# Forum Fintech ACPR-AMF

## Groupe de travail sur
## l'application des règles de LCB-FT
## au secteur des crypto-actifs
## Compte-rendu des travaux

Ce compte-rendu retrace les réflexions du groupe de travail réunissant l'Autorité de contrôle prudentiel et de résolution (ACPR), l'Autorité des marchés financiers (AMF), la Direction générale du Trésor, Tracfin et des acteurs du secteur des crypto-actifs ainsi que des institutions financières[1]. Il ne saurait engager l'ACPR ou l'AMF.

## Table des matières



[1] Voir composition du groupe de travail en annexe

# 1 Résumé

Dans le cadre du Forum Fintech ACPR-AMF, **un groupe de travail** a été constitué avec les acteurs de la place et les autorités publiques concernées **pour étudier l'application des règles de lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT) au secteur des crypto-actifs**.

L'objectif de ce groupe était double : d'une part, **sensibiliser un secteur récemment réglementé** (loi PACTE de 2019, extension des Recommandations du GAFI aux crypto-actifs en 2018 et 2019), d'autre part, faire **un premier état des lieux des pratiques de LCB-FT** des acteurs ainsi que des spécificités et des perspectives ouvertes en la matière par l'exploitation des technologies *blockchain*.

Le présent rapport rend compte des travaux de ce groupe, menés entre fin novembre 2019 et début juillet 2020.

Il en ressort que **les acteurs français du secteur des crypto-actifs les plus expérimentés ont déjà su, dans une large mesure, adapter les principes généraux de la LCB-FT au contexte technique et opérationnel de leur activité** (entrée en relation et opérations à distance, mode d'identification des portefeuilles sur la *blockchain* déconnecté de la notion de client, *etc.*)

**Les technologies de *blockchain* permettent de façon générale de tracer les transactions effectuées**, à l'exception des produits ou des modes de transactions conçus spécifiquement pour renforcer l'anonymat. Exploitant cette caractéristique de traçabilité, des **outils d'analyse transactionnelle** ont été développés par des prestataires spécialisés afin de caractériser les comportements et les portefeuilles potentiellement suspects, en ayant recours à des techniques d'analyse des réseaux et en étudiant l'historique sur longue période des opérations sur la *blockchain*. **Certains prestataires de services en actifs numériques (PSAN) utilisent** quotidiennement **ces outils, complétés par leurs bases de connaissance, pour suivre leurs opérations et maîtriser leurs risques de blanchiment de capitaux et de financement du terrorisme (BC-FT)**.

**Ces outils, inhérents à l'écosystème** des *blockchains* publiques**, renforcent utilement la connaissance de la clientèle et les investigations menées sur les transactions**. Même si leur développement récent nécessite des perfectionnements afin de répondre aux quelques limites (coût, champ des crypto-actifs couverts) relevées dans le rapport, **ils constituent cependant un axe essentiel pour la prévention du BC-FT**. Il est d'ailleurs primordial tant par les acteurs du secteur, au titre de la mise en œuvre de leur politique de risque, que par les autorités, dans leur mission de contrôle **de s'assurer d'une compréhension fine de leur fonctionnement et de leur bonne maîtrise**.

L'application de **la transparence des virements électroniques (*travel rule*)** aux transferts d'actifs virtuels reste en revanche un défi de taille pour les prestataires de services liés à des actifs virtuels dans le monde. Il s'agit en effet d'établir les conditions minimales nécessaires à la communication rapide et sécurisée des informations et à la confiance entre les acteurs. Les **principales initiatives de standardisation en cours au niveau mondial** (standardisation des messages, protocoles de communication) ont été examinées par le groupe de travail, qui s'est également attaché à identifier et à discuter les **actions complémentaires** à entreprendre (registre de prestataires, sécurisation, stockage et conservation des données…) pour aboutir à une mise en œuvre de la *travel rule* satisfaisante sur le plan technique.

Cette analyse a montré la **nécessité d'une mobilisation de l'écosystème français** et de son intégration aux réflexions transnationales en cours, faute de quoi le respect de la règle de transparence ne pourra être que coûteux et imparfait pour chaque acteur. À cet égard, **les travaux législatifs européens sur les crypto-actifs** pourraient être l'occasion pour la place française de s'inscrire dans une **dynamique européenne** afin d'accompagner le volet réglementaire par le **développement des solutions techniques** correspondantes.

# 2 Introduction

À la demande du G20, le Groupe d'action financière (GAFI) a modifié en octobre 2018 et en juin 2019 ses recommandations en matière de lutte contre le blanchiment et le financement du terrorisme (LCB-FT) pour y inclure certains acteurs du secteur des crypto-actifs, désignés sous le nom de prestataires de services liés à des actifs virtuels (PSAV)[2]. Ces prestataires doivent être agréés ou inscrits sur un registre, soumis au contrôle des autorités, et ont l'obligation de mettre en place des systèmes effectifs de vigilance fondée sur une approche par les risques (connaissance de la clientèle, surveillance des transactions, …) et de déclaration de soupçon.

Le GAFI a également publié en juin 2019 des orientations détaillant et clarifiant l'application de ses recommandations concernant les actifs virtuels (*virtual assets*)[3] et les prestataires de services sur actifs virtuels.

La mise en œuvre et le suivi des recommandations du GAFI sur les actifs virtuels ont fait l'objet d'une évaluation, douze mois après leur adoption[4]. Par ailleurs, un Groupe de contact sous l'égide du GAFI, rassemblant plusieurs contrôleurs LCB-FT, surveille l'évolution du secteur des crypto-actifs, la mise en œuvre de ses obligations au titre de la LCB-FT et le développement de solutions techniques visant à renforcer la conformité du secteur avec les recommandations du GAFI.

Parallèlement, la loi PACTE du 22 mai 2019 a créé le statut de prestataire de services sur actifs numériques (PSAN). Les prestataires offrant le service de conservation d'actifs numériques pour compte de tiers ou celui d'achat-vente d'actifs numériques en monnaie ayant cours légal doivent être enregistrés auprès de l'AMF, après avis conforme de l'ACPR. L'enregistrement en tant que PSAN suppose la mise en place d'une organisation, de procédures et d'un dispositif de contrôle interne propres à assurer le respect des obligations au titre de la LCB-FT[5]. La définition des activités des PSAN et leurs modalités d'enregistrement ont été précisées par décrets[6], par le règlement général de l'AMF[7] et par une instruction de cette autorité[8].

Dans le contexte de l'enregistrement en cours des acteurs du secteur des crypto-actifs, un groupe de travail de place a été créé fin 2019, sous l'égide du Forum Fintech ACPR-AMF, associant notamment les autorités de contrôle et des acteurs représentatifs du secteur des crypto-actifs en France.

---

[2] *Cf.* [1] du glossaire.
[3] *Cf.* [2] du glossaire.
[4] Le rapport d'évaluation à douze mois des Recommandations du GAFI sur les actifs virtuels a été publié en juillet 2020, *cf.* [4] des références documentaires.
[5] Article L. 54-10-3 du code monétaire et financier.
[6] Décrets n°2019-1213 du 21 novembre 2019 et n°2019-1248 du 28 novembre 2019.
[7] Titre II du livre VII du règlement général de l'Autorité des marchés financiers homologué par arrêté du 5 décembre 2019.
[8] Instruction DOC-2019-23 de l'Autorité des marchés financiers portant sur le régime applicable aux prestataires de services sur actifs numériques.

Les objectifs de ce groupe de travail étaient les suivants :

- La sensibilisation du secteur aux enjeux de la LCB-FT et aux recommandations du GAFI ;
- L'identification de solutions techniques disponibles aux acteurs du secteur, notamment pour l'application de la 16ème Recommandation du GAFI relative aux virements électroniques garantissant le respect de la vie privée des clients (ainsi que les éventuels verrous entravant le développement de ces solutions) ;
- L'identification des facteurs de risque et l'impact des recommandations du GAFI sur le secteur;
- Et, de façon plus générale, la discussion, la remontée d'informations et le retour d'expérience de la Place sur l'application des nouvelles recommandations auprès du GAFI.

Le présent document rassemble les principaux enseignements, diagnostics et pistes identifiés par le groupe de travail.

# 3 Rappel sur l'encadrement en matière de LCB-FT applicable aux activités sur crypto-actifs

## 3.1 Les travaux du GAFI

L'utilisation croissante des crypto-actifs à des fins de blanchiment de capitaux et de financement du terrorisme au cours des dernières années a mis en évidence la nécessité d'assujettir le secteur des crypto-actifs à la réglementation en matière de LCB-FT.

Mandaté en ce sens par le G20, le GAFI a modifié en octobre 2018 sa 15ème Recommandation pour prévoir l'application de ses standards au secteur des actifs virtuels et a adopté en juin 2019 une note interprétative précisant leurs modalités de mise en œuvre, notamment en matière d'enregistrement et de contrôle des prestataires de services sur actifs virtuels et de transparence des transferts d'actifs virtuels. Ces exigences ont également été détaillées par des orientations publiées en juin 2019.

Les Recommandations du GAFI prévoient désormais l'assujettissement des prestataires de services sur actifs virtuels aux standards internationaux en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme. Ces prestataires doivent être *a minima* agréés ou inscrits à un registre dans leur pays de création (ou dans le pays de localisation de leur activité s'il s'agit d'une personne physique) et mettre en place un dispositif adapté de lutte contre le blanchiment des capitaux. Les États doivent sanctionner les personnes physiques ou morales exerçant des activités sur actifs virtuels sans agrément ou inscription préalable.

Par ailleurs, le GAFI a étendu le champ de la transparence des transferts (ou « *travel rule* ») au secteur des actifs virtuels. Cette règle vise à garantir l'intégrité du système des transferts d'actifs virtuels, en permettant en particulier le gel des avoirs, et à assurer la transparence et la traçabilité de ces transferts.

La 16ème Recommandation du GAFI requiert en particulier la collecte et la transmission des informations élémentaires sur le donneur d'ordre et le bénéficiaire pour tout transfert sur actifs virtuels impliquant au moins un PSAV. La transmission de ces informations doit être immédiate et sécurisée mais il n'est pas nécessaire que ces informations soient directement attachées au transfert d'actifs virtuels, ni même que la transmission des informations soit effectuée via une *blockchain*.

Le GAFI a publié un premier bilan de la mise en œuvre de la *travel rule* à la suite de sa session plénière de juin 2020. S'il n'existe pas à l'heure actuelle de solution technologique permettant la mise en œuvre au niveau mondial de la transparence des transferts d'actifs virtuels, un standard technique permettant la transmission des informations entre PSAV a été élaboré par des acteurs privés. Plusieurs défis sont également identifiés, comme l'interopérabilité des différents systèmes de transmission des informations, l'identification du PSAV de la contrepartie à une transaction, ou la sécurisation des informations transmises. Un nouveau bilan sera réalisé par le GAFI deux ans après l'adoption de ses Recommandations relatives aux actifs virtuels.

## 3.2 Le cadre français

### 3.2.1 Le statut de PSAN

#### (i) Les enregistrements obligatoires

Conformément à l'article L. 54-10-3 du code monétaire et financier (« CMF »), les candidats à l'enregistrement en tant que PSAN[9] doivent mettre en place une organisation, des procédures et un dispositif de contrôle interne adaptés et propres à assurer le respect des dispositions relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme ainsi qu'à la mise en œuvre des mesures de gel des avoirs.

L'instruction DOC-2019-23 de l'AMF relative au régime applicable aux prestataires de services sur actifs numériques précise la liste des documents attendus à cet effet, notamment l'élaboration d'une classification des risques et la mise en place d'un dispositif de LCB-FT adapté à cette classification. Le dispositif LCB-FT du candidat doit inclure des procédures internes comprenant les diligences à l'égard des clients, les modalités de vigilances des opérations de la clientèle et un dispositif de mise en œuvre des mesures de gel des avoirs. Le candidat est également tenu de mettre en place un dispositif de contrôle interne.

Une fois enregistrés par l'AMF après avis conforme de l'ACPR, les PSAN sont soumis au contrôle permanent de l'ACPR.

#### (ii) Les agréments optionnels

Certains services sur actifs numériques, dont l'échange d'actifs numériques contre d'autres actifs numériques ainsi que l'exploitation d'une plateforme de négociation d'actifs numériques, peuvent être offerts par des PSAN sans enregistrement obligatoire.[10] Ils ont la possibilité de demander un agrément optionnel à l'AMF afin d'être assujettis[11] à la réglementation en matière de LCB-FT[12] et de gel des avoirs.

### 3.2.2 Les émetteurs de jetons (ICO)

La loi PACTE a créé un régime de visa optionnel d'offres aux publics de jetons (ou *initial coin offering, ICO*) attribué par l'AMF. Cette dernière a analysé l'applicabilité de la réglementation LCB-FT aux émetteurs de jetons compte tenu de leurs spécificités (souscription en crypto-actifs, petites structures, client occasionnel) et rappelé de manière synthétique sur son site internet les principales obligations des émetteurs de jetons[13].

---

[9] Pour les services de conservation d'actifs numériques pour compte de tiers ainsi que d'achat-vente d'actifs numériques en monnaie ayant cours légal (*cf.* [1] du glossaire).

[10] La description porte sur le cadre réglementaire en vigueur au moment de la rédaction de ce rapport. Des modifications pourraient être apportées prochainement à ce cadre.

[11] L'agrément optionnel implique également le respect d'obligations qui ne sont pas liées à la LCB-FT (assurance professionnelle, ou fonds propres, politique commerciale, etc.)

[12] L'agrément optionnel pour les services sur actifs numériques par ailleurs soumis à enregistrement obligatoire (article L. 54-10-5 du code monétaire et financier) ne sera pas abordé dans la suite de ce rapport.

[13] Document accessible en ligne : https://www.amf-france.org/sites/default/files/2020-02/ico_obligations_lutte-contre-le-blanchiment_5edirective.pdf

## 3.3 Principaux risques de blanchiment de capitaux et de financement du terrorisme présentés par les activités sur crypto-actifs

Différentes analyses au niveau national (COLB, Tracfin) et supranational (Commission européenne, autorités européennes de surveillance) confirment que le risque BC-FT en matière de crypto-actifs est avéré. Au regard de la réglementation actuelle, l'intervention des tiers assujettis à la LCB-FT se limite aux phases de placement et/ou de conversion du produit du blanchiment en crypto-actifs, à savoir la conversion entre monnaie ayant cours légal et crypto-actifs[14]. Une fois la conversion effectuée, les crypto-actifs permettent de transférer des fonds de manière efficace, sûre, rapide, peu onéreuse et transfrontalière sous couvert d'un relatif anonymat ou pseudonymat, sans l'intermédiation d'un tiers assujetti.

Ces caractéristiques peuvent rendre les crypto-actifs attractifs pour les flux financiers occultes inhérents à la pratique du blanchiment de capitaux ou du financement du terrorisme.

S'il est possible d'observer les flux sur un actif choisi, et donc, sur une *blockchain* déterminée, l'utilisation de plateformes permettant la conversion d'un actif vers un autre sans que ces transactions soient enregistrées dans la *blockchain* favorise la fragmentation de la chaîne de détention et complique le travail des analystes.

### 3.3.1 Blanchiment de capitaux

On observe deux tendances distinctes dans les techniques de blanchiment impliquant des crypto-actifs. D'une part, ces derniers peuvent être l'objet, le support, ou le produit de l'infraction ; d'autre part, ils peuvent être utilisés indépendamment de l'infraction d'origine, comme simple instrument de blanchiment.

**(i) Criminalité spécifique aux crypto-actifs**

La cybercriminalité est un domaine particulièrement propice à l'utilisation de crypto-actifs. De nombreux modes opératoires y font appel, que ce soit en tant qu'outil de l'infraction ou en tant que produit de celle-ci. À titre d'exemple, on peut citer le minage pirate (*cryptojacking*), les logiciels rançonneurs (*ransomware*) ou le piratage de plateformes d'échange.

**(ii) Criminalité de droit commun ayant recours aux crypto-actifs**

L'émergence de nouvelles technologies et leur démocratisation permettent à la délinquance de développer de nouveaux modes opératoires de blanchiment. On observe ainsi le développement du trafic de stupéfiants et de son blanchiment sur l'Internet clandestin (*dark web*), ainsi que l'achat et la vente de produits illicites, ou de services illégaux tels que la vente d'armes, de coordonnées bancaires volées, de contenus pédopornographiques, etc.

En dehors de l'internet clandestin, la délinquance de droit commun recourt également aux crypto-actifs dans le cadre d'escroqueries, de mouvements de fonds transfrontaliers liés à tout type de criminalité financière ou organisée.

[14] Il s'agit des phases du blanchiment, *cf.* [3] du glossaire.

### 3.3.2 Financement du terrorisme

Le recours aux crypto-actifs par des groupements terroristes est également documenté. Plusieurs organisations ont eu recours à des appels au don réalisés sur les réseaux sociaux, des forums ou des groupes privés diffusant des adresses de crypto-actifs sur lesquelles envoyer des fonds afin de financer leurs activités criminelles.

### 3.3.3 Caractéristiques et pratiques propices aux risques de BC-FT

Outre les caractéristiques évoquées plus haut, les crypto-actifs offrent la possibilité d'effectuer des transactions sans l'intervention d'un tiers de confiance ou tiers assujetti à la réglementation LCB-FT. L'une des possibilités de limiter les risques de BC-FT consiste à réglementer l'entrée et la sortie de cette économie, à savoir l'achat ou la vente de crypto-actifs contre de la monnaie ayant cours légal.

Il ressort des travaux du groupe de travail que ce contrôle est nécessaire afin de circonscrire le risque BC-FT propre aux crypto-actifs, mais ne permet pas d'en appréhender la pleine mesure. En effet, de nombreuses pratiques permettent de contourner ces contrôles.

L'une des principales lacunes de ce système est l'absence d'assujettissement à la règlementation en matière de LCB-FT des échanges entre crypto-actifs. Il est donc possible pour un délinquant de changer d'un actif à l'autre sans avoir à déclarer son identité, fragmentant la chaîne de détention, via la pratique du *chain swapping*[15]. Combinée à l'usage de *privacy coins*, cette technique, dite d'*obfuscation*, rend impossible le traçage des fonds et l'identification de l'utilisateur.

Les travaux des différents acteurs du groupe ont convergé vers la même solution concernant ces pratiques, à savoir :

- La prise en compte des échanges entre crypto-actifs dans la réglementation en matière de LCB-FT.
- L'intensification des mesures de vigilances des acteurs assujettis lorsqu'ils sont confrontés à des actifs numériques favorisant l'anonymat (*anonymity-enhanced cryptocurrencies* ou AEC).

[15] *Cf.* [9] du glossaire

# 4 État des lieux des pratiques

Un questionnaire a été envoyé en décembre 2019 aux membres du groupe et d'autres acteurs de la place afin de mieux connaître leur activité et leur exposition aux risques de BC-FT. Les principaux résultats sont analysés ci-dessous en reprenant la structure du questionnaire.

## 4.1 L'évaluation de l'exposition aux risques de BC-FT

Les principaux critères de risque identifiés par les répondants pour évaluer leur exposition aux risques, au regard des axes de la classification des risques prévus par la réglementation[16], sont résumés ci-après.

Il est ainsi apprécié, en vue d'identifier les risques BC-FT élevés liés à un client :

- La localisation ou la résidence du client dans un pays à haut risque, comme ceux figurant sur les listes du GAFI ou de la Commission européenne ;
- Un comportement potentiellement à risque (par exemple des connexions avec un réseau privé virtuel ou « VPN », utilisation d'un navigateur de type Tor[17]) ;
- Un mauvais score d'analyse transactionnelle du portefeuille du client ;
- Le montant total des opérations réalisées par le client (montant anormalement élevé par rapport au profil ou aux habitudes du client, sans justification économique ni objet licite apparent) ;
- Une fréquence anormalement élevée de transactions au regard du profil client ou de son historique de transaction ;
- Le recours à des moyens de paiement considérés à risque.

Pour identifier les risques BC-FT élevés liés à une transaction :

- Le fractionnement des transactions ;
- Des liens suspects entre plusieurs clients ;
- Une usurpation d'identité ;
- Un montant de transaction important ou anormalement élevé au regard du profil du client ;
- Une fréquence anormale de transactions au regard du profil client ou de son historique de transactions ;
- La réalisation d'opérations d'échanges entre crypto-actifs (« *crypto-to-crypto* ») — en particulier lorsque la transaction est réalisée hors *blockchain* — dans la mesure où ils n'impliquent pas de monnaie ayant cours légal et qu'ils rendent le risque BC-FT plus difficilement appréciable[18] ;
- L'historique des crypto-actifs concernés ainsi que les portefeuilles, dans la mesure d'une altération de la chaîne de détention des crypto-actifs (par exemple via l'utilisation de mixeurs ou mélangeurs[19], ou encore via un passage par des plateformes d'échange), évalué notamment par l'utilisation d'outils d'analyse transactionnelle.

[16] Article L. 561-4-1 du code monétaire et financier.
[17] *Cf.* [5] du glossaire
[18] Un répondant modère ce critère sur la base d'un rapport thématique de l'association de place représentative du secteur (ADAN) sur les activités entre actifs numériques réalisées depuis la France.
[19] *Cf.* [4] du glossaire

## 4.2 L'identification et la connaissance de la clientèle

### 4.2.1 L'identification et la vérification d'identité à l'entrée en relation d'affaires

En premier lieu, la réglementation impose la mise en œuvre de mesures de vigilance à l'égard de la clientèle en relation d'affaires, qui portent sur l'identification et la vérification d'identité du client, en principe avant l'entrée en relation[20].

En cas d'entrée en relation d'affaires à distance, des mesures spécifiques de vérification d'identité sont prévues[21]. Des précédents travaux du Forum Fintech ont par ailleurs traité de la problématique de la vérification d'identité à distance des personnes physiques et morales[22].

Un répondant a relevé que « *dans le monde des actifs numériques, l'entrée en relation d'affaires à distance est la norme. Par conséquent, la mise en place de mesures de vigilance complémentaire ne peut être systématique* ». Toutefois, depuis l'ordonnance n°2020-115 du 12 février 2020, les entrées en relation d'affaires à distance ne sont plus considérées comme présentant un risque fort de blanchiment de capitaux nécessitant systématiquement la mise en œuvre de mesures de vigilance complémentaires. La mise en œuvre, en pratique, des nouveaux textes n'a pas fait l'objet de travaux spécifiques de la part de ce groupe de travail.

En second lieu, les clients occasionnels d'un PSAN doivent être identifiés et leur identité vérifiée, soit en cas de soupçon de BC-FT quel que soit le montant de l'opération, soit lorsque le client effectue une ou plusieurs opérations dépassant le seuil de 1000 euros prévu par le 5° du II de l'article R. 561-10 du code monétaire et financier. La question de la pertinence de ce seuil - en deçà duquel l'identification du client n'est pas obligatoire - a fait l'objet d'échanges au sein du groupe de travail. De fait un PSAN exerçant des activités plus risquées d'un point de vue BC-FT (distributeurs automatiques de crypto-actifs par exemple[23]) peut trouver pertinent d'identifier tous ses clients, dès le premier euro, pour atténuer ses risques.

#### L'authentification du client lors d'une transaction

Au-delà des outils et techniques utilisées dans le secteur financier traditionnel, des solutions plus spécifiques à l'écosystème *blockchain* pourraient être employées afin de renforcer l'authentification des clients lors de l'exécution des transactions. Ces mécanismes ne doivent cependant pas être confondus avec l'identification au sens de la conformité, et il s'applique de fait sur un client qui a été préalablement validé à travers les diligences KYC appliquées par le PSAN.

Les solutions évoquées sont essentiellement prospectives et pourraient s'appuyer par exemple sur des architectures d'identité auto-souveraine[24] ou des services fournis par des prestataires techniques de type regtech. Au-delà de la finalité directe d'authentification à proprement dit, ces solutions

[20] I de l'article L. 561-5 du code monétaire et financier.
[21] Article R. 561-5-2 du code monétaire et financier.
[22] Cf. les synthèses du groupe de travail du forum Fintech sur la vérification d'identité à distance des personnes physiques et morales.
[23] Sur un rappel de l'obligation d'enregistrement auprès de l'AMF des prestataires déployant des distributeurs automatiques de crypto-actifs en France, voir le communiqué de presse conjoint de l'ACPR et de l'AMF du 27 juillet 2020, https://acpr.banque-france.fr/communique-de-presse/lamf-et-lacpr-rappellent-leurs-obligations-aux-operateurs-de-distributeurs-automatiques-de-crypto
[24] Cf. [8] du glossaire.

permettraient d'entrevoir des opportunités supplémentaires pour renforcer la conformité en offrant de nouveaux cas d'utilisation[25].

### 4.2.2 Connaissance de la clientèle et analyse transactionnelle

Comme pour tout organisme assujetti à la réglementation LCB-FT, les PSAN doivent en fonction de l'exposition aux risques recueillir des éléments de connaissance de la clientèle afin de mieux appréhender la nature de la relation d'affaires et établir un profil de risques BC-FT[26].

Le mode de recueil des éléments nécessaires à cette connaissance n'est pas toujours lié à la technologie propre aux crypto-actifs et requiert parfois des méthodes comparables à d'autres secteurs réglementés. Il en est ainsi de l'adresse géographique du client ou de l'origine des fonds (avec cette particularité que les fonds en crypto-actifs peuvent provenir d'activités de minage et pas seulement d'achats ou d'échanges).

Toutefois, en matière de crypto-actifs, l'économie des *blockchains* publiques permet d'enrichir et de vérifier cette connaissance grâce à des outils d'analyse transactionnelle (*Know Your Transaction* ou « *KYT* »).

Ces outils informatiques exploitent en effet la caractéristique qu'ont les *blockchains* publiques de tracer l'ensemble des transactions et mouvements de crypto-actifs. Par l'analyse de ces transactions, ils permettent de mettre en exergue de potentiels risques quant à l'origine ou à la destination d'actifs numériques en attribuant une note (*scoring*) du portefeuille de crypto-actifs du client (ou *wallet*).

Les outils d'analyse transactionnelle permettent notamment de déterminer si des crypto-actifs ont transité par des adresses publiques associées à des malfaiteurs ou à des pirates. L'analyse et le recoupement de données permettent, dans certains cas, de dévoiler l'origine, la destination et les parties prenantes à une transaction. Ces outils permettent aussi de rapprocher certaines adresses d'un propriétaire (plateforme d'échange, site d'achat en ligne). Cependant, il s'agit d'outils encore imparfaits qui ne permettent pas d'analyser les transactions liées à des crypto-actifs à anonymat renforcé : aussi en sus de cet outil, un PSAN doit pouvoir s'appuyer sur son expérience consolidée par les bases de connaissance acquises et se tourner vers son client pour obtenir des précisions complémentaires (contrepartie de la transaction, objet et nature de l'opération envisagée, justificatifs). Ces outils font l'objet d'une analyse plus approfondie dans la partie 5 de ce document.

[25] Par exemple un répondant a évoqué une solution permettant la génération d'un identifiant cryptographique propre au client et qui pourrait être attaché aux transactions — renforçant ainsi la traçabilité des opérations — une fois le processus de KYC accompli et validé; cet identifiant pourrait de plus être exploité techniquement comme une condition préalable à l'exécution des opérations.

[26] Article L. 561-5-1 du code monétaire et financier

## 4.3 La vigilance

La vigilance, et notamment la surveillance des opérations et des flux de crypto-actifs, constitue un point-clé du dispositif de LCB-FT des PSAN. En la matière, l'usage de la *blockchain* publique présente des particularités qui amènent à envisager des méthodes de surveillance des transactions très spécifiques.

### 4.3.1 Opérations fractionnées et adresses publiques multiples

Les opérations fractionnées par un même client dans un but frauduleux peuvent être détectées à partir d'une identité cryptographique ou d'un compte nominatif attaché à chaque utilisateur.

À cet égard, l'utilisation par un seul client d'adresses publiques multiples sur la *blockchain* peut constituer un problème. Un client peut en effet générer un nombre quasi infini d'adresses de portefeuilles cryptographiques à partir d'un portefeuille initial (physique ou logiciel) même si un répondant indique que cette utilisation « *n'est pas dans la grande majorité des cas malveillante* ». De fait, l'utilisation de plusieurs adresses sur une *blockchain* publique peut avoir pour objectif de préserver la vie privée des utilisateurs de cette *blockchain*.

Pour pallier les effets négatifs de l'utilisation d'adresses multiples sur la connaissance client, certains répondants ont fait observer que les PSAN peuvent demander communication de l'ensemble des adresses publiques dont le client a la maîtrise. Certains limitent également le nombre de portefeuilles associés à un client. Certaines difficultés ont toutefois été relevées. Les adresses de destination des actifs numériques indiquées par le client peuvent en effet ne pas être la propriété de ce dernier. Inversement, un client peut avoir la maîtrise de plusieurs adresses de retrait[27] et n'en dévoiler qu'un nombre limité au PSAN dont il est le client.

### 4.3.2 Technologies favorisant l'anonymat sur internet

Les technologies favorisant l'anonymat en ligne (utilisation d'un réseau privé virtuel ou VPN ou d'un navigateur de type Tor) peuvent être des indicateurs de doute sur le client induisant un renforcement des diligences en termes de justificatifs collectés auprès de ce dernier. Les participants au groupe ont cependant relevé que l'utilisation de réseaux privés était courante parmi les utilisateurs avertis du secteur des crypto-actifs. Selon les membres du groupe, ces outils présentent un intérêt du point de vue des clients (comme le chiffrage d'informations en cas de connexion à un réseau de Wi-Fi public, la sécurisation de l'envoi et de la réception de données personnelles) mais sont également porteurs de risques (contournement de mesures d'embargo). D'autres PSAN autorisent l'utilisation d'un VPN qui peut servir à assurer la sécurité d'une clientèle en évitant d'être tracé par une partie tierce[28] dans la mesure où le client est par ailleurs connu du PSAN via des mécanismes de connaissance client et l'utilisation d'un matériel informatique propre servant à l'authentification.

---

[27] La diversité des offres disponibles pour créer des portefeuilles, en termes de fournisseur de service ainsi qu'en typologie de portefeuille (en ligne ou mobile, sur ordinateur, support physique protégé, …) ainsi que leur facilité d'utilisation favorise la mise à disposition de multiples portefeuilles par une personne client d'un PSAN.

[28] L'usage des VPN est généralisé parmi les professionnels et fréquent pour les particuliers (au sein de la communauté des *gamers* par exemple). Aussi l'usage du VPN doit être rapproché d'autres indices afin d'affiner le profil d'un utilisateur, en complément des listes discernant les VPN à usage non professionnel.

### 4.3.3 Portefeuilles non hébergés

Concernant les flux d'actifs numériques en provenance de portefeuilles non hébergés[29] (*unhosted wallets*), les PSAN peuvent demander à un client qui utilise un portefeuille non hébergé de leur communiquer l'adresse publique du portefeuille afin d'utiliser un outil d'analyse transactionnelle pour reconstituer l'historique des mouvements ayant eu lieu sur ce portefeuille depuis sa création (montants, dates, portefeuilles d'origine et de destination).

Un PSAN peut également utiliser un outil d'analyse transactionnelle pour évaluer si une adresse publique de passage de crypto-actifs a été générée par un autre PSAN : dans le cas contraire, il s'agit possiblement d'un portefeuille privé. Cependant dans la mesure où les adresses des PSAN ne sont pas toutes identifiées et que certains PSAN génèrent une nouvelle adresse par transaction, cette information ne suffit pas à déterminer si le flux provient d'un portefeuille non hébergé.

### 4.3.4 Technologies favorisant l'anonymat des détenteurs de crypto-actifs

Il est en principe possible d'analyser l'intégralité des flux (montant, adresse de l'émetteur et du destinataire, horodatage) sur un actif numérique. Néanmoins certains actifs numériques ont pour objectif de favoriser l'anonymat de leurs utilisateurs : le GAFI parle d'AEC ou *privacy coins*[30] (*cf. supra* 3.3.3.). Ces derniers sont un obstacle à l'analyse de risque en amont d'une opération avec un PSAV.

La réglementation française n'interdit pas les crypto-actifs à anonymat renforcé. Les PSAN qui souhaitent vendre ou acheter des crypto-actifs de cette nature doivent toutefois disposer d'un dispositif LCB-FT suffisamment performant pour analyser et atténuer les risques inhérents à ces crypto-actifs.

Dans une certaine mesure, les outils d'analyse transactionnelle de *blockchain* peuvent aider à appréhender ces risques relatifs aux technologies permettant de dissimuler l'identité de l'émetteur, du destinataire, du détenteur ou du bénéficiaire effectif (*AEC*, mixeurs, *etc.*) Il est ainsi possible d'identifier si des crypto-actifs proviennent d'un échange, d'un mixeur, d'une transaction sur l'internet clandestin (*dark web*) ou d'autres processus permettant de brouiller l'origine des actifs numériques. Certains de ces dispositifs permettent par ailleurs l'émission de « certificats de conformité » à destination des PSAN et dont l'objectif est d'attester de la traçabilité des opérations. La récupération de ces certificats ou d'autres justificatifs auprès du client constitue cependant une démarche coûteuse et complexe, qui ne sera *a priori* réalisée que lorsque d'autres indices laissent à penser que la transaction examinée est à risque.

Pour donner une référence au marché, une liste des actifs numériques à haut risque, impliquant un risque accru de BC-FT et nécessitant par conséquent la mise en place d'une vigilance renforcée de la part d'un PSAV, pourrait être construite en collaboration avec les acteurs de la place au travers de leurs associations représentatives.

---

[29] Dans le cas du portefeuille non hébergé, le détenteur de crypto-actifs assure lui-même la conservation de ses clés et ne recourt pas au service de stockage d'un PSAV.
[30] *Cf.* [6] du glossaire.

### 4.3.5 *Blockchain* et origine ou destination géographique des fonds et des crypto-actifs

En cas d'achat ou de vente d'actifs numériques contre monnaie ayant cours légal, la localisation du compte bancaire du client ou de sa contrepartie permettent de déterminer l'origine ou la destination géographique des fonds.

La question se pose différemment lorsqu'on en vient à rechercher l'origine ou la destination géographique des actifs numériques. Cette notion est en effet étrangère aux principes constitutifs d'une *blockchain*. Aucune donnée géographique n'est en effet attachée à une adresse de crypto-actif. L'information peut donc être difficile à obtenir, eu égard au fait que les actifs sont sous le contrôle du détenteur de la clé privée de chaque adresse.

### 4.3.6 *Blockchain* et gel des avoirs

Dans la pratique, un PSAN conservateur des actifs numériques de ses clients, doit être en capacité d'appliquer proactivement des mesures appropriées de gel des avoirs, en vue de bloquer l'accès à un compte ainsi que de consigner temporairement les actifs numériques liés dans un compte séquestre (ou *wallet* de quarantaine). Cela afin d'empêcher le client concerné de mouvementer ses actifs numériques vers une autre adresse publique.[31]

Il serait techniquement envisageable de filtrer automatiquement les portefeuilles faisant l'objet de mesures de gel des avoirs à l'aide de *smart contracts*[32] basés sur une liste noire d'adresses régulièrement mise à jour. Ces possibilités techniques ouvriraient également la perspective de listes partagées de portefeuilles soumis à des mesures restrictives, listes qui permettraient de repérer les portefeuilles aisément afin de suivre une piste d'audit et apprécier *a posteriori* l'application des mesures de gel des avoirs.

[31] Par construction il n'est cependant pas possible d'empêcher un transfert d'actif numérique à destination d'une adresse publique sur *blockchain.* Aussi le volume des actifs numériques d'un portefeuille faisant l'objet d'une mesure de gel peut croître durant la période de gel si celui-ci fait l'objet de transferts à son crédit; mais ces fonds seront bloqués par les mesures du PSAN conservateur.

[32] *Cf.* [7] du glossaire.

## 4.4 La mise en œuvre de la *travel rule*

Le GAFI a étendu en 2019 l'application de sa 16ème Recommandation relative à la transparence des virements électroniques aux transferts d'actifs virtuels. Comme indiqué dans son évaluation à douze mois, le GAFI invite les acteurs du secteur à intensifier leurs efforts pour développer une solution permettant de mettre en œuvre la transparence des transferts d'actifs virtuels.

Dans cette perspective, les acteurs de la place ont été interrogés sur les technologies possibles et les potentiels obstacles identifiables.

Les répondants ont unanimement souligné la nécessité d'un développement coordonné, à l'échelon supranational, de solutions de mise en œuvre de la transparence des transferts d'actifs virtuels ou de solutions interopérables. L'une des conditions préalables à la construction d'une solution technique efficace de partage d'informations serait la mise en place d'une norme de messagerie ou d'un accord sur le contenu et la structure des messages entre fournisseurs de services d'actifs virtuels.

À ce titre, les répondants ont cité les initiatives engagées dans une approche de standardisation (voir 5.2).

Des projets reposant sur l'identité auto-souveraine[33] ont également été cités comme étant une piste technique possible et décentralisée pour exposer les informations d'identité tout en renforçant la maîtrise des risques en termes de confidentialité des données individuelles et de cybersécurité.

Quant à l'accès aux données pour les instances de contrôle, le groupe de travail n'a pas identifié d'obstacle technologique a priori. Un membre du groupe a par exemple décrit une solution possible s'appuyant sur la mise en œuvre d'API et qui permettrait d'apporter la transparence des transferts et rendre les informations disponibles en temps réel aux autorités.

[33] *Cf.* [8] du glossaire.

# 5 Pistes technologiques identifiées

## 5.1 Outils d'analyse transactionnelle de *blockchains*

### 5.1.1 Description sommaire du fonctionnement

Les outils d'analyse transactionnelle de *blockchains* sont utilisés par de nombreux PSAN pour faciliter la mise en œuvre de leurs obligations au titre de la réglementation LCB-FT.

Leur principe est d'exploiter un nœud d'une (ou plusieurs) *blockchain(*s) qui leur donne accès aux données en temps réel et leur permet de suivre et d'analyser les transactions portant sur des crypto-actifs au fil de l'eau. Sur la base des opérations enregistrées sur une longue période et en recourant à des techniques d'intelligence artificielle, ces outils peuvent aussi établir l'analyse comportementale d'une adresse liée à un portefeuille de crypto-actifs. Ces outils permettent donc d'identifier un portefeuille à risque en analysant les flux de crypto-actifs qui y entrent ou en sortent. À partir d'un portefeuille signalé à risque, les outils peuvent également remonter des alertes, aider à retracer le parcours de fonds d'origine suspecte.

Concrètement, pour une transaction donnée, l'outil fournit à son utilisateur les adresses d'origine ou de destination de crypto-actifs et attribue un score de risque (« *scoring* »)[34] aux adresses analysées.

Par ailleurs, ces outils contribuent à une forme partielle de désanonymisation de la *blockchain.* La pratique du *clustering* permet en effet d'identifier l'ensemble des adresses liées à un client souhaitant passer une transaction. Ces outils permettent également d'associer une identité à des adresses publiques, par la détection de l'appartenance d'adresses ou de portefeuilles à des entreprises en les faisant correspondre à des personnes physiques ou morales (plateformes d'échange, places de marché, etc.)[35]. Pour cela plusieurs techniques complémentaires sont employées à travers des transactions de test sur des acteurs ciblés, s'appuyant sur le *screening* de ressources internet accessibles (incluant les réseaux sociaux ou encore l'exploitation de l'internet clandestin) et permettant de repérer ou d'identifier des adresses suspectes.

Enfin certains outils d'analyse transactionnelle intègrent également des bases de données publiques[36], permettant une automatisation partielle des investigations manuelles d'identification.

Ces outils sont développés par un petit nombre de prestataires spécialisés : ils fonctionnent avec des API qui peuvent être interfacées avec les logiciels de *trading* des PSAN. Le développement d'outils de ce type par les PSAN eux-mêmes serait, de l'avis des membres du groupe, long, coûteux et nécessiterait des compétences techniques importantes. Un avantage du développement externe de ces outils est que la remontée d'informations par leurs utilisateurs aboutit à une coopération de fait entre tous ces utilisateurs permettant de déclarer des activités suspicieuses. L'inconvénient potentiel associé peut être une normalisation excessive des approches de l'ensemble des acteurs du marché.

Ces outils offrent toutefois une importante liberté de paramétrage au profit de leurs utilisateurs, susceptible d'atténuer cet inconvénient. Par ailleurs, en fonction des paramétrages et des algorithmes de *clustering*, les résultats reposent sur des probabilités de concordance de noms : comme pour

---

[34] Le score de risque calculé est la résultante pondérée de plusieurs catégories de risques parmi lequels *exchange*, *mixing*, *gambling*, *darknet*, *ransomware*, *hacking*, *Ponzi* ou terrorisme.
[35] Des techniques de *web scraping* et d'*open source intelligence* sont notamment utilisées.
[36] Comme des listes de sanctions OFAC.

d'autres outils d'alerte, les acteurs sont donc amenés à faire eux-mêmes la part entre les faux positifs et les cas où il est nécessaire, par exemple, de stopper les transactions.

Ces outils restent relativement récents et rencontrent un certain nombre de limites techniques. Il est ainsi impossible de reconstituer l'historique et le suivi de transactions impliquant des crypto-actifs à anonymat renforcé (*AEC*, *privacy coins*). Il en est de même concernant des protocoles de second niveau tels que *Lightning Network,* SKALE, Loopring, etc. Enfin l'antériorité de ces outils est encore limitée pour assurer une bonne objectivation de leur performance au regard des cas d'utilisation identifiés.

### 5.1.2 Questions identifiées par le groupe

Les questions qui se posent aux acteurs du marché et aux autorités sont toutes en lien avec l'opportunité de l' adoption de ces outils d'analyse transactionnelle et de leur utilisation systématique à des fins de LCB-FT. À cet égard, le groupe de travail a recensé les points suivants.

En premier lieu, le coût de ces solutions (abonnement au cas par cas, solution permanente) peut représenter une charge financière conséquente pour des acteurs PSAN au volume d'activité modeste et justifier, pour ces acteurs et en fonction de leur niveau de risque, l'utilisation de techniques d'analyse alternatives moins sophistiquées.

En second lieu, le champ couvert par ces outils n'est pas exhaustif. En particulier :

- Il peut être nécessaire pour un PSAN de recourir à plusieurs outils complémentaires en fonction du portefeuille de crypto-actifs couvert par son activité ;
- Comme mentionné plus haut dans le rapport, certains crypto-actifs ne sont pas couverts par les outils d'analyse transactionnelle parce qu'ils sont récents ou peu utilisés [37] ; d'autre part ces outils ne sont pas adaptés à certains crypto-actifs développés sur des *blockchains* privées ou spécialement développés pour ne pas être traçables (*AEC*, *privacy coins*)[38].

Enfin, le marché et les autorités doivent encore acquérir une appréciation plus fine quant aux performances de ces outils et leur paramétrage.

En effet le degré de performance de ces outils dépend de l'exhaustivité et la qualité des données collectées sur le web, ainsi que de l'efficience des modèles de *clustering* employés, qu'ils soient déterministes ou probabilistes.

Le paramétrage pose, quant à lui, la question des avantages comparés des différentes approches actuellement constatées sur le marché : certains PSAN s'appuient sur le paramétrage par défaut de l'outil, tandis que d'autres le modifient soit à des fins de test de l'outil, soit pour une meilleure intégration dans les processus. Dans les deux cas de figure (paramètre par défaut, personnalisation), la question qui se pose aux autorités est celle de la qualité du paramétrage, au regard de la réglementation et de l'approche par les risques de l'utilisateur.

---

[37]. De fait, un grand nombre de crypto-actifs ne sont pas couverts par ces outils mais ils représentent une faible part des volumes de crypto-actifs échangés.

[38] L'usage de ces crypto-actifs est toutefois marginal dans l'activité des PSAN, notamment au regard de l'intensification des mesures de vigilance appliquées par ces derniers

## 5.2 Initiatives de standardisation des communications

### 5.2.1 L'industrie s'est emparée du sujet

Les travaux du groupe de travail ont permis d'identifier des initiatives proposant une démarche de standardisation ainsi que des solutions d'acteurs regtech s'appuyant sur ces initiatives. Ces travaux s'attèlent à définir et mettre en œuvre en priorité un protocole de communication en vue de permettre aux PSAV d'échanger les informations requises ; le traitement de la problématique d'identification mutuelle des PSAV (« *Know your VASP* »), qu'il convient de distinguer de la codification technique normalisée des identifiants de PSAV, semble moins avancé alors qu'il est crucial pour le déroulement du processus d'ensemble de la *travel rule*.

Dans le cadre de ses travaux le groupe de travail a notamment évoqué les initiatives interVASP et OpenVASP. InterVASP est une initiative de standardisation du format de message[39] de la *travel rule*, conduite par des experts internationaux réunis au sein d'un groupe de travail international. OpenVASP vise à concevoir et développer une solution de protocole d'échange de ces messages ; les travaux sont menés par un collectif d'acteurs suisses de l'industrie *blockchain* et crypto, dans une démarche ouverte et collaborative.

De façon générale, les diverses initiatives en cours, qu'elles soient en termes d'élaboration de standards[40] ou de protocoles[41], guidant le développement de solutions *ad hoc*, ou bien de solutions *open source*[42] ou commerciales[43] prêtes à l'emploi ou à l'intégration et s'appuyant sur les standards ou protocoles précités, démontrent la volonté de l'industrie des crypto-actifs de prendre en compte les exigences de la *travel rule* et de proposer des solutions pratiques.

Cette multiplicité de l'offre fait toutefois émerger en creux la question de l'interopérabilité qui doit être assurée afin d'éviter une fragmentation des flux en crypto-actifs entre différentes communautés de PSAV réunis par un même outil de *travel rule*. À cet égard, il convient d'éviter que les réglementations des différentes juridictions ne contribuent à figer une situation fragmentée, alors même que les solutions techniques peuvent converger à moyen terme[44].[45]

Enfin certains membres du groupe soulignent les enjeux commerciaux et de compétitivité qui doivent permettre d'assurer le libre-choix des PSAV dans l'adoption d'un outil de *travel rule*, c'est-à-dire sans devoir dépendre nécessairement d'acteurs prépondérants dans l'écosystème ou de zones régionales en particulier.

La définition de standards interopérables apparaît donc comme une condition nécessaire pour une applicabilité effective et la plus large possible de la *travel rule* ; son succès devrait dépendre de la

---

[39] Autrement dit les spécifications définissant le format précis du message (ou *payload*) échangé entre les contreparties appliquant la règle de la *travel rule* ; les travaux du groupe ont abouti à un standard dénommé IVMS101 qui semble s'imposer parmi les acteurs mettant en œuvre des solutions de *travel rule*.

[40] Par exemple le *Joint Working Group interVASP* ou le *Travel Rule working group*

[41] Par exemple *Open VASP* ou le *Travel Rule Protocol*

[42] Par exemple *TRISA*

[43] Par exemple *Shyft* ou *Sygna Bridge*

[44] À titre d'illustration les travaux du protocole de communication OpenVASP s'appuient désormais sur le format de message standardisé interVASP.

[45] Ce problème est dénommé en anglais *sunrise issue*, caractérisant des juridictions transposant la *travel rule* successivement mais de façon non concomittante, ce qui complique l'applicabilité de la *travel rule* pour un PSAV effectuant une transaction avec une contrepartie dépendant d'une juridiction n'appliquant pas encore cette règle.

participation la plus large possible des représentants de l'industrie des PSAV et des PSAN aux groupes de discussion et de définition de ces standards.

### 5.2.2 Enjeux et perspectives d'une mise en œuvre de la *travel rule*

Les travaux du groupe de travail ont permis de mettre en lumière les enjeux et les perspectives suivantes.

**(i) Le constat : une dynamique à concrétiser**

Le constat posé par le GAFI en juin 2020 sur la mise en œuvre de la *travel rule* n'a pas significativement changé depuis mai 2019 (lors de sa session ouverte du GAFI à l'industrie), notamment sur l'absence de solution technique prête à l'emploi pour les PSAV.

À cet égard, peu d'initiatives de discussion sur le sujet de la *travel rule* entre PSAV ont été recensées par le groupe de travail au niveau national et européen ainsi qu'une faible participation aux initiatives internationales. Cet état de fait peut être dû à une insuffisante prise de conscience collective de ces sujets ou un manque de disponibilité ou de ressources des acteurs. La difficulté anticipée à mettre en œuvre l'échange des données requises peut également être un frein à la participation à des initiatives collectives.

Aujourd'hui, les acteurs sont en mesure de collecter les données (entrantes et sortantes) nécessaires à la *travel rule* mais la véracité de ces données collectées reste un enjeu, notamment pour les clients personnes physiques non professionnels. Les outils d'analyse à disposition n'intègrent actuellement pas les protocoles requis pour mettre en œuvre la *travel rule*.

Surtout, se pose de manière aiguë la question de la confiance au sein de la communauté des PSAV, en particulier dans le contexte d'un rythme accru de création de plateformes opérant depuis l'étranger. La principale difficulté actuelle réside d'ailleurs dans l'impossibilité d'identifier avec certitude les acteurs exerçant l'activité de PSAV dans le monde ainsi que leurs adresses sur la *blockchain*.

Dans ce contexte, la communication entre les PSAV est une pratique essentielle pour la mise en œuvre des règles de conformité. Celle-ci se fait notamment via des groupes de discussion en ligne restreints et sécurisés, ou au sein d'associations représentatives[46], et permet d'échanger des bonnes pratiques. Toutefois ces moyens d'échange sont limités par leur effet de réseau (par exemple les responsables de conformité pour une zone géographique donnée) et par les restrictions de confidentialité qui ne permettent pas la transmission de données individuelles, notamment pour les besoins de la *travel rule*.

Les dispositifs d'enregistrement des plateformes dans certaines juridictions[47] sont un facteur important pour établir la confiance nécessaire entre PSAV, faciliter l'identification et la communication entre acteurs mais les champs des PSAV concernés restent limités et fractionnés géographiquement. La question de la signification des enregistrements suivant les juridictions et de la différence des exigences associées se pose également.

Certains acteurs français témoignent aujourd'hui de leur ouverture pour approfondir les réflexions engagées sur le sujet : par exemple au sein des associations de place, auprès de contacts européens, auprès de représentants des initiatives internationales de standardisation, en participant à des démarches de test ou bien des expérimentations si l'opportunité se présentait, ou encore en créant une *task force* thématique. Cette démarche ne pourra cependant se développer qu'en s'assurant de la

[46] Comme l'ADAN (Association pour le Développement des Actifs Numériques)
[47] Par exemple, en France, l'enregistrement créé par la loi PACTE.

création d'une dynamique partagée et en intégrant les contraintes en ressources des acteurs participants. La dynamique pourrait également être étendue en intégrant des acteurs d'autres juridictions, habitués à opérer avec les PSAN français.

**(ii) La question de l'identification des PSAV contreparties**

La bonne mise en œuvre de la *travel rule* nécessite un niveau minimal de confiance entre les deux PSAV éventuellement concernés par un transfert de crypto-actifs : si l'un des deux PSAV fait défaut dans ses obligations, l'autre PSAV partie prenante ne pourra pas accomplir sa tâche de conformité de façon vraiment satisfaisante.

Cette confiance peut être facilitée par les mécanismes permettant l'identification des PSAV. En la matière, plusieurs options sont possibles, et sur la base de ces mécanismes, plusieurs pratiques envisageables pour les PSAV.

Dans le contexte actuel où les dispositifs d'enregistrement ou les mécanismes d'identification des PSAV restent fractionnés et peu harmonisés ou coordonnés, une solution possible pour les PSAV est l'établissement d'une liste d'adresses de confiance (*white-listing*) : en d'autres termes, le PSAV n'autoriserait le transfert d'actifs numériques qu'entre adresses certifiées. Cette procédure serait toutefois moins aisée à mettre en œuvre dans le cadre d'une activité « de détail » que dans celui d'une activité « BtoB ».

D'autres perspectives seraient naturellement ouvertes par la création d'un registre mondial des PSAV, sur la base éventuelle d'enregistrements effectués par les différentes juridictions responsables[48]. La mise en place d'un tel registre nécessiterait un minimum d'harmonisation entre juridictions, afin de garantir la symétrie et la qualité des informations requises pour la bonne application de la *travel rule*.

Les membres du groupe de travail sont particulièrement sensibles à ce dernier point. À défaut, la création d'un registre global des PSAV pourrait avoir l'effet indésirable d'autoriser – voire d'inciter – à opérer avec des PSAV enregistrés indépendamment de leur niveau réel de conformité aux principes réglementaires de la LCB-FT. Par ailleurs, l'enregistrement d'un PSAV doit être envisagé dans la durée ; son maintien dans le registre doit donner une assurance suffisante que son niveau de conformité n'est pas significativement inférieur à celui qui était le sien au moment de l'enregistrement.

Aussi un registre mondial des PSAV ne devrait pas être considéré comme un outil suffisant à lui seul à l'établissement de la confiance, mais plutôt comme une aide dans l'évaluation qu'un PSAV peut faire d'un PSAV contrepartie, en assurant son identification et en fournissant des renseignements sur sa juridiction et son éventuelle autorité de contrôle. Le recours à d'autres méthodes comme les outils d'analyse transactionnelle cités devrait permettre à un PSAV de compléter son évaluation du risque.

L'établissement d'un registre global des PSAV pourrait être favorisé au niveau de l'Union européenne par les réflexions en cours du législateur européen, visant une harmonisation du secteur des actifs virtuels[49]. Cette dernière, allant au-delà de la LCB-FT, porte sur l'ensemble du cadre applicable au

[48] La question de l'identification du PSAV d'une contrepartie est une thématique dans le champ de réflexion du GAFI.

[49] Le plan d'action de la Commission européenne propose de mettre en place une norme de *travel rule*. Cette intégration de la *travel rule* au cadre juridique européen pourrait se faire à l'occasion des propositions législatives relatives aux crypto-actifs (fin 2020) ou à la lutte anti-blanchiment (début 2021).

secteur des actifs numériques et notamment des exigences en matière d'enregistrement et de contrôle, ce qui pourrait renforcer l'intérêt d'un registre.

On rappellera enfin que les transactions ne s'effectuent pas toujours entre deux PSAV : la contrepartie d'un PSAV peut être par exemple une plateforme non répertoriée (plateforme de jeu par exemple) ou bien encore un portefeuille non hébergé (« *self custody* »). Dans ces circonstances et en application des règles de la *travel rule*, le PSAV doit demander les informations d'identification de la contrepartie auprès de son client, ce qui pose la question du degré de confiance à accorder aux informations fournies par celui-ci (erreurs faites par inadvertance ou par volonté de dissimuler). Les PSAV doivent donc vérifier les déclarations de leur client. Cette problématique est bien identifiée par le GAFI. Elle n'est pas fondamentalement différente d'autres situations, dans le secteur financier traditionnel, où l'information est déclarative. Il est vrai toutefois que, pour les PSAV, ces vérifications peuvent s'avérer techniquement complexes ou difficiles à assurer suivant les cas de figure.

#### (iii) La mobilisation nécessaire à la mise en œuvre d'une solution opérationnelle

La mise en œuvre opérationnelle de la *travel rule* nécessite une certaine collaboration entre PSAV : au niveau national, européen mais aussi international ; un enjeu est d'assurer cette collaboration incluant l'ensemble des acteurs.

En effet, une infrastructure ou un protocole susceptible de faciliter la *travel rule* ne peut relever que d'une démarche collective, intégrant non seulement les questions d'identification déjà évoquées, mais également celles de la sécurité, la souveraineté, le stockage et la gestion des données. Les PSAV peuvent contribuer à la définition de ces processus et à leur mise en œuvre, notamment ceux relatifs à l'obtention des informations de la part des clients. D'autres acteurs, tels que les prestataires d'analyse sur *blockchain* (*cf.* 5.1. notamment) pourraient avoir un rôle à jouer, en fournissant des composantes d'une solution, notamment par leur capacité à tracer une partie des flux.

Une telle démarche collective implique une identification bien comprise et partagée des rôles, ainsi qu'un consensus sur les moyens techniques à retenir pour assurer les opérations requises. En particulier, les acteurs français et européens gagneraient à se positionner plus clairement vis-à-vis des initiatives internationales identifiées et, si elles leur paraissent un point de départ utile, à identifier les compléments ou ajustements à apporter pour aboutir à un processus opérationnel partagé répondant à l'ensemble des défis posés par la *travel rule*. Enfin une alternative pourrait être le lancement d'initiatives ou projets analogues au sein des acteurs de l'écosystème français ou européen.

Il ressort des échanges du groupe de travail que le niveau d'information du secteur français des PSAV sur la *travel rule* est perfectible. Le présent rapport est susceptible de renouveler leur prise de conscience. D'autres démarches telles que le test par les PSAV français des solutions de *travel rule* pourraient renforcer la sensibilisation de la place et l'identification des enjeux opérationnels. Enfin, pour s'intégrer à des dynamiques déjà existantes, la place française pourrait utilement développer ses contacts avec les porteurs des initiatives internationales en cours. Des réflexions ou actions en ce sens ont été engagées par certains acteurs PSAV de la place et par l'association représentative de l'industrie.

Au niveau européen, un groupe de réflexion représentant les intérêts de l'industrie *blockchain* et des crypto-actifs (*The Blockchain and Virtual Currencies Working Group*, BVC WG) a été cité et vise à faire valoir ces enjeux auprès du législateur. Le présent groupe de travail n'a pas identifié d'autre enceinte européenne qui aurait significativement avancé dans ses réflexions sur la mise en œuvre de la *travel rule*. Une dynamique est donc à créer là aussi, pour accompagner au plan opérationnel les travaux réglementaires en cours.

### (iv) La question des solutions temporaires ou de « transition »

Le temps nécessaire au développement d'un outil partagé à une échelle significative (au moins européenne) a amené le groupe de travail à évoquer rapidement l'existence de solutions alternatives ou de transition.

Outre les standards techniques précités, des solutions techniques alternatives ou de transition existent en effet, comme des solutions de messagerie avec une fonctionnalité de chiffrement asymétrique (p. ex. « PGP »). L'enjeu pour le PSAV utilisateur de ces solutions est d'être en capacité de les intégrer dans son système d'information afin d'automatiser les actions sans valeur ajoutée. En outre, ces solutions alternatives ne semblent pas de nature à résoudre les problématiques générales déjà exposées (mise en œuvre d'un outil partagé, qui suppose un minimum de consensus entre les acteurs).

De manière plus générale, le risque que les différentes juridictions adoptent un rythme différent et une approche plus ou moins proactive pour répondre aux exigences de la *travel rule* a été évoqué par certains membres du groupe de travail. Ces éventuels décalages d'exigences dans le temps pourraient constituer un désavantage compétitif pour les PSAV devant supporter plus tôt que leurs homologues une charge de conformité accrue et les coûts d'éventuelles solutions temporaires.

# 6 Annexes

## 6.1 Glossaire

| | | |
|---|---|---|
| **[1]** | PSAV (*VASP*), PSAN | Le GAFI définit les Prestataires de services en actifs virtuels (PSAV, ou *VASP — Virtual Asset Service Provider* — en anglais) comme toute personne exerçant à titre commercial l'une des activités suivantes au regard des actifs virtuels : l'échange d'actifs virtuels contre monnaie ayant cours légal ; l'échange entre actifs virtuels ; le transfert; la conservation et/ou l'administration; la participation à la fourniture de services financiers liés à une offre d'un émetteur et/ou une vente d'un actif virtuel.<br><br>La réglementation française introduit les prestataires de services en actifs numériques (PSAN) dont le périmètre des activités réglementées s'applique aux actifs numériques (voir note suivante) et recouvre : d'une part, pour le compte de tiers, la conservation, l'échange contre monnaie ayant cours légal, l'échange contre actifs numériques, la réception et la transmission d'ordres, la fourniture de différents services financiers (gestion de portefeuille, conseil aux souscripteurs, prise ferme, placement garanti et non garanti) ; et d'autre part l'exploitation d'une plateforme de négociation. |
| **[2]** | Actifs virtuels, Actifs numériques, Crypto-actifs | Le GAFI définit les actifs virtuels (ou *Virtual Assets* en anglais) comme la représentation numérique d'une valeur qui peut être échangée de manière digitale, ou transférée, et qui peut être utilisée à des fins de paiement ou d'investissement. Les actifs virtuels n'incluent pas les représentations numériques des monnaies fiduciaires, valeurs mobilières et autres actifs financiers qui font déjà l'objet d'autres dispositions des Recommandations du GAFI.<br><br>La réglementation française utilise le terme d'actif numérique comme étant : 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), à l'exception des instruments financiers et des bons de caisse ; ou bien toute représentation numérique d'une valeur qui n'est pas émise ou garantie par une banque centrale ou par une autorité publique et qui ne possède pas le statut juridique d'une monnaie, mais qui est acceptée comme un moyen d'échange et qui peut être transférée, stockée ou échangée électroniquement.<br><br>Les crypto-actifs sont un terme générique désignant l'ensemble des actifs émis et échangés sur la *blockchain* : ils englobent les actifs virtuels et actif numériques. |
| **[3]** | Phases du blanchiment | Le blanchiment des capitaux est caractérisé par trois phases : une phase initiale de placement qui est l'introduction de bénéfices illégaux dans le système financier ; une phase de dissimulation qui consiste en une série de conversions ou de déplacements des fonds |

| | | |
|---|---|---|
| | | pour les éloigner de leur source ; une phase de conversion qui vise à réintroduire les fonds dans des activités économiques légitimes. |
| **[4]** | Mixeurs (*mixers*), Mélangeurs (*tumblers*) | Les mixeurs (*mixers*) ou mélangeurs (*tumblers*) sont des services permettant de favoriser l'anonymat d'actifs numériques en mélangeant des flux d'un même type d'actif numérique traçable (le bitcoin par exemple) issus de différents portefeuilles en vue de les reventiler vers des adresses cryptographiques souhaitées, entraînant une rupture de la chaîne de traçabilité de ces actifs numériques dans l'historique des différents portefeuilles de détention. |
| **[5]** | Navigateur Tor | Les navigateurs Tor exploitent le réseau informatique décentralisé Tor favorisant une navigation anonymisée des ressources sur le web. Plusieurs solutions logicielles ont été développées pour tirer partie du réseau Tor, incluant outre les navigateurs web, des plateformes, systèmes d'exploitation et modules de messagerie. |
| **[6]** | *AEC*, *Privacy coins* | Les *AEC* (*Anonymity-Enhanced Cryptocurrencies*) désignent une classe d'actifs virtuels conçus pour favoriser l'anonymat de ses détenteurs en s'appuyant sur des *blockchains* intraçables ; Monero, Zcash, Grin ou Dash sont des exemples cités usuellement en tant qu'*AEC*. Leur usage permet aux contreparties d'une transaction d'assurer leur anonymat tout en permettant une configuration du niveau de confidentialité. L'expression usuelle *Privacy coin* est équivalente à *AEC*. |
| **[7]** | *Smart contracts* | Un *smart contract* désigne une fonctionnalité des *blockchain*s permettant le déploiement et l'exécution de programmes autonomes et spécifiques sur une *blockchain* donnée ; ils se déclenchent automatiquement lorsque les conditions prédéfinies sont rencontrées. |
| **[8]** | Identité auto-souveraine (*Self Sovereign Identity)* | Un dispositif d'identité auto-souveraine (ou *Self Sovereign Identity — SSI* — en anglais) permet à une personne ou organisation de garder le contrôle des éléments de justification de son identité en lui permettant d'exposer, avec son consentement, les caractéristiques appropriées de son identité. Son fonctionnement peut être expliqué par analogie avec celui d'un portefeuille dont le propriétaire extrait à la demande les justificatifs requis. L'identité auto-souveraine s'affranchit d'intermédiaires et peut s'appuyer sur une architecture décentralisée, comme une blockchain. |
| **[9]** | *Chain swap* | Le *chain swap* (littéralement « permutation de chaîne ») est un processus assurant le déplacement d'un actif virtuel d'une *blockchain* vers une autre *blockchain*. Il permet ainsi aux détenteurs des actifs déplacés d'étendre le périmètre d'utilisation de leurs fonds. |

## 6.2 Références documentaires

| | | |
|---|---|---|
| **[1]** | GAFI | Recommandations du GAFI (mises à jour en juin 2019) |
| **[2]** | GAFI | *Guidance for a risk-based approach Virtual assets and Virtual asset service providers* (juin 2019) |
| **[3]** | GAFI | *Public Statement on Virtual Assets and Related Providers* (juin 2019) |
| **[4]** | GAFI | *12-month review of the revised FATF Standards on Virtual Assets and Virtual Asset Service Providers* (juillet 2020) |
| **[5]** | GAFI | *Virtual Assets Red flag indicators of money laundering and terrorist financing* (septembre 2020) |
| **[5]** | TRACFIN | Rapports « Tendances et analyse des risques de BC-FT » |
| **[6]** | JWG interVASP | IVMS101 interVASP data model standard - Issue 1 Final (mai 2020) |
| **[7]** | OpenVASP | OpenVASP : an open protocol to implement FATF's Travel rule for Virtual assets (livre blanc, novembre 2019) |
| **[8]** | Travel Rule Protocol (TRP) | *TRP specifications* |

## 6.3 Composition du groupe de travail sur l'application des règles en matière de LCB-FT au secteur des crypto-actifs

Ont été représentés en tant que membres du groupe de travail et ont participé aux discussions ou contribué aux travaux :

- Pour les autorités publiques :
  - L'ACPR
  - L'AMF
  - La Direction générale du Trésor
  - Tracfin

- Pour l'industrie des crypto-actifs et de la *blockchain* :
  - Bitit
  - Coinhouse
  - Consensys
  - Ledger
  - LGO markets
  - Thesaur.io
  - Woorton

- Pour l'industrie des institutions financières bancaires :
  - BNP Paribas
  - CACEIS
  - SG Forge