordonne la transaction doit disposer de la clef publique, qui permet de diriger les crypto-assets vers ce *wallet* particulier et non vers un autre. La clef privée, que seul le détenteur du *wallet* détient, en est le véritable code d'accès, qui permet à son détenteur de disposer des avoirs qui y sont déposés. Il convient de relever cependant que certaines crypto-monnaies recourent à d'autres techniques de chiffrement pour sécuriser les transactions entre deux *wallets*.

Crypto-monnaie: synonyme pour «monnaie virtuelle». Voir *infra*.

Darknet: les darknets sont les réseaux Internet qui utilisent des protocoles d'accès permettant à leurs utilisateurs de rester anonymes, notamment en brouillant les adresses IP de connexion. Ils sont situés sur le *deep web*, soit la partie d'Internet à laquelle les navigateurs habituels ne donnent pas accès, et il en existe plusieurs, dont le plus célèbre est TOR (*The onion router*), pour lesquels des moteurs de recherches spécifiques existent. Réseaux anonymes, ils hébergent des sites légaux, utilisés notamment pour l'échange de données confidentielles, mais également de nombreux sites de ventes de produits et services illégaux, appelés *dark markets,* qui proposent notamment des stupéfiants, du matériel pédo-pornographique, des armes ou des cartes de crédit volées. Le contenu des darknets est dénommé *darkweb*.

DLT (Distributed Ledger Technology): la technologie du registre distribué ou DLT est une technologie qui permet à des acteurs individuels («nœuds») au sein d'un système de proposer, de valider et d'enregistrer en toute sécurité des opérations dans un ensemble synchronisé de données («*ledger*» ou «registre») réparties entre tous les nœuds du système.

Ether: lancée en 2015, l'ether ou ethereum est la crypto-monnaie la plus importante après le bitcoin.

ICO: les ICOs sont un moyen de lever des fonds. Dans le cadre d'une ICO, les investisseurs transfèrent des moyens financiers (habituellement sous forme de crypto-monnaies) à l'organisateur d'une ICO. En contrepartie, ils reçoivent des «coins» ou «tokens» basés sur la blockchain qui sont créés et enregistrés de manière décentralisée sur une nouvelle blockchain développée dans ce cadre ou à l'aide d'un *smart contract* sur une blockchain existante.

Mineurs / miners: les mineurs sont responsables de la validation d'une transaction. Les mineurs (également appelés «nœuds de validation») vérifient que l'individu qui ordonne une transaction détient bien les avoirs ou les données qu'il prétend transmettre. Une telle opération de validation est effectuée grâce à la résolution de problèmes mathématiques. Les transactions sont rassemblées en un bloc et envoyées au réseau pour vérification. Les nœuds n'acceptent un bloc que si les transactions qu'il contient sont valables. Les mineurs sont rémunérés en bitcoins nouvellement créés («opération de minage») et en frais de transaction.

Monnaie-fiat: une monnaie-fiat est une monnaie décrétée par un État, dont la Banque centrale en impose et en contrôle le cours légal.

Monnaie virtuelle: une monnaie virtuelle est la représentation électronique d'une valeur, échangeable sur Internet et qui peut être utilisée comme moyen de paiement pour des biens et services réels. Elle a sa propre dénomination mais, le plus souvent, elle n'est pas acceptée comme moyen de paiement légal. Une monnaie virtuelle n'est qu'un code numérique et n'a donc pas de contrepartie physique, par exemple sous forme de pièces ou de billets.

Clef publique / clef privée: les clefs publiques (ou adresses) correspondent aux identités des utilisateurs de crypto-monnaies. Un utilisateur de crypto-monnaies peut envoyer un message (ou initier une transaction) depuis son adresse s'il le signe avec sa clef privée. Ainsi, la clef privée est la clef de signature et la clef publique la clef de vérification. La clef privée doit être tenue secrète, tandis que la clef de vérification est généralement portée à la connaissance du public.

Smart contract: les *smart contracts*, ou «contrats intelligents» sont des protocoles informatiques qui exécutent automatiquement les termes d'un contrat, en fonction d'algorithmes qui fixent à quelles conditions quelle décision doit être prise. Développés à l'origine par la fondation Ethereum, dont la crypto-monnaie, l'ether, était la première à rendre possible le recours à de tels protocoles, ils permettent d'exécuter des contrats et de surveiller les transactions sur la blockchain qu'ils engendrent en supprimant les risques d'arbitraire inhérents à l'action humaine, selon le principe qu'on ne peut pas déroger au protocole du *smart contract*, entièrement rationnel et équitable envers tous, qui devient en conséquence la loi de ceux qui y ont recours.

Token: dans le contexte d'une blockchain, un token est une unité ayant une valeur intrinsèque ou représentant un autre actif ou une fonction d'utilisation. Les tokens de blockchain sont généralement fongibles et peuvent être échangés entre les participants du réseau.

Wallet: un *wallet* est un logiciel qui permet de gérer des tokens cryptographiques grâce à une interface.

Introduction

Le Conseil fédéral a pris connaissance du premier rapport national sur les risques de blanchiment d'argent et de financement du terrorisme en Suisse en juin 2015. Le rapport d'analyse nationale des risques, appelé National Risk Assessment (NRA), est la première évaluation intersectorielle générale des risques de blanchiment d'argent et de financement du terrorisme en Suisse. Il révèle que la Suisse n'est pas épargnée par la criminalité financière et que les gains issus de crimes commis le plus souvent à l'étranger peuvent aussi être blanchis dans ce pays. Par la publication de la NRA, le Conseil fédéral applique les recommandations révisées 1 et 2 du Groupe d'action financière (GAFI). Les recommandations de l'organisation interétatique imposent aux États d'introduire un dispositif visant à lutter efficacement contre le blanchiment d'argent et le financement du terrorisme. Le rapport NRA fait partie intégrante de ce dispositif, en ce sens qu'il vise à identifier les risques de blanchiment d'argent et de financement du terrorisme en Suisse, à prendre des mesures ciblées et à contrôler leur efficacité à intervalles réguliers (*identify and assess their money laundering and terrorism financing risk on an ongoing basis*)[2]. La publication du rapport NRA n'achève pas le processus d'analyse nationale des risques. La NRA est un processus continu. D'autres analyses de risques seront réalisées pour répondre aux recommandations du GAFI à long terme et pour adapter l'efficacité du dispositif suisse de lutte contre le blanchiment d'argent et le financement du terrorisme aux nouvelles menaces.

Le présent rapport sur le risque de blanchiment d'argent et de financement du terrorisme associé à deux des principales formes d'application des FinTech, les crypto-assets et le crowdfunding online, doit être considéré comme l'une de ces études complémentaires à caractère sectoriel. Il aborde dans un premier temps le risque associé aux crypto-assets, puis, dans un second temps et plus brièvement, celui associé au crowdfunding online.

On entend par «crypto-asset» toute forme d'avoirs virtuels stockés sur un support électronique, permettant à une communauté d'utilisateurs qui les acceptent comme moyens de paiement de réaliser des transactions libellées en de tels avoirs, sans recourir à une monnaie légale. Bien que la notion de «crypto-asset» englobe une réalité plus large que celle de «monnaie virtuelle» ou de «crypto-monnaie» (voir l'index *supra*), ces termes seront utilisés de façon interchangeable dans le présent rapport.

À la fin de 2017, l'envol spectaculaire du cours du bitcoin a attiré l'attention du public et des médias sur les crypto-assets. Élaboré comme une réponse à la crise financière mondiale de 2008, le bitcoin est le plus ancien de ces crypto-assets qui proposent de contourner le système bancaire traditionnel, en adoptant un mode de transaction anonyme et complètement décentralisé, non soumis donc à quelque autorité de régulation que ce soit, et dont le support est l'Internet. Très tôt, l'absence de contrôle et l'anonymat qui caractérisent les bitcoins ont conduit les autorités à se pencher sur les risques de fraude et de blanchiment d'argent, voire de financement du terrorisme, qui pouvaient leur être associés. Ainsi, en 2014 et 2015, le GAFI a attiré l'attention de ses membres sur ce risque et rédigé un premier guide de conseils pour l'élaboration d'une approche fondée sur le risque de blanchiment d'argent et de financement du terrorisme associé aux crypto-monnaies[3]. En Suisse, dès 2013, des interpellations et postulats parlementaires ont été déposés à ce sujet, portant le Conseil fédéral à publier en 2014 un rapport sur les monnaies virtuelles[4]. Il concluait à un risque encore peu important, qui ne réclamait pas de mesures particulières dans l'immédiat. Depuis lors cependant, les nouvelles utilisations

[2] GAFI, *National Money Laundering and Terrorist Financing Risk Assessment*, 2013, p. 6, http://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf.

[3] GAFI, *Virtual currencies. Key definitions and potential AML/CFT risks*, juin 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf; id, *Virtual currencies. Guidance for a risk-based approach*, 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf.

[4] Conseil fédéral, *Rapport du Conseil fédéral sur les monnaies virtuelles en réponse aux postulats Schwab (13.3687) et Weibel (13.4070), 25 juin 2014*, https://www.news.admin.ch/NSBSubscriber/message/attachments/35353.pdf.

économiques des crypto-assets, leur multiplication – leur nombre se porte actuellement à plus de 2000, l'évolution des technologies sur lesquelles ils se fondent et le récent engouement qu'ils ont suscité de la part du public en raison de l'envol du cours du bitcoin, ont conduit instances nationales et internationales à considérer la nécessité de réévaluer les risques de blanchiment d'argent et de financement du terrorisme qui leur sont associés. Le GAFI se propose d'élaborer à leur propos une stratégie plus approfondie[5], plusieurs juridictions, notamment l'Union européenne, modifient leur législation en fonction du risque qu'elles représentent[6], tandis que plusieurs autorités et organisations multiplient les rapports qui en traitent[7].

Une telle réévaluation est particulièrement importante pour la Suisse, qui se positionne comme un État «crypto-friendly». Le canton de Zoug attire en effet de nombreuses entreprises du secteur et est souvent désigné comme la «Crypto Valley» suisse. À sa suite, le canton de Genève tente de lui emboîter le pas en favorisant l'implantation de telles sociétés sur son territoire et le développement du secteur crypto de ses banques. Alors que le potentiel d'innovation des crypto-assets et leurs implications du point de vue du droit civil et du droit du marché financier font l'objet d'un rapport séparé du Conseil fédéral[8], le présent rapport a pour but de le compléter, en examinant les risques de blanchiment d'argent et de financement du terrorisme associés aux crypto-assets.

Contrairement à d'autres risques de blanchiment d'argent et de financement du terrorisme, celui associé aux crypto-monnaies est par nature nouveau. Les sources pour l'évaluer ne sont pas encore très nombreuses. En particulier, les communications de soupçons reçues par le Bureau de communication en matière de blanchiment d'argent (MROS) ne sont pas nombreuses et ne permettent pas d'en tirer des enseignements statistiques fiables. Aussi, bien que les communications de soupçons reçues par le MROS aient été mises à profit dans la mesure du possible, il a fallu puiser également à d'autres sources et adopter une approche plus qualitative que quantitative. La littérature spécialisée sur le sujet, les articles de presse et les rapports d'autres autorités étrangères constituent en conséquence le fondement de ce rapport, qui a été enrichi par la consultation de plusieurs autorités suisses de police et de justice et du secteur privé, que nous remercions pour leur disponibilité.

La première partie, consacrée à la définition des termes et concepts relatifs à la problématique des crypto-assets et de leur technologie, est volontairement courte. Le lecteur désireux d'en savoir plus pourra se référer au rapport du Conseil fédéral qui sera publié d'ici à la fin de 2018, qui traitera cet aspect de façon extensive[9]. Le second chapitre est dédié à la présentation des principaux services qui interviennent dans les transactions en tokens, ainsi que de leur qualification juridique. En particulier, il donne un exposé et une définition des Initial Coin Offering (ICOs), qui se sont multipliées en Suisse depuis un peu plus d'une année, s'érigeant ainsi en une problématique propre pour le législateur comme pour le secteur économique. Le rapport aborde ensuite, dans son troisième chapitre, l'analyse des risques proprement dite. Fondée sur l'expérience des autorités suisses en la matière, autant que sur les tendances constatées à l'étranger, elle sera divisée en un examen des menaces et une présentation des vulnérabilités, tout en soulignant que ni les unes ni les autres ne sont particulières à la Suisse, mais doivent être considérés comme globales. Une évaluation des risques est proposée à la fin du chapitre. Enfin, dans le quatrième chapitre, les facteurs qui permettent d'atténuer le risque de blanchiment

---

[5] GAFI, *FATF Fintech & RegTech Initiative*, http://www.fatf-gafi.org/fintech-regtech/?hf=10&b=0&s=desc(fatf_releasedate).

[6] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0178+0+DOC+PDF+V0//FR.

[7] EUROPOL, *2017 Virtual Currencies Money Laundering Typologies*, 2017; FANUSIE Yaya et ROBINSON, Tom, *Bitcoin laundering: an analysis of illicit flows into digital currency services*, Center on Sanctions & Illicit Finance et ELLIPTIC, 12 janvier 2018; European Parliament, *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*, mai 2018, http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf;

[8] Rapport du Conseil fédéral «Bases légales pour la *distributed ledger technology* et la *blockchain* en Suisse», 7 décembre 2018.

[9] *Ibid*.

d'argent et de financement du terrorisme par les crypto-monnaies seront énumérés. Le principal d'entre eux est la soumission extensive à la loi sur le blanchiment d'argent (LBA; RS 955.0) des sociétés de différents services relatifs au commerce de tokens, mais d'autres instruments à la fois normatifs et opérationnels sont également pris en compte.

Le rapport aborde enfin, dans son cinquième chapitre, la question du crowdfunding online et des risques de blanchiment d'argent et de financement du terrorisme qui lui sont associés. Liée, comme celle des crypto-assets, au développement des FinTech, cette problématique est également au centre de l'agenda politique national et international, parce que plusieurs cas de financement du terrorisme recourant à de telles techniques de levée de fonds ont été répertoriés à l'étranger[10]. Alors que le GAFI a déjà souligné ce risque en 2015[11], il paraît utile d'analyser si la Suisse est armée pour y faire face.

[10] Voir par exemple : TRACFIN, *Tendances et analyse de risques de blanchiment de capitaux et de financement du terrorisme en 2015*, 2015, p. 64 et seq., https://www.economie.gouv.fr/tracfin/tendances-et-analyse-des-risques-en-2015.

[11] GAFI, *Emerging Terrorist Financing Risks*, October 2015, p. 6 et 31 *et seq*., http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf.

1. Monnaies virtuelles

1.1. Définition

Une monnaie virtuelle est une représentation numérique d'une valeur, négociable sur Internet et qui peut être utilisée comme moyen de paiement pour des biens et des services réels. Elle a sa propre dénomination, mais elle n'est généralement pas acceptée comme moyen de paiement ayant cours légal. Une monnaie virtuelle n'existe que sous la forme d'un code numérique et n'a donc pas de pendant physique, par exemple sous la forme de pièces ou de billets[12]. Dans le présent rapport, l'expression «monnaies virtuelles» est utilisée comme synonyme de « crypto-monnaies ».

La présente analyse de risques porte sur le risque de blanchiment d'argent et de financement du terrorisme associé aux monnaies virtuelles décentralisées, et donc aux crypto-monnaies, terme qui est également utilisé ci-après.

1.2. Évolutions depuis 2014

Le Conseil fédéral a publié le rapport sur les monnaies virtuelles en réponse aux postulats Schwaab (13.3687) et Weibel (13.4070) en 2014[13]. À l'époque déjà, le bitcoin était la première monnaie virtuelle et sa valeur au 5 janvier 2014 était inférieure à 1000 dollars par bitcoin[14] pour une capitalisation boursière d'environ 10,5 milliards de dollars. Le 9 octobre 2018, un bitcoin valait 6644 dollars, pour une capitalisation de près de 115 milliards de dollars, soit une part de marché de 52 % pour 2047 crypto-monnaies[15]. Tant la valeur d'un bitcoin que la valeur globale des bitcoins actuellement en circulation ont considérablement augmenté. Beaucoup d'autres monnaies virtuelles, comme le ripple et le litecoin, ont, elles aussi, vu leur valeur énormément progresser par rapport à 2014. Les monnaies virtuelles sont donc devenues intéressantes, tant pour les investisseurs que pour les criminels.

1.3. Typologies des monnaies virtuelles

Les monnaies virtuelles peuvent être catégorisées selon deux caractéristiques: les monnaies virtuelles convertibles et non convertibles et les monnaies virtuelles centralisées et décentralisées.

1.3.1. Monnaies virtuelles convertibles et non convertibles

Les monnaies virtuelles convertibles peuvent être échangées contre des monnaies officielles. C'est notamment le cas du bitcoin et de l'ether, Les monnaies virtuelles non convertibles ne peuvent être utilisées pour le paiement de biens virtuels ou réels que dans un système fermé et elles ne peuvent pas être converties en monnaies officielles. C'est notamment le cas de l'amazon coin, qui ne peut être utilisé que sur le site Internet d'Amazon et possède la fonction d'un bon d'achat[16].

[12] Cf. aussi la définition dans le rapport du Conseil fédéral sur les monnaies virtuelles en réponse aux postulats Schwaab (13.3687) et Weibel (13.4070) du 25 juin 2014, 7-8.

[13] SANSONETTI Riccardo, « Le bitcoin : opportunités et risques d'une monnaie virtuelle », dans La Vie économique, 9-2014, p. 44-46.

[14] Cf. «https://www.coindesk.com/bitcoin-price-2014-year-review/» (dernière consultation le 14.05.2018).

[15] Cf. https://coinmarketcap.com (dernière consultation le 09.10.2018).

[16] SERAINA GRÜNEWALD, «Währungs- und geldwäschereirechtliche Fragen bei virtuellen Währungen», dans: Rolf H. Weber et. al (Hrsg.), *Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme*, ZIK Bd. 61, Zürich/Basel/Genf 2015, 95.

1.3.2. Monnaies virtuelles centralisées et décentralisées

Toutes les monnaies virtuelles non convertibles sont des monnaies centralisées. Les monnaies virtuelles convertibles peuvent être centralisées ou décentralisées. Les monnaies virtuelles centralisées sont gérées de manière centralisée par un administrateur qui émet la monnaie, règle son utilisation et contrôle le système. Il peut également retirer la monnaie de la circulation. On peut citer comme exemples de monnaies virtuelles centralisées: World of Warcraft gold ou «linden dollars» Second Life. Les monnaies décentralisées sont toujours des monnaies virtuelles convertibles sans administrateur central pouvant contrôler le système. Ces monnaies reposent sur la résolution de problèmes mathématiques par un réseau d'ordinateurs et elles sont aussi appelées «crypto-monnaies». On peut citer à titre exemples le bitcoin, le ripple et le litecoin[17].

1.3.3. Fonctionnement de la technologie

La mise en place du bitcoin au début de 2009 a fait souffler un vent nouveau: le bitcoin permet à des participants qui ne se font pas confiance, ne se connaissent pas et ne savent pas combien le système compte d'autres participants de tenir une comptabilité commune. Appelée «blockchain», la technologie sous-jacente fournit un nouveau modèle de gestion de données. Le terme «blockchain» fait aussi référence au fait que des transactions sont regroupées en blocs et validées ensemble. La validation, quant à elle, rattache le bloc des nouvelles transactions à une chaîne de blocs antérieurs et élabore ainsi par incrémentation un historique des transactions.

La diversité des systèmes créés dans la pratique dépasse le cadre de la blockchain et c'est la raison pour laquelle la notion plus vaste de technologie des registres distribués (*Distributed Ledger Technology*, DLT) a été introduite.

De par son caractère décentralisé, la technologie des registres distribués permet aux parties d'effectuer directement des transactions entre elles, (de pair à pair), sans intermédiaire tel que des banques ou prestataires de services de paiement. Les transactions sont enregistrées dans un registre tenu de manière décentralisée. Aux fins de l'organisation et de la conservation de la structure de données, les partenaires doivent donc s'accorder (1) sur les transactions valables et (2) sur un registre valable (consensus distribué).

La validité des transactions est généralement déterminée par les participants qui s'entendent sur les transactions jugées «véritables» et qui doivent donc être ajoutées au registre valable. Dans les modèles DLT actuels, les voix des participants décideurs peuvent s'exprimer de deux manières, étant précisé qu'une combinaison des systèmes est également possible[18]:

- *Preuve de travail (minage)*: certains systèmes se fondent sur le mécanisme de la preuve de travail («*proof of work*») pour trouver le consensus nécessaire à la création de blocs. Dans ces systèmes, des fonctions cryptographiques sont exécutées jusqu'à ce que le résultat présente certaines caractéristiques. On parle de preuve de travail valable quand la caractéristique recherchée est obtenue. Si la fonction cryptographique n'a pas été effectivement exécutée, tout contrôle de la validité de la preuve de travail est impossible. Lorsqu'une entrée valable est saisie, il n'est normalement pas nécessaire d'en vérifier la validité. Le participant est ainsi contraint de procéder à des tests répétés (travail) pour obtenir une entrée valable. Le bitcoin applique une fonction à sens unique (concrètement: une fonction de hachage SHA-256) jusqu'à ce que le résultat affiche un certain préfixe (concrètement: plusieurs zéros).

[17] GAFI, Report-Virtual Currencies, Key Definitions and Potential AML/CFT Risks, juin 2014, 5.

[18] LUZIUS MEISSER, Kryptowährungen: Geschichte, Funktionsweise, Potential, dans: Rolf H. Weber et. al (Hrsg.), Rechtliche Herausforderung durch webbasierte und mobile Zahlungssysteme, ZIK Bd. 61, Zürich/Basel/Genf 2015, 82 ss.

- *Preuve d'enjeu:* pour la validation de la transaction, un participant est choisi par le biais d'un algorithme. Les participants qui détiennent des avoirs élevés et/ou au bénéfice d'une durée de détention prolongée sont privilégiés. Dans ce système, les tokens ne sont généralement créés qu'au début et leur nombre n'augmente pas par la suite. La rémunération est donc obtenue par le biais des frais de transaction.

Puisque le registre, c'est-à-dire la structure des données, est décentralisé, une copie est enregistrée auprès d'un ou de plusieurs utilisateurs et est en permanence ajustée selon les règles du protocole[19]. Est donc considérée comme authentique la version qui est confirmée[20] comme telle par la majorité des dépositaires de la structure de données (appelés nœuds complets ou «*full (blockchain) nodes*»[21]).

2. Les crypto-monnaies en pratique

2.1 Les crypto-monnaies comme instrument financier

Depuis 2017, on observe une nette augmentation des Initial Coin Offerings (ICOs) effectuées ou proposées en Suisse. Il n'existe actuellement pas de définition légale ou théorique des ICOs, mais elles désignent généralement la création d'un token et son offre initiale au public[22]. L'ICO est généralement un moyen pour son promoteur de diffuser les tokens et de lever des capitaux à des fins professionnelles, exclusivement à l'aide de la technologie des registres distribués ou de celle de la blockchain. Lors d'une ICO, les investisseurs prennent part à un projet basé sur une blockchain du promoteur de l'ICO. Les investisseurs virent les fonds au promoteur de l'ICO et, en contrepartie, reçoivent des tokens de la blockchain. Ces tokens sont créés et enregistrés de manière décentralisée sur une nouvelle blockchain développée dans ce cadre ou à l'aide d'un «*smart contract*» sur une blockchain existante. Il s'agit en fin de compte d'une forme de crowdfunding sans plateforme intermédiaire (cf. ch. 2 ci-dessous). Les expressions «*token sale*» ou «*token generating event*» sont également employées comme synonymes. Les participants à une ICO investissent fréquemment dans des installations de projet ou des idées commerciales et ils espèrent que le projet sera un succès. En définitive, les ICOs sont très similaires aux cycles de financement traditionnels ou aux placements privés. Les moyens financiers reçus par l'intermédiaire des tokens émis peuvent alors revêtir un caractère de capitaux propres ou de capitaux étrangers. Habituellement, les détenteurs de tokens ne doivent cependant être ni actionnaires, ni créanciers de la société. Il est alors souvent possible d'éviter l'établissement de documentations coûteuses (notamment l'obligation de prospectus) lors de l'émission[23], et de contourner les règles de transparence concernant les personnes morales. Lorsque les tokens sont délivrés dans le but d'émettre des actions cryptographiques, se pose la question, relevant du droit des sociétés, de savoir comment cela peut justifier une qualité d'actionnaire.

Les ICOs sont habituellement conçues de façon à ce que les investisseurs puissent acquérir les nouveaux tokens devant être délivrés en transférant des ethers (ETH) ou des bitcoins (BTC) vers une adresse de blockchain (p. ex. un *smart contract*) appartenant au promoteur de l'ICO. Dans certains cas,

---

[19] LUZIUS MEISSER, précité, 83 ss

[20] MARTIN HESS/PATRICK SPIELMANN, Cryptocurrencies, Blockchain. Handelsplätze & Co. – Digitalisierte Werte unter Schweizer Recht, in: Reutter, Thomas U. / Werlen, Thomas (Hrsg.): Kapitalmarkt – Recht und Transaktionen XII. Zürich: Schulthess 2017, p. 154.

[21] Dépositaires du *protocole blockchain* (y compris du registre des transactions) Les *full blockchain nodes* (nœuds blockchain complets) vérifient en permanence le *protocole blockchain* et garantissent ainsi qu'aucune transaction erronée ne soit effectuée. En outre, les transactions interviennent par l'intermédiaire des *full blockchain nodes*.

[22] Les ICO se déroulent souvent en plusieurs phases. L'ICO publique adressée au grand public est généralement précédée de préventes («*pres-sales*») ou de ventes privées («*private sales*») auxquelles seul un groupe restreint d'utilisateurs peut participer.

[23] L'obligation d'établir un prospectus d'emprunt lors de l'émission d'emprunts obligataires selon l'art. 1156 du code des obligations fait exception.

les organisateurs d'ICOs acceptent également des paiements en monnaie-fiat. La participation à une ICO requiert régulièrement l'enregistrement préalable (parfois avec identification) du participant sur le site Internet du promoteur. Il n'existe toutefois guère de normes uniformes en matière d'accueil des clients.

Un placement privé des tokens à des conditions préférentielles, effectué sous la forme d'une prévente auprès d'investisseurs choisis, peut parfois précéder l'ICO. Dans le cadre d'ICOs, il peut arriver, en cas de préfinancement et d'achat préalable, qu'aucun token ne soit délivré, mais que des droits (conditionnels)[24] sur des tokens à créer soient accordés.

Le graphique ci-dessous[25] illustre la nette augmentation des projets d'ICOs dans le monde:

Il est difficile d'obtenir des données uniformes sur le nombre d'ICOs effectuées dans le monde, ainsi que sur le volume total collecté. Selon une étude de PWC Suisse, 450 ICOs se sont déroulées l'année dernière dans le monde entier. Elles ont rapporté un montant total de près de 4,6 milliards de francs, c'est-à-dire un volume plus de vingt fois supérieur à celui atteint en 2016. Rien qu'en Suisse, 70 ICOs ont permis de collecter 1 milliard de francs[26]. Ces chiffres mettent en évidence l'importance de la place financière suisse sur le marché des ICOs. La Suisse est un centre mondial pour les ICOs. Les ICOs réalisées en 2017 ont souvent été effectuées sur la base d'une fondation, mais on assiste, en 2018, à une multiplication des ICOs promues par des sociétés anonymes ou des sociétés à responsabilité limitée. Face à la forte hausse du nombre des ICOs menées en Suisse, la FINMA a publié un guide

[24] Par exemple, les «Terms of Token Sale» stipulent qu'il n'existe pas de droit aux tokens correspondants si le projet ne voit pas le jour.

[25] Le graphique provient du site internet https://www.coindesk.com/ico-tracker/ («All-time Cumulative ICO Funding»; consulté pour la dernière fois le 27 juillet 2018).

[26] Cf. https://www.srf.ch/news/wirtschaft/finanzierung-mit-digitalgeld-millionen-generieren-mit-bitcoin-und-co; avec renvoi à l'étude de PWC (consultée pour la dernière fois le 27 mars 2018). L'ICO TEZOS (achevée le 14 juillet 2017), par exemple, avait permis de collecter 228 590 404 dollars.

pratique[27] expliquant comment, sur la base du droit actuel régissant les marchés financiers, elle classe les ICOs selon le droit de la surveillance.

L'organisation concrète des ICOs diffère beaucoup, selon les cas, sur les plans technique, fonctionnel et économique, de sorte qu'une catégorisation générale n'est pas possible. Dans certaines ICOs, par exemple, des tokens sont créés pour jouer un rôle monétaire, de sorte qu'ils peuvent être qualifiés de moyen de paiement au sens de la loi sur le blanchiment d'argent (LBA). Dans ce contexte, le groupe de travail du Conseil fédéral «Blockchain/ICO»[28] doit se pencher plus attentivement sur les différentes organisations et sur les implications juridiques des divers modèles de tokens.

Les moyens de paiement sont des instruments qui permettent à des tiers de transférer des valeurs patrimoniales[29]. Le terme n'est pas défini de manière uniforme dans la législation suisse. L'émission de moyens de paiement constitue toutefois une activité soumise à la LBA. La loi cite les cartes de crédit et les chèques de voyage comme exemples de moyens de paiement (art. 2, al. 3, let. b, LBA). L'énumération d'exemples montre que la réglementation se fonde sur une acception large des moyens de paiement.

Un token délivré dans le cadre d'une ICO est considéré comme un moyen de paiement au sens de la loi sur le blanchiment d'argent s'il doit être utilisé, réellement ou selon l'intention de l'émetteur, comme un moyen de paiement pour l'achat de produits ou services. Contrairement aux pièces ou aux billets et aux dépôts à vue auprès de la BNS, les crypto-monnaies ne sont pas acceptées comme un moyen de paiement ayant cours légal et ne sont pas libellées en francs suisses (p. ex. BTC, ETH). Contrairement à la monnaie électronique, par exemple, les crypto-monnaies ne constituent pas nécessairement une créance vis-à-vis de l'émetteur. Elles n'existent que sous la forme d'un code numérique et n'ont pas de pendant matériel sous forme de pièces ou de billets. En outre, certains tokens ne deviennent une crypto-monnaie qu'avec le temps, une fois obtenue l'acceptation comme moyen de paiement. Mais il est aussi possible qu'une crypto-monnaie existe déjà au moment de la réalisation de l'ICO, si la création d'un moyen de paiement est envisagée.

Le déroulement des paiements suit habituellement le modèle (quelque peu simplifié) suivant:

(1) Le débiteur saisit par l'intermédiaire de son compte, directement ou via un compte sur une plateforme d'échanges (cf. let. d ci-dessous), l'adresse de réception du créancier et le nombre de tokens à envoyer.

(2) Les informations sont envoyées dans le réseau blockchain.

(3) Sur la base du mécanisme de consensus défini dans le protocole correspondant, le réseau blockchain confirme la validité de la transaction et le crédit à l'adresse du créancier.

Malgré d'importantes variations des cours, de plus en plus de commerçants (principalement dans la vente en ligne ou la prestation de services informatiques) acceptent les crypto-monnaies comme moyen de paiement[30].

---

[27] Cf. https://www.finma.ch/fr/news/2018/02/20180216-mm-ico-wegleitung/ (consulté pour la dernière fois le 29 mars 2018).

[28] Rapport du Conseil fédéral «Bases légales pour la *distributed ledger technology* et la *blockchain* en Suisse», 7 décembre 2018.

[29] Cf. FINMA-RS 2011/1 «Activité d'intermédiaire financier au sens de la LBA», point 55.

[30] Le bitcoin reste cependant le plus répandu. Des exemples en Suisse sont le contrôle des habitants de la ville de Zoug et l'office chargé de la tenue du registre du commerce de Zoug. Cf. aussi https://bitcoin-stores.ch/ (consulté pour la dernière fois le 29 mars 2018); ce site propose une liste des magasins suisses qui acceptent les bitcoins, ainsi qu'un annuaire des boutiques en ligne en bitcoin. Il ne liste que les commerces et boutiques en ligne suisses qui acceptent les bitcoins comme moyen de paiement.

Selon les indications de Coinmarketcap, il existe actuellement 2094 crypto-monnaies dans le monde[31]. Sur les quarante premières crypto-monnaies avec une capitalisation supérieure à 300 millions de dollars (version: 08.11.2018), les entreprises suivantes ont un lien avec la Suisse:

Rang	***Nom***	***Capitalisation (en milliards de dollars)***	***Lien avec la Suisse***
# 2	Ethereum (ETH)	21.7	Foundation Ethereum, Zoug
# 8	Cardano (ADA)	1.9	Cardano Stiftung, Zoug
# 18	Tezos (XTZ)	0.78	Tezos Stiftung, Zoug
# 29	Lisk (LSK)	0.3	Lisk Stiftung, Zoug
# 37	Icon (ICX)	0.2	Icon Stiftung, Zoug

2.2 Fournisseurs de wallets

Une paire de clefs cryptographiques est nécessaire pour effectuer des transactions à l'aide de la DLT. Elle se compose d'une clef publique (PUK) qui sert d'adresse (une sorte de numéro de compte) et d'une clef privée (PIK) qui donne un accès total à l'adresse (comparable au code PIN). L'élément déterminant pour effectuer une transaction est la clef privée, puisqu'elle est indispensable pour qu'une transaction soit valablement signée et donc déclenchée. La perte de la clef privée entraîne aussi la perte du pouvoir de disposer de la crypto-monnaie. Il est donc important de conserver la clef privée en lieu sûr, ce qui peut se faire au moyen d'un «*wallet*». Ce terme désigne généralement un logiciel permettant de gérer des tokens cryptographiques grâce à une interface.

Les *wallets* peuvent fonctionner différemment selon les développeurs d'applications correspondants. En principe, on distingue les applications de wallets *décentralisées* et les fournisseurs de *custody* wallets. Les premières sont habituellement des projets Open Source décentralisés qui ne peuvent pas forcément être rattachés à des entreprises spécifiques. Ces applications sont souvent fournies gratuitement sous forme de *freeware* (p. ex. Mycelium / Electrum; également appelés «*non-custodian wallets*», «*private wallets*» ou «*self-hosted wallets*»). Ces *wallets* permettent aux utilisateurs de gérer eux-mêmes leurs paires de clefs (à distinguer des *crypto custodians* ou des fournisseurs de *custody wallet*), c'est-à-dire que le développeur ne connaît généralement pas les paires de clefs générées par l'utilisateur de l'application ou ne peut pas y accéder. Par opposition, les fournisseurs de *custody wallets* entretiennent souvent une relation durable avec leurs clients et, à cette fin, gèrent aussi les paires de clefs correspondantes (c'est-à-dire aussi, en particulier, les clefs privées du client).

Une étude de l'université de Cambridge[32] réalisée en 2017 fournit l'estimation approximative suivante du marché des fournisseurs de *wallets*:

- On estime que le nombre de *wallets* est passé de 8,2 millions en 2013 à près de 35 millions en 2016.

[31] Cf. https://coinmarketcap.com/all/views/all/ (consulté pour la dernière fois le 12 novembre 2018).

[32] Les estimations reposent sur la Global Cryptocurrency Benchmarking Study 2017 de Garrick Hileman & Michel Rauchs, Cambridge Centre for Alternative Finance, université de Cambridge, Judge Business School (consulté pour la dernière fois le 28 mars 2018).

- L'année dernière, le nombre de *wallets* actifs était compris entre 5,8 et 11,5 millions selon les estimations.
- Environ 80 % des fournisseurs de *wallets* sont domiciliés en Amérique du Nord ou en Europe, alors que seuls 60 % des utilisateurs proviennent de ces régions.
- Environ 73 % des *wallets* ne contrôlent pas la clef privée («*private wallets*»), 15 % sont des *custodian wallets* et 12 % permettent à l'utilisateur de définir l'accès à la clef privée.
- Seuls 40 % des *wallets* soutiennent plusieurs crypto-monnaies.
- Les applications mobiles de *wallets* sont les plus répandues (65 %), suivies des *desktop-wallets* (42 %) et des *Internet-wallets* (38 %).
- La distinction entre *wallets* et plateformes de négociation est de plus en plus floue. Environ la moitié des *wallets* disposeraient d'une fonction de change (cf. ch. 4.1 ci-dessous).
- Environ 24 % des *fournisseurs de wallets* détiennent une licence de l'État. Tous ces *fournisseurs de wallets* permettent de convertir une crypto-monnaie en monnaie-fiat. Toutefois, seuls 75 % des fournisseurs permettant la conversion détiennent une licence de l'État.

Le 30 mai 2018 le Parlement européen et le Conseil européen ont adopté une modification de la 4e directive LBC[33]. Celle-ci prévoit notamment que, désormais, le champ d'application de la directive est élargi aux plateformes de conversion de monnaies virtuelles et aux fournisseurs de *custodian wallets*, afin que les utilisateurs des monnaies virtuelles puissent être identifiés plus facilement.

Le GAFI examine la question des monnaies virtuelles et de la DLT dans le cadre du «Risk, Trends and Methods Group» (RTMG) et formule des recommandations. Dans un Virtual Currencies Update (octobre 2017), le RTMG s'est intéressé au rôle des fournisseurs de *hosted wallets* qui permettent également à des utilisateurs sans bases techniques de transférer simplement des monnaies virtuelles, ainsi qu'aux ICOs. Ces sujets sont considérés comme les défis et thèmes de discussion de l'avenir.

2.3 Bureaux de change et plateformes de négociation centralisées/décentralisées

On établit en principe une distinction entre les bureaux de change en ligne et les plateformes de négociation (centralisées et décentralisées). Dans les opérations de change, les organismes de change proposent l'achat et la vente de crypto-monnaies directement à partir de leurs propres avoirs. Ils ne jouent pas le rôle d'intermédiaire ou de marché entre des acheteurs et des vendeurs de crypto-monnaies, mais plutôt celui de bureaux de change (rapport entre deux parties). Les opérations de change impliquant des crypto-monnaies sont des activités d'intermédiaire financier au sens de la LBA.

Les plateformes de négociation centralisées disposent d'un carnet de commandes, de «matching rules» et de différents types d'ordres, comme les centres de commerce traditionnels. Leur particularité est que les utilisateurs négocient directement sur la plateforme (*non-intermediated access*) au lieu de passer par un intermédiaire financier réglementé (tel qu'une banque ou un courtier en valeurs). L'utilisateur dépose ses tokens sur la plateforme ou utilise un *wallet* auquel a accès la plateforme. Les transactions interviennent par l'intermédiaire de la plateforme et les tokens restent généralement accessibles sur la plateforme (clefs privées) jusqu'à ce qu'ils soient transférés vers un autre *wallet*. Ces plateformes de négociation se distinguent des bureaux de change par le fait qu'elles jouent un rôle d'intermédiaire et qu'il existe donc une relation entre trois parties. Le négociant reçoit de l'argent ou des crypto-monnaies de la part de clients et les transmet à d'autres utilisateurs. Elles fonctionnent donc comme un marché de devises où se rencontrent l'offre et la demande de devises et sur lequel des devises sont échangées au cours négocié. Ces plateformes de négociation sont qualifiées de «*money transmitters*» et sont donc

[33] Cf., 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, Journal officiel de EU. L 156 du 19 juin 2018, p.43.

soumises à la LBA. Outre cette activité, de nombreuses plateformes de négociation proposent aussi l'achat et la vente de crypto-monnaies provenant de leurs propres avoirs et, de ce point de vue, fonctionnent comme un bureau de change traditionnel. À cet égard, le présent rapport se concentre sur les questions liées au domaine de la loi sur le blanchiment d'argent. Habituellement, les plateformes de négociation centralisées en Suisse doivent cependant obtenir des autorisations complémentaires de la FINMA[34]. Il n'existe actuellement pas de plateforme de négociation agréée pour les crypto-monnaies en Suisse.

Le secteur du change de crypto-monnaies est le marché le plus important et il regroupe la plus grande population d'entreprises exerçant dans ce domaine. Le 12 novembre 2018, selon les chiffres de Coinmarketcap, 2094 crypto-monnaies étaient négociées sur 15840 «marchés» dans le monde[35]. Le même site Internet propose un classement de 207 plateformes de négociation qui affichent le plus gros volume de transactions quotidiennes[36]. Les cinq premières plateformes de négociation actuelles (mesurées en volume de bitcoins échangés) sont Bifinex (Hong Kong), OKEx (Bélize/Hong Kong), Binance (Hong Kong), Huobi (Pékin) et Bitflyer (Japon). En Suisse, des plateformes correspondantes sont actuellement en phase de planification et de mise en œuvre. Sur le marché secondaire, en revanche, il existe déjà des courtiers (notamment Bitcoin Suisse[37] et Bity[38]) qui exercent l'activité de change. Selon le droit en vigueur, ceux-ci doivent être affiliés à un OAR ou agréés par la FINMA comme intermédiaire financier directement soumis à la FINMA (IFDS) à moins qu'ils ne soient déjà au bénéfice d'une autre autorisation que leur activité nécessite en vertu de la législation sur les marchés financiers.

Dans des lignes directrices de juin 2015[39], le GAFI a notamment souligné les risques associés à la conversion de crypto-monnaies en monnaie-fiat et attiré l'attention sur la nécessité de réglementer les échanges de capital-risque, en application de ses recommandations 14, 16 et 26.

2.4 Plateformes de négociation décentralisées

Comme les plateformes de négociation centralisées, les plateformes de négociation décentralisées tiennent un carnet de commandes classique, mais elles ne contrôlent pas les *wallets* de tokens des clients, car elles ne disposent pas des clefs privées. Les tokens sont détenus de façon décentralisée dans les *wallets* du client et ne sont pas conservés de manière centralisée par la plateforme, ce qui vise à minimiser le risque de hacking. Le paiement («*settlement*») intervient directement sur la blockchain par le biais d'un *smart contract*. Souvent, les plateformes décentralisées acceptent aussi directement leurs clients privés dans le cercle des participants.

Contrairement aux plateformes de négociation bilatérales ou aux bureaux de change, une plateforme entièrement décentralisée n'est jamais la contrepartie d'une transaction et, par opposition aux plateformes centralisées, les ordres regroupés (après autorisation / confirmation de la transaction) sont directement traités sur la blockchain par les utilisateurs de la plateforme. Puisque la plateforme

[34] Dans le négoce de tokens considérés comme des valeurs mobilières au sens de la loi sur l'infrastructure des marchés financiers, il s'agit en particulier de l'autorisation d'exercer en tant que système multilatéral de négociation ou négociant en valeurs (avec ou sans autorisation d'exploitation d'un système organisé de négociation). Une autorisation d'exercer en tant que banque est également envisageable, selon l'activité déclarée de la plateforme.

[35] Cf. https://coinmarketcap.com/ (consulté pour la dernière fois le 12 novembre 2018).

[36] Cf. https://coinmarketcap.com/exchanges/volume/24-hour/all/ (consulté pour la dernière fois le 28 mars 2018).

[37] Cf. https://www.bitcoinsuisse.ch/ (consulté pour la dernière fois le 13 mars 2018).

[38] Cf. https://bity.com/ (consulté pour la dernière fois le 13 mars 2018).

[39] GAFI, «Virtual Currencies – Guidance for a risk-based approach 6/2015».

d'échanges permet, en définitive, de transférer des valeurs patrimoniales, on peut se demander si la plateforme fournit un service d'intermédiaire financier au sens de la LBA[40].

2.5 Systèmes de paiement off chain

Compte tenu de la lenteur des transactions sur la blockchain, des efforts de redimensionnement sont entrepris depuis longtemps. Une solution à ce problème est promise par les fournisseurs de «systèmes de paiement off chain»[41]. Il s'agit d'un réseau dans lequel les utilisateurs peuvent effectuer des paiements en faveur d'autres utilisateurs du réseau en ligne (mais off chain). Le système de paiement est décentralisé et n'a pas accès aux valeurs patrimoniales des utilisateurs.

2.6 Crypto-fonds

Outre la possibilité d'investir directement dans des crypto-monnaies, des efforts ont également été entrepris pour répondre à la demande de solutions d'investissement indirectes. Différents acteurs envisagent de lancer un crypto-fonds. Ce terme désigne généralement des placements collectifs qui investissent leurs actifs principalement ou exclusivement dans des crypto-monnaies ou d'autres crypto-assets. Ces placements ne sont pas traités différemment des autres placements collectifs par la législation sur le blanchiment d'argent, autrement dit, ils sont considérés comme des intermédiaires financiers s'ils disposent d'une autorisation d'exercer en tant que direction de fonds, SICAV, SCmPC ou SICAF[42]. Il n'existe actuellement pas de crypto-fonds suisse agréé.

3. Analyse des risques

Parallèlement au spectaculaire développement des crypto-assets depuis l'invention du bitcoin en 2009, les risques de leur utilisation criminelle ont également crû. Alors qu'économistes et autorités de régulation attirent régulièrement l'attention sur les risques spéculatifs que constituent les investissements en crypto-monnaies, notamment dans les ICOs, pour les investisseurs[43], plusieurs instances nationales et internationales soulignent la menace de blanchiment d'argent et de financement du terrorisme que représentent les crypto-monnaies[44]. Dans son rapport de 2014 en réponse aux postulats Schwaab (13.3687) et Weibel (13.4070) déjà, le Conseil fédéral soulignait ce risque[45]. Alors que le nombre de crypto-monnaies a fortement augmenté dans les dernières années et que leur utilisation gagne en importance, l'expérience acquise entre temps par les autorités de surveillance de la criminalité économique permet désormais de mieux cerner les tendances qui caractérisent actuellement ce risque de blanchiment d'argent et de financement du terrorisme. Son évaluation se situe au croisement de la menace que représentent les crypto-monnaies pour l'intégrité du système financier et des vulnérabilités qui caractérisent ce dernier. À propos des menaces, il convient de distinguer celles intrinsèquement liées aux technologies des crypto-monnaies, de celles associées à

[40] Voir Rapport du Conseil fédéral «Bases légales pour la *distributed ledger technology* et la *blockchain* en Suisse», 7 décembre 2018, p. 140-152.

[41] Cf. p. ex. la solution de Liquidity Network (consulté pour la dernière fois le 12 juillet 2018).

[42] Art. 2, al. 2, let. b et let. b^{bis}, LBA.

[43] Voir par exemple les nombreux avertissements que publie la *Securities and Exchange Commission* américaine depuis 2014: https://www.sec.gov/news/statements.

[44] GAFI, *Virtual currencies. Key definitions and potential AML/CFT risks*, juin 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

[45] *Rapport du Conseil fédéral sur les monnaies virtuelles en réponse aux postulats Schwaab (13.3687) et Weibel (13.4070),* du 25 juin 2014, https://www.news.admin.ch/NSBSubscriber/message/attachments/35353.pdf.

l'utilisation qui peut en être faite dans des crimes économiques qui pourraient également recourir à des monnaies-fiat, mais qui représentent une menace supplémentaire en raison de l'application de crypto-monnaies. Exposées dans un second temps, les vulnérabilités de la Suisse à la menace de blanchiment d'argent et de financement du terrorisme associée aux crypto-assets sont également celles qui caractérisent la plupart des pays face à un risque nouveau et croissant.

3.1. Les menaces associées aux crypto-assets

3.1.1. La menace intrinsèquement liée à la technologie des crypto-assets

a. L'anonymat des transactions et les difficultés de l'identification des ayants droit économiques

La principale menace que représentent les crypto-assets est l'anonymat qui entoure les transactions qui y font recours.

Les échanges en crypto-assets ne réclament en effet que de disposer d'un portefeuille électronique ou *wallet*, qu'il est facile de créer gratuitement grâce à de nombreux logiciels disponibles sur Internet. A part lorsqu'il s'agit de *wallets* mis en gestion auprès d'une société spécialisée (*custodian wallets)*, le processus de création d'un *wallet* est le plus souvent anonyme. Pour effectuer une transaction, il suffit au détenteur d'un *wallet* d'ordonner, au moyen de sa clef cryptographique privée, un transfert vers une autre adresse du même type ou de donner son adresse publique à un autre utilisateur désireux de créditer le portefeuille, par exemple en paiement d'un achat ou d'un service. Pour les crypto-monnaies comme le bitcoin, fondées sur les technologies combinées de la cryptographie asymétrique et de la blockchain, les transactions sont validées – ou non - par les mineurs en fonction du solde réellement constaté sur le portefeuille d'où elles sortent et elles sont visibles par tous les utilisateurs de la crypto-monnaie en question. La traçabilité des transactions est ainsi totale, mais l'identité réelle de la personne associée au portefeuille reste inconnue des autres utilisateurs. En outre, si ce système permet d'identifier toutes les transactions émanant de ou dirigées vers une même adresse, la plupart des logiciels de portefeuilles électroniques génèrent automatiquement plusieurs adresses pour un même portefeuille et un même utilisateur peut disposer de plusieurs portefeuilles et en utiliser un différent pour chaque transaction, de sorte qu'il devient pratiquement impossible d'associer une personne physique aux transactions qu'elle ordonne.

Depuis sa conception pour le lancement du bitcoin, le perfectionnement de la technologie blockchain a par ailleurs permis à certaines crypto-monnaies d'atteindre un degré encore supérieur d'anonymat. C'est par exemple le cas de celles qui reposent sur la technologie cryptonote, comme les bytecoins ou leurs avatars, les moneros, basés sur un procédé cryptographique différent de celui des bitcoins ou des ethers, celui de la «signature par cercles» (*ring signature*). Cette technologie permet de regrouper les utilisateurs en ensembles, de sorte que lorsque l'un d'eux fait une transaction, il n'est pas possible de savoir lequel des membres de l'ensemble l'a ordonnée. L'algorithme cryptonote permet en outre de masquer totalement l'historique des transactions, contrairement à la blockchain du bitcoin, dans laquelle toute la chaîne de toutes les transactions peut être consultée par n'importe quel utilisateur qui le souhaite. Enfin, cryptonote permet de fractionner les sommes transmises lors d'une transaction en passant par des comptes tiers intermédiaires, de telle sorte que leur montant réel devient illisible et, partant, intraçable.

Un tel procédé de fractionnement des transactions peut par ailleurs être effectué par les services de «mélange» soit les mixers/tumblers, pour accentuer l'anonymat des transactions en crypto-monnaies qui, comme le bitcoin, recourent à la technologie blockchain. Ces services consistent à envoyer les crypto-monnaies sur une plateforme qui les distribue vers d'autres adresses grâce à des milliers de transactions de petites sommes, avant de les rediriger vers l'adresse du destinataire. Si, notamment

pour les bitcoins, les services de mixing sont proposés par des serveurs externes, certains crypto-assets développés récemment, par exemple Dash, les ont intégrés directement dans leur protocole, accentuant ainsi l'anonymat inhérent aux transactions en tokens. L'anonymat est cependant déjà très important dans les autres crypto-monnaies, qui, pour cette raison, revêtent toutes un attrait particulier pour les criminels.

Enfin, le développement récent de nouvelles technologies d'utilisation des crypto-monnaies permet également de renforcer leur anonymat. C'est le cas des cartes de débit prépayées en crypto-assets et des crypto-billets, lancés récemment par une société zougoise, également implantée à Singapour[46].

Du point de vue de l'anonymat, l'argent liquide présente un risque similaire aux crypto-monnaies[47]. Mais la menace que représentent ces dernières est accentuée par la rapidité et la mobilité des transactions qu'offre la technologie sur laquelle elles reposent. Contrairement à l'argent liquide, les crypto-monnaies permettent le déplacement de sommes énormes d'un compte électronique à l'autre en quelques secondes sans que l'on sache qui effectue de telles transactions. Les montants impliqués peuvent ainsi être mis presque immédiatement à disposition d'utilisateurs anonymes disséminés aux quatre coins du globe. En outre, le détenteur d'un *wallet* peut transmettre à sa guise la clef cryptographique privée qui y donne accès à un tiers dans le plus parfait anonymat. De nouveau, une telle pratique est similaire à la transmission d'argent liquide de la main à la main, mais la possibilité de le faire par Internet en tout anonymat accentue également la menace que représentent de ce point de vue les crypto-monnaies. C'est donc la combinaison de l'anonymat, de la rapidité et de la mobilité qui fonde la menace de blanchiment qui caractérise les crypto-monnaies.

b. Les failles de sécurité des technologies sous-jacentes aux crypto-monnaies

Les technologies sur lesquelles reposent les crypto-assets, en particulier la blockchain et ses dérivés et la cryptographie asymétrique, ont été conçues pour permettre, tout en garantissant l'anonymat, de sécuriser parfaitement les transactions. Grâce au contrôle exercé collectivement par les mineurs, celles-ci ne peuvent être effectuées que par des utilisateurs qui disposent réellement dans leur *wallet* des valeurs en crypto-monnaies qu'ils souhaitent débiter. En outre, grâce à la cryptographie asymétrique, seul le détenteur effectif du *wallet* peut disposer des avoirs qui y sont déposés pour effectuer des transactions. Enfin, une fois qu'elle est validée par les mineurs, une transaction est inscrite dans la blockchain et est supposée irréversible. On ne peut en effet l'effacer qu'en modifiant la blockchain en entier. Une telle opération n'est possible qu'en disposant de plus de 50 % des capacités de minage sur la blockchain, à savoir une puissance de calcul informatique évaluée, pour la blockchain bitcoin, à plus de cinquante fois supérieure à celle d'une entreprise comme Google.

Néanmoins, ces technologies ne sont pas infaillibles. En effet, réclamant des preuves de travail de plus en plus lourdes, l'opération de minage ne peut plus, comme au moment de la création des crypto-monnaies, être effectuée par un seul mineur depuis son ordinateur privé. Elle réclame la mise en commun des ressources et la création de consortium de minage, qui se partagent les revenus de leurs opérations. De telles mises en commun des ressources font planer la menace d'une concentration de plus de 50 % de la puissance de minage d'une blockchain entre les mains d'une seule entité ou consortium de minage, qui se trouverait ainsi en situation de modifier à sa guise toute la blockchain, d'y effacer des transactions effectuées ou de faire valider des transactions fictives par ses propres

[46] Emmanuel Garessus, «Une société suisse veut émettre des billets de bitcoins», in *Le Temps*, 8 mai 2018, https://www.letemps.ch/economie/une-societe-suisse-veut-emettre-billets-bitcoins; «Singapour: les premiers billets Bitcoins visent à favoriser l'adoption de l'actif », in *Crypto-France.com*, https://www.crypto-france.com/singapour-premiers-billets-bitcoin/.

[47] GCBF, *Rapport sur l'utilisation du numéraire et les risques inhérents d'utilisation abusive pour le blanchiment d'argent et le financement du terrorisme en Suisse*, octobre 2018.

mineurs[48]. De ce point de vue, le développement de processeurs toujours plus puissants représente une menace. Généralement conçus à des fins industrielles ou administratives, et non pour le minage de crypto-monnaies, ils sont de plus en plus souvent la cible de pirates informatiques qui tentent de détourner leur puissance de calcul vers le minage. Dans d'autres cas de figure, ce sont les utilisateurs légitimes de ces ordinateurs qui les détournent à des fins de minage. C'est ce qui est survenu en février 2018, lorsque 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, l'un des ordinateurs les plus puissants du monde, pour effectuer des opérations de minage de bitcoins[49]. Par ailleurs, les profits découlant du minage sont tels, qu'il n'est pas inenvisageable que des criminels désireux de blanchir les produits de leurs activités illégales les investissent massivement dans l'achat d'ordinateurs destinés à la constitution de fermes de minage. De tels exemples montrent que le risque de concentration de plus de 50 % de la puissance de minage d'une blockchain entre les mêmes mains n'est pas uniquement théorique. Si les principales crypto-monnaies semblent désormais trop développées pour en être la cible, d'autres plus récentes en ont été victimes. Cela a été le cas récemment à propos du Verge, du Monacoin ou du Bitcoin Gold, dont un mineur a réussi à prendre le contrôle de la blockchain. Les coûts importants qu'une telle opération réclamait pour réunir la puissance de calcul nécessaire ont été amortis par les transactions qu'il a effectuées en volant des Bitcoins Gold, en les échangeant contre d'autres crypto-monnaies puis en effaçant les transactions pour récupérer les Bitcoins Gold qu'il avait déjà échangés[50].

Au-delà de cette menace, les technologies de la blockchain et de la cryptographie asymétrique présentent, plus que leurs concepteurs ne l'imaginaient, une certaine vulnérabilité au piratage. D'habiles hackers peuvent en effet prendre le contrôle des clefs cryptographiques privées des *wallets* de tiers, pour y effectuer des transactions à leur guise. Plusieurs exemples de piratage de plateformes de négociation et de stockage de crypto-monnaies ont ainsi été répertoriés depuis 2011, lors desquels les vols se chiffrent souvent à des sommes équivalant à plusieurs dizaines de millions de dollars[51]. Rien qu'au premier trimestre de 2018, les sommes dérobées lors de piratage de plateformes de crypto-monnaies atteindraient l'équivalent de 670 millions de dollars[52]. Toutes les crypto-monnaies y sont vulnérables et si la plupart des cas répertoriés semblent correspondre à des vols de bitcoins, le record des sommes dérobées a été atteint en janvier 2018, lorsque des pirates informatiques ont soustrait à la plateforme Coincheck, basée au Japon, plus de 500 millions de XEM, la crypto-monnaie du réseau NEM, soit un équivalent d'environ 530 millions de dollars[53]. Mais un tel phénomène ne touche pas que des sociétés d'échanges et de stockage de monnaies virtuelles. Les *wallets* de simples particuliers, gérés sans le recours à un fournisseur de portefeuille électronique, peuvent également être piratés, générant des pertes importantes, comme dans ce cas connu par les autorités suisses en 2014, qui a coûté une perte de près de CHF 100 000 au lésé[54].

---

[48] DE PREUX Pascal et TRAJILOVIC Daniel, «Blockchain et lutte contre le blanchiment d'argent. Le nouveau paradoxe ?», in *Resolution LP*, https://resolution-lp.ch/wp-content/uploads/2018/02/064_L_14_De_Preux_Trajilovic.pdf.

[49] « Ils minaient des bitcoins dans un centre nucléaire », in *La Tribune de Genève*, 10 février 2018, https://www.tdg.ch/faits-divers/Ils-minaient-des-bitcoins-dans-un-centre-nucleaire/story/30448246.

[50] «Bitcoin Gold: une attaque double dépense fait perdre plusieurs millions de dollars à des plateformes d'échanges », publié sur le site Crypto-France. https://www.crypto-france.com/bitcoin-gold-attaque-double-depense-pertes-millions-dollars-plateformes-echange/.

[51] LOUBIRE Paul, «La très longue liste de vols de bitcoins par des hackers», in *Challenges*, 08.12.2017, https://www.challenges.fr/finance-et-marche/la-tres-longue-liste-de-vols-de-bitcoins-par-des-hackers_518541.

[52] «670 millions de dollars de crypto-monnaies ont été dérobés au cours du premier trimestre 2018», in *Crypto-France.com*, avril 2018, https://www.crypto-france.com/670-millions-dollars-crypto-monnaies-voles-premier-trimestre-2018/.

[53] «Cryptomonnaie: la plateforme japonaise Coincheck victime d'un vol record», 29 janvier 2018, http://www.rfi.fr/economie/20180129-coincheck-vol-cryptomonnaie-injonction-japon.

[54] *Rapport du Conseil fédéral sur les monnaies virtuelles en réponse aux postulats Schwab (13.3687) et Weibel (13.4070), 25 juin 2014, https://www.news.admin.ch/NSBSubscriber/message/attachments/35353.pdf, cit.,* p. 22.

Enfin, en permettant la technologie des *smart contracts*, certaines crypto-monnaies comme l'ether – mais pas le bitcoin- présentent également une certaine vulnérabilité au détournement de fonds et à son blanchiment successif. Dérivée d'un perfectionnement de la blockchain telle qu'elle a été conçue pour le bitcoin, la technologie des *smart contracts*, développée à l'origine par Ethereum, consiste en l'élaboration de protocoles qui exécutent automatiquement les termes d'un contrat, en fonction d'algorithmes informatiques qui fixent à quelles conditions quelle décision doit être prise. Cela permet d'exécuter des contrats et de surveiller les transactions sur la blockchain qu'ils engendrent en supprimant les risques d'arbitraire inhérents à l'action humaine, selon le principe qu'on ne peut pas déroger au protocole du *smart contract*, entièrement rationnel et équitable envers tous, qui devient en conséquence la loi de ceux qui y font recours. Mais l'exemple du projet DAO montre que de tels protocoles prétendument indéfectibles sont également vulnérables à certains défauts de conception. Conçu pour anticiper de façon utopique une économie parfaitement décentralisée et démocratique, le DAO, fondé en 2016 sur la blockchain ethereum et géré depuis la Suisse par la société DAI.LINK Sàrl, peut être défini comme une sorte de fond d'investissement décentralisé et automatisé. Il devait permettre à ses utilisateurs de voter sur des projets pour leur accorder ou non des financements, effectués ensuite automatiquement par *smart contract*. Mais une faille dans la programmation de ce *smart contract* a permis à l'un de ses utilisateurs d'en détourner les finalités sans pour autant le modifier, de sorte qu'il a pu, tout en respectant le protocole, subtiliser l'équivalant de USD 53 millions au moment des faits. Pour remédier à cette situation, il a fallu obtenir des utilisateurs qu'ils acceptent de modifier la blockchain et d'annuler toutes les transactions survenues depuis le détournement. Contrevenant aux principes mêmes de la blockchain, cette décision a cependant été avalisée par la majorité des utilisateurs. Mais l'opposition de la minorité a conduit à une scission et à un dédoublement de la blockchain ethereum. Ainsi, malgré les précautions de leurs concepteurs, les *smart contracts* peuvent être les instruments de détournement de crypto-monnaies qui, une fois détournée, peuvent être blanchies grâce à l'anonymat des transactions sur la blockchain. Le seul remède est, pour l'instant, la modification de la blockchain elle-même.

c. Les menaces liées à l'effet de nouveauté et au noviciat des utilisateurs

La troisième menace de blanchiment d'argent inhérente aux technologies sous-jacentes aux crypto-monnaies provient de l'engouement nouveau pour ce type de monnaies et du défaut de surveillance de ceux qui y recourent et qui sont souvent peu au fait des mesures de précaution minimales qu'il convient d'observer à leur égard. En effet, en raison de la nouveauté relative que représentent les crypto-monnaies et les différentes utilisations qui en sont faites, elles suscitent un attrait parfois irréfléchi, souvent vulnérable à l'escroquerie. Le facteur de risque le plus courant est la simple négligence dans le stockage des clefs cryptographiques privées donnant accès aux *wallets*. Lorsqu'elles ne sont pas placées dans des lieux assez sécurisés, les données d'accès des utilisateurs à leur portefeuille électronique peuvent facilement être subtilisées et utilisées par des tiers sans même que ces derniers ne recourent au piratage informatique. Mais au-delà de cette banale erreur de débutant, des schémas plus élaborés d'escroquerie sont intrinsèquement liés à la multiplication des crypto-monnaies et piègent les néophytes attirés par la nouveauté qu'elles proposent et les gains spectaculaires qu'elles permettent d'espérer en tirer.

Le nombre des crypto-monnaies croît en effet continuellement et se porte actuellement à environ deux mille, dont la moitié à peu près ont été abandonnées. Parmi celles-ci, certaines ne relèvent parfois que de l'escroquerie pure et simple. Il s'agit le plus souvent de crypto-monnaies qui, tout en fonctionnant sur la technologie de la blockchain, ne sont pas décentralisées pour autant. Dans ce genre de cas, les promoteurs – en réalité des escrocs – ne dévoilent pas le code base de la blockchain et préminent à l'avance tous ou la majorité des jetons, dont ils gèrent eux-mêmes les échanges. Lorsque ce genre de crypto-monnaies sont gérées par des institutions clairement identifiables et bien contrôlées, elles peuvent présenter des avantages réels en matière de lutte contre la criminalité financière, dans la mesure où les promoteurs peuvent plus facilement connaître l'identité de leurs clients et, éventuellement, en informer les autorités de surveillance financière ou de poursuite pénale. Mais dans

de nombreux cas, il s'agit d'escroqueries qui relèvent de système de Ponzi, dont précisément les crypto-monnaies réellement décentralisées permettent de se prémunir. Le MROS a reçu plusieurs communications de soupçons associées à des cas de crypto-monnaies qui semblent relever de ce type d'escroqueries. Dans tous ces cas, les clients achetaient des jetons de ces monnaies, appâtés pas les revenus fixes et élevés que promettaient leurs promoteurs. Ils étaient en outre instamment encouragés à parrainer de nouveaux clients parmi leurs amis. En réalité, tout porte à croire que, dans tous les cas de ce type recensés par le MROS, les intérêts versés aux anciens clients étaient financés par les investissements des nouveaux, même si à ce jour la pyramide de ces escroqueries ne s'est pas encore écroulée. Cela n'a pas empêché les autorités de plusieurs pays, par exemple l'Allemagne, l'Italie ou la Bulgarie, d'interdire le commerce de l'une d'elles. En Suisse également, la FINMA a prononcé, en septembre 2017, la mise en liquidation judiciaire des sociétés promotrices et gérantes d'une crypto-monnaie soupçonnée de relever d'un schéma criminel similaire : le E-Coin[55].

Une menace similaire d'escroquerie aux investisseurs pourrait également caractériser les ICOs. L'engouement récent pour ce type de levées de fonds, à la fois de la part d'investisseurs attirés par les profits considérables qui semblent caractériser les FinTech et de la part de start ups désireuses d'obtenir des financements pour des projets que les instituts traditionnels d'investissement refuseraient probablement de soutenir, laisse en effet la porte ouverte à de nombreuses possibilités d'escroquerie. Un cas de figure fréquent relève de fausses ICOs, où les prétendus concepteurs d'un projet lancent des appels aux investissements sans avoir en réalité l'intention de développer quelque projet que ce soit. Le MROS a récemment connu un cas de ce type.

Cas de fausse ICO

Un bureau de change online signale un cas au MROS après qu'un de ses clients l'a alerté à propos d'une arnaque dont il a été victime. Le client en question avait investi dans un projet d'ICOs lancé par une société enregistrée dans une autre juridiction européenne, qui prévoyait le développement d'un portefeuille électronique sous une forme physique, similaire à une carte de débit. Désirant investir dans ce projet qui semblait innovant, le client a transmis à l'intermédiaire financier une somme en bitcoins, destinée à être échangée en ethers avant d'être déplacée vers le portefeuille électronique du destinataire, hébergé par une plateforme de droit étranger. Il s'est cependant vite avéré que ce projet d'ICO était en réalité une escroquerie. Transmis aux autorités de poursuite pénale compétentes, celles-ci ont cependant refusé d'entrer en matière, estimant que le for juridique compétent ne pouvait se trouver en Suisse du seul fait de la domiciliation de l'intermédiaire financier.

Une deuxième menace liée aux ICOs provient de l'abandon d'un projet au-dessus des capacités de ses promoteurs, qui pourraient préférer se déclarer en faillite et éventuellement reconstituer de nouvelles sociétés et recourir de nouveau à des ICOs pour les financer, plutôt que de persévérer dans la réalisation du projet pour lequel ils ont lancé l'ICO initiale.

Un autre schéma criminel potentiel lié aux ICOs est la manipulation du cours des tokens émis par les promoteurs de l'ICO. Des soupçons de ce type planent sur la société zougoise envion SA. Selon plusieurs sources publiquement disponibles, le directeur de cette ICO, qui a récolté plus de USD 100 millions pour développer des fermes de minage mobiles, capables de réduire l'emprunte écologie du minage, aurait émis frauduleusement des tokens et les aurait revendus sur des places d'échanges de crypto-monnaies, dans l'idée de prendre le contrôle de la société. À la suite de ces soupçons, le cours du token émis s'est effondré, de sorte que les investisseurs risquent de perdre presque la totalité de leur placement. La FINMA a ouvert une enquête à l'encontre de la société promotrice de cette ICO

[55] Communiqué de presse de la FINMA du 19 septembre 2017, https://www.finma.ch/fr/news/2017/09/20170919-mm-coin-anbieter/.

pour une possible violation du droit bancaire découlant d'éventuelles acceptations, sans autorisation, de dépôts du public[56].

Comme dans de nombreux cas d'ICOs, les jetons reçus par les investisseurs en contrepartie de leurs investissements ne sont pas considérés comme des parts sociétaires mais comme des droits d'utilisation prioritaire, les investissements pourraient être perdus sans recours en cas d'escroquerie, sauf pour les promoteurs de l'ICO. En raison des sommes astronomiques qui caractérisent souvent les ICOs connues récemment, des escroqueries de ce type représentent une menace importante. Selon certaines études, environ deux tiers des ICOs lancées se sont soldées par des échecs ou se sont révélées être des escroqueries, alors qu'au niveau mondial, rien que dans les cinq premiers mois de 2018, il semble que plus de USD 12 milliards aient été récoltés par le biais d'ICOs[57].

d. Les maliciels et *ransomwares*

L'anonymat des tokens et leur support électronique en font un instrument privilégié des pirates informatiques, notamment dans les cas de *ransomwares*. Tant en Suisse qu'à l'étranger, de tels cas de figure ne sont pas rares : des pirates informatiques attaquent des ordinateurs tiers, généralement d'entreprises, en chiffrent les fichiers grâce à des logiciels malveillants et exigent le versement de rançons en crypto-monnaies pour les débloquer. Une fois versées, ces rançons sont transférées sur des *wallets* enregistrés dans d'autres juridictions à partir desquelles ils peuvent être transmis plus loin ou échangés, rendant le plus souvent vaine la poursuite pénale de tels actes d'extorsion. Un exemple célèbre de ces *ransomwares* est celui de *WannaCry* qui, en mai 2017, a réussi à chiffrer les données de plus de 300 000 ordinateurs dans plus de 150 pays. Une rançon était exigée en bitcoins pour les débloquer. Quelques entreprises touchées ont versé la rançon. Les sommes ainsi recueillies semblent ensuite avoir été changées par petites tranches en moneros, grâce aux services de plateformes de négociation, notamment d'une plateforme de négociation de tokens de Zoug. Comme celle-ci n'est pas une plateforme de négociation centralisée, disposant d'un accès aux *wallets* de ses utilisateurs, ni d'une plateforme décentralisée de négociation avec pouvoir de disposer des valeurs des utilisateurs, elle n'est pas soumise à la LBA et n'avait donc pas procédé aux vérifications qui auraient pu permettre d'identifier l'origine criminelle des fonds ainsi échangés. Dès les premier indices cependant, cette plateforme a collaboré avec les autorités de poursuite pénale dans l'objectif de bloquer le processus de blanchiment[58].

e. Le blanchiment de crypto-assets d'origine illicite

En raison de leurs caractéristiques intrinsèques et en particulier de l'anonymat qu'elles procurent, les technologies sous-jacentes aux crypto-assets offrent de nombreuses possibilités de blanchir les tokens acquis illégalement. Il convient cependant de relever que, dans certains cas, l'assimilation de

---

[56] FARINE Mathilde, «La FINMA enquête sur une ICO à 100 millions de francs», in *Le Temps*, 26 juillet 2018, https://www.letemps.ch/economie/finma-enquete-une-ico-100-millions-francs; FINMA, Communiqué de presse du 26 juillet 2018, https://www.finma.ch/fr/news/2018/07/20180726-mm-envion/?pk_campaign=News-Service&pk_kwd=La%20FINMA%20ouvre%20une%20proc%C3%A9dure%20%C3%A0%20l%27encontre%20d%27un%20%C3%A9metteur%20d%27ICO.

[57] FARINE Mathilde, «Comment investir dans les cryptomonnaies», in *Le Temps*, 22 juillet 2018, https://www.letemps.ch/economie/investir-cryptomonnaies; FAUCETTE James, GRASECK Betsy et SHAH Sheena, *Update: Bitcoin, Cryptocurrencies and Blockchain*, Morgan Stanley, 1er juin 2018, p. 35, https://www.macrobusiness.com.au/wp-content/uploads/2018/06/82012860.pdf

[58] SUBERG William, «Bitcoin exchange ShapeShift helps police as WannaCry attacker converts to monero», in https://cointelegraph.com/news/bitcoin-exchange-shapeshift-helps-police-as-wannacry-attacker-converts-to-monero; EUROPOL, *2017 Virtual Currencies Money Laundering Typologies*, 2017, p. 11.

l'acquisition illégitime de crypto-assets à un crime et, partant, à une infraction préalable au blanchiment d'argent, n'est pas clairement établie. En effet, en l'absence de jurisprudence sur la question, il n'est pas évident que les attaques des 51 % ou le détournement de *smart contracts* relèvent en eux-mêmes du droit pénal, dans la mesure où, dans l'un comme dans l'autre cas, les individus qui y procèdent ne font qu'exploiter les possibilités offertes par les technologies blockchain et *smart contrat* telles qu'elles sont mises à disposition de tous leurs utilisateurs. En revanche, le vol ou l'extorsion de tokens ou leur acquisition par des fraudes aux investisseurs constituent sans ambigüité des crimes économiques et des infractions préalables au blanchiment d'argent.

Les opérations de blanchiment dépendent de l'habileté informatique des criminels. Le système de validation des transactions de pair à pair constitue en effet une certaine garantie d'autocontrôle. Les *wallets* qui accueillent les sommes détournées peuvent ainsi être blacklistés et les transactions qui en proviennent refusées par la communauté des utilisateurs, de sorte que souvent, les avoirs volés ne peuvent pas être utilisés. Mais pour qu'un *wallet* soit blacklisté, il faut que les membres de la communauté des utilisateurs identifient l'origine criminelle des fonds qui le créditent, ce qui, selon des informations policières, est rarement le cas.

Pour blanchir des crypto-assets illégalement acquis, les criminels recourent souvent aux darknets et à la possibilité que ceux-ci offrent d'y vendre, parfois à des prix sous-évalués, les tokens d'origine criminelle sur les plateformes de négociation décentralisées qui y sont hébergées. Cette modalité de blanchiment semble avoir été mise à profit à propos des XEM volés à la plateforme Coincheck, dont plus de 40 % auraient pu être écoulés rapidement par des échanges contre des bitcoins sur de tels marchés[59]. Le recours à des services de mixing constitue également un obstacle particulièrement important à l'identification de l'origine criminelle de bitcoins, de sorte que les criminels désireux de cacher l'origine illégale de leurs crypto-monnaies y font souvent recours. Mais la conversion en d'autres crypto-monnaies, le retrait à des bornes automatiques ou le jeu à des casinos online constituent également des façons de blanchir des crypto-assets mal acquis[60]. Une autre technique de blanchiment consiste à ouvrir, auprès de fournisseurs reconnus de portefeuilles électroniques, des *wallets* au nom de money mules munis de faux documents, d'où les avoirs sont par la suite transférés vers des comptes bancaires également ouverts au nom de money mules, mais sur lesquels les criminels, grâce à de faux documents, ont également le contrôle[61].

3.1.2. Les menaces d'utilisation frauduleuse des crypto-monnaies

Parallèlement à ces menaces inhérentes aux technologies des crypto-monnaies, celles-ci présentent également une menace importante du point de vue d'autres activités économiques criminelles qui ne recourent pas spécifiquement aux crypto-monnaies, mais pour lesquelles ces dernières revêtent un intérêt particulier en raison de leur anonymat, de la rapidité des transactions qu'elles permettent et de l'absence d'intermédiaire financier dans leur réalisation.

a. Le financement du terrorisme par les crypto-monnaies

Peu de cas de financement du terrorisme par le recours à des crypto-monnaies semblent avoir été répertoriés pour l'instant à l'échelle mondiale. Les organisations terroristes et leurs partisans semblent

[59] «Coincheck: les pirates servaient déjà parvenus à blanchir 40 % des 500 millions de XEMs dérobés», https://www.crypto-france.com/coincheck-pirates-blanchiment-xems/.

[60] FANUSIE Yaya et ROBINSON, Tom, *Bitcoin laundering: an analysis of illicit flows into digital currency services*, Center on Sanctions & Illicit Finance et ELLIPTIC, 12 janvier 2018.

[61] EUROPOL, *2017 Virtual Currencies Money Laundering Typologies*, 2017, p. 8.

privilégier d'autres types de financement et de moyens de paiement[62]. Cela a conduit le Royaume-Uni à considérer comme faible le risque réel que représentent les monnaies digitales du point de vue du financement du terrorisme[63]. Néanmoins, l'intensité de la menace est illustrée par les nombreuses discussions sur l'utilisation de crypto-monnaies que des partisans internationaux de l'État islamique mènent sur les réseaux sociaux, où de réels cours de formation à l'utilisation des crypto-assets sont distribués par les plus experts d'entre eux[64]. Dans ce contexte, les appels aux donations en crypto-monnaies pour financer l'État islamique n'ont pas manqués, ce qui attire l'attention sur la menace particulière que représente le crowdfunding de token du point de vue du financement du terrorisme[65]. Cette technique semble avoir été utilisée par une organisation terroriste salafiste palestinienne pour se financer[66]. Et bien qu'aucune preuve n'ait pu en être apportée à ce jour, plusieurs journalistes, ainsi que l'organisation de contre-terrorisme Ghost Security Group, prétendent que des *wallets* de bitcoins ont contribué au financement des récents attentats terroristes en France et en Indonésie et que l'État islamique en détenait plusieurs, crédités de l'équivalent de plusieurs millions de dollars[67]. À cet égard, la facilité et l'anonymat qui entoure les transactions en crypto-monnaies permettant de déplacer rapidement des avoirs d'un point à l'autre du globe constituent une menace importante de financement du terrorisme, même si pour l'instant, ce risque est plus théorique qu'avéré. Une menace similaire, bien que pour l'instant non avérée, pourrait résulter des ICOs, dont les profits pourraient être appliqués au financement du terrorisme. En revanche, le recours aux crypto-monnaies et notamment à la levée de fonds en crypto-monnaies par les organisations d'extrême droite, souvent défiantes vis-à-vis des institutions financières traditionnelles qu'elles considèrent comme contrôlées par des Juifs, est plus fréquent, notamment aux États-Unis. Il leur permet de remplacer les systèmes traditionnels de payement dont ils sont souvent exclus en raison de leurs activités. Il n'y a cependant pas de cas avérés où de telles organisations aient utilisé des crypto-assets pour des activités de financement du terrorisme[68].

En Suisse, aucun cas de financement du terrorisme par le recours à des crypto-monnaies n'a pour l'instant été repéré. Néanmoins, le MROS a reçu d'un de ses homologues étrangers des informations faisant état de soupçons de ce type. Des transactions bancaires en monnaies-fiat en provenance de différents pays européens dont la Suisse créditaient un compte du pays dont la CRF a alerté le MROS. Une fois créditées sur ce compte, les sommes transférées étaient converties en bitcoins et semblaient contribuer au financement d'activités terroristes. Faute de base légale l'autorisant à adresser des demandes d'informations aux intermédiaires financiers sur la base d'une demande en provenance d'un homologue étranger, le MROS n'a pas été en mesure de procéder à de plus amples vérifications sur ce cas. Mais le simple signalement de tels soupçons témoigne de la grande menace que représentent les crypto-assets du point de vue du financement du terrorisme. S'ils permettent potentiellement de transférer rapidement et anonymement de grosses sommes d'argent destinées à financer des organisations terroristes, ils peuvent également être utilisés par de simples partisans de telles organisations désireux de commettre des attentats terroristes. A cet égard, ils représentent une menace particulière dans la mesure où ils peuvent être mis à profit pour acheter illégalement le matériel nécessaire à ce but sur un darknet.

---

[62] European Parliament, *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*, mai 2018, http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf.

[63] HM Treasury et Home Office, *National risk assessment of money laundering and terrorist financing 2017*, Londres, 2017, p. 38, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf.

[64] BRANTLY Aaron, «Financing Terror Bit by Bit», in *CTC Sentinel*, vol. 7, n° 10, octobre 2014, p. 4, https://ctc.usma.edu/financing-terror-bit-by-bit/.

[65] WILE Rob, «Supporter of extremist group ISIS explains how bitcoin could be used to fund Jihad», in *Business Insider Australia*, 8 juillet 2014, https://www.businessinsider.com.au/isis-supporter-outlines-how-to-support-terror-group-with-bitcoin-2014-7.

[66] European Parliament, *Virtual currencies and terrorist financing…, cit.*, p. 29.

[67] IRWIN Angela S.M. et MILAD, George, «The use of crypto-currencies in funding violent jihad», in *Journal of Money Laundering Control*, vol. 19, no 4, 2016, pp. 410-411.

[68] European Parliament, *Virtual currencies and terrorist financing…, cit.*, p. 30.

b. Les crypto-monnaies comme moyen de paiement de biens et services illégaux

Les plateformes digitales proposant l'achat et la vente de biens et de services illégaux, situées sur les darknets, recourent de façon privilégiée aux crypto-monnaies. Alors que le bitcoin a pendant longtemps été la monnaie la plus utilisée sur ce genre de plateformes, le monero, qui offre un anonymat plus grand et garantit l'intraçabilité des transactions, semble désormais y acquérir une importance croissante. Les crypto-assets sont ainsi le principal instrument de paiement sur les darknets, où les criminels peuvent se fournir en matériel pornographique interdit, en particulier pédopornographique, en armes, en numéros de carte de crédit volées et surtout en drogues, dont le trafic passe de plus en plus par ce genre de plateformes digitales illégales, même si, selon des sources policières, dans une majorité écrasante, les trafics de stupéfiants s'effectuent encore en argent liquide[69].

La traçabilité des transactions effectuées sur les darknets est faible. D'une part, la technologie liée aux protocoles qui y donnent accès, par exemple 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. D'autre part, les transactions sur les darknets s'effectuent par l'intermédiaire de plateformes de mixing qui s'interposent entre le vendeur et l'acheteur de produits ou de services illégaux, ce qui constitue un obstacle supplémentaire à l'identification des uns et des autres. Enfin, bien que certains *wallets* puissent être signalés comme contaminés par des avoirs provenant du commerce illégal sur les darknets et, partant, blacklistés, rien ne distingue, sur la chaine des transactions bitcoin, une transaction effectuée sur un darknet d'une autre transaction. En réalité, actuellement, pour faire tomber l'anonymat des transactions sur les darknets, il faut que l'utilisateur commette une erreur et, par exemple, publie sur un site tiers d'Internet son adresse cryptographique ou d'autres données personnelles. Grâce à un patient travail de recoupage, les autorités de poursuite peuvent, dans de tels cas, rapporter différentes transactions en crypto-monnaies à des *wallets* d'un même utilisateur et parfois à une personne identifiée[70].

Bien que les darknets ne soient pas exclusivement caractérisés par des activités criminelles, la possibilité d'y acheter, sous couvert d'un anonymat difficile à percer, des armes, d'autres types de matériel de guerre ou des tutoriels sur la confection d'explosifs accentue en conséquence la menace que représentent les crypto-assets du point de vue du financement du terrorisme, même si, de ce point de vue également, aucun cas avéré n'a été identifié en Suisse. Du point de vue du blanchiment d'argent en revanche, le risque provient du recyclage des revenus des ventes illégales en crypto-monnaies et à cet égard, plusieurs cas ont été répertoriés en Suisse. Dans la plupart d'entre eux, les vendeurs de produits illégaux sur les darknets recourent à des bureaux de change online, parfois établis en Suisse, pour y convertir leurs crypto-monnaies en monnaies-fiat. Les sommes en jeu sont souvent faibles, lorsqu'il s'agit de simples vendeurs occasionnels. Mais elles peuvent atteindre des montants considérables lorsqu'il s'agit des organisateurs d'un trafic de drogue ou d'armes, ou des gestionnaires d'une plateforme digitale de commerce illégal, comme dans le cas suivant que le MROS a traité en 2017.

Blanchiment d'argent d'un commerce digital illégal en crypto-monnaies:

Un bureau de change online communique au MROS les soupçons qu'il nourrit à l'encontre d'un de ses clients. Son nom est signalé dans la presse comme celui du gestionnaire d'une plateforme digitale

[69] Voir également HAEDERLI Alexandre et STÄUBLE Mario, «De la drogue livrée en courrier A. Comment fonctionne le marché des stupéfiants sur le Darknet», in *La Tribune de Genève*, 02.05.2018, https://www.tdg.ch/extern/interactive_wch/darknet/.

[70] AL JAWAHERI Husam, AL SABAH Mashael, BOSHMAF Yazan et ERBAD Aiman, "When a small leak sinks a great ship: deanonymizing Tor hidden service users throught bitcoin transactions analysis", in *arXiv*: 1801.07501v2, avril 2018, https://arxiv.org/abs/1801.07501.

de commerce illégal, démantelée grâce à la collaboration de trois polices nationales de deux pays américains et d'un pays asiatique. Arrêté dans ce dernier où il résidait depuis de nombreuses années, cet individu avait accumulé une fortune considérable grâce à la vente de produit illégaux, en particulier des armes et des stupéfiants, sur la plateforme de commerce qu'il gérait sur un darknet. Pour en blanchir les revenus engrangés en bitcoins, il avait recouru au bureau de change online communicant. Celui-ci lui avait remis, contre ses bitcoins, des monnaies fiat qu'il a investies particulièrement dans des achats immobiliers dans plusieurs pays et dans des produits de luxe. En raison des services de mixing utilisés sur les darknets, il n'était en effet pas possible de remonter, par une analyse des transactions, à l'origine criminelle des sommes échangées. Néanmoins, les autorités étrangères qui ont initié les poursuites pénales à son égard ont pu séquestrer et confisquer des avoirs à hauteur de plusieurs dizaines de millions de dollars en crypto-monnaies, grâce aux informations récoltées lors de l'analyse de ses ordinateurs.

Ce cas l'illustre: même lorsque l'identité de la personne qui convertit des crypto-monnaies en monnaies-fiat est connue et même lorsque la crypto-monnaie en question est le bitcoin, dont toutes les transactions sont traçables, l'anonymat qui entoure les *wallets* à partir desquels ils sont transférés rend l'identification de leur origine criminelle à peu près impossible.

c. Le recours aux crypto-monnaies dans des cas de phishing

Nombreuses, les escroqueries liées à l'utilisation frauduleuse d'un ordinateur impliquent de plus en plus souvent des crypto-assets, même si dans l'écrasante majorité des cas, elles s'effectuent encore en monnaies fiat. L'examen des communications de soupçon reçues par le MROS témoigne de ce recours croissant aux crypto-monnaies dans ce type d'infraction préalable au blanchiment d'argent. Deux variantes principales de ce type de criminalité témoignent de l'utilisation de token pour les opérations de blanchiment des avoirs obtenus frauduleusement. Grâce au piratage des informations électroniques d'accès aux comptes bancaires de tiers, des criminels effectuent, dans la première variante, des virements en monnaies fiat vers des comptes de particuliers désireux de vendre leurs crypto-monnaies. Dès qu'ils reçoivent les sommes correspondantes, ceux-ci effectuent la transaction de crypto-monnaies vers les *wallets* qui leur sont indiqués, mais ces derniers n'appartiennent pas aux ayants droit économiques des comptes qui ont été débités frauduleusement en monnaie-fiat. En raison de l'anonymat qui les entoure, les autorités de poursuite pénales sont généralement incapables d'en identifier les ayants droit économiques, de sorte que les procédures pénales ouvertes à leur propos sont classées. La deuxième variante, plus sophistiquée, fait intervenir une mule, sur le compte de laquelle les avoirs soutirés des relations d'affaires piratées sont transférés. Le plus souvent appâtée par un faux contrat de travail ou par d'autres prétextes frauduleux, la mule se charge alors d'acheter des crypto-monnaies pour le compte des criminels et d'en créditer les *wallets* qui lui ont été indiqués. Dans ces deux variantes, l'utilisation de crypto-monnaies permet de perfectionner des schémas criminels classiques, en brouillant le *paper trail* grâce à l'anonymat des détenteurs de portefeuille électronique en crypto-monnaies, généralement enregistrés dans d'autres juridictions que la Suisse, ce qui rend la poursuite pénale de tels cas encore plus difficile que dans les cas de phishing traditionnels.

d. L'investissement d'argent d'origine criminelle dans les crypto-assets

En raison de l'anonymat qui caractérise les crypto-assets et des possibilités de blanchiment d'argent qu'offrent leurs transactions et leurs conversions, les crypto-monnaies semblent de plus en plus recherchées par les criminels désireux d'investir, à des fins de blanchiment, leur argent d'origine

criminelle[71]. La fréquence croissante avec lesquels ils interviennent dans le blanchiment d'argent provenant d'escroquerie sur Internet est une illustration de cette tendance, mais les revenus de toutes les infractions préalables possibles sont susceptibles de servir à acheter des crypto-assets. À cet égard, les ICOs présentent un risque similaire et il n'est pas exclu que des avoirs d'origine criminelle y soient investis, comme le suggère le nombre important de communications de soupçon transmises au MROS par des sociétés promotrices d'ICOs, après avoir découvert que leurs clients ont recouru à des papiers d'identité usurpés ou falsifiés pour ouvrir leur relation d'affaires. Il semble toutefois qu'actuellement l'infraction préalable dont les profits sont le plus souvent blanchis par l'achat de crypto-assets soit le trafic de stupéfiants contrôlé par des organisations criminelles. Outre le recours aux crypto-monnaies pour vendre des produits stupéfiants sur les darknets, les réseaux criminels actifs dans ce genre de trafic commencent également à les utiliser pour rapatrier depuis l'Europe leurs revenus illicites vers les régions exportatrices. A cet égard, les facilités de transferts transfrontaliers rapides et massifs qui caractérisent les tokens apparaissent clairement, comme le montre l'exemple récent d'un cas traité par Europol. Les membres d'un réseau criminel qui revendait en Europe de la cocaïne importée de Colombie employaient des money mules chargés de changer en bitcoins l'argent liquide issu de leur trafic à des distributeurs automatiques de bitcoins, puis de les transférer vers des *wallets* contrôlés par des money mules au service des expéditeurs de la drogue en Colombie[72]. Les autorités américaines constatent également un recours croissant aux crypto-monnaies de la part des organisations criminelles actives dans la vente de stupéfiants aux Etats-Unis, en Europe et en Australie, qui investissent les revenus de leur commerce illicite dans l'achat de bitcoins[73]. Si aucun cas de la sorte n'a pour l'instant été détecté en Suisse, il n'est pas exclu qu'ils y apparaissent. À cet égard, la multiplication des distributeurs automatiques de bitcoins pourrait constituer une menace, que les criminels actifs dans d'autres activités que le trafic de stupéfiants pourraient également mettre à profit.

3.2. Les vulnérabilités de la Suisse face à la menace de blanchiment d'argent et de financement du terrorisme associée aux crypto-monnaies

Les différents aspects exposés jusqu'ici témoignent de la menace importante que représentent les crypto-monnaies en matière de blanchiment d'argent et de financement du terrorisme. Bien qu'elle ne se soit pour l'instant pas traduite par un nombre conséquent de cas avérés, cela ne signifie pas que le risque qu'elles représentent soit faible. En effet, les vulnérabilités du système financier à cette menace sont considérables et ne sont du reste pas spécifiques à la Suisse. La qualification juridique des crypto-assets n'en fait cependant pas partie. En Suisse, les crypto-assets sont généralement considérés par les autorités de poursuite pénale comme un type parmi d'autres de valeurs patrimoniales, susceptibles de concourir au blanchiment d'argent. Ce point de vue correspond également à celui de la FINMA, chargée de la surveillance des marchés financiers.

3.2.1. La vulnérabilité des intermédiaires financiers actifs dans les transactions en crypto-monnaies

[71] EUROPOL, *2017 Virtual Currencies Money Laundering Typologies*, 2017, p. 12; FANUSIE Yaya et ROBINSON, Tom, *Bitcoin laundering: an analysis of illicit flows into digital currency services*, Center on Sanctions & Illicit Finance et ELLIPTIC, 12 janvier 2018, p. 5.

[72] Koos Couvée, «European traffickers pay colombian cartels through bitcoin ATMs: Europol Official», in ACAMS Moneylaundering.com, 28 février 2018, https://www.moneylaundering.com/news/european-traffickers-pay-colombian-cartels-through-bitcoin-atms-europol-official/.

[73] U.S. Department of Justice and Drug Enforcement Administration, *2017 National Drug Threat Assesment*, octobre 2017, p. 130; TZANETAKIS Meropi, "Comparing cryptomarkets for drugs: a charachterisation of sellers and buyers over time", in *International Journal of Drug Policy*, vol. 56, juin 2018, pp. 176-186.

D'après les conceptions de la FINMA, en Suisse, tous les différents types d'intermédiaires financiers actifs dans les transactions en crypto-monnaies sont soumis à la LBA, qu'il s'agisse des bureaux de change online qui échangent des crypto-monnaies contre des monnaies fiat, de plateformes centralisées d'échange entre différents crypto-assets -dont cependant aucune n'est enregistrée en Suisse-, des fournisseurs de *custodian wallets,* des plateformes décentralisées d'échanges entre différents crypto-assets qui disposent de la possibilité d'intervenir dans les transactions de leurs clients ou des sociétés à l'origine d'ICOs dont les jetons peuvent servir de moyens de paiement.

Néanmoins, le caractère décentralisé de la technologie sous-jacente à la plupart des crypto-monnaies permet souvent aux utilisateurs d'effectuer des transactions sans recourir à des intermédiaires financiers, ce qui constitue une importante vulnérabilité du dispositif anti-blanchiment. Ainsi, les *non-custodian wallet providers* et les plateformes décentralisées d'échanges en crypto-monnaies qui ne disposent pas de la possibilité d'intervenir dans les transactions ordonnées par leurs clients, échappent à une telle réglementation. En effet, les sociétés qui proposent de tels services n'interviennent à aucun moment dans les transactions effectuées par les utilisateurs et, partant, n'ont aucune activité d'intermédiation financière. C'est particulièrement le cas des plateformes de négociation décentralisées en crypto-monnaies[74]. L'exemple cité plus haut, où une société suisse de ce type a converti des bitcoins acquis par le *ransomware Wannacry* contre des moneros, sans identifier ni les auteurs des transactions ni l'origine criminelle des tokens échangés, illustre cette vulnérabilité. En conséquence, une large partie des transactions en crypto-monnaies[75], échappe à tout contrôle.

Par ailleurs, les intermédiaires financiers actifs dans les échanges en crypto-assets ne semblent pas tous également conscients de leur soumission à la LBA et des devoirs de diligence que celle-ci implique. Aussi ne les appliquent-ils pas toujours de façon adéquate, ne connaissent-ils pas toujours leurs clients de façon détaillée et se montrent-ils incapables, malgré leur disponibilité à collaborer avec les autorités de poursuite pénale, de fournir les informations relatives soit à l'identité de leurs clients, soit à l'origine des tokens qu'ils traitent. De ce point de vue cependant, le nombre croissant de communications de soupçons reçues par le MROS de la part des sociétés spécialisées dans le commerce en crypto-monnaies illustre la conscience croissante qu'ont ces intermédiaires financiers de leurs devoirs de diligence. En outre, le MROS constate également que, depuis que la FINMA a publié, en février 2018, un guide pratique sur les ICOs, qui définit à quelles conditions elles sont assimilées à des intermédiaires financiers, les sociétés qui font appels à ce type de financement en crypto-assets commencent également à adresser des communications de soupçons.

Néanmoins, quand bien même tous les intermédiaires financiers seraient conscients de leurs devoirs de diligence, l'efficacité de telles mesures ne peut que rester limitée, en raison de la nature transnationale des transactions en crypto-monnaies, qui passent par des sociétés de services enregistrées dans de très nombreuses juridictions. Par exemple, les conversions d'une crypto-monnaie à une autre sont souvent effectuées par des bureaux de change online enregistrés en Suisse à la demande de fournisseurs de *custodian wallets* étrangers sur mandat de leurs clients. Dans de tels cas de figure, la plateforme suisse n'a pas accès au KYC du client de la plateforme étrangère pour le compte de laquelle elle effectue une opération de change, de sorte qu'elle n'en connaît pas l'identité. De même, en raison de l'anonymat qui entoure les transactions en crypto-monnaies, les intermédiaires financiers qui opèrent des transactions pour le compte de leurs clients n'ont aucun moyen de vérifier que les *wallets* d'où proviennent les valeurs qu'ils traitent ou en faveur desquels ils effectuent des virements appartiennent effectivement aux personnes qui leur sont indiquées par leurs clients. Pour atténuer cette vulnérabilité, certains intermédiaires financiers concentrent leurs activités sur la gestion de fortune de leurs clients et préfèrent délaisser les activités relevant du trafic de paiements en faveur de tiers. En

[74] Cf. *Infra*, 4.1.4.

[75] "76% of incorporated wallet providers do not have a license", HILEMAN Garrick et RAUCHS Michel, *Global Cryptocurrency Benchmarking Study*, Cambridge, Center for Alternative Finance/University of Cambridge, 2017, p.62.

outre, ils n'acceptent des crypto-monnaies anonymes qu'après un processus de clarification extrêmement précis et uniquement pour le compte de clients qu'ils connaissent bien.

De tels efforts sont particulièrement louables parce qu'en réalité, les seules transactions en crypto-assets qui permettent l'identification de l'ayant droit économique des valeurs en jeu sont leur acquisition et leur vente contre des monnaies fiat. Les bureaux de change online qui effectuent de telles transactions semblent conscients de leurs devoirs de diligence, les mettent en application et fournissent, le cas échéant, les informations à leur disposition aux autorités de poursuite pénale, comme tous les intermédiaires financiers traditionnels. De l'avis des autorités compétentes de police et de justice, de tels bureaux de change online sont les seuls intermédiaires financiers actifs dans les transactions en crypto-monnaies, qui soient en mesure de leur fournir des informations précises sur l'identité des ayants droit économiques des valeurs en jeu. Cela ne les garantit cependant pas entièrement contre les fraudes. Ils n'ont en effet aucun moyen de vérifier l'identité de l'ayant droit économique des portefeuilles électroniques qu'ils créditent sur ordre de leurs clients. De même, lorsqu'un client veut vendre ses tokens contre des monnaies-fiat, l'intermédiaire financier n'a que peu de moyens d'identifier une éventuelle origine criminelle des valeurs qu'il achète. Dans le cas des crypto-monnaies comme le bitcoin, où toutes les transactions sont traçables, il peut vérifier, grâce à une analyse de chaîne (*chain analysis*), que le *wallet* du client contient bien les tokens qu'il désire vendre et peut éventuellement reconnaître que les avoirs en question sont passés par un service de mixing ou, plus rarement encore, par un *wallet* blacklisté. En revanche, il ne peut pas savoir si c'est le client lui-même qui a eu recours à ce service de mixing ou à ce *wallet* blacklisté ou s'il a acquis légalement les tokens en question, après leur passage par ces étapes suspectes.

En outre, il semble que les processus d'ouverture d'un compte que les bureaux de change online prévoient laissent souvent une certaine marge de manœuvre aux criminels désireux de recourir à des tokens pour blanchir des fonds mal acquis. Le MROS a connu des cas où de tels intermédiaires financiers suisses ont signalé des soupçons de blanchiment d'argent associés à des relations d'affaires qui avaient été ouvertes en leurs livres grâce à des documents d'identité usurpés. Comme le processus d'ouverture de comptes s'effectue souvent par Internet, une telle usurpation d'identité n'avait pas pu être détectée. C'est une vulnérabilité similaire qui caractérise les sociétés promotrices d'ICOs assimilées à des intermédiaires financiers. Toutes les communications que les sociétés de ce type ont adressées au MROS se fondent sur des soupçons provenant de l'utilisation de faux documents lors de l'ouverture des relations d'affaires. Ainsi, une société promotrice d'une ICO a communiqué au MROS plus d'une centaine de relations d'affaires avec des clients qui avaient présenté de faux papiers d'identité pour investir dans le projet suscitant l'ICO. Cela alimentait les soupçons que les sommes investies dans l'ICO pouvaient être d'origine criminelle.

Par ailleurs, comme les bureaux de change traditionnels, ceux actifs online dans le commerce de crypto-assets ne sont tenus d'appliquer des devoirs de diligence à leurs clients qu'à partir d'un seuil de conversion de CHF 5000 (art. 51, al. 1, let. 1 OBA-FINMA; RS *955.033.0*). Cela laisse une marge de manœuvre à la multiplication d'opérations de change complètement anonymes en-deçà de ce seuil. La multiplication de distributeurs automatiques de monnaies virtuelles accentue également cette vulnérabilité, comme l'illustrent plusieurs communications de soupçons reçues par le MROS.

Cas de fractionnement d'achats de crypto-monnaies:

Une plateforme de services de payement qui accepte les payements en crypto-assets adresse une communication de soupçons au MROS, pour lui signaler qu'un même *wallet* a été crédité de bitcoins achetés en onze opérations à des bornes automatiques en un laps de temps très court, qui portaient à chaque fois sur le maximum du montant autorisé. Illustration de l'incertitude des intermédiaires financiers actifs dans le trafic de paiement en crypto-monnaies qui n'impliquent aucune opération de change avec des monnaies fiat, la plateforme de services communicante ne connaissait pas l'identité de l'ayant droit économique du *wallet* crédité. Pour identifier la ou les personne(s) ayant effectué ces

opérations de change, le seul moyen à disposition du MROS était des numéros de téléphone portables suisses. Malgré l'obligation légale qui leur était faite par la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT, RS *780.1*), les opérateurs qui avaient délivré ces numéros de téléphone n'avaient pas respecté leur obligation d'identification de leur client, de sorte que les numéros de téléphone étaient enregistrés sous des noms de fantaisie comme Donald Duck. En l'absence d'obligations pénales prévues par la LSCPT, de tels manquements de la part des opérateurs n'étaient pas punissables. Le MROS n'avait en conséquence aucun moyen de connaître les détenteurs de ces téléphones. En outre, il ne disposait pas non plus d'informations relatives à l'origine des avoirs échangés contre des bitcoins, de sorte qu'il a dû classer ce dossier. Dans ce cas, l'intermédiaire financier a bien repéré les transactions suspectes et les a dûment communiquées au MROS. Mais en l'absence de moyens d'identification du détenteur du *wallet* crédité, il n'était pas possible de poursuivre les enquêtes. La modification de la LSCPT, entrée en vigueur au 1er janvier 2018 et qui prévoit des sanctions pénales pour les manquements au devoir d'identification des clients de la part des opérateurs de téléphonie mobile, devrait supprimer l'anonymat total des transactions qui était possible dans le présent cas. Néanmoins, elle ne peut éviter qu'un téléphone portable ne puisse être utilisé à des fins criminelles par quelqu'un qui n'en est pas le détenteur légitime, par exemple par un voleur.

C'est ainsi une grande vulnérabilité à la menace de blanchiment d'argent et de financement du terrorisme qui caractérise les intermédiaires financiers actifs dans les transactions en crypto-assets. Leur nombre limité constitue du reste une vulnérabilité supplémentaire pour la place financière suisse, qui caractérise cependant également d'autres pays. En effet, le fait que les sociétés actives dans l'intermédiation financière en crypto-monnaies soient peu nombreuses implique que d'innombrables transactions s'effectuent directement entre des utilisateurs qui recourent à des plateformes qui ne font que mettre à disposition des programmes dont les utilisateurs se servent sans leur intervention et qui, partant, ne sont pas assimilés à de l'intermédiation financière. En outre, à quelques exceptions près comme les États-Unis, le Japon et récemment la Malaisie, la plupart des juridictions ne soumettent pas encore les *custodian wallet providers* à la législation LBA. Cela permet aisément à des utilisateurs suisses de recourir, potentiellement pour des opérations de blanchiment d'argent, à des services d'intermédiation financière en crypto-monnaies enregistrés dans d'autres juridictions, où la règlementation anti-blanchiment à leur égard est soit inexistante, soit mal appliquée. A cet égard, la dilution des juridictions traditionnelles sur Internet constitue également l'un des principaux obstacles à la répression de la criminalité financière qui recourt aux tokens.

3.2.2. La difficile répression du blanchiment d'argent et du financement du terrorisme par le recours aux crypto-monnaies

Pour les autorités de police et de justice chargées de la répression de la cyber-criminalité, notamment du blanchiment d'argent et du financement du terrorisme par les crypto-assets, les obstacles sont nombreux, même s'ils ne sont pas propres à la place financière suisse et caractérisent toutes les juridictions. En raison de l'anonymat qui entoure les transactions en token, l'identification des transactions suspectes et des ayants droit économiques de *wallets* qui y sont impliqués est extrêmement difficile. A cet égard, l'analyse de chaîne n'est que d'un secours très partiel. D'abord, elle n'est possible que pour les crypto-monnaies qui prévoient la traçabilité des transactions sur leur blockchain et ne peut être pratiquée pour les tokens comme le monero ou le verge, complètement anonymes. Ensuite, le passage par un service de mixer rompt définitivement le *paper trail*, même pour des crypto-monnaies traçables, comme le bitcoin. Enfin, même lorsque la traçabilité des avoirs en jeu peut être établie par une analyse de chaîne, elle ne dit rien ni des ayants droit économiques des *wallets* impliqués dans les transactions, ni de la nature potentiellement criminelle d'une transaction relevant d'un acte de blanchiment d'argent, ni même des adresses IP des ordinateurs utilisées pour effectuer ces transactions. Néanmoins, certains programmes d'analyse de chaîne permettent de recouper assez finement les transactions effectuées entre différents *wallets* pour pouvoir établir, selon une très grande

probabilité, que leur ayant droit économique est le même. En outre, ils peuvent également signaler que l'un des *wallets* par lequel les avoirs ont transité a été blacklisté pour une raison ou une autre, notamment parce qu'il a accueilli des avoirs provenant de la vente de biens ou de services illégaux sur le darknet.

Sans un tel signalement cependant, rien ne distingue, dans une analyse de chaîne, une transaction illégale ou effectuée sur un darknet d'une transaction légale. Aussi, pour identifier une transaction susceptible de concourir à des actes de blanchiment d'argent issus de ventes sur un darknet, les autorités de police sont le plus souvent contraintes d'infiltrer ces marchés illégaux, d'y repérer les pseudonymes des criminels et d'espérer qu'ils commettent des erreurs permettant de percer leur anonymat, par exemple en dévoilant sur un site public des informations qui permettent, par recoupement, d'établir leur identité et leur contrôle sur un *wallet* particulier. L'identification de transactions frauduleuses en tokens qui ne proviennent pas d'un darknet est encore plus difficile, dans la mesure où les autorités de poursuite pénale ne savent pas *a priori* dans quel périmètre orienter leurs recherches. Les signalements sont alors adressés au MROS par les intermédiaires financiers, mais eux-mêmes sont soumis aux mêmes difficultés que les autorités de poursuite pénale du point de vue de l'analyse des transactions, de sorte que leurs signalements sont le plus souvent la conséquence d'une plainte pénale ou d'une réclamation déposée par l'un de leurs clients, à propos d'une escroquerie dont il s'estime la victime, ou du recours à des papiers d'identité usurpés ou falsifiés lors de l'ouverture de la relation d'affaires.

Une fois une transaction suspecte identifiée, il reste à identifier l'ayant droit économique des valeurs qu'elle met en jeu. D'après les autorités judiciaires consultées, ce sont les informations fournies par les intermédiaires financiers qui permettent cette identification. Mais il se peut qu'une transaction douteuse soit effectuée sans le recours à un intermédiaire financier ou, dans le cas où un intermédiaire financier est impliqué, qu'il ne dispose pas d'information à ce sujet. Enfin et surtout, il arrive souvent que les transactions suspectes soient effectuées depuis des plateformes de services en crypto-assets qui ne sont pas enregistrées en Suisse. Dans de telles situations, il ne reste aux autorités de poursuite que l'espoir que le criminel présumé commette une erreur qui permette de percer son anonymat ou que les échanges d'informations policières et judiciaires avec leurs homologues étrangers se révèlent productifs. Si la voie de l'entraide internationale constitue certainement l'un des instruments les plus efficaces de la répression de la criminalité en crypto-monnaies, elle est cependant souvent dépassée par la rapidité des transactions d'une juridiction à l'autre. En outre, même en cas d'identification de *wallets* accueillant des avoirs d'origine suspecte et de leurs ayants droit économiques, le séquestre des valeurs patrimoniales qui y sont déposées n'est possible que si les autorités de poursuite pénale disposent des clefs cryptographiques privées de ces *wallets*. Avec un peu de chance, un fournisseur de *custodian wallets* collaboratif en dispose et les remet à la justice. Du point de vue des autorités helvétiques cependant, il faut que ce fournisseur de *custodian wallets* soit enregistré en Suisse, ce qui n'est que très rarement le cas. Dans d'autres cas, le criminel, déjà soumis à une procédure pénale, peut dévoiler la clef cryptographique de son *wallet*, ouvrant la voie au séquestre et à la confiscation des avoirs qui y sont déposés. Mais si aucun de ces deux cas de figure ne s'avère, le produit du blanchiment d'argent par les crypto-monnaies est irrémédiablement perdu pour les autorités de poursuite pénale, du moins dans l'état actuel de la technologie.

Aussi, dans la majorité des cas, les autorités de police et de justice n'arrivent pas à percer l'anonymat inhérent aux transactions en crypto-monnaies et aux *wallets* qui les accueillent. De même, établir que le lancement d'une nouvelle crypto-monnaie ou d'une ICO relève d'un simple *scam* n'est pas aisé. Des soupçons peuvent certes émerger, mais leur confirmation est souvent impossible. Enfin, la dilution des juridictions pénales sur Internet entraîne souvent d'importants problèmes de for juridique, en plus des lenteurs du processus d'entraide internationale. Il en résulte de nombreux obstacles à la poursuite du blanchiment d'argent et du financement du terrorisme par les crypto-monnaies, qui expliquent que, dans de nombreux cas de soupçons de blanchiment d'argent par les crypto-monnaies que le MROS a transmis à un ministère public, des ordonnances de non-entrée en matière ont été prononcées. Le plus

souvent, elles étaient justifiées par l'impossibilité, à la fin d'enquêtes préliminaires, d'identifier l'ayant droit économique des *wallets* accueillant des crypto-monnaies dont l'origine paraissait suspecte.

3.3. Bilan de l'analyse des risques

Malgré leur augmentation, le petit nombre de cas de soupçons de blanchiment d'argent par les crypto-assets répertoriés par les autorités suisses rend l'évaluation du risque qui leur est associé difficile. Ce nombre réduit pourrait témoigner d'un risque réel somme toute faible, provenant d'une technologie qui, certes en expansion, reste encore nouvelle et à laquelle il n'est que très marginalement fait recours à des fins criminelles de blanchiment d'argent ou de financement du terrorisme. Mais il pourrait également être le résultat des failles dans l'élaboration des soupçons et dans l'identification des cas de blanchiment d'argent et de financement du terrorisme par les tokens. Quoi qu'il en soit, la menace importante que représentent les crypto-monnaies est avérée et les vulnérabilités de la Suisse en la matière sont considérables, même si elles caractérisent également tous les pays. À cet égard, il convient de constater que la dilution des juridictions pénales sur Internet constitue un risque particulièrement élevé, sans que l'on puisse, par conséquent, affirmer qu'il concerne spécifiquement la Suisse. Un utilisateur désireux de rester anonyme, par exemple pour effectuer des transactions liées à un schéma criminel de blanchiment d'argent, peut aisément recourir à des sociétés de services en crypto-monnaies établies dans une juridiction soit où leur soumission à la législation anti-blanchiment n'est pas effective, soit où son application est négligée, même s'il agit lui-même dans une juridiction qui connaît de sévères réglementations anti-blanchiment.

4. Facteurs de diminution des risques

Bien que la menace représentée par les crypto-monnaies soit importante et que les vulnérabilités soient considérables, plusieurs facteurs permettent néanmoins de diminuer le risque qu'elles représentent. Certaines, déjà évoquées, sont inhérentes à la technologie sous-jacente aux crypto-monnaies. En cas de vols ou de détournements frauduleux de tokens, les utilisateurs peuvent identifier et blacklister les *wallets* qui les accueillent, interdisant ainsi tout blanchiment. De même, les erreurs de débutants que peuvent commettre les utilisateurs honnêtes peuvent également caractériser les criminels, de sorte que, de l'avis des autorités de poursuite pénale compétentes, la meilleure chance d'éviter l'utilisation de crypto-monnaies à des fins de blanchiment réside dans les erreurs que les auteurs de ces crimes commettent, qui permettent de les identifier et, si possible, de les mettre hors d'état de perpétuer leurs méfaits. Cependant, outre ces facteurs de diminution des risques internes aux technologies des crypto-monnaies, les autorités suisses s'efforcent de développer les instruments les plus efficaces possibles pour atténuer le risque de blanchiment d'argent et de financement du terrorisme par les crypto-monnaies. En particulier, malgré les limites inhérentes à une règlementation nationale dans cette problématique par nature transnationale, la soumission des intermédiaires financiers dont les activités se déploient dans ce domaine est particulièrement étendue en Suisse, même si elle ne peut empêcher que la majorité des transactions en crypto-assets ne passent par des services ne relevant pas de l'intermédiation financière, comme les fournisseurs de *non custodian wallets* ou des plateformes de négociation décentralisées non soumises à la LBA ou enregistrées à l'étranger.

4.1. Classement des cas d'application impliquant les crypto-monnaies selon le droit de la surveillance

4.1.1. Initial Coin Offerings

Si, dans le cadre d'une ICO[76], des tokens sont émis et sont, effectivement ou selon l'intention du promoteur, acceptés comme moyens de paiement pour l'achat de produits ou services et/ou doivent servir à un transfert d'argent ou de valeurs, cette opération constitue, du point de vue de la loi sur le blanchiment d'argent, une émission de moyens de paiement soumise à la LBA selon l'art. 2, al. 3, let. b, LBA, en relation avec l'art. 4, al. 1, let. b, OBA.

Diverses obligations de diligence découlent de la LBA, de même que l'obligation de s'affilier à un OAR ou de se soumettre directement à la FINMA pour la surveillance selon la LBA. Selon la pratique de la FINMA, cette obligation est réputée 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.

L'obligation de vérification de l'identité du cocontractant selon l'art. 3 LBA constitue un principe élémentaire de la prévention du blanchiment d'argent. L'obligation d'identification s'applique sans montant minimum. L'OBA-FINMA, la CDB 16 et les règlements des OAR prévoient cependant, pour certaines activités et jusqu'à certains seuils, en fonction des risques, la renonciation totale au respect de l'obligation ou une identification simplifiée. Pour l'émission de moyens de paiement dans le cadre d'une ICO, la FINMA prévoit la possibilité d'une identification simplifiée lorsque le montant de l'investissement est compris entre 0 et 3000 francs (simple copie de la pièce d'identité)[77]. Une identification complète n'est requise qu'à partir de 3000 francs. Une telle simplification se justifie par les risques inhérents à une ICO: le risque principal est qu'il s'agisse d'une arnaque (*scam*) ou que le promoteur de l'ICO utilise les fonds pour financer des actes de terrorisme[78]. Un autre risque est que des

[76] La FINMA a fait connaître sa pratique concernant le classement des ICOs selon le droit de la surveillance dans le Guide pratique pour les questions d'assujettissement concernant les initial coin offerings (ICO) du 16 février 2018.

[77] Par analogie à l'art. 12, al. 2, let. d, OBA-FINMA

[78] Voir *supra*, 3.1.1.c.

sommes d'origine criminelle puissent être investies dans une ICO[79]. La soumission à la LBA des ICOs qui émettent des jetons de paiement constitue une mesure appropriée face au risque de blanchiment d'argent.

En général, on constate que les ICOs sont très similaires aux cycles de financement traditionnels ou aux placements privés de personnes morales. Dans la mesure où les détenteurs de tokens ne sont généralement ni actionnaires, ni créanciers de la société, il est possible, lors de l'émission, de contourner la nécessité d'établir des documentations volumineuses et coûteuses (notamment l'obligation de prospectus), d'une part, et les règles de transparence relatives aux personnes morales, d'autre part.

4.1.2. Fournisseurs de wallets

Un fournisseur de *wallets* qui conserve la clef privée du client (fournisseur de «*custody wallets*») permet l'envoi et la réception de crypto-monnaies et fournit ainsi un service dans le domaine du trafic des paiements soumis à la LBA au sens de celle-ci (art. 2, al. 3, let. b, LBA, en relation avec l'art. 4, al. 1, let. a, OBA). La fonction et la situation en matière de risque sont identiques à celles des *money transmitters*. Les crypto-monnaies, en particulier, peuvent servir à transférer rapidement et simplement des valeurs patrimoniales dans le monde entier, ce qui soulève le risque que des sanctions soient ainsi contournées et des terroristes financés.

Par conséquent, les fournisseurs de *wallets* doivent s'affilier à un OAR ou se soumettre directement à la FINMA pour assurer la surveillance selon la LBA. Dans la mesure où ils ne peuvent pas limiter géographiquement les transactions, la pratique de la FINMA impose une obligation d'identification, sans montant minimum, comme lors de transferts à l'étranger par des *money transmitters*. En raison de l'analogie avec les nouvelles méthodes de paiement («New Payment Methods»), une identification simplifiée (simple copie de la pièce d'identité) est aussi admise pour les fournisseurs de *wallets* s'ils limitent le volume des transactions à 500 francs par mois et 3000 francs par année civile.

La soumission des fournisseurs de *custody wallets* à la LBA ne permet qu'en partie de tenir compte de risques de blanchiment d'argent[80]. La grande majorité des fournisseurs de *wallets* ne contrôle pas les clefs privées des clients (fournisseurs de *non-custody wallets*, cf. ch. 2.2 ci-dessus). Dans la situation juridique actuelle, une soumission serait possible, tout au plus, sur la base d'une interprétation extensive de l'art. 4, al. 1, let. a, LBA, qui dispose qu'il existe un service dans le domaine du trafic des paiements lorsque l'intermédiaire financier «ordonne» le virement des valeurs financières liquides au nom et sur ordre du cocontractant. La FINMA a étudié une telle interprétation et est parvenue à la conclusion que celle-ci n'était pas compatible avec la systématique de la LBA ou avec l'acception de la notion d'intermédiation financière, qui s'appuie sur le pouvoir de disposition de valeurs étrangères.

4.1.3. Bureaux de change et plateformes de négociation centralisées

Dans l'activité de change, les organismes de change proposent l'achat et la vente de crypto-monnaies directement à partir de leurs propres avoirs. Les opérations de change impliquant des crypto-monnaies sont des activités d'intermédiaire financier au sens de la LBA (cf. art. 2, al. 3, let. c, LBA, en relation avec l'art. 5, al. 1, let. a, OBA).

Le risque de blanchiment d'argent lié aux activités d'organismes de change dans le domaine des crypto-monnaies est le même que pour l'activité traditionnelle de change, c'est-à-dire moins élevé que dans le trafic des paiements, car les valeurs sont simplement échangées avec le client, et non transférées à des tiers. Pour répondre à l'obligation d'identification, la FINMA applique donc aussi aux crypto-

[79] Voir *supra*, 3.2.1.

[80] Cf. cas MROS au ch. 3.2.1 qui n'a pas pu faire l'objet de poursuites en l'absence d'obligation d'identification du fournisseur de *wallets*.

monnaies le seuil de 5000 francs valable pour les organismes de change. Dans le domaine des crypto-monnaies, distinguer l'activité de change (avec renonciation totale à l'identification jusqu'à 5000 francs par transaction) du service dans le domaine du trafic des paiements constitue un véritable défi. Dans le cadre d'une opération de change traditionnelle se déroulant à un guichet, l'intermédiaire financier peut savoir avec certitude qu'il s'agit véritablement d'une opération de change, car la personne qui remet la somme à changer se tient juste devant lui. Sur Internet, en revanche, l'organisme de change ne sait pas si le *wallet* destinataire indiqué par le client lui appartient ou s'il s'agit du *wallet* d'un tiers (auquel cas il s'agirait d'un virement, c'est-à-dire d'un trafic de paiement plus risqué). L'organisme de change de crypto-monnaies doit donc s'assurer, par des mesures appropriées, qu'il n'existe qu'un rapport entre deux parties, afin de pouvoir bénéficier du seuil plus élevé de 5000 francs. Il est libre de déterminer le mode d'application de cette consigne.

Contrairement aux bureaux de change, les plateformes de négociation centralisées exercent une fonction d'intermédiaire entre les utilisateurs de la plateforme. Le négociant reçoit de l'argent ou des crypto-monnaies de la part de clients et les transmet à d'autres utilisateurs. Ces plateformes de négociation sont appelées «*money transmitter*s» et sont donc soumises à la LBA. Selon la pratique de la FINMA, les plateformes de négociation sont soumises au même seuil que les fournisseurs de *custody wallets* (cf. ch. 4.1.2 ci-dessus).

4.1.4. Plateformes de négociation décentralisée

Sur les plateformes de négociation décentralisées, contrairement aux plateformes de négociation centralisées, les ordres regroupés (après autorisation / confirmation de la transaction) sont directement traités sur la blockchain par les utilisateurs[81]. Puisque la plateforme de négociation permet, en définitive, de transférer des valeurs patrimoniales, on peut se demander si la plateforme fournit un service d'intermédiaire financier dans le domaine du trafic des paiements au sens de la LBA.

Pour la soumission à la LBA d'une telle plateforme d'échanges, l'élément déterminant est de savoir si l'exploitant de la plateforme a ou non le pouvoir de disposer des crypto-monnaies échangées. C'est souvent le cas, puisque la plateforme doit confirmer les ordres (sous quelque forme que ce soit) pour garantir le bon déroulement de la transaction ou en autoriser ou en bloquer l'exécution. En outre, afin de garantir que toutes les transactions conclues puissent être exécutées en bonne et due forme, l'exploitant se réserve souvent la possibilité d'intervenir et de ne pas autoriser des remboursements demandés par l'utilisateur des crypto-monnaies conservées dans le cadre du «settlement smart contract». Selon la pratique de la FINMA, les plateformes de négociation décentralisées sont soumises à la LBA.

La plateforme de négociation décentralisée n'échappe à la soumission à la LBA que dans les cas où elle n'a aucune possibilité d'intervention dans l'exécution de la transaction (p. ex. dans le cas d'une simple mise à disposition d'un «escrow smart contract» nécessaire à la transaction, sans possibilité d'accès de la plateforme). Comme pour les fournisseurs de *non-custody wallets*, la FINMA ne prévoit pas la possibilité de soumettre de telles plateformes de négociation à la LBA compte tenu de la situation juridique en vigueur.

4.1.5. Minage

La prospection ou le minage de crypto-monnaies en Suisse ne sont pas soumis à autorisation selon la législation sur les marchés financiers. S'agissant de la vente des crypto-monnaies obtenues par minage,

[81] Le transfert peut aussi se faire à l'aide de systèmes de paiement *off chain*. Dans ce cadre, le système de paiement ou l'exploitant n'a pas le pouvoir de disposer des valeurs des utilisateurs. Ces derniers transfèrent entre eux des crypto-monnaies à l'aide de l'infrastructure du système de paiement.

il peut exister une activité d'échange correspondante au regard du droit sur le blanchiment d'argent, notamment quand la transaction intervient pour le compte de tiers.

4.1.6. Tableau récapitulatif des types de services en crypto-assets soumis à la LBA

Catégorie de services	Soumis à la LBA	Non soumis à la LBA	Soumis à la LBA à certaines conditions
ICOs			Soumis à la LBA lorsque l'ICO émet des jetons qui peuvent être assimilés à des moyens de paiement (jetons de paiement)
Fournisseurs de custodian wallets	Soumis à la LBA dans tous les cas		
Fournisseurs de non custodian wallets		Non soumis à la LBA	
Bureaux de change online en crypto-monnaies	Soumis à la LBA au même titre que les bureaux de change traditionnel		
Plateformes de négociation centralisées	Soumises à la LBA dans tous les cas		
Plateformes de négociation décentralisées			Soumises à la LBA lorsqu'elles ont la possibilité d'intervenir dans les transactions de leurs utilisateurs, par exemple pour bloquer une transaction
Mineurs		Non soumis à la LBA	

4.2. La coopération internationale

Comme on l'a vu plus haut, les autorités de poursuite pénale suisses sont relativement démunies face à la criminalité financière qui fait usage des crypto-monnaies, notamment face au blanchiment d'argent et au financement du terrorisme qu'elles peuvent favoriser. Dans ce domaine plus encore que dans d'autres, elles semblent avoir un temps de retard sur les criminels. Néanmoins, elles disposent de certains instruments traditionnels qui leur sont utiles à cet égard, en particulier la coopération avec leurs homologues étrangers.

Les autorités de police et de justice sont unanimes pour dire que l'entraide judiciaire et policière internationale n'est pas moins efficace en matière de traque de la criminalité financière en crypto-monnaies que dans d'autres domaines. C'est grâce à ce type de collaboration internationale, dans lequel justice et police suisses sont profondément impliquées, qu'au niveau international, les plus beaux succès en matière de répression de la criminalité financière en crypto-monnaies et notamment du blanchiment d'argent ont été récoltés[82], en particulier lors de la fermeture des principaux marchés illégaux sur les darknets comme Silkroad, Hansa ou Alpha Bay. Les autorités suisses de justice et de police collaborent souvent à ces opérations de grande envergure, ce qui conduit parfois à des condamnations en Suisse.

Condamnation en Suisse d'un cyber-criminel actif sur un darknet:

Dans le cadre des opérations menées de concert par les autorités de police et de justice de plusieurs pays contre le marché noir Silk Road 2, la Suisse a reçu une demande d'entraide judiciaire internationale concernant un des sites de ce marché illégal accessible par un darknet, qui était géré depuis la Suisse. Les enquêtes menées par des autorités de police étrangères avaient réussi à en identifier l'adresse IP, ce qui a conduit le ministère public cantonal compétent à ouvrir une procédure pénale. Coordonnées à l'échelle internationale, des perquisitions ont eu lieu au même moment dans différents pays. Celle effectuée en Suisse dans l'appartement où se trouvait le raccordement identifié a permis de saisir le serveur recherché et d'identifier le créateur et webmaster du site de ventes illégales incriminé. Les investigations de la police ont également révélé que le précité avait proposé à la vente des marchandises illégales fictives et avait ainsi perçu en quelques mois environ USD 125 000.- sous forme de bitcoins, qu'il a presque intégralement perdus en jouant sur des sites de poker en ligne. Néanmoins, il conservait sur un *wallet* électronique une vingtaine de bitcoins provenant de son activité délictueuse. Acceptant de collaborer avec la justice, le prévenu lui a remis la clef cryptographique privée de ce *wallet*, de sorte que ce montant a pu être saisi puis confisqué, tandis que le prévenu a été condamné pour escroquerie.

Outre les dispositions de la Loi fédérale sur l'entraide internationale en matière pénale (EIMP ; RS 351.1), la Convention du Conseil de l'Europe sur la cybercriminalité, approuvée par l'Assemblée fédérale et mise en application par l'Arrêté fédéral du 18 mars 2011[83], offre une base légale importante pour la règlementation de la collaboration judiciaire et policière en la matière. Elle autorise notamment les polices des différents États signataires à s'adresser directement aux entreprises étrangères pour obtenir les données informatiques nécessaires à leurs enquêtes (art. 32). Même si les entreprises sollicitées ne sont pas tenues de répondre positivement à ces demandes, plusieurs d'entre elles, dans la mesure où la législation nationale à laquelle elles sont soumises le permet, collaborent activement à ce genre de procédures, selon les autorités de police compétentes. En outre, un tel instrument légal permet, même en cas de refus de la part des entreprises sollicitées, de les engager à conserver particulièrement soigneusement les données qui ont fait l'objet de la requête, dans l'attente d'une

[82] «Significant law enforcement actions», in European Parliament, *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*, mai 2018, p. 85, http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf.

[83] https://www.admin.ch/opc/fr/official-compilation/2011/6293.pdf.

demande d'entraide judiciaire en bonne et due forme. D'après les polices compétentes en la matière, cet instrument légal s'avère particulièrement important. En outre, la pratique prouve que les entreprises en question, dans la mesure où elles sont des intermédiaires financiers, peuvent adresser à leur CRF des communications de soupçons sur la base de telles demandes. Celles-ci peuvent ensuite faire l'objet d'une information spontanée au MROS.

La réciproque est également vraie et les intermédiaires suisses sollicités par des demandes de police étrangères au titre de l'art. 32 de la Convention sur la cybercriminalité du Conseil de l'Europe, sans leur répondre directement, adressent les informations demandées au MROS, qui les transmet alors à ses homologues étrangers. Par ailleurs, le MROS envoie également à ses homologues étrangers des demandes d'informations et des informations spontanées relatives à des soupçons de blanchiment d'argent par les crypto-monnaies, même s'il est encore trop tôt pour en évaluer les résultats.

4.3. Les progrès technologiques à l'aide des autorités de poursuite pénales

Si, dans l'état actuel de la technologie, les instruments de *chain analysis* ne sont que d'un secours partiel pour les enquêteurs qui traquent le blanchiment d'argent et le financement du terrorisme par les crypto-monnaies, la situation pourrait évoluer rapidement. Plusieurs projets de recherches permettent en effet d'espérer que des progrès significatifs puissent être accomplis prochainement en la matière. Ainsi, plusieurs sociétés tentent actuellement de développer des instruments informatiques permettant de rétablir le *paper trail* des transactions en crypto-monnaies qui passent par des services de mixer/tumbler. Au niveau international également, la Suisse participe au projet TITANIUM (Tools for the Investigation of Transaction in Underground Markets), qui rassemble chercheurs en informatiques et autorités de poursuite pénales de différents pays, sous le pilotage d'INTERPOL. Ce projet a pour objectif de développer un instrument capable d'améliorer la transparence des transactions en crypto-assets sur les marchés des darknets, notamment par une analyse simultanée de blockchains de différentes crypto-monnaies, de façon à percer l'anonymat de ceux qui y font recours[84].

4.4. Divers

Outre les facteurs évoqués jusqu'ici, plusieurs initiatives sont prises par différentes autorités pour améliorer l'efficacité de la répression de la criminalité financière associée aux crypto-monnaies, notamment du blanchiment d'argent et du financement du terrorisme. Elles consistent par exemple en un effort de formation des autorités concernées. Procureurs, policiers et analystes financiers du MROS commencent ainsi d'être sensibilisés à la problématique des crypto-monnaies et de la criminalité qui peut leur être associée. La formation des policiers comprend notamment des cours sur la cybercriminalité, distribués par l'Institut suisse de Police. Une telle démarche est particulièrement importante, tant une bonne connaissance technique du sujet est indispensable pour comprendre les possibilités techniques offertes par les technologies associées aux crypto-monnaies pour le blanchiment d'argent et le financement du terrorisme comme pour sa répression. Cet effort, encore balbutiant, devrait être systématisé et approfondi. A cet égard, la constitution, au sein des différentes polices cantonales, de brigades spécialisées dans la cybercriminalité représente une avancée importante

Un autre exemple d'initiative adoptée pour contrer la menace de blanchiment d'argent et de financement du terrorisme associée aux crypto-monnaies est la création d'un groupe de travail sur le sujet au sein

[84] https://www.interpol.int/News-and-media/News/2017/N2017-069.

de Ministère public de la Confédération. Plusieurs ministères publics cantonaux ont également constitué des pools de procureurs spécialisés dans ces questions.

Ces différentes initiatives ont été couronnées à l'été 2018 par la création d'une plateforme nationale de coopération judiciaire et policière, le Cyberboard, réunissant les principaux acteurs de la lutte contre la cybercriminalité en Suisse, soit des représentants de la CCDJP, de la CCPCS, de la Conférence des procureurs suisses (CPS), de fedpol, du Ministère public de la Confédération, de la prévention (PSC), du RNS, du SRC et de l'UPIC. Cette plateforme, de structure modulaire, a pour but de permettre à ces acteurs de travailler ensemble et de coordonner leur action afin de lutter plus efficacement contre la cybercriminalité. En particulier, son premier module, le Cyber-CASE, réunit des procureurs et policiers cantonaux et fédéraux spécialisés en matière de cybercriminalité ainsi que des représentants de MELANI. Actif depuis le 6 juillet 2018, il est chargé de la coordination des cas opérationnels entre les procureurs et les polices des cantons et de la Confédération, ainsi que des échanges d'expériences et de connaissances entre ceux-ci.

De même, la Commission fédérale des maisons de jeux (CFMJ) est attentive à la problématique du blanchiment d'argent par les crypto-assets qui est susceptible de peser sur les casinos. Inexistante jusqu'à présent, une telle menace est susceptible d'apparaître avec la levée de l'interdiction des jeux en ligne, votée par le peuple suisse avec l'approbation de la nouvelle Loi fédérale sur les jeux d'argent, le 10 juin 2018. La surveillance exercée sur de tels jeux en ligne par la Commission fédérale des maisons de jeux déterminera s'il y a lieu de prendre des mesures spécifiques contre une éventuelle utilisation abusive des crypto-monnaies dans ce domaine. Disposant notamment, en vertu de l'art. 76, al. 2 du projet d'ordonnance sur les jeux d'argent (OJAr), actuellement en consultation en vue de son approbation par le Parlement, de la compétence d'interdire certains moyens de paiement, la Commission fédérale des maisons de jeux se réserve la possibilité d'en faire usage à l'égard de certaines crypto-monnaies, si cela s'avère nécessaire.

5. Plateformes de crowdfunding

5.1. Différents types de crowdfunding

Avant même l'apparition des ICOs, des fonds étaient collectés sur Internet par l'intermédiaire de plateformes de crowdfunding. Le crowdfunding désigne le financement d'un projet par une multitude de bailleurs de fonds. L'objectif est de faire financer par un grand nombre de personnes des projets qui seront mis en ligne par des emprunteurs sur une plateforme de crowdfunding. Une telle plateforme est en principe chargée de la gestion du site Internet correspondant ainsi que de la mise en ligne, de la coordination du projet et du rassemblement des bailleurs de fonds et des emprunteurs. En fonction de leur modèle commercial, les plateformes exercent différentes (ou d'autres) activités. Par exemple, de nombreuses plateformes reçoivent et transfèrent des fonds, parfois seulement après l'obtention d'une certaine somme d'argent dans un délai imparti. Si le montant total n'est pas obtenu dans le délai imparti, les plateformes ont généralement une obligation de remboursement envers les bailleurs de fonds. Il existe différentes formes de soutien fourni par le crowdfunding (les définitions et notions peuvent toutefois varier et d'autres termes peuvent au besoin être utilisés):

a) Crowddonating: les bailleurs de fonds mettent une certaine somme à la disposition des emprunteurs sous forme de don sans contrepartie. Ils n'escomptent pas le remboursement du montant versé.

b) Crowdsupporting: les bailleurs de fonds mettent une certaine somme à la disposition des emprunteurs sous forme de don avec une contrepartie symbolique ou de faible valeur (p. ex. exemplaire signé du CD produit). Généralement, ils n'escomptent pas le remboursement du montant versé.

c) Crowdlending (participation aux capitaux de tiers): dans ce type de crowdfunding, les parties conviennent à la fois d'un remboursement des fonds versés et du paiement régulier d'intérêts. En droit privé, il s'agit donc d'un contrat de prêt.

d) Crowdinvesting (mise à disposition de capitaux propres): il s'agit là d'un financement de société dans le cadre duquel des droits de participation et, éventuellement, une participation au résultat sont promis en contrepartie de la remise des fonds.

D'une façon générale, la forme la plus récente d'ICO constitue, elle aussi, un crowdfunding. Les différences tiennent, en pratique, au fait que, 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. Dans la plupart des ICOs, il n'existe aucune plateforme et les bailleurs de fonds versent les fonds directement aux emprunteurs. En outre, le montant est souvent (mais de loin pas systématiquement) reçu en crypto-monnaies.

5.2. Analyse des risques

Comme pour les crypto-assets, il est actuellement difficile d'évaluer le risque représenté par les plateformes de crowdfunding online du point de vue du blanchiment d'argent et du financement du terrorisme, parce que le nombre de cas répertoriés par les autorités suisses est très restreint. Néanmoins, la menace que représentent de telles plateformes est avérée. Elle est constituée par l'anonymat, qui en renforcé par le fait que les plateformes en question opèrent sur Internet. Ainsi, les plateformes de crowdfunding permettent de participer à des projets au-delà des frontières nationales[85].

[85] ADVANCED FINANCIAL CRIME PROFESSIONALS WORLDWIDE (ACAMS), *Financial Institutions and Crowdfunding*, K.M. Veldhuizen-Koeman, 2016, p. 6 et seq., http://files.acams.org/pdfs/2016/Financial_Institutions_and_Crowdfunding_K_Veldhuizen.pdf)

La menace est particulièrement marquée dans le crowddonating. Des fonds peuvent être collectés par des organisations d'utilité publique frauduleuses, sous couvert de l'aide humanitaire, par le biais des réseaux sociaux ou de plateformes officielles de crowdfunding. Comme le montrent plusieurs communications reçues par le MROS, de telles levées de fonds peuvent, comme les ICOs, relever de l'escroquerie aux investisseurs, lorsque le projet pour lequel les fonds sont prétendument levés n'est pas mené à bien et que ses promoteurs s'approprient les donations pour leur compte propre. Néanmoins, la menace principale est que les fonds collectés puissent servir de soutien matériel (billets d'avion, une communication mobile, etc.) pour des combattants terroristes étrangers (*Foreign Terrorist Fighters*) ou de capitaux pour l'exécution d'actes terroristes[86].

Le GAFI explique dans le rapport «Emerging Terrorist Financial Risks» que les bailleurs de fonds ne savent souvent pas quel sera l'usage final des fonds qu'ils ont remis sur les réseaux sociaux (y compris les plateformes de crowdfunding), ce qui constitue un risque dont des organisations terroristes pourraient tirer profit[87]. La menace de financement du terrorisme devrait augmenter à court terme, puisque ces systèmes gagnent en popularité et sont utilisés de plus en plus fréquemment. Certes, les transactions peuvent être suivies, mais identifier l'utilisateur final ou le bénéficiaire réel est difficile lorsque la plateforme de crowdfunding n'a pas d'obligations en matière de KYC. Selon le GAFI, on ne sait pas actuellement avec certitude dans quelle mesure les groupes terroristes et leurs partisans utilisent ces technologies. Le recours aux techniques organisées de crowdfunding constitue un risque émergent de financement du terrorisme. Le crowdfunding court le risque d'être utilisé à des fins illégales, y compris lorsque la finalité indiquée dans le cadre de la campagne de crowdfunding est fausse. Les individus et les organisations qui entendent collecter des fonds pour soutenir le terrorisme et l'extrémisme pourraient affirmer qu'ils s'engagent dans des activités caritatives ou humanitaires légitimes et créer des organisations d'utilité publique à cette fin. Dans une étude de cas basée sur l'exemple du FIU canadien, le GAFI montre que des personnes qui avaient été contrôlées en lien avec des infractions terroristes avaient tenté de quitter le pays à des fins terroristes et avaient utilisé au préalable des sites Internet de crowdfunding pour y parvenir.

L'organisme français Tracfin souligne les risques considérables de financement du terrorisme par le crowddonating. Il décrit aussi un cas dans lequel l'analyse d'une plateforme de crowddonating a révélé que certains flux monétaires provenaient de zones géographiques sensibles et que le montant total donné avait été récolté de façon inhabituellement rapide compte tenu du type de projet financé. Certains des projets lancés sur cette plateforme présentaient manifestement des liens avec des islamistes radicaux[88]. Depuis l'entrée en vigueur de l'ordonnance n°2016-1635 du 1er décembre 2016 renforçant le dispositif français de lutte contre le blanchiment et le financement du terrorisme fin 2016, le statut d'intermédiaire en financement participatif n'est plus facultatif mais obligatoire pour les plateformes de dons, c'est-à-dire les plateformes de crowddonating. Celles-ci doivent désormais respecter les règles relatives à la lutte contre le blanchiment d'argent et le financement du terrorisme[89].

En outre, l'Association of Certified Anti-Money Laundering Specialists (ACAMS) relate un cas dans lequel il est reproché à deux membres d'une campagne de levée des fonds à but caritative française d'avoir financé le terrorisme en Syrie. Le site de la campagne collectait notamment des fonds pour les enfants syriens. Bien que des produits alimentaires et des médicaments aient été envoyés en Syrie, nombre de ces livraisons avaient aussi été utilisées pour faire parvenir de l'argent à des groupes djihadistes. Selon l'ACAMS, le nombre de rapports sur des activités illégales en lien avec le crowdfunding de l'autorité américaine FinCEN est certes encore faible, mais il ne cesse d'augmenter.

---

[86] Cf., sur la question du financement du terrorisme: GAFI, *Emerging Terrorist Financing Risks*, octobre 2015 (http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf).

[87] *Ibid.*, p. 6, 31 *et seq*.

[88] TRACFIN, *Tendances et analyse de risques de blanchiment de capitaux et de financement du terrorisme en 2015*, 2015, https://www.economie.gouv.fr/tracfin/tendances-et-analyse-des-risques-en-2015

[89] Cf. art. L548-2, II et art. L561-2, 4° du code monétaire et financier, https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006072026.

L'examen et l'analyse de ces signalements montre que des plateformes de crowdfunding, en particulier, sont utilisées pour blanchir de l'argent[90].

En Suisse, on ne connaît pas encore de cas d'usage abusif d'une plateforme de crowdfunding. Aucun signalement de ce type n'est parvenu au MROS. Mais cela pourrait aussi tenir au fait que, actuellement, de nombreuses plateformes ne sont pas soumises à la LBA et ne peuvent donc pas faire de signalement. Certaines grandes plateformes de crowddonating et de crowdsupporting exercent sur le marché sans être soumises à la LBA, en examinant toutefois au préalable les projets annoncés et les bailleurs de fonds. Cet état de fait constitue une réelle vulnérabilité de la Suisse à cet égard.

5.3. Facteurs d'atténuation des risques

L'obligation de soumission à la LBA est notamment réglée à l'art. 2, al. 3, LBA, ainsi que dans l'ordonnance sur le blanchiment d'argent (OBA; RS *955.01*). Elle s'applique notamment aux personnes qui, à titre professionnel, acceptent, gardent en dépôt ou aident à placer ou à transférer des valeurs patrimoniales appartenant à des tiers, en particulier des personnes qui fournissent des services dans le domaine du trafic des paiements (art. 2, al. 3, let. b, LBA). On parle notamment de services dans le domaine du trafic des paiements quand l'intermédiaire financier, sur mandat de son cocontractant, transfère des valeurs financières liquides à un tiers et prend lui-même physiquement possession de ces valeurs, les fait créditer sur son propre compte ,ordonne un virement au nom et sur ordre du cocontractant ou exécute une activité de transmission de fonds ou de valeurs (art. 2, al. 3, let. b, LBA, en relation avec l'art. 4 OBA; cf. aussi circulaire 2011/1 de la FINMA, point 58). S'il fournit un service dans le domaine du trafic des paiements et s'il agit à titre professionnel (art. 7 OBA), l'intermédiaire financier est tenu de respecter les obligations de diligence prévues aux art. 3 à 7 LBA.

L'activité de recouvrement de créances n'est pas considérée comme une intermédiation financière. Le recouvrement repose sur un acte juridique bilatéral ou multilatéral qui n'implique généralement pas la personne chargée du recouvrement. Cette dernière encaisse, sur mandat du créancier, des créances échues. Le mandataire agit soit en qualité de représentant direct du créancier, soit en son propre nom à l'égard du débiteur. Soumettre l'activité de recouvrement à la LBA serait le plus souvent sans effet, puisque la société de recouvrement, en l'absence de relation contractuelle avec le débiteur, ne pourrait pas être tenue d'identifier ce dernier en vertu de l'art. 3 LBA[91]. Ce n'est que dans des cas exceptionnels que le mandataire entretient des relations contractuelles à la fois avec le créancier et avec le débiteur de la créance. Ce nonobstant, on peut considérer qu'il existe en pareil cas une activité de recouvrement de créances en se fondant sur le point 9 de la circulaire 2011/1 de la FINMA . Pour cela, il convient d'identifier, sur la base d'indices, la personne ayant émis le mandat d'effectuer le virement ou le transfert. Dans ce cas, la prestation est généralement rémunérée par le mandant.

Dans la mesure où les plateformes de crowdfunding reçoivent généralement des fonds de tiers qu'elles transmettent aux projets à financer, une telle opération constitue, en principe, un service dans le domaine du trafic des paiements soumis à la LBA (cf. art. 2, al. 3, let. b, LBA, en relation avec l'art. 4, al. 1, let. a, OBA). Dans le cadre juridique actuel, il est toutefois possible d'exploiter les plateformes de crowddonating sans autorisation. Les exploitants de plateformes de crowddonating et de crowdsupporting peuvent en effet se fonder sur l'art. 2, al. 2, let. a, ch. 2, OBA pour invoquer l'exception concernant le recouvrement de créances . En Suisse, seules les plateformes de crowdlending et de crowdinvesting (c'est-à-dire celles sur lesquelles les bailleurs de fonds obtiennent des intérêts ou des dividendes) sont actuellement soumises à la loi sur le blanchiment d'argent (art. 2, al. 3, LBA), car elles

[90] ADVANCING FINANCIAL CRIME PROFESSIONALS WORLDWIDE (ACAMS), *Crowdfunding: The New Face of Financial Crime?*, Financial Institutions and Crowdfunding, 2017, p. 14 *et seq*., http://files.acams.org/pdfs/2017/Crowdfunding_The_New_Face_of_Financial_Crimes_S.Sessoms.pdf

[91] Cf. circulaire 2011/1 de la FINMA, point 8; Pratique de l'Autorité de contrôle en matière de lutte contre le blanchiment d'argent relative à l'art. 2, al. 3, LBA du 29 octobre 2008, ch. 4.1, p. 31 (https://www.finma.ch/FinmaArchiv/gwg/d/dokumentationen/publikationen/gwg_auslegung/pdf/59402.pdf), qui a servi de base à l'OIF; ATF 2A.62/2007, considérant 8.

permettent des flux monétaires bilatéraux entre bailleurs de fonds et emprunteurs, le mandat de recouvrement ne pouvant donc pas provenir du seul bailleur de fonds. Les autres plateformes sont généralement conçues de telle façon (en particulier s'agissant de leurs conditions générales et des flux monétaires) qu'elles peuvent invoquer l'exception relative au recouvrement de créances cité à l'art. 2, al. 2, let. a, ch. 2, OBA.

Le 1er août 2017, des simplifications ont été introduites dans l'ordonnance sur les banques (OB) pour les acteurs des marchés financiers, dont le crowdfunding peut aussi largement profiter[92]. Les modifications n'ont toutefois aucune influence sur l'application de la LBA aux plateformes de crowdfunding[93].

[92] «Si l'exploitant d'une plateforme de crowdfunding accepte des avoirs dans un but autre que celui de les transmettre aux responsables du projet dans un délai de 60 jours (un délai maximal de 7 jours ouvrables était autorisé selon la pratique en vigueur avant le 1er août 2017) et que les avoirs en question, pour quelque raison que ce soit, restent donc pendant une période prolongée sur ses comptes (par exemple pour garantir la présence des fonds à l'échéance du délai prescrit pour la récolte des fonds), on considère qu'il s'agit d'une activité soumise à l'obtention préalable d'une autorisation en vertu de la loi sur les banques si elle est exercée à titre professionnel. Depuis le 1er août 2017, aucune autorisation n'est nécessaire dans ce cas pour une activité non exercée à titre professionnel si le montant récolté en vue d'être transmis n'excède pas un million de francs. L'investisseur doit alors être informé avant le virement des fonds sur la plateforme que celle-là n'est pas soumise à la surveillance de la FINMA et que les dépôts ne sont couverts par une garantie» (fiche d'information de la FINMA sur le crowdfunding, état: 1er août 2017).

[93] Commentaires du Département fédéral des finances (DFF) sur la modification de l'ordonnance sur les banques (FinTech) du 5 juillet 2017, ch. 1.1.3.

6. Conclusion / recommandations

6.1. Conclusions de l'analyse des risques liés aux crypto-assets

La menace de blanchiment d'argent et de financement du terrorisme que représentent les crypto-assets est forte, même si le nombre de cas avérés en Suisse est pour l'instant restreint. Elle est constituée par l'anonymat qui entoure les transactions en tokens et se traduit à la fois par l'exploitation criminelle de failles de conception des crypto-monnaies, par des escroqueries aux investisseurs, notamment dans le cadre d'ICOs, par l'utilisation de crypto-monnaies pour les paiements de *ransomwares*. En outre, la menace représentée par les crypto-monnaies s'exprime aussi par leur utilisation à des fins illégales dans des schémas criminels qui existent par ailleurs: financement du terrorisme, blanchiment d'argent issus de la vente de produits et de services illégaux, d'escroquerie sur Internet de type *phishing*, de trafic de stupéfiants, notamment en mains d'organisations criminelles. En raison de leur anonymat, les crypto-monnaies se prêtent particulièrement bien au blanchiment d'argent.

Néanmoins, le nombre de cas avérés d'utilisation de tokens à des fins de blanchiment d'argent en Suisse est peu élevé et il est même nul en matière de financement du terrorisme. Si l'évaluation du risque qu'ils représentent est en conséquence difficile, les vulnérabilités de la Suisse face à la menace qu'ils constituent sont cependant considérables, même si elles ne sont pas spécifiques à la place financière helvétique.

En effet, l'identification des tokens d'origine criminelle et de leurs ayants droit économiques est extrêmement compliquée pour les autorités de poursuite pénale comme pour les intermédiaires financiers qui les traitent, en raison de l'anonymat des transactions en crypto-monnaies. Par ailleurs, un grand nombre de transactions échappe à tout contrôle, en raison de la nature décentralisée des technologies sur lesquelles reposent les crypto-monnaies, qui permettent leur échange et leur conversion de façon anonyme, sans le recours à des intermédiaires financiers et souvent sans qu'il soit possible d'établir depuis quelle juridiction ces transactions sont ordonnées. Un tel constat confirme la responsabilité déterminante qui repose sur les plateformes de négociation entre monnaies fiat et crypto-assets, seuls intermédiaires financiers qui, à l'heure actuelle, semblent en mesure de mettre à exécution, malgré une efficacité relative, leurs devoirs de diligence à l'égard de leurs clients.

Bien que des modifications législatives destinées à diminuer le risque de blanchiment d'argent et de financement du terrorisme que représentent les crypto-monnaies puissent être envisagées[94], les autorités suisses ont su adapter les instruments que leur offre la législation existante. Aussi toutes les sociétés qui fournissent des services d'intermédiation financière dans le domaine des tokens sont soumises à la LBA, même les fournisseurs de *custodian wallets*, les plateformes de négociation décentralisées qui disposent de la possibilité d'intervenir dans les transactions ordonnées par leurs clients et certaines ICOs, que d'autres juridictions ne considèrent pas comme relevant de l'intermédiation financière. Néanmoins, les fournisseurs de *non-custodian wallets* et les plateformes de négociation décentralisées qui n'ont aucune possibilité d'intervenir dans les transactions de leurs clients échappent au dispositif anti-blanchiment. En outre, il semble que tous les intermédiaires financiers actifs dans ce domaine soumis à la LBA ne sont pas également conscients de leurs devoirs de diligence.

De même, les autorités de poursuite pénale s'efforcent de traquer la criminalité qui recourt aux crypto-monnaies avec les instruments à leur disposition. Le plus important est sans doute la coopération internationale et l'entraide judiciaire et policière avec leurs homologues étrangers. Mais la rapidité des transactions qui permet aux tokens d'origine criminelle de passer en quelques secondes et en quelques

[94] Voir à cet égard les recommandations émises par le rapport du Conseil fédéral «Bases juridiques pour la *distributed ledger technology* et la *blockchain* en Suisse», 7 décembre 2018.

clics d'un point à l'autre du globe, sans que les auteurs ne quittent leur ordinateur, rend souvent cette coopération vaine.

En raison de la nature transnationale de la menace de blanchiment d'argent et de financement du terrorisme associée aux crypto-monnaies, les principales mesures qui permettraient de diminuer le risque qui leur est associé – même si son intensité est pour l'instant difficile à évaluer- doivent être coordonnées à l'échelle internationale. À cet égard, l'engagement de la Suisse au sein du GAFI en faveur d'une uniformisation internationale des réglementations imposées aux sociétés actives dans le commerce et les transactions en crypto-assets constitue une réponse adéquate. Sans une telle harmonisation en effet, toute demande de renseignement à l'étranger risque d'être vaine et tout renforcement de la législation helvétique risque de s'avérer contreproductif, incitant simplement les activités nouvelles auxquelles des devoirs de diligence nouveaux seraient imposés, à quitter la Suisse pour d'autres juridictions.

À côté de l'engagement suisse sur la scène internationale, plusieurs initiatives nationales ou cantonales permettent de diminuer, dans la mesure du possible, le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets. La principale est la création, à l'été 2018, d'une plateforme nationale de coordination judiciaire et policière en matière de cybercriminalité, le Cyber Board. Mais les efforts de formation des policiers suisses en matière de cybercriminalité économique, la constitution d'un groupe de travail spécialisé au sein de MPC et de brigades spécialisées dans la cybercriminalité financière au sein des polices cantonales constituent également d'importantes avancées qui, combinées avec l'étroite collaboration judiciaire, policière et administrative entre la Suisse et les États étrangers, forment le meilleur arsenal possible pour faire face à la menace élevée que représentent les crypto-assets en matière de blanchiment d'argent et de financement du terrorisme.

6.2. Conclusions et recommandations relatives à l'analyse des risques liés aux plateformes de crowdfunding

Le risque associé au crowdfunding online est essentiellement un risque de financement du terrorisme. Bien qu'aucun cas de ce type n'ait pour l'instant été répertorié par les autorités helvétiques, la Suisse présente des vulnérabilités à cet égard qu'il pourrait être utile de combler.

La réglementation en vigueur ne tient pas correctement compte des risques observés. Une modification au niveau réglementaire est à étudier, dont le point central serait la soumission explicite des plateformes de crowddonating et de crowdsupporting à la LBA. En l'absence d'une telle modification, les plateformes de collecte de fonds (intermédiaires), contrairement aux plateformes de crowdlending et de crowdinvesting, seraient exclues du champ d'application de la LBA, alors que celles qui collectent des fonds pour elles-mêmes (ICOs) sont aujourd'hui déjà soumises à la LBA dans certaines circonstances (émission de jetons de paiement). Or, dans sa conception même, la LBA se fonde sur la fonction de contrôle des flux monétaires incombant aux intermédiaires. Par ailleurs, si elle n'est pas modifiée, la réglementation actuelle ne permet pas de prévenir le risque de détournement et d'utilisation abusive des fonds collectés.

7. Bibliographie

ADVANCED FINANCIAL CRIME PROFESSIONALS WORLDWIDE (ACAMS), *Financial Institutions and Crowdfunding*, K.M. Veldhuizen-Koeman, 2016, http://files.acams.org/pdfs/2016/Financial_Institutions_and_Crowdfunding_K_Veldhuizen.pdf).

ADVANCING FINANCIAL CRIME PROFESSIONALS WORLDWIDE (ACAMS), *Crowdfunding: The New Face of Financial Crime?*, Financial Institutions and Crowdfunding, 2017, p. 14 ss, http://files.acams.org/pdfs/2017/Crowdfunding_The_New_Face_of_Financial_Crimes_S.Sessoms.pdf.

AL JAWAHERI Husam, AL SABAH Mashael, BOSHMAF Yazan et ERBAD Aiman, «When a small leak sinks a great ship: deanonymizing Tor hidden service users throught bitcoin transactions analysis», dans *arXiv*: 1801.07501v2, avril 2018, https://arxiv.org/abs/1801.07501.

ANONYME, «Singapour: les premiers billets Bitcoins visent à favoriser l'adoption de l'actif», dans *Crypto-France.com*, https://www.crypto-france.com/singapour-premiers-billets-bitcoin/.

ANONYME, «Ils minaient des bitcoins dans un centre nucléaire», dans *La Tribune de Genève*, 10 février 2018, https://www.tdg.ch/faits-divers/Ils-minaient-des-bitcoins-dans-un-centre-nucleaire/story/30448246.

ANONYME, «Bitcoin Gold: une attaque double dépense fait perdre plusieurs millions de dollars à des plateformes d'échange», dans Crypto-France, https://www.crypto-france.com/bitcoin-gold-attaque-double-depense-pertes-millions-dollars-plateformes-echange/.

ANONYME, «670 millions de dollars de crypto-monnaies ont été dérobés au cours du premier trimestre 2018», dans *Crypto-France.com*, avril 2018, https://www.crypto-france.com/670-millions-dollars-crypto-monnaies-voles-premier-trimestre-2018/.

ANONYME, «Cryptomonnaie: la plateforme japonaise Coincheck victime d'un vol record», 29 janvier 2018, http://www.rfi.fr/economie/20180129-coincheck-vol-cryptomonnaie-injonction-japon.

ANONYME, «Coincheck: les pirates servaient déjà parvenus à blanchir 40% des 500 millions de XEMs dérobés», https://www.crypto-france.com/coincheck-pirates-blanchiment-xems/.

BRANTLY Aaron, «Financing Terror Bit by Bit», dans *CTC Sentinel*, vol. 7, n° 10, octobre 2014, p. 4, https://ctc.usma.edu/financing-terror-bit-by-bit/.

Code monétaire et financier français, version consolidée au 1er octobre 2018, https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006072026.

Conseil fédéral, *Rapport du Conseil fédéral sur les monnaies virtuelles en réponse aux postulats Schwab (13.3687) et Weibel (13.4070),* 25 juin 2014, https://www.news.admin.ch/NSBSubscriber/message/attachments/35353.pdf.

Conseil fédéral, *Bases juridiques pour la distributed ledger technology et la blockchain en Suisse*, 7 décembre 2018. Disponible sur : www.admin.ch > Documentation > Communiqués > communiqué du 14 décembre 2018 (Etat au 14.12.2018).

DE PREUX Pascal et TRAJILOVIC Daniel, «Blockchain et lutte contre le blanchiment d'argent. Le nouveau paradoxe?», dans *Resolution LP*, https://resolution-lp.ch/wp-content/uploads/2018/02/064_L_14_De_Preux_Trajilovic.pdf.

European Parliament, *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*, mai 2018, http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf;

EUROPOL, *2017 Virtual Currencies Money Laundering Typologies*, 2017.

FANUSIE Yaya et ROBINSON, Tom, *Bitcoin laundering: an analysis of illicit flows into digital currency services*, Center on Sanctions & Illicit Finance et ELLIPTIC, 12 janvier 2018.

FARINE Mathilde, «Comment investir dans les cryptomonnaies», dans *Le Temps*, 22 juillet 2018, https://www.letemps.ch/economie/investir-cryptomonnaies.

FARINE Mathilde, «La Finma enquête sur une ICO à 100 millions de francs», dans *Le Temps*, 26 juillet 2018, https://www.letemps.ch/economie/finma-enquete-une-ico-100-millions-francs.

FAUCETTE James, GRASECK Betsy et SHAH Sheena, *Update: Bitcoin, Cryptocurrencies and Blockchain*, Morgan Stanley, 1er juin 2018, p. 35, https://www.macrobusiness.com.au/wp-content/uploads/2018/06/82012860.pdf

FINMA, Communiqué de presse de la FINMA du 19 septembre 2017, https://www.finma.ch/fr/news/2017/09/20170919-mm-coin-anbieter/.

FINMA, Communiqué de presse du 26 juillet 2018, https://www.finma.ch/fr/news/2018/07/20180726-mm-envion/?pk_campaign=News-Service&pk_kwd=La%20FINMA%20ouvre%20une%20proc%C3%A9dure%20%C3%A0%20l%27encontre%20d%27un%20%C3%A9metteur%20d%27ICO

GAFI, *National Money Laundering and Terrorist Financing Risk Assessment*, 2013, http://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf.

GAFI, *Virtual Currencies. Key Definitions and Potential AML/CFT Risks*, juin 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

GAFI, *Virtual currencies. Guidance for a risk-based approach*, 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf.

GAFI, *FATF Fintech & RegTech Initiative*, http://www.fatf-gafi.org/fintech-regtech/?hf=10&b=0&s=desc(fatf_releasedate).

GARESSUS Emmanuel, «Une société suisse veut émettre des billets de bitcoins», dans *Le Temps*, 8 mai 2018, https://www.letemps.ch/economie/une-societe-suisse-veut-emettre-billets-bitcoins

GCBF, *Rapport sur l'utilisation du numéraire et les risques inhérents d'utilisation abusive pour le blanchiment d'argent et le financement du terrorisme en Suisse, octobre 2018.* Publication prévue le 18 décembre 2018. Après publication disponible sur : www.admin.ch > Documentation > Communiqués > communiqué du 18 décembre 2018.

GRÜNEWALD Seraina, «Währungs- und geldwäschereirechtliche Fragen bei virtuellen Währungen», dans Rolf H. Weber *et. al* (Hrsg.), *Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme*, ZIK Bd. 61, Zürich/Basel/Genf 2015.

HAEDERLI Alexandre et STÄUBLE Mario, «De la drogue livrée en courrier A. Comment fonctionne le marché des stupéfiants sur le Darknet», dans *La Tribune de Genève*, 02.05.2018, https://www.tdg.ch/extern/interactive_wch/darknet/.

HESS Martin et SPIELMANN Patrick, «Cryptocurrencies, Blockchain. Handelsplätze & Co. – Digitalisierte Werte unter Schweizer Recht», in: Reutter, Thomas U. / Werlen, Thomas (Hrsg.): Kapitalmarkt – Recht und Transaktionen XII. Zürich: Schulthess 2017, p. 154.

HILEMAN Garrick et RAUCHS Michel, *Global Cryptocurrency Benchmarking Study*, Cambridge, Center for Alternative Finance/University of Cambridge, 2017.

HM Treasury et Home Office, *National risk assessment of money laundering and terrorist financing 2017*, Londres, 2017, p. 38,

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf.

IRWIN Angela S.M. et MILAD, George, «The use of crypto-currencies in funding violent jihad», dans *Journal of Money Laundering Control*, vol. 19, n°4, 2016, p. 410 et 411.

Koos Couvée, «European Traffickers Pay Colombian Cartels Through Bitcoin ATMs: Europol Official», dans ACAMS Moneylaundering.com, 28 février 2018, https://www.moneylaundering.com/news/european-traffickers-pay-colombian-cartels-through-bitcoin-atms-europol-official/.

LOUBIRE Paul, «La très longue liste de vols de bitcoins par des hackers», dans *Challenges*, 8 Décembre 2017, https://www.challenges.fr/finance-et-marche/la-tres-longue-liste-de-vols-de-bitcoins-par-des-hackers_518541.

MEISSER Luzius, «Kryptowährungen: Geschichte, Funktionsweise, Potential», dans WEBER Rolf H. *et al* (Hrsg.), Rechtliche Herausforderung durch webbasierte und mobile Zahlungssysteme, ZIK Bd. 61, Zürich/Basel/Genf 2015.

SANSONETTI Riccardo, « Le bitcoin : opportunités et risques d'une monnaie virtuelle », dans La Vie économique, 9-2014, p. 44-46.

SUBERG William, «Bitcoin Exchange ShapeShift Helps Police As WannaCry Attacker Converts To Monero», dans https://cointelegraph.com/news/bitcoin-exchange-shapeshift-helps-police-as-wannacry-attacker-converts-to-monero.

TRACFIN, *Tendances et analyse de risques de blanchiment de capitaux et de financement du terrorisme en 2015*, 2015, https://www.economie.gouv.fr/files/TRACFIN_analyse_2015.pdf.

TZANETAKIS Meropi, «Comparing cryptomarkets for drugs: a characterisation of sellers and buyers over time», dans *International Journal of Drug Policy*, vol. 56, juin 2018, p. 176 à 186.

U.S. Department of Justice and Drug Enforcement Administration, *2017 National Drug Threat Assesment*, octobre 2017.

US Securities and Exchange Commission, https://www.sec.gov/news/statements.

WILE Rob, «Supporter Of Extremist Group ISIS Explains How Bitcoin Could Be Used To Fund Jihad», in *Business Insider Australia*, 8 juillet 2014, https://www.businessinsider.com.au/isis-supporter-outlines-how-to-support-terror-group-with-bitcoin-2014-7.