La conformité anti-blanchiment face aux crypto-actifs

Solène Clément, Juliette Lelieur

Dans Revue de science criminelle et de droit pénal comparé 2021/1 N° 1 , pages 15 à 27
Éditions Dalloz

ISSN 0035-1733
ISBN 9782995521012
DOI 10.3917/rsc.2101.0015
Date de mise en ligne : 14/07/2021

Le succès des « cryptomonnaies » ou « crypto-actifs » auprès du monde des affaires comme du grand public n'est plus à démontrer. Ces nouveaux instruments financiers reposant sur la technologie blockchain génèrent toutefois des inquiétudes en rapport avec leur réputation de monnaie du crime et en raison des opérations de blanchiment de capitaux qu'elles peuvent favoriser. Le GAFI et l'Union européenne ont adapté leur dispositif de prévention du blanchiment. Depuis la loi PACTE du 22 mai 2019, complétée par l'ordonnance du 9 décembre 2020, le droit français comporte un système normatif complet d'assujettissement des professionnels du secteur des crypto-actifs aux obligations de prévention du blanchiment. Le présent article analyse les risques de blanchiment à partir de la blockchain au regard de la définition pénale du blanchiment, puis met en perspective les deux régimes d'assujettissement des professionnels du secteur. Il étudie enfin les difficultés de mise en œuvre de l'obligation d'identification du client dans le contexte cryptographique, face aux tentatives de reconquête technologique de l'anonymat.

La conformité anti-blanchiment face aux crypto-actifs

Solène **Clément**
Avocate, présidente de l'Observatoire de la lutte anti blanchiment et contre le financement du terrorisme (OLAB)
Juliette **Lelieur**[1]
Professeure de droit pénal à l'Université de Strasbourg, UMR DRES (7354)

There is no longer any doubt that "cryptocurrencies", or "crypto-assets", are a huge success, not only in the business world but also with the general public. These blockchain-based financial instruments raise concerns about their use by criminals, however, and in particular their ability to facilitate money laundering. The FATF and the European Union have therefore updated their money-laundering prevention laws and France passed the PACTE Act (May 22, 2019) and issued an order (December 9, 2020) which requires crypto-asset industry professionals to combat money laundering. This article analyzes the possibility that the French Penal Code definition

(1) Les auteures remercient Alexandre Ultré pour ses explications techniques relatives à la technologie de la *blockchain* et ses rapports avec l'anonymat (v. en particulier la troisième partie de l'article).

of money laundering does not prohibit blockchain from being used in money laundering operations. It then compares the two regimes applicable to crypto-asset industry professionals : some are required to follow anti-money laundering procedures while others are not. It ends with a review of the problems industry professionals encounter when trying to satisfy the know-your-customer obligations given the continuing technological efforts to maintain anonymity.

Si la création des premières cryptomonnaies – ou monnaies cryptographiques – remonte au tournant du millénaire, leur généralisation en tant que mode de paiement et d'investissement est plus récente. C'est au début des années 2010 que notre société prend conscience de l'existence d'un nouvel instrument financier, qui se distingue des précédents par son support numérique – la *blockchain*[2] – et son indépendance par rapport à toute organisation de type étatique[3].

Simultanément, un nouveau terreau pour le blanchiment de capitaux voit le jour[4]. Réputées pour leur capacité à garantir l'anonymat de leurs utilisateurs, les cryptomonnaies acquièrent rapidement une renommée sulfureuse. *De facto*, elles supportent de nombreux échanges illicites : trafic de stupéfiants et d'armes, transactions liées à la cybercriminalité ou à la pédophilie, marchés noirs de toute espèce… Même le *bitcoin*, la plus répandue et respectée d'entre elles[5], peine à se détacher de son image de « monnaie des truands ». On cite souvent l'exemple de Silkroad, un marché en ligne fermé en 2013 par le FBI parce qu'il servait de plaque tournante aux trafiquants de drogue. Or Silkroad imposait l'utilisation du *bitcoin* pour toutes les transactions passant par son intermédiaire[6]. Quant aux nombreuses autres cryptomonnaies (ether, ripple, litecoin, IOTA, dash, dogecoin, peercoin, monero, etc.)[7], leur caractère plus ou moins opaque suscite d'importants doutes quant à l'honnêteté des échanges qu'elles véhiculent. Dans le même temps, ces cryptomonnaies suscitent la convoitise et constituent également la cible d'appropriation frauduleuse par des tiers au moyen de *cryptojacking*[8] ou

(2) Depuis l'Ord. n° 2016-520 du 28 avr. 2016, l'art. L. 223-12 du code monétaire et financier (ci-après C. mon. fin.) évoque la *blockchain* en tant que « dispositif d'enregistrement électronique partagé permettant l'authentification [*d'*] opérations ». Pour une analyse approfondie de la *blockchain*, v. Ph. Rodriguez, *La Révolution Blockchain. Algorithmes ou institutions, à qui donnerez-vous votre confiance ?*, Dunod, 2017 ; Primavera de Filippi, *Blockchains et cryptomonnaies*, Paris, PUF, coll. « Que sais-je ? », n° 4141, 2018. F. Marmoz (dir.), *Blockchain et droit*, Paris, Dalloz, coll. « Thèmes et commentaires », 2019.

(3) En 2018 toutefois, les premières cryptomonnaies étatiques sont créées (par les Iles Marshall et le Venezuela).

(4) Comme le souligne Y. Muller-Lagarde, La dimension criminelle des cryptomonnaies est quasi concomitante à leur apparition, *in* Cryptomonnaies et LCB-FT : état des lieux, *Revue Internationale de la Compliance et de l'Éthique des Affaires* n° 1, févr. 2020. Étude 37 ; v. égal. A. Elkahwagy, La délinquance économique à l'heure du numérique : Bitcoin, blanchiment et autres observations, Arch. Polit. Crim. 2017, n° 39, p. 55-66.

(5) Le *bitcoin* a été créé en janvier 2009. En moins de dix ans, il est devenu une monnaie d'échange mondiale avant que son cours, qui a prodigieusement augmenté jusqu'en déc. 2017, s'effondre précipitamment. Loin d'être réservé aux activités criminelles, le *bitcoin* est apprécié des jeunes générations comme instrument de placement financier. Il sert d'instrument courant de paiement au Japon (où il a cours légal) et en Corée du Sud. Pour une étude approfondie, v. A. Takkal Bataille et J. Favier, *Bitcoin : la monnaie acéphale*, CNRS Éditions, 2017.

(6) V. égal. Bitcoin et darknet, les nouveaux outils des dealers européens, Euraktiv.fr, 1er déc. 2017 https://www.euractiv.fr/section/economie/news/bitcoin-et-darknet-les-nouveaux-outils-des-dealers-europeens/

(7) Qu'on appelle encore *altcoin* (alternatives au bitcoin). On compterait près de 1 600 cryptomonnaies dans le monde. (https://masterthecrypto.com/breakdown-of-cryptocurrency-market/?lang=fr)

(8) « Utilisation clandestine de la puissance de calcul d'un ordinateur afin de "miner" des crypto-actifs au bénéfice exclusif du cybercriminel », définition par J. Martinon, Crypto-actifs : la justice pénale à l'épreuve des cryptomonnaies, Dalloz IP/IT 2019. 531 ; v. aussi W. O'Rorke, La mise en œuvre des obligations de LCB-FT par l'industrie « crypto », Revue Internationale de la Compliance et de l'Éthique des Affaires, févr. 2020. Étude 39.

de cyberattaque contre des plateformes d'échange [9].

La réaction des États ne pouvait se faire attendre. Face à un phénomène dépassant les frontières, elle devait être coordonnée au niveau international. En 2014, le Groupe d'action financière (GAFI) publie un rapport entièrement dédié aux risques de blanchiment par le biais des cryptomonnaies – ou monnaies virtuelles selon sa terminologie [10]. L'année suivante, il émet des lignes directrices relatives à l'approche par les risques appliquée aux monnaies virtuelles [11]. Toutefois, l'actualisation des fameuses 40 Recommandations s'est fait attendre jusqu'en octobre 2018. La Recommandation nº 15, consacrée aux nouvelles technologies, suggère désormais aux États de s'assurer que les fournisseurs d'accès à des « actifs virtuels », notion plus large que celle de monnaie cryptographique ou virtuelle [12], soient assujettis à la législation sur la lutte contre le blanchiment et le financement du terrorisme (ci-après « LAB/FT »), qu'ils soient agréés ou enregistrés, ainsi que soumis à des systèmes efficaces de suivi et de mise en conformité avec les préconisations des Recommandations du GAFI. Enfin, sont publiées en juin 2019 des lignes directrices relatives à l'approche par les risques appliquée aux « actifs virtuels et les prestataires de service sur actif virtuel » [13], les « monnaies virtuelles » de 2014 faisant dorénavant place aux « actifs virtuels ».

Au niveau européen, l'adaptation du dispositif de prévention du blanchiment aux nouvelles réalités virtuelles s'est opérée par la directive 2018/843 du 30 mai 2018, relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme. La « 5e directive anti-blanchiment » limite toutefois son champ d'application aux cryptomonnaies, qu'elle a le mérite de définir [14]. Elle n'évoque pas la notion d'actifs virtuels ou numériques.

Enfin, en France, l'ordonnance nº 2016-1635 du 1er décembre 2016 [15] ajoute à la liste des professionnels assujettis au dispositif de prévention du blanchiment ceux qui, à titre de profession habituelle, interviennent en vue de l'acquisition ou de la vente de cryptomonnaies [16]. L'année suivante, dans son rapport « Tendances et analyses des risques de blanchiments de capitaux et de financement du terrorisme en 2017 et 2018 », la cellule de renseignement financier TRACFIN choisit le terme « crypto-actifs » et développe les risques LAB-FT associés. Puis les règles françaises sont révisées au regard de la Recommandation nº 15 du GAFI, notamment pour introduire la notion de crypto-actif. La loi nº 2019-486 du 22 mai 2019 relative à la croissance et à la transformation des entreprises, plus connue sous le nom de « loi PACTE », procède ainsi à un certain nombre d'ajustements, qui sont complétés par des dispositions décré-

(9) J. Martinon, Phénomènes criminels célèbres ou exotiques dans le champ des crypto-actifs, Dalloz IP/IT 2019. 534.

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

(11) *Guidance for a risk-based approach. Virtual Currencies,* https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

(12) V. le glossaire du GAFI, qui s'est vu complété des définitions des termes *virtual asset* (actif virtuel) et *virtual asset service provider* (prestataire de service d'actif virtuel).

(13) *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,* June 2019, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html

(14) L'art. 1er pt 2 d) de la directive définit les cryptomonnaies comme des « représentations numériques d'une valeur qui ne sont émises ou garanties ni par une banque centrale ni par une autorité publique, qui ne sont pas nécessairement liées non plus à une monnaie établie légalement et qui ne possèdent pas le statut juridique de monnaie ou d'argent, mais qui sont acceptées comme moyen d'échange par des personnes physiques ou morales et qui peuvent être transférées, stockées et échangées par voie électronique ».

(15) Ordonnance renforçant le dispositif français de lutte contre le blanchiment et le financement du terrorisme. Hélène Lefebvre, Simon Polrot et Charles Abitbol, Blockchain : premier(s) pas vers la réglementation des « cryptomonnaies » et autres actifs numériques, JCP E 2017, nº 19, 1255.

(16) C. mon. fin., ancien art. L. 561-2, 7° *bis.*

tales. L'ordonnance n° 2020-1544 du 9 décembre 2020 renforçant le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme applicable aux actifs numériques fait finalement évoluer le régime juridique mis en place par la loi PACTE.

Cette étude a pour objectif d'analyser comment les règles de lutte contre le blanchiment d'argent et le financement du terrorisme, que les professionnels concernés doivent traduire dans leur dispositif de conformité, s'adaptent aux évolutions financières liées à la cryptographie. À cette fin, il convient d'abord de présenter les risques posés par cette nouvelle technologie en termes de blanchiment de capitaux. Cette première étape fait émerger la notion de crypto-actif ou actif numérique, qui dépasse celle de cryptomonnaie (**I**). La détermination des professionnels assujettis au dispositif de prévention du blanchiment constitue par ailleurs un enjeu majeur, car elle définit le champ d'application des règles de conformité (**II**). Enfin, la mise en œuvre par les professionnels assujettis des obligations de vigilance, en particulier de l'obligation d'identification du client, prend une dimension particulière dans le contexte cryptographique (**III**).

I - Le blanchiment des crypto-actifs

Si le GAFI et le législateur français ont préféré le terme de crypto-actif à celui de cryptomonnaie, c'est que les modes opératoires pour blanchir des fonds à partir de la technologie de la cryptographie dépassent l'utilisation des cryptomonnaies (**A**). Comme ces modes opératoires répondent dans leur ensemble à la définition juridique du blanchiment de capitaux, ils justifient l'extension du dispositif de prévention à tous les crypto-actifs (**B**).

A - Les modes opératoires de blanchiment à partir de la cryptographie

Par une opération de blanchiment, un agent entend dissimuler l'origine de fonds provenant d'une activité criminelle pour leur donner une apparence légale, afin de pouvoir les utiliser sans attirer l'attention des autorités. Blanchir de l'argent à partir d'une cryptomonnaie est techniquement simple pour qui manipule aisément internet (**1**). Si l'utilisation de jetons numériques requiert une étape supplémentaire dans le processus de blanchiment, elle reste largement accessible d'un point de vue technique et peu contraignante d'un point de vue pratique (**2**).

1 - Exemple de blanchiment à partir d'une cryptomonnaie

Une illustration classique est celle d'un trafiquant de stupéfiants en possession d'une somme importante d'argent de source délictueuse, qu'il veut investir dans l'économie légale. Par exemple, il souhaite s'acheter un immeuble dans une capitale européenne, Paris.

Afin de blanchir les fonds en cause, le trafiquant achète des valeurs dans une ou plusieurs cryptomonnaie(s) de son choix, à partir d'une plateforme d'échange hébergée dans n'importe quel État du monde. L'achat se fait par le biais d'un virement bancaire, en utilisant un compte sur lequel auront été dépo-

sés les fonds provenant des activités délictueuses. Par précaution, ce compte ne laisse pas apparaître le nom du trafiquant mais se rattache à une société-écran ou un prête-nom. La somme investie en cryptomonnaie est ensuite reconvertie en euros et transférée sur le compte bancaire d'une société française qui ne présente aucun signe de reconnaissance par rapport au précédent compte. Derrière la société française, on trouve comme actionnaire principal le trafiquant en tant que personne physique ou une personne morale, qui a elle-même comme actionnaire principal le trafiquant ou un prête-nom.

Ainsi, le simple fait de convertir une devise en cryptomonnaie(s) puis de reconvertir les valeurs cryptographiques dans la monnaie valant cours dans le pays choisi pour l'investissement final est très efficace pour dissimuler l'origine illégale des fonds.

2 - Exemple de blanchiment à partir d'un crypto-actif non monétaire

S'agissant des levées de fonds en crypto-actifs *(Initial coin offering* ou « *ICO* »*)*, l'accession à la qualité d'investisseur permet à ce dernier de devenir porteur de jetons. Une fois l'opération d'investissement effectivement réalisée, la justification de l'origine des fonds se rapporte à cet investissement heureux dans un projet financé par la levée de fonds.

L'analyse des déclarations de soupçon relatives aux crypto-actifs révèle majoritairement des cas d'escroquerie – qu'elles soient simples, de type *blockchain* fictive, ou subtiles telles des opérations de manipulation de cours ou des escroqueries de type Ponzi. C'est pourquoi TRACFIN conclut qu'« en ce sens, les *blockchains* ne créent pas véritablement de nouvelles méthodes d'escroquerie mais offrent un nouveau champ d'application pour les méthodes éprouvées » [17].

B - L'application du dispositif anti-blanchiment à l'ensemble des crypto-actifs

La définition juridique du blanchiment d'argent est donnée par l'article 324-1 du code pénal. Selon l'alinéa 1er de cette disposition, « le blanchiment est le fait de faciliter, par tout moyen, la justification mensongère de l'origine des biens ou des revenus de l'auteur d'un crime ou d'un délit ayant procuré à celui-ci un profit direct ou indirect ». Selon son 2e alinéa, « constitue également un blanchiment le fait d'apporter un concours à une opération de placement, de dissimulation ou de conversion du produit direct ou indirect d'un crime ou d'un délit ». Le code pénal ne se réfère ni à la notion de monnaie, ni à la notion d'actif. Les termes employés sont ceux de biens, de revenus et de produit (d'un crime ou d'un délit). Il est donc nécessaire de vérifier si les cryptomonnaies et, plus généralement, les crypto-actifs, entrent dans ces catégories juridiques permettant de qualifier une opération de blanchiment.

Le code monétaire et financier ne définit pas la notion de monnaie. Il suggère uniquement que les cryptomonnaies, qu'il évoque en son article L. 54-10-1 [18]

(17) Rapport « Tendance et Analyse des risques de blanchiments de capitaux et de financement du terrorisme en 2016 », p. 63.

(18) C. mon. fin., art. L. 54-10-1, 2° : « Toute représentation numérique d'une valeur qui n'est pas émise ou garantie par une banque centrale ou par une autorité publique, qui n'est pas nécessairement attachée à une monnaie ayant cours légal et qui ne possède pas le statut juridique d'une monnaie, mais qui est acceptée par des personnes physiques ou morales comme un moyen d'échange et qui peut être transférée, stockée ou échangée électroniquement ». Cette définition découle de l'art. 1er pt 2 d) de la directive 2018/843 du 30 mai 2018.

depuis la loi « PACTE » du 22 mai 2019, ne sont pas des monnaies. Toutefois, ce code intègre les cryptomonnaies dans la catégorie plus large des « actifs numériques » ou crypto-actifs [19], en écho à la notion d'actif virtuel développée au sein du GAFI [20]. Ces crypto-actifs se composent, à côté des cryptomonnaies, de jetons représentant un droit sous une forme numérique. Le code monétaire et financier définit le jeton comme un « bien incorporel » [21], permettant ainsi la qualification juridique de blanchiment de s'appliquer. En revanche, la loi ne définit pas à proprement parler les « actifs numériques ». Aussi la question de savoir si une cryptomonnaie ou « représentation numérique d'une valeur » répond, en tant qu'actif numérique, à la définition du « bien » n'est-elle pas définitivement tranchée [22].

Une cryptomonnaie pourrait néanmoins constituer un « revenu » ou un « produit » au sens de l'article 324-1 du code pénal. L'article L. 54-10-1, 2° du code monétaire et financier précise en effet qu'une cryptomonnaie est « acceptée par des personnes physiques ou morales comme un moyen d'échange ». Cet élément permet de retenir la qualification de revenu ou de produit.

Il résulte de cette brève analyse que l'ensemble des crypto-actifs s'intègrent dans les qualifications juridiques définissant le blanchiment d'argent. Il est donc pleinement justifié d'étendre le dispositif de prévention du blanchiment aux crypto-actifs, ce qui suppose avant tout d'assujettir à ce dispositif l'ensemble des professionnels impliqués dans leur création et leur utilisation.

II - Le champ d'application de la réglementation LAB-FT

Historiquement créée pour les professions financières, la réglementation LAB-FT impulsée par le GAFI n'a cessé d'étendre son champ d'application à de nouveaux secteurs professionnels. Sont ainsi concernés, outre le secteur bancaire, financier ou des assurances, de nombreuses professions « non financières » telles les professions juridiques (notaires, avocats, etc.), le secteur de l'immobilier, les casinos, les bijoutiers, les professionnels de l'art ou encore les agents sportifs. Aujourd'hui, la liste des professionnels assujettis est longue de dix-neuf catégories de professions recensées à l'article L. 561-2 du code monétaire et financier.

Succédant à une première ébauche d'assujettissement des professionnels des cryptomonnaies par l'ordonnance du 1er décembre 2016, la loi du 22 mai 2019 prend en compte la nature des acteurs de l'écosystème *blockchain* pour créer deux régimes distincts d'assujettissement (**A**) et mobilise des institutions différentes pour le contrôle et la sanction (**B**).

A - La dichotomie des régimes d'assujettissement

La réglementation LAB-FT innove à propos des professionnels du secteur des crypto-actifs en ce qu'elle prévoit

(19) C. mon. fin., art. L. 54-10-1.

(20) Le glossaire du GAFI définit l'actif virtuel : "*A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes*".

(21) V. C. mon. fin., art. L. 54-10-1, 1°, renvoyant à l'art. L. 552-2 : « Au sens du présent chapitre, constitue un jeton tout bien incorporel représentant, sous forme numérique, un ou plusieurs droits pouvant être émis, inscrits, conservés ou transférés au moyen d'un dispositif d'enregistrement électronique partagé permettant d'identifier, directement ou indirectement, le propriétaire dudit bien ».

(22) V. A. Le Teurnier, Crypto-actifs et droit pénal. Un objet juridique non identifié au service de la criminalité financière et organisée, AJ pénal 2020. 506.

pour la première fois deux régimes d'assujettissement. Le premier est de plein droit, c'est-à-dire qu'il s'applique sans condition préalable, obligatoirement (**1**). Le second est optionnel : certains professionnels du secteur des actifs numériques ne sont en effet assujettis à la réglementation LAB-FT que s'ils ont requis un agrément auprès de l'Autorité des marchés financiers (ci-après « AMF ») pour exercer leur activité (**2**).

1 - L'assujettissement de plein droit

Depuis la loi PACTE, l'article L. 561-2 du code monétaire et financier comporte, à la suite de l'alinéa 7° relatif aux changeurs manuels, les alinéas 7° *bis*, 7° *ter* et 7° *quater*[23], tous trois relatifs aux « prestataires de service sur actifs numériques » (PSAN). Le périmètre de l'alinéa 7° *bis* a été étendu par l'ordonnance du 9 décembre 2020, qui lui ajoute deux catégories de prestataires[24]. Il en résulte que sont désormais obligatoirement assujettis les prestataires de quatre catégories de services : le service de conservation, pour le compte de tiers, d'actifs numériques ou d'accès à des actifs numériques, le cas échéant sous la forme de clés cryptographiques privées, [...] ; le service d'achat d'actifs numériques à partir d'une monnaie fiduciaire, ou de revente de ces actifs contre une telle monnaie ; le service d'échange d'actifs numériques contre d'autres actifs numériques, encore appelé échange « crypto-to-crypto » ; enfin, l'exploitation d'une plateforme de négociation d'actifs numériques.

La définition de la première catégorie de prestataires, relative au service de conservation, suscite une difficulté au regard du texte de la 5e directive anti-blanchiment. Celle-ci prévoit d'assujettir à la réglementation LAB-FT les « prestataire[s] de services de portefeuille[25] de conservation » (*custodian wallet providers*), définis comme des « entité[s] fournissant des services de conservation de clés cryptographiques privées pour le compte de ses clients à des fins de détention, de stockage et de transfert de monnaies virtuelles ». Or, bien que transposant la 5e directive, la loi PACTE n'a pas entièrement repris la définition donnée par le texte européen. Elle lui a retiré la notion de « portefeuille » pour retenir la formule « prestataire de services de conservation pour le compte de tiers d'actifs numériques ou d'accès à des actifs numériques, le cas échéant sous la forme de clés cryptographiques privées, en vue de détenir, stocker et transférer des actifs numériques ». Se posait alors la question de savoir si les entités qui ne fournissent qu'une technologie permettant de stocker des actifs ou des clés, mais sans les contrôler elles-mêmes, étaient assujetties. Dans l'affirmative, cela revenait « à imposer des règles de lutte contre le blanchiment à un fabricant de porte-monnaie au motif que les porte-monnaie permettent d'utiliser des pièces »[26]. Le décret n° 2019-1213 du 21 novembre 2019 a cependant défini chaque service à l'article D. 54-10-1 du code monétaire et financier. La rédaction du premier alinéa réintègre, sans toutefois la nommer expressément, la notion de « portefeuille » en assujettissant les entités proposant le service d'accès, pour le compte de tiers, actifs

(23) L'art. L. 561-2, 7° *bis* du C. mon. fin. vise « les prestataires des services mentionnés aux 1° et 2° de l'article L. 54-10-2 ». L'art. L. 561-2, 7° *ter* concerne « les émetteurs de jetons ayant obtenu le visa mentionné à l'article L. 552-4 dans le cadre de l'offre ayant fait l'objet du visa et dans la limite des transactions avec les souscripteurs prenant part à cette offre ». L'art. L. 561-2, 7° *quater* est relatif aux « prestataires agréés au titre de l'article L. 54-10-5, à l'exception des prestataires mentionnés au 7° *bis* du présent article ».
(24) Il s'agit des alinéas 3° et 4° de l'art. L. 54-10-2 du C. mon. fin.
(25) Ce sont les auteures qui soulignent.
(26) Député Person, Commission spéciale chargée d'examiner le projet de loi relatif à la croissance et la transformation des entreprises, 6 mars 2019, séance de 22 heures, Compte rendu n° 30.

numériques, cumulé à la tenue d'un registre de positions, ouvert au nom du tiers. Au regard de cette définition, qu'on aurait préféré trouver dans le texte légal, la difficulté semble résolue.

L'assujettissement de plein droit entraîne l'obligation pour les professionnels concernés de demander leur enregistrement à l'Autorité des marchés financiers, qui doit recueillir l'avis conforme de l'Autorité de contrôle prudentiel et de résolution (ci-après « ACPR ») avant de procéder à l'enregistrement. De la même manière, la radiation de ces professionnels est décidée par l'AMF sur avis conforme de l'ACPR.

Une fois n'est pas coutume, les autorités françaises avaient devancé les instances internationales. Dès 2014, l'ACPR posait pour principe que « l'activité d'intermédiation consistant à recevoir des fonds de l'acheteur de *bitcoins* pour les transférer au vendeur de *bitcoins* [*relevait*] de la fourniture de services de paiement », qu'ainsi elle « [*impliquait*] de disposer d'un agrément ». Cet agrément était délivré à certaines conditions, notamment celle de mettre en place « un dispositif de contrôle interne et des mesures de vigilance en matière de lutte contre le blanchiment et le financement du terrorisme »[27]. La loi PACTE a entériné cette position en opérant un simple changement sémantique puisqu'elle prévoit l'« enregistrement » des assujettis de plein droit « avant d'exercer leur activité »[28]. L'article D. 54-10 issu du décret du 21 novembre 2019 renvoie au règlement général de l'Autorité des marchés financiers « pour de ce qui est des documents à renseigner par les demandeurs ». Faisant bon usage de cette prescription, l'AMF a précisé dans son instruction publiée le 19 décembre 2019[29] que doivent être fournis par les candidats à l'enregistrement (assujettissement obligatoire) ou à l'agrément (assujettissement optionnel) tous les outils de *compliance* LAB-FT mis en place.

Cependant, l'ordonnance du 9 décembre 2020 introduit des exigences différenciées selon le type de prestataire pour l'obtention de l'enregistrement. Les « anciens » assujettis obligatoires (depuis la loi PACTE) se voient soumis à un contrôle préalable sur leur entier dispositif LAB-FT[30] tandis que les « nouveaux » assujettis obligatoires (depuis l'ordonnance) y échappent. Ils bénéficient d'un contrôle préalable limité à l'honorabilité et à la compétence. Ce changement est expliqué par un « souci d'allègement de la procédure »[31], à comprendre par l'accélération des délais pour l'enregistrement.

2 - L'assujettissement optionnel

À côté de l'assujettissement de plein droit, les alinéas 7°*ter* et 7°*quater* de l'article L. 561-2 du code monétaire et financier proposent un régime d'assujettissement volontaire pour les émetteurs de jetons[32] et les autres prestataires de service sur actifs numériques[33]. En d'autres termes, les émetteurs de jetons et ces « autres » prestataires de services ne sont assujettis à la réglementation LAB-FT que s'ils en font la demande. L'assujettissement optionnel concerne l'ensemble des services assimilables à des services financiers en rapport avec des crypto-actifs, tels

(27) Position 2014-P-01 de l'ACPR relative aux opérations sur *bitcoin* en France, 29 janv. 2014.
(28) C. mon. fin., art. L. 54-10-3.
(29) Instruction AMF-DOC-201-9-23.
(30) C. mon. fin., art. L. 54-10-3 al. 4.
(31) Rapp. au président de la République accompagnant l'ord. n° 2020-1544.
(32) C. mon. fin., art. L. 552-4 : « Préalablement à toute offre au public de jetons, les émetteurs peuvent solliciter un visa de l'Autorité des marchés financiers ».
(33) C. mon. fin., art. L. 54-10-5 : « Pour la fourniture à titre de profession habituelle d'un ou plusieurs services mentionnés à l'article L. 54-10-2, les prestataires établis en France peuvent solliciter un agrément auprès de l'Autorité des marchés financiers, dans des conditions prévues par décret ».

que la réception et la transmission d'ordres sur actifs numériques, la gestion de portefeuille d'actifs numériques, le conseil aux souscripteurs d'actifs numériques ou encore le placement d'actifs numériques y sont inclus. La France a manifestement souhaité rester compétitive sur ces marchés, face à une concurrence extra-européenne présentée comme rude [34].

L'ACPR n'intervient pas dans la procédure d'obtention de l'agrément des assujettis optionnels, ni à propos de leur radiation, qui échoient exclusivement à l'AMF. Cet assujettissement volontaire donne lieu au recensement et à la publication d'une liste « blanche » par l'AMF. Le législateur a fait le pari de l'avantage réputationnel procuré par la figuration dans ladite liste pour ces professionnels plutôt que celle de la contrainte [35].

La dichotomie de régimes d'assujettissement et ses conséquences sur la compétence des autorités de contrôle et de sanction poseront la question de la qualification des services offerts par les prestataires. La lettre de la loi opère une distinction nette entre les services, mais la pratique ne s'accommode pas toujours des catégories préétablies. Par exemple, une plateforme de négociation permettant aux traders d'acheter et de vendre des crypto-actifs pourrait tout à fait parallèlement développer, de manière directe ou indirecte, des services de conseil financier. Il reviendra à la jurisprudence de trancher la question de qualification définitive et d'en tirer les conséquences pour le régime d'assujettissement.

B - Le contrôle et la sanction des assujettis : la pluralité d'autorités compétentes

La dichotomie entre les assujettis de plein droit et les assujettis volontaires trouve son prolongement dans les autorités investies du pouvoir de les contrôler et de les sanctionner. Ainsi, aux termes de l'article L. 561-36-1 du code monétaire et financier, l'ACPR est désignée comme autorité de contrôle et de sanction des assujettis de plein droit, tandis que l'article L. 561-36 confie le contrôle du respect et, le cas échéant, le pouvoir de sanctionner les assujettis optionnels à l'AMF. Cette répartition des compétences pose d'emblée une question dont les enjeux sont en partie politiques : a-t-elle pour fonction – ou aura-t-elle pour effet – d'organiser un partage ou une concurrence entre les autorités concernées ?

En ce qui concerne le contenu et les modalités de contrôle et de sanction, la loi PACTE n'apporte pas de nouveauté. Elle ne fait qu'assujettir de nouveaux professionnels au dispositif de contrôle et de sanction existant. Ainsi, est d'abord prévue une phase de contrôle, sur pièce et sur place, au cours de laquelle l'autorité de contrôle peut se faire communiquer tout document par l'entité contrôlée, ordonner la conservation de toute information, recueillir des explications auprès des personnes agissant pour le compte ou sous l'autorité de l'entité contrôlée et vérifier auprès de tiers les informations obtenues. Elle peut enfin accéder aux locaux professionnels. Plus concrètement, il s'agit d'examiner l'existence et le contenu des documents

(34) S. Polrot, La régulation LCB-FT face à l'émergence des cryptomonnaies, Revue Internationale de la Compliance et de l'Éthique des Affaires, févr. 2020. Étude 38. En faveur de « l'optionnalité », v. W. O'Rorke, La mise en œuvre des obligations de LCB-FT par l'industrie « crypto », Revue Internationale de la Compliance et de l'Éthique des Affaires, févr. 2020. Étude 39.

(35) C. Le Moign, ICO Françaises : un nouveau mode de financement, AMF, nov. 2018, p. 23.

requis par la réglementation LAB-FT, de vérifier que sont mises en œuvre les procédures d'entrée en relation et notamment l'identification du client (qui sera détaillée dans les développements suivants), les procédures de détection des situations de risque spécial (mesure de vigilance complémentaire, examen renforcé, renforcement des mesures de vigilance), les procédures de déclaration de soupçon et de rupture de relation d'affaires, ainsi que l'obligation de formation et d'information du personnel de l'entreprise en matière de LAB-FT.

Il reviendra également aux autorités de contrôle d'examiner plusieurs dossiers opérationnels pour en vérifier la conformité du contenu aux articles L. 561-2 et suivants du code monétaire et financier. Si le contrôle révèle des manquements, une procédure de sanction sera initiée. Les sanctions encourues de manière cumulative sont des sanctions pécuniaires, d'exercice ou encore de réputation, qui peuvent être dirigées contre l'entité personne morale et contre le dirigeant à titre personnel.

III - L'identification du client dans le contexte cryptographique

Les obligations de conformité mises à la charge des professionnels assujettis à la réglementation LAB-FT peuvent être regroupées en quatre ensembles. Le premier consiste en l'identification, l'évaluation et la classification des risques de blanchiment auxquels est exposé le professionnel en raison du service qu'il propose [36]. Le deuxième se rapporte à l'obligation d'identification du client, acteur potentiel d'une opération de blanchiment. Cette obligation est couramment appelée *know your customer* (KYC). Le professionnel doit en troisième lieu analyser l'objet et la nature de la relation d'affaires avec son client afin d'être en mesure de détecter d'éventuelles transactions anormales. Enfin, quatrièmement, le professionnel qui n'a pu écarter les doutes qu'il s'est forgés en remplissant ses obligations précédentes, quant à l'existence d'une opération suspecte, doit procéder à une déclaration de soupçons auprès de la cellule de renseignement financier TRACFIN.

Au regard de la technologie *blockchain*, l'obligation d'identification du client mérite une attention particulière. En effet, une raison pouvant inciter un délinquant à blanchir de l'argent par le biais des crypto-actifs est l'anonymat que semble lui conférer ce procédé. En particulier, pour acheter des valeurs en cryptomonnaies, nul besoin de rencontrer le professionnel (comme on rencontre un agent immobilier) ni de lui communiquer son nom et son prénom (comme on se présente à son banquier). L'achat se fait en ligne, à partir d'une adresse e-mail dont le libellé est entièrement choisi par l'utilisateur et d'un compte bancaire qui ne porte pas nécessairement le nom de cet utilisateur. Le recours aux crypto-actifs paraît donc propice à la disparition des traces du délinquant.

Le dispositif légal de prévention du blanchiment tente de remédier à cette situation en imposant aux professionnels assujettis d'identifier leur client (**A**). Il reste que les professionnels non assujettis du secteur des crypto-actifs échappent à cette réglementation et que des situations spécifiques, propres à la technologie *blockchain* et à d'autres

(36) C. mon. fin., art. L. 561-4-1.

technologies sophistiquées du monde virtuel, continuent de faire triompher l'anonymat (**B**).

A - La mise en œuvre de l'obligation d'identification du client

L'article L. 561-5 du code monétaire et financier impose aux professionnels assujettis d'identifier leurs clients avant d'entrer en relation d'affaires avec eux. L'identification d'une personne physique est simple : elle s'opère par la présentation d'une carte d'identité, dont le professionnel doit prendre la copie. Pour les personnes morales, en particulier pour les sociétés, l'identification se fait à partir de l'extrait *Kbis* délivré par le tribunal de commerce. De plus, le professionnel doit se procurer les statuts de la personne morale afin de rechercher les bénéficiaires effectifs des transactions réalisées pour le compte de la personne morale.

Les professionnels du secteur des crypto-actifs assujettis sont tenus de respecter l'article L. 561-5 du code monétaire et financier. En particulier, les plateformes d'échange permettant de se procurer des cryptomonnaies à partir d'une monnaie fiduciaire doivent identifier leurs clients avant de leur vendre ou de leur acheter des cryptomonnaies. La création d'un portefeuille de cryptomonnaies nécessite donc, selon la loi, de rompre avec l'anonymat –l'interdiction de l'anonymat de l'article L. 561-14 est du reste étendue aux prestataires de services d'actifs numériques obligatoirement assujettis depuis l'ordonnance du 9 décembre 2020. Cependant, un assouplissement traditionnel de la réglementation LAB-FT est prévu à l'article R. 561-10 du code monétaire et financier pour les clients occasionnels, c'est-à-dire ceux qui ne s'engagent pas dans une relation d'affaires destinée à s'étendre dans le temps, mais qui souhaitent par exemple faire un achat ponctuel en *bitcoin*. Si l'achat ou l'opération ne dépasse pas 1 000 €, et en l'absence de doute, le professionnel peut s'abstenir d'identifier son client occasionnel.

Il est naturellement possible qu'un professionnel assujetti ne respecte pas ses obligations d'identification ou que le client réponde à la demande d'identification par des documents d'identité falsifiés [37]. Ces situations s'apparentent à une absence d'identification en dépit de l'obligation légale. L'anonymat peut-il néanmoins être levé par les services répressifs ?

En principe, la technologie *blockchain* offre des garanties exceptionnelles contre l'anonymat [38]. En effet, la *blockchain* n'est autre qu'un gigantesque registre informatique, infalsifiable et indestructible. Chaque utilisateur dispose d'une copie identique du registre entier et peut, par la preuve cryptée irréfutable de l'ensemble des transactions réalisées sur la *blockchain* depuis l'origine, reconstruire l'historique complet des transactions d'un portefeuille donné. Il en résulte que la traçabilité des transactions effectuée est totale. Certes, une transaction en cryptomonnaie se fait à partir d'un portefeuille numérique dont l'identifiant est un numéro. Le portefeuille n'est donc pas directement relié à une personne mais son numéro renvoie à un nom, qui peut encore être un pseudonyme. Plutôt que d'anonymat, il est plus correct d'évoquer le « pseudonymat ». L'énigme peut généralement être levée du fait que l'utilisateur du pseudonyme opère à partir d'un ordinateur qui est connecté à internet par le biais d'une adresse IP. Or l'adresse IP renvoie nécessairement au nom d'une personne. Si le chemin est long, il mène *in fine* à l'identification d'une personne.

(37) Y. Burnichon, De quelques facettes de la mission d'enquêteur financier face aux fraudes numériques, AJ pénal 2014. 62.
(38) S. Polrot, *op. cit.*

Certes, le donneur d'ordre d'une transaction n'est pas nécessairement la personne enregistrée sous l'adresse IP. Le blanchisseur qui veut garder l'anonymat absolu prendra la précaution d'utiliser l'ordinateur d'autrui, d'opérer à partir d'un cybercafé ou encore de « sniffer » l'adresse IP de son voisin [39]. Tout comme un trafiquant de drogue ne transporte jamais lui-même les valises d'argent liquide émanant du délit, mais emploie des porteurs qui ignorent son identité…

En réponse au problème des falsifications, l'identité numérique certifiée a vu le jour. Elle permet au professionnel de s'assurer que la personne connectée à internet est bien celle qu'elle prétend être, en associant le dispositif numérique aux caractéristiques physiques de la personne. En France, la Poste propose l'identité numérique certifiée à tous les ressortissants et résidents français [40]. Dans ce même sens, le GAFI a publié le 6 mars 2020 des Lignes directrices sur l'identité numérique. Il poursuit l'idée que, correctement utilisée, l'identité numérique a le potentiel de réduire les risques LAB-FT [41].

B - Les situations d'absence d'identification du client

Le monde numérique possède ses retranchements. L'identification du client est parfois tenue en échec en raison de la technologie employée pour créer les monnaies cryptographiques (**1**) ou des systèmes sophistiqués spécialement conçus pour organiser l'anonymat (**2**).

1 - Le blanchiment par minage

De manière anecdotique, évoquons une façon peu commune de se procurer des cryptomonnaies. La technologie *blockchain* permet à tout individu de créer soi-même des unités monétaires, par minage. Ainsi, un internaute en mesure de trouver une solution nouvelle pour résoudre l'équation algorithmique d'une cryptomonnaie, appelée « preuve de calcul », mine des unités monétaires. Les mineurs sont rémunérés pour leurs opérations par l'obtention de valeurs dans cette monnaie. Or ces mineurs sont, comme tout un chacun, des blanchisseurs potentiels. Le minage demande une très grande puissance de calcul, laquelle nécessite des processeurs très puissants et une forte consommation d'énergie. Un délinquant très investi dans le monde virtuel pourrait, en véritable *geek*, investir son argent sale dans un matériel informatique très puissant – et donc très coûteux – et s'acquitter d'une facture d'électricité très élevée pour acquérir des cryptomonnaies par minage. Au fil des opérations, qui sont certes longues, l'argent provenant du crime se transforme en cryptomonnaie. Cependant, la loi n'impose nullement aux mineurs de s'identifier avant d'opérer sur la *blockchain*. Une faille apparaît ici dans le dispositif de prévention du blanchiment.

2 - Les techniques numériques d'organisation de l'anonymat

Bien conscients des aptitudes à la traçabilité de la *blockchain*, les utilisateurs de cryptomonnaies désirant bénéficier d'un réel anonymat peuvent recourir à des technologies spécialement développées pour reconquérir cet anonymat dans le monde numérique.

La première d'entre elles consiste à masquer l'accès de l'utilisateur à la *blockchain*, en plaçant un outil inter-

(39) Y. Burnichon, *op. cit.*
(40) https://lidentitenumerique.laposte.fr/
(41) http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf

médiaire à l'endroit de la connexion entre cet utilisateur et la *blockchain* : un réseau privé virtuel (ou VIN, *virtual private network*). Ce réseau se compose d'un ensemble de serveurs reliés entre eux, qui se transmettent les données à expédier pour une transaction. Un utilisateur envoie ses données vers l'un des serveurs mais celles-ci sont réexpédiées par un autre serveur. De l'extérieur, il n'est pas possible d'identifier la provenance initiale des données, mais seulement d'observer un flux de données provenant d'un serveur. L'anonymat de l'utilisateur est donc garanti. Une variante de cette technique est proposée par TOR (*The Onion Routeur*), développé par la CIA pour protéger ses agents. Le principe est similaire à ceci près que les serveurs sont remplacés par les utilisateurs eux-mêmes. Des paquets de données transitent d'un utilisateur à l'autre en application d'un algorithme faisant un important usage du hasard. Chaque utilisateur endosse le rôle d'expéditeur pour le suivant, si bien que nul ne peut savoir qui est l'expéditeur réel des données. Pour aller plus loin encore, un dernier outil a été développé, l'I2P (*Invisible Internet Project*). Le fonctionnement ressemble beaucoup à celui de TOR, avec une différence notable : les connexions des utilisateurs sont groupées de façon à mieux se noyer dans la masse.

Une autre technique est celle du dépôt fiduciaire auprès d'un tiers. Elle était utilisée par Silkroad. Lors d'une transaction, la somme devait d'abord être déposée auprès d'un tiers de confiance – ici Silkroad – qui ne la reversait au vendeur qu'une fois que la marchandise avait été reçue par l'acheteur. Pour l'expéditeur de la somme, l'intérêt d'éviter une escroquerie se double de celui de masquer son identité puisque c'est le tiers fiduciaire qui procède à l'envoi. Certaines cryptomonnaies comme Dash (DASH) ou NavCoin (NAV) intègrent dans leur algorithme la pratique du tiers fiduciaire, tout en y adjoignant d'autres techniques de dissimulation. Elles garantissent donc l'anonymat sans besoin qu'un marché en ligne s'en charge.

La technique suivante consiste à chiffrer la *blockchain* elle-même. Puisque le registre est lisible et transparent, le chiffrer permet de le rendre opaque et de faire ainsi échapper à la traçabilité l'ensemble des transactions qu'il recense. Certaines monnaies, comme Monero (XMR) utilisent une *blockchain* chiffrée. Leurs utilisateurs doivent porter une confiance aveugle à leur fonctionnement algorithmique puisqu'ils ne sont pas en mesure de le vérifier, mais ils sont en contrepartie assurés que leur portefeuille Monero ne pourra pas être relié à leur identité.

Enfin, on peut échapper à la traçabilité de la *blockchain* en s'attaquant au cœur du problème, c'est-à-dire en anéantissant l'enregistrement systématique des transactions. Pour cela, certaines cryptomonnaies fonctionnent à partir d'une preuve de calcul qui s'abstient d'enregistrer l'historique des transactions. La création d'une unité monétaire se produit alors sans laisser de trace. On parle de preuve de calcul sans divulgation de connaissance (*Zero-Knowledge-Proof* ou ZKP). La *blockchain* est toujours là, mais sans mémoire. Les unités monétaires ont un historique vierge. Ces cryptomonnaies véritablement anonymes existent bel et bien, par exemple Zcash (ZEC), Pivx (PIVX), Komodo et Zcoin (XZC).