Forum Fintech ACPR-AMF

Groupe de travail sur

l'accès des prestataires de services sur actifs numériques (PSAN)

aux comptes bancaires

et sur le fonctionnement des comptes de clients bancaires lors d'achat ou de vente d'actifs numériques

Compte rendu des travaux

Ce compte rendu retrace les réflexions d'un 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, des acteurs du secteur des crypto-actifs ainsi que des institutions financières[1]. Il ne saurait engager les autorités de contrôle et entités administratives précitées (ACPR, AMF, DG Trésor, Tracfin).

Table des matières

1 Résumé 3

2 Introduction 4

3 L'accès des PSAN au compte bancaire : l'entrée en relation 5

3.1 Les constats 5

3.2 Les pistes d'amélioration 6

3.2.1 Première étape : identifier le modèle d'affaires et les enjeux en termes de LCB-FT 7

3.2.2 Seconde étape : les éléments de connaissance clients spécifiques aux PSAN 9

4 La surveillance des opérations du PSAN par sa banque 12

4.1 Le profil de risque des PSAN 12

4.2 Les moyens d'assurer une vigilance constante vis-à-vis des PSAN 12

4.3 Les scénarios de surveillance 13

4.3.1 La distinction entre les flux en lien avec les clients et ceux en rapport avec les plateformes d'échange 13

4.3.2 L'élaboration des scénarios 14

4.4 L'examen renforcé 15

5 Les opérations bancaires des clients bancaires lors d'achat ou de vente de crypto-actifs 17

5.1 Les constats 17

[1] Voir composition du groupe de travail en annexe 6.4 et la note annexée de la FBF en annexe 6.5.

5.1.1 Les difficultés rencontrées par les particuliers à l'occasion de vente ou d'achat de crypto-actifs 17
5.1.2 Les procédures mises en œuvre par les établissements bancaires 18
5.2 Les pistes d'amélioration 18
6 Annexes 20
6.1 Glossaire 20
6.2 Références documentaires 22
6.3 Description sommaire des travaux de l'ASB 23
6.4 Composition du groupe de travail 25
6.5 Note annexée au présent compte-rendu à la demande de la FBF 26

1 Résumé

Les **difficultés rencontrées par les prestataires de services sur actifs numériques (PSAN)**, et plus généralement les entrepreneurs en lien avec les technologies *blockchain*, **pour ouvrir des comptes bancaires en France** sont identifiées depuis quelques années par certains observateurs comme **un frein à l'innovation et au développement** de l'écosystème. La loi PACTE publiée en 2019, instaurant à la fois un cadre réglementaire pour ces prestataires et un accès facilité aux services de comptes de paiement, n'a pas changé fondamentalement la situation.

Un groupe de travail du Forum Fintech ACPR-AMF a donc été constitué mi-2020 pour **établir un état des lieux des problématiques rencontrées** et, sur cette base, identifier les **pistes possibles d'amélioration**. Il a rassemblé et permis le dialogue entre autorités publiques, représentants du secteur des crypto-actifs, du secteur bancaire et des consommateurs.

Les principales pistes identifiées par le groupe en matière d'entrée en relation et d'ouverture de comptes bancaires sont les suivantes.

En premier lieu, **améliorer la compréhension commune des modèles d'affaires** : parmi les actions susceptibles de contribuer à cet objectif, **une collaboration entre le secteur bancaire et le secteur des crypto-actifs** pourrait utilement porter, d'une part, **sur une meilleure formation** des acteurs de la conformité bancaire aux spécificités des services sur crypto-actifs et, d'autre part, sur une **sensibilisation des acteurs du secteur des crypto-actifs** aux contraintes de la conformité bancaire.

En second lieu, **permettre aux PSAN de mieux anticiper les demandes des établissements bancaires lors du processus d'entrée en relation.** À cet égard, le **guide pratique** développé par l'Association suisse des banquiers (ASB) fournit un exemple intéressant, en fournissant au marché un **cadre commun d'analyse** pour l'entrée en relation. Le présent rapport examine rapidement ce que pourrait être la transposition d'une telle démarche à un contexte français :

- En identifiant les **deux grandes étapes** qui pourraient structurer l'analyse préalable à l'ouverture d'un compte bancaire (1° identification du modèle d'affaires de l'entreprise future cliente et des enjeux sous-jacents en termes de LCB-FT ; 2° dans le cas des PSAN, recueil des éléments de connaissance client spécifiques au modèle d'affaires identifié)
- En mentionnant **les outils** (questionnaires, liste d'exigences) qui pourraient être développés en application de cette démarche.

Les travaux du groupe l'ont également amené à discuter de la **question de la surveillance des opérations du PSAN** client par sa banque, en cours de relation d'affaires. Cette question est en effet primordiale pour les banques qui doivent anticiper, dès l'entrée en relation, les modalités de mise en œuvre de cette surveillance.

Cette discussion a permis de clarifier les obligations des établissements bancaires teneurs de compte. Elle a également permis d'identifier **un autre axe de collaboration entre les secteurs** : l'élaboration d'une **liste commune des plateformes d'échanges de crypto-actifs** susceptibles de faciliter la surveillance des opérations et d'améliorer la pertinence des alertes générées.

À l'occasion de ses travaux, le groupe a évoqué une question d'une nature différente mais également source de difficultés : celle des **blocages, par certaines banques, des opérations d'achat (ou de vente) de crypto-actifs** par leurs clients (généralement des particuliers). Dans ce domaine, des pistes de collaboration ont aussi été identifiées, notamment **l'élaboration d'une « liste blanche »** de plateformes considérées comme étant de confiance. D'autres améliorations possibles, relatives aux procédures des établissements de crédit et à l'information des clients, sont également évoquées.

2 Introduction

Dans le secteur de la « Fintech[2] » française, les acteurs proposant des services liés aux crypto-actifs connaissent des difficultés dans leurs interactions avec le secteur financier traditionnel.

En particulier, la difficulté d'ouvrir des comptes courants auprès d'établissements de crédit français a été relevée par un rapport d'information parlementaire[3] comme un frein au développement de « l'écosystème *blockchain* » en France. Celui-ci affirmait ainsi, début 2019 : « *[…] la capacité de la France à attirer des plateformes de change sur son territoire est de fait limitée. La relation bancaire est aujourd'hui l'un des principaux freins à l'essor d'un écosystème blockchain en France. En effet, l'impossibilité d'ouverture de compte en France est un des premiers motifs de fuite des capitaux et technologie à l'étranger. En outre, il serait vain de légiférer pour favoriser l'émergence de nouveaux acteurs en France si ces derniers ne pouvaient y voir leur activité et leurs capitaux hébergés. La présence – et persistance – d'acteurs sur le territoire français renforcerait le poids de notre pays dans les négociations internationales sur la régulation des plateformes d'échanges.* »

La réticence des établissements bancaires français à effectuer ces ouvertures de comptes semble généralement liée au risque de blanchiment des capitaux et de financement du terrorisme (LCB-FT) propre aux actifs numériques et aux services associés.

En 2019, la loi PACTE est venue donner un cadre réglementaire aux prestataires de services sur actifs numériques (PSAN) et les a soumis, notamment, à l'obligation de mettre en place un dispositif assurant le respect des règles relatives à la LCB-FT ainsi que des mesures de gel des avoirs. Cette clarification réglementaire n'a pas semblé, pour autant, induire un changement profond dans les relations entre les PSAN et les établissements de crédit.

Parallèlement, avec le développement des services sur crypto-actifs, le nombre de particuliers désireux d'acheter des crypto-actifs a crû, et avec lui les difficultés rencontrées auprès de certaines banques pour l'exécution des paiements correspondant à ces transactions.

L'existence et la permanence de ces phénomènes ont motivé la mise en place d'un groupe de travail *ad hoc* du Forum Fintech ACPR-AMF, rassemblant – outre les autorités de contrôle concernées et des représentants de la Direction générale du Trésor - des représentants du secteur des crypto-actifs, du secteur bancaire et des consommateurs. Ce groupe a eu comme objectif d'établir un état des lieux des problématiques rencontrées et, sur cette base, d'identifier les pistes possibles pour atténuer ou lever les éventuels freins existants, y compris en apportant les éclairages réglementaires nécessaires.

Le présent document rend compte de ces travaux en traitant successivement :

- La question de l'accès au compte bancaire des prestataires de services en actifs numériques (PSAN) ;
- Celle de la surveillance des opérations du PSAN par sa banque teneuse de compte ;
- Et enfin, les questions liées aux opérations bancaires des clients souhaitant acheter ou vendre des crypto-actifs.

---

[2] On désigne par ce terme les entreprises, notamment les jeunes pousses, innovantes qui utilisent les technologies pour repenser les services financiers.

[3] Rapport d'information n°1624 d'Éric Woerth et de Pierre Person en conclusion des travaux d'une mission d'information relative aux monnaies virtuelles, 30 janvier 2019, p. 90-97. Le premier rapport du Comité de suivi et d'évaluation de la loi PACTE (France Stratégie, sept. 2020) évoque également ce point (« La capacité pour les PSAN à ouvrir un compte bancaire sur le territoire national », pp. 95-96)

3 L'accès des PSAN au compte bancaire : l'entrée en relation

3.1 Les constats

Les échanges entre les participants du groupe de travail confirment l'existence de difficultés rencontrées par les PSAN pour obtenir ou maintenir une domiciliation bancaire en France, obtenir des financements ou utiliser certains systèmes de paiements.

Pour expliquer ces difficultés, les représentants de l'industrie bancaire mettent en avant leur souhait de renforcer le cadre applicable aux PSAN ainsi que leurs propres contraintes en matière de LCB-FT.

Le respect de la réglementation LCB-FT est une priorité de contrôle pour l'ACPR. Comme le rappellent l'analyse nationale des risques (ANR) du COLB et l'analyse sectorielle des risques (ASR) de l'ACPR, les actifs numériques présentent des vulnérabilités intrinsèques élevées, tant en ce qui concerne le blanchiment de capitaux que le financement du terrorisme. Dès lors que ces acteurs sont soumis à la réglementation en matière de LCB-FT et de gel des avoirs, sous le contrôle de l'ACPR après enregistrement par l'AMF, le secteur des actifs numériques est toutefois considéré comme présentant un risque global modéré par l'ANR et l'ASR. Les politiques des établissements de crédit ne sont certes pas uniformes. Toutefois, il semble que, dans le cadre de leur politique de risques et de leur politique commerciale, une partie d'entre eux écarte toute relation d'affaires avec les entités opérant dans le secteur des crypto-actifs : cette politique n'est pas seulement le fait d'établissements « traditionnels », elle est aussi adoptée par certaines « néo-banques » ou établissements de paiement. Le refus de traiter avec les acteurs du monde de la *blockchain* s'étend parfois au-delà des seuls prestataires de services sur actifs numériques pour toucher des entreprises innovantes qui proposent des services non financiers[4] sur les registres distribués.

D'autres établissements ont des politiques de risques et des politiques commerciales qui permettent de nouer des relations d'affaires avec des acteurs du secteur des crypto-actifs, mais ils soulignent la complexité des dispositifs LCB-FT supplémentaires qu'il faut alors mettre en œuvre, et par voie de conséquence leur coût. Certains établissements peuvent reporter une partie ce coût sur les PSAN eux-mêmes en conditionnant par exemple une ouverture de compte à la réalisation d'audits d'évaluation des dispositifs de LCB-FT des acteurs concernés.

Dans ce contexte certains entrepreneurs français agissant dans le secteur des crypto-actifs ont préféré sélectionner des acteurs bancaires étrangers pour la gestion de leurs fonds et certains envisagent une délocalisation de leur activité et des emplois Selon les représentants de l'industrie des crypto-actifs, cette situation peut également dissuader des entreprises étrangères spécialisées dans les crypto-actifs de s'implanter en France par crainte de ne pouvoir accéder aux services bancaires voire accéder aux financements.

Aucune amélioration notable ne semble avoir été observée depuis l'introduction du statut de PSAN par la loi PACTE, qui a renforcé les exigences LCB-FT applicables aux PSAN. Le groupe n'a pas non plus relevé de cas d'exercice du « droit au compte » prévu par la loi[5] ; les représentants de l'industrie des

[4] Logistique, gestion de chaines d'approvisionnement, par exemple.

[5] L'article L. 312-23 du code monétaire et financier prévoit que les établissements de crédit doivent mettre en place des règles objectives, non discriminatoires et proportionnées pour régir l'accès des émetteurs de jetons ayant obtenu le visa de l'AMF conformément à l'article L. 552-4, des PSAN enregistrés conformément à l'article L. 54-10-3 et des PSAN ayant obtenu l'agrément conformément à l'article L. 54-10-5 aux services de comptes de dépôt et de paiement qu'ils tiennent. L'article D. 312-23 décrit les conditions de recours en cas de refus constitué

crypto-actifs précisent à cet égard que l'accès à un compte bancaire avec des services de base n'est pas nécessairement suffisant pour exercer une activité opérationnelle d'entreprise, incluant l'accès au financement, et soulignent par ailleurs le caractère fondamental de la confiance pour établir une relation bancaire durable.

Une enquête menée par l'Association pour le développement des actifs numériques (ADAN)[6]permet de préciser les difficultés ressenties par les PSAN et leur fréquence[7]. Ainsi, sur les 28 répondants à l'enquête, dont 26 possèdent, achètent, vendent des actifs numériques ou s'interposent dans ces opérations :

- 50 % affirment avoir eu des difficultés pour ouvrir un compte en France ;
- 68 % ont expérimenté un refus ou une fermeture de compte ;
- 45 % déclarent qu'il est impossible ou difficile d'avoir recours à un financement bancaire ;
- 57 % disent que leurs clients ont des difficultés dans leurs propres relations avec les banques ;
- 42% des dirigeants de plateforme ont des problèmes dans leurs propres relations bancaires.

Les répondants estiment par ailleurs, pour 85 % d'entre eux, que les relations sont moins difficiles dans le reste de l'Union européenne et 64 % envisagent de délocaliser leurs activités.

3.2 Les pistes d'amélioration

Les discussions du groupe de travail ont fait ressortir un relatif manque de confiance entre les acteurs du secteur bancaire et du secteur des crypto-actifs. Dans le contexte d'un dialogue encore à construire entre ces acteurs, ce manque de confiance s'expliquerait, d'une part, par un faible degré de connaissance par les acteurs bancaires de l'écosystème encore naissant des PSAN et des diligences LCB-FT mises en œuvre dans cet écosystème et, d'autre part, par une connaissance également limitée des PSAN des obligations des établissements bancaires en matière de LCB-FT. Ce constat débouche sur plusieurs pistes d'amélioration possibles.

En premier lieu, des actions peuvent être envisagées pour **améliorer la compréhension des modèles d'affaires par les établissements bancaires**. Certaines de ces actions peuvent être menées par les autorités publiques : ainsi, la publication récente des travaux du groupe de travail du Forum Fintech sur l'application des règles de LCB-FT au secteur des crypto-actifs[8] peut contribuer à cet objectif, tout comme le rapport du présent groupe de travail. D'autres actions peuvent être menées, et le sont parfois, par les établissements et les groupes bancaires eux-mêmes : création de centre de compétences en crypto-actifs ou écosystème *blockchain*, susceptibles de prendre le relais d'agences bancaires généralistes en tant que de besoin, sensibilisation et formation des départements conformité aux risques et spécificités de l'écosystème… Sur ce dernier point, des représentants du secteur bancaire ont mentionné les difficultés d'accès à la formation des collaborateurs en matière de crypto-actifs dans un environnement évoluant très rapidement. Une collaboration renforcée entre les

---

des établissements de crédit : sur saisie de la personne se voyant refuser l'accès aux services demandés, l'ACPR se prononce dans un délai de deux mois et peut décider le cas échéant de mettre en œuvre ses pouvoirs de sanction et de contrôle à l'égard de l'établissement. L'ACPR peut également proposer au demandeur de saisir la Banque de France pour une demande de désignation d'un établissement de crédit, au nom et pour le compte du demandeur.

[6] Voir référence en annexe

[7] Lors de l'exposé de cette enquête au groupe de travail, un représentant d'une association professionnelle bancaire a regretté qu'aucune information sur l'activité et le statut réglementaire des répondants ni sur leur dispositif de LCB-FT n'ait été recueillie pour permettre de pondérer les résultats. Il a également souligné l'intérêt qu'aurait pu revêtir une étude comparative au niveau européen.

[8] Voir référence en annexe

deux secteurs ouvrirait la possibilité d'établir des programmes et des contenus pédagogiques pertinents et à l'état de l'art.

En second lieu, et c'est l'axe principal exploré par le groupe, il paraît nécessaire **d'améliorer la visibilité des PSAN sur le processus d'entrée en relation** et les demandes susceptibles d'être faites par l'établissement ouvrant le compte. À cet égard, certains membres ont appelé l'attention du groupe sur l'exemple de la Suisse. L'Association suisse des banquiers (ASB) a publié en 2018 un *guide pratique pour l'ouverture de comptes d'entreprises pour les sociétés blockchain*[9] . Élaboré par un groupe de travail indépendant de l'autorité de contrôle, ce guide traduit la volonté des acteurs de la place de se mettre d'accord sur des exigences communes pour l'ouverture de compte. Il définit un cadre d'analyse et recense de façon pratique les attentes et informations nécessaires aux banques pour l'établissement de la relation d'affaires[10].

Le groupe de travail a examiné dans quelle mesure une approche inspirée de cet exemple était transposable dans un contexte français. De fait, la démarche suisse fournit quelques grandes étapes qui pourraient servir de base à un socle commun de la pratique des établissements français, notamment les deux suivantes :

- Identifier le modèle d'affaires et les enjeux spécifiques en termes de LCB-FT ;
- Dans le cas des PSAN, recueillir des éléments de connaissance clients spécifique au modèle d'affaires.

3.2.1 Première étape : identifier le modèle d'affaires et les enjeux en termes de LCB-FT

Comme dans la démarche suisse, il semble opportun de distinguer à l'entrée en relation le cas des entreprises exerçant une activité non-financière de celui des entreprises relevant de l'industrie des crypto-actifs (émission, services). De même il convient de déterminer si l'activité de l'entreprise demandant l'ouverture d'un compte comporte des enjeux spécifiques sur le plan de la LCB-FT.

Dans ce double objectif, la compréhension du modèle d'affaires s'avère primordiale.

La liste de points d'analyse suivante, indicative et non exhaustive, peut être utile à cette fin :

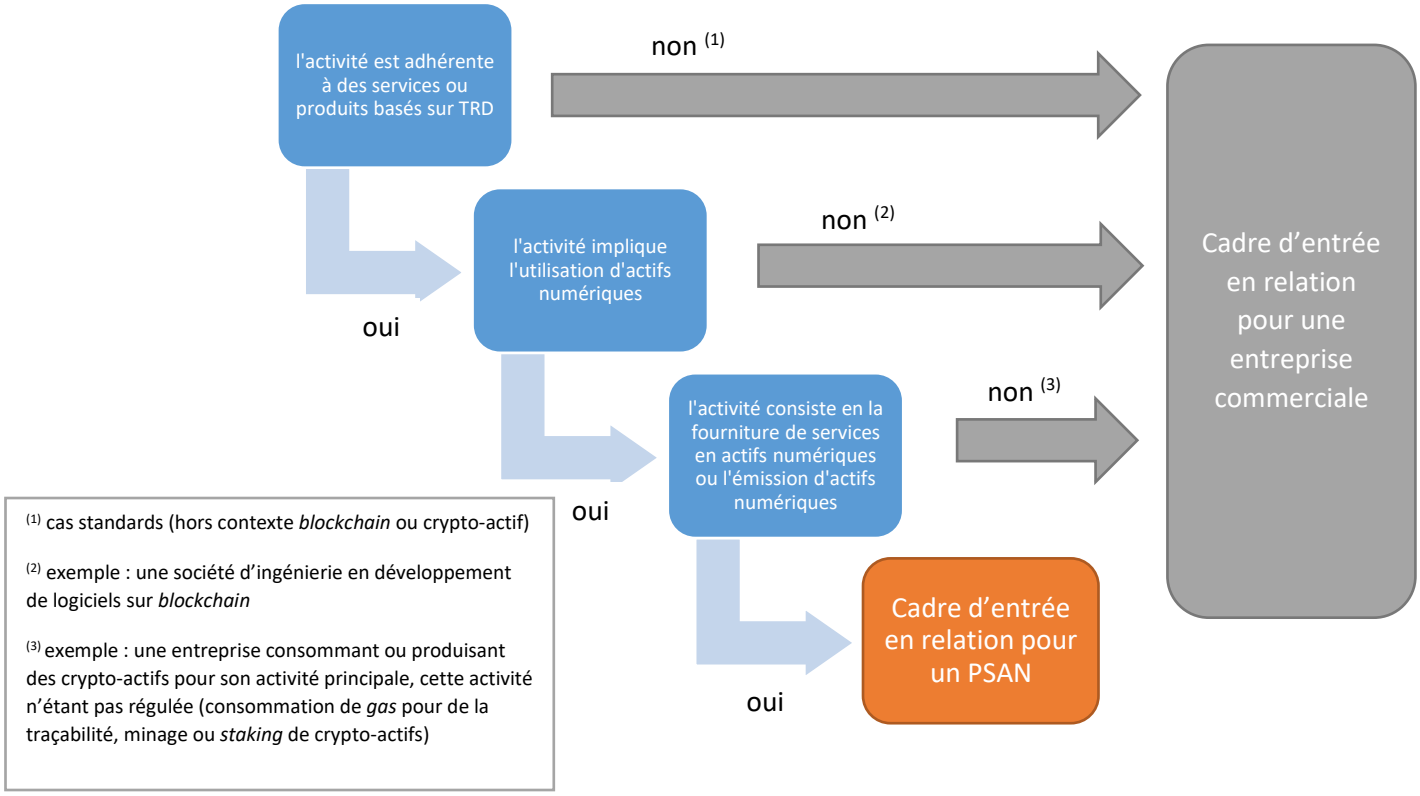
- **Mise en contexte de l'usage des technologies de registre distribué (TRD[11]) ou de crypto-actifs.** Les entreprises ayant recours aux technologies *blockchain* (ou plus généralement TRD) sont de natures diverses : prestataires de services technologiques fournissant des solutions autour de la TRD (société de service ou de conseil en informatique, éditeur de logiciel), entreprises exploitant des services de TRD pour des activités de traçabilité logistique ou industrielle, prestataires de services en crypto-actifs, etc. Une description et une mise en contexte de l'usage des TRD ou des crypto-actifs dans le cadre de l'activité de l'entreprise doivent permettre d'identifier rapidement les situations qui relèvent du cadre général de l'entrée en relation avec une entreprise commerciale et celles qui peuvent nécessiter des procédures spécifiques (cas des PSAN, notamment). On notera en particulier que l'utilisation de crypto-actifs (par exemple, l'Ethereum) comme « gaz » consommable nécessaire à l'utilisation de services de TRD n'entraine pas nécessairement des risques spécifiques de BC-FT.

[9] Voir référence en annexe
[10] Pour plus de détail, on pourra se reporter au communiqué de presse de l'ASB, voir référence en annexe
[11] Voir glossaire

- **Autres aspects du modèle d'affaires.** La description des autres aspects de l'activité et notamment des flux financiers (dont de paiement) et des flux en crypto-actifs doit permettre à la banque de compléter son évaluation du risque de BC-FT présenté par la relation d'affaires.
- **Statut réglementaire et situation de conformité.** En cas d'activité entrant dans le champ de la réglementation en matière de LCB-FT, il apparaît utile de collecter un certain nombre d'informations spécifiques : réglementation applicable, autorités en charge du contrôle, personnes responsables de la conformité dans l'entreprise, etc. Ces informations doivent permettre à la banque d'affiner son évaluation[12] des risques de BC-FT et faciliter la communication éventuelle d'informations complémentaires.

En résumé, sur la base des informations collectées, la banque doit pouvoir préciser les diligences à mettre en œuvre pour finaliser le processus d'entrée en relation. On peut considérer en substance trois familles de cas au regard de l'utilisation d'actifs numériques dans l'activité de l'entreprise : l'absence d'utilisation d'actifs numériques ; l'utilisation d'actifs numériques pour les besoins du fonctionnement de l'entreprise (*gaz* de la *blockchain* par exemple) ; l'émission d'actifs numériques ou la fourniture de services sur actifs numériques en tant que prestataire (réglementé ou non réglementé). Dans les deux premiers cas de figure, la banque s'interroge si un processus d'entrée en relation générique à une entreprise commerciale est suffisant ; autrement il convient de compléter celui-ci par un processus d'entrée en relation spécifique à des activités portant sur des crypto-actifs (voir chapitre suivant).

La figure ci-dessous illustre un arbre de décision possible :



[12] Ainsi, toutes choses égales par ailleurs, un prestataire de services en actifs numériques réglementé tel qu'un PSAN en France peut être considéré comme présentant *a priori* moins de risque qu'un acteur équivalent non réglementé.

En cas d'entrée en relation d'affaires, c'est-à-dire en cas d'ouverture de compte bancaire, il devrait être convenu que l'entreprise communique sans délai à sa banque tout changement significatif dans son recours à la TRD, susceptible d'impacter l'évaluation du risque de BC-FT faite par la banque de son client.

3.2.2 Seconde étape : les éléments de connaissance clients spécifiques aux PSAN

Le résultat d'une analyse de premier niveau (voir chapitre précédent) peut aiguiller vers un cadre d'entrée en relation spécifique à des activités de services sur actifs numériques. Dans ce cadre spécifique, les informations collectées appellent des compléments, en tenant compte des risques identifiés dans la classification des risques, notamment dans deux domaines :

1. **La description des activités**

Exemples d'éléments du modèle d'affaires justifiant une collecte complémentaire d'informations :

- Description et caractéristiques de la clientèle visée : segmentation (particuliers vs institutionnels, montants), zones géographiques de la clientèle (pays de résidence ou de localisation : clientèle locale dans le cas d'infrastructures physiques, nationale, européenne, internationale) ;
- Nature des produits et services proposés par le PSAN, avec une description résumée du fonctionnement technique (schéma de flux, *smart contracts* utilisés). En particulier, l'utilisation ou non d'AEC ou de *privacy coins*[13] constitue une information pertinente;
- Modes de règlements acceptés par le PSAN : encaissement d'espèces, réception de virements, de cartes prépayées, règlement par cartes bancaires ou par chèques, etc. ;
- Identification des principaux fournisseurs, prestataires ou partenaires, notamment les plateformes d'échange (*exchanges*) avec leurs coordonnées et leurs références bancaires et une information sur leur caractère réglementé ou non ;
- Estimation des flux prévisionnels des opérations réalisées par le PSAN, en distinguant d'une part les flux liés aux approvisionnements auprès de PSAN enregistrés et supervisés ou non et d'autre part les flux d'activités, notamment le montant moyen des transactions courantes et des estimations relatives aux transactions exceptionnelles ;

Une fois le compte ouvert, l'ensemble de ces informations collectées par la banque doivent permettre de mettre en place d'une surveillance pertinente des opérations de son client (voir partie 4).

2. **La description du dispositif de conformité LCB-FT et de sa gouvernance.**

La connaissance du modèle d'activité du PSAN et de son dispositif LCB-FT doit permettre à la banque, d'une part, d'évaluer le niveau du risque porté par son futur client et, d'autre part, d'adapter les mesures de vigilance mises en œuvre, notamment en matière de surveillance des opérations. Le fait que le client d'une banque soit par ailleurs assujetti à des obligations en matière de LCB-FT et soumis au contrôle d'une autorité de contrôle ne dispense pas la banque de ses obligations de vigilance à son égard, même si le caractère réglementé de l'activité est à prendre en compte dans l'appréciation du risque.

Afin d'assurer une approche cohérente, les banques pourraient recueillir la description générale du dispositif LCB-FT par le biais d'un questionnaire qui pourrait couvrir les points suivants :

- la classification des risques réalisée par le client PSAN (voir paragraphe suivant),

[13] Voir glossaire

- le dispositif d'identification, de vérification d'identité et de connaissance de la clientèle,
- les mesures en matière de vigilance constante incluant la surveillance des opérations (dont les modalités d'examen renforcé) et les moyens matériels et humains mis en œuvre à cette fin,
- le dispositif permettant de mettre en œuvre les mesures de gel des avoirs,
- les moyens mis en œuvre pour assurer le contrôle interne du dispositif de LCB-FT et de gel des avoirs.

Ce questionnaire est l'occasion d'obtenir des précisions techniques complémentaires[14] aux informations plus générales collectées sur le modèle d'affaires ou le dispositif LCB-FT, comme par exemple :

- **concernant ses clients :** le PSAN ouvre-t-il l'accès à ses services aux clients recourant à un VPN ou un navigateur Tor ? est-il en mesure de disposer de l'historique de détention des actifs numériques de ses clients ? est-il en mesure de bloquer, le cas échéant, les clés publiques de ses clients et ainsi de geler le fonctionnement de leurs *wallets* ?
- **concernant ses produits** : le PSAN offre-t-il des services relatifs aux crypto-actifs à anonymat renforcé[15] ? si oui, dans quelles conditions ? quelles mesures spécifiques de vigilance met-t-il en œuvre dans ce cas ?
- **concernant les transactions** : s'il effectue des transactions avec des client occasionnels, le client PSAN est-il en mesure de détecter le contournement de seuils d'identification par des transactions fractionnées ? les liens suspects entre plusieurs clients ? utilise-t-il des outils d'analyse des transactions ? si oui, lesquels et dans quels objectifs ?

L'analyse des réponses au questionnaire peut au besoin aboutir à des demandes complémentaires, pour tester la cohérence des réponses ou préciser certains points, comme par exemple la consultation de certaines procédures qui pourrait s'avérer nécessaire (il est entendu que les informations et documents fournis par le PSAN doivent être analysés par les départements conformité des banques dans le strict respect de leur confidentialité). À cette fin, il peut être utile, dans le questionnaire initial, d'identifier les interlocuteurs de conformité du PSAN afin de faciliter les échanges ultérieurs d'informations[16].

De façon générale, les membres du groupe de travail insistent sur l'importance de proportionner les demandes à l'objectif poursuivi, selon une approche par les risques. En particulier, il importe que la charge de l'analyse ne soit pas systématiquement reportée sur le PSAN futur client (demandes d'audit, de paraphrase de documents internes techniques existants…).

Les banques peuvent également élaborer une liste des exigences qui leur sont propres dans le cadre de leur politique de risque : refus de relation d'affaires avec les acteurs acceptant les AEC, utilisation d'un outil d'analyse transactionnelle de *blockchain,* demandes liées à la mise en œuvre de la *travel rule* du GAFI[17]…

*

[14] Pour une description des problématiques liées à ces questions, on se reportera au Rapport du groupe de travail du Forum Fintech sur l'application des règles de LCB-FT au secteur des crypto-actifs (voir référence en annexe).
[15] Également dénommés *Privacy coins* ou *Anonymity Enhanced Cryptocurrencies (AECs)*, voir glossaire.
[16] L'identification de ces contacts pourra être utile également en prévision des examens renforcés.
[17] Il convient toutefois de rappeler ici que la *travel rule* n'a pas, à ce jour, été transposée dans les textes réglementaires nationaux ou européens en raison, notamment, de l'absence de solution technique partagée Pour plus de détail on se reportera au Rapport du groupe de travail du Forum Fintech sur l'application des règles de LCB-FT au secteur des crypto-actifs cité *supra*.

Afin de d'assurer une certaine prévisibilité de l'entrée en relation, l'ensemble des éléments évoqués par le groupe de travail lors de ses travaux (démarche d'analyse du modèle d'affaire selon les différentes étapes décrites *supra*, questionnaire, exigences ou recommandations éventuelle des banques) gagnerait à faire l'objet d'un cadre minimal commun, à l'image du guide pratique adopté par l'ASB. En l'absence d'un tel cadre, le développement de tels éléments au sein des groupes bancaires constituerait déjà un progrès : le groupe de travail a d'ailleurs noté avec intérêt que de telles initiatives étaient en cours dans certains établissements. Selon une association professionnelle de la place financière et bancaire, ce type d'approche pourrait se généraliser au sein des établissements bancaires.

4 La surveillance des opérations du PSAN par sa banque

Lors des travaux du groupe de travail, la question de la surveillance des opérations du PSAN par sa banque a été soulevée à plusieurs reprises. Il est en effet nécessaire d'anticiper, lors de l'entrée en relation, les modalités pratiques de cette surveillance. C'est pourquoi il a paru utile de retracer, dans une partie spécifique du présent rapport, les principales conclusions et clarifications issues des discussions du groupe.

4.1 Le profil de risque des PSAN

Les organismes bancaires doivent déterminer un profil de risque pour chacune de leurs relations d'affaires (comme introduit dans le paragraphe 3.2) :

- En fonction de leur propre classification des risques. Pour rappel, l'ANR[18] et les ASR de l'ACPR et de l'AMF[19] considèrent que compte tenu de leur assujettissement à la réglementation en matière de LCB-FT et de gel des avoirs ainsi que du processus d'enregistrement et de supervision AMF/ACPR spécifique aux PSAN enregistrés, leur niveau de risques résiduel est modéré. Le niveau de risque des PSAN enregistrés/agréés est plus faible que celui d'acteurs non supervisés.

- En fonction des éléments recueillis lors de l'entrée en relation d'affaires avec le PSAN. Les critères d'appréciation du risque BC-FT peuvent tenir compte de la nature des clients du PSAN (clients institutionnels/particuliers, secteur d'activité, etc.), des produits ou services offerts (notamment des actifs numériques commercialisés ou acceptés et des services sur actifs numériques proposés), des risques géographiques, notamment concernant les flux financiers des opérations (si les fonds proviennent ou sont à destination d'un établissement assujetti à la LCB-FT dans l'UE/EEE ou hors de cette zone, notamment dans un pays tiers à risque), de la qualité du dispositif LCB-FT mis en œuvre par le PSAN, etc.

Le profil de risques permet de définir le niveau de vigilance qui devra être exercé par l'établissement bancaire.

4.2 Les moyens d'assurer une vigilance constante vis-à-vis des PSAN

La banque est tenue de mettre en œuvre des mesures de vigilance à l'égard de son client direct (le PSAN) et non à l'égard des clients de son client (les propres clients du PSAN).

Pour un PSAN qui propose le service d'achat/vente d'actifs numériques contre monnaie ayant cours légal, la banque enregistrera sur le compte du PSAN d'une part des flux en monnaie ayant cours légal vers ou en provenance de clients du PSAN et d'autre part vers ou en provenance des propres fournisseurs du PSAN.

Dans le cadre de ses obligations de vigilance constante, il appartiendra à la banque de veiller, selon une approche par les risques (en fonction notamment du profil de risques du client), à la cohérence des opérations au regard des informations recueillies sur la connaissance actualisée de la relation

[18] Publiée en septembre 2019, voir référence en annexe
[19] Voir référence en annexe

d'affaires dont dispose la banque (modèle d'activité du PSAN renseigné lors de l'entrée en relation d'affaires et mis à jour tout au long de celle-ci, notamment ses marchés-cibles, principales caractéristiques de la clientèle du PSAN, types d'opérations et de services proposées par le PSAN, volumes et montants prévisionnels des opérations réalisées par le PSAN, circuits de règlement/livraison des actifs numériques, notamment la provenance et la destination des fonds, modes de règlement acceptés, justification économique déclarée par le client PSAN ou fonctionnement envisagé du compte, cf. supra.).

Il est donc particulièrement important que la banque dispose d'une connaissance approfondie et actualisée de sa relation d'affaires (voir *supra*, partie 3).

Par ailleurs le groupe de travail s'est interrogé sur l'intérêt pratique pour les PSAN de fonctionner avec plusieurs comptes bancaires afin d'identifier les flux de trésorerie liés aux règlements avec les *exchanges* « fournisseurs » des PSAN, des flux liés à la commercialisation.

4.3 Les scénarios de surveillance

Dans le cadre de la surveillance des opérations par les institutions bancaires, il convient d'étudier quels seraient les scénarios envisageables permettant de prendre en compte les activités portant sur des actifs numériques. La question essentielle est de déterminer si les scénarios généraux existants mis en œuvre par les banques sont pertinents et suffisants pour surveiller l'activité des PSAN ou bien si des scénarios spécifiques doivent être construits à cet effet. Plusieurs situations doivent être distinguées.

4.3.1 La distinction entre les flux en lien avec les clients et ceux en rapport avec les plateformes d'échange

Pour la surveillance des flux financiers en monnaie ayant cours légal (euro) du compte d'un client PSAN, un établissement bancaire peut utilement distinguer plusieurs cas :

- Les flux entre le PSAN et les personnes (physiques ou morales) clientes du PSAN, en particulier les flux sortants correspondant à l'achat par le PSAN des actifs numériques détenus par ses clients.

- Les flux entre le PSAN et d'autres plateformes d'échanges (le PSAN a ici un profil de « broker »), en particulier les flux sortants correspondant à l'approvisionnement en actifs numériques du PSAN auprès de ses fournisseurs ; pour ces flux sortants une distinction peut être faite entre les achats de actifs numériques par le PSAN en compte propre et ceux pour le compte de tiers (à savoir ses clients).

Ces profils d'opérations ont en effet des logiques de fonctionnement différentes et appellent des schémas de surveillance différents.

À cet égard, une première difficulté consiste à bien distinguer les différents types de flux. Pour mettre en œuvre cette distinction, les représentants de l'industrie bancaire et de l'industrie des actifs numériques ont souligné l'intérêt de disposer d'une liste de référence centralisée de plateformes proposant des actifs numériques, avec leur identifiant bancaire IBAN. Actuellement, des listes sont créées individuellement par les acteurs bancaires ou les PSAN mais celles-ci ne sont pas exhaustives et

se recouvrent partiellement. Une liste globale consolidée et mutualisée[20] aurait l'avantage de la fiabilité et d'un moindre coût. Les discussions du groupe montrent que l'élaboration d'une telle liste par les acteurs des deux secteurs n'a rien d'insurmontable. Elle serait au contraire l'occasion de construire un premier schéma de collaboration opérationnelle entre les deux industries françaises, propre à favoriser à terme le développement d'une approche collaborative au niveau européen, dans le contexte de la définition du futur cadre réglementaire des crypto-actifs par exemple.

4.3.2 L'élaboration des scénarios

En première approche, la détection des opérations atypiques peut s'effectuer via des scénarios construits sur la base de critères classiques (critères géographiques, contreparties, volume, fréquence des flux, fonctionnement attendu du compte, type de clientèle, etc.) complétés par des critères spécifiques aux activités des PSAN.

Les difficultés rencontrées par les banques pour construire des scénarios pertinents spécifiques aux activités des PSAN semblent être les suivantes :

- d'une part, avoir une bonne compréhension de la façon dont les actifs numériques peuvent être utilisés à des fins de blanchiment de capitaux ou de financement du terrorisme et des dispositifs requis pour empêcher que les actifs numériques puissent être utilisés à de telles fins ;
- d'autre part, prendre en compte les évolutions du marché des actifs numériques (liste des actifs numériques existants ; risques spécifiques présentés par certains actifs numériques ; fluctuation des cours des différents actifs numériques ; liste des plateformes enregistrées et supervisées).

S'agissant du premier point, le groupe de travail a noté avec intérêt les pistes esquissées par le dernier rapport du GAFI sur les actifs virtuels[21], en date du 14 septembre 2020. Celui-ci vise à aider les autorités nationales mais aussi le secteur des PSAN et les établissements financiers à détecter si les actifs virtuels sont utilisés à des fins criminelles, sur la base de 100 études de cas collectées à travers le monde sur les trois dernières années.

S'agissant du second point, la question principale débattue par le groupe a été celle de la volatilité des actifs numériques qui rend les montants des flux en devises correspondant aux opérations plus difficiles à interpréter. Un autre facteur de complexité réside dans la grande disparité des patrimoines des clients des PSAN. Il peut être particulièrement ardu d'élaborer des critères ou des seuils pertinents dans le cadre d'un scénario opérationnel.

Ces caractéristiques ne sont toutefois pas sans rappeler certains produits boursiers et le groupe s'est interrogé sur les possibilités de tirer parti d'une analogie entre l'activité des PSAN et celle du courtier en bourse traditionnel ou du prestataire de services en investissement (pour l'achat de titres, CFD, options binaires par une personne physique par exemple)[22]. Ces produits boursiers, bien que leur cotation soit réglementée, peuvent présenter une volatilité proche de certains crypto-actifs ; en

---

[20] Cette liste ne viserait pas à identifier les plateformes vertueuses (« liste blanche ») dont les critères seraient difficiles à définir, mais seulement à inventorier l'ensemble des plateformes avec l'information de leur IBAN ainsi que leur juridiction de rattachement.

[21] *Virtual Assets Red flags indicators*, voir référence en annexe

[22] Plus précisément, la comparaison porte sur un établissement de crédit teneur du compte d'un PSAN et un établissement bancaire teneur du compte d'un *broker* ou d'un Prestataire de service en investissements - et non de la clientèle de ces derniers (toutefois, si les clients finaux sont clients de l'établissement bancaire alors cette dernière a davantage de moyens pour effectuer une surveillance ad hoc car il s'agit de ses clients dont elle a la connaissance).

revanche, les caractéristiques de traçabilité des produits boursiers et des crypto-actifs ne sont pas comparables, du moins pour de nombreux crypto-actifs.

Des démarches pragmatiques peuvent être envisagées afin de définir un jeu complet de scénarios spécifiques aux PSAN. Ainsi une démarche possible, mise en œuvre par certains établissements, consiste à mettre en place des scénarios de surveillance génériques (tenant compte des typologies diffusées par Tracfin, le GAFI, etc.) en les adaptant en fonction des réponses au questionnaire d'entrée en relation et en distinguant les grandes catégories de contreparties (cf. supra 4.3.1). Ces scénarios évolueraient, par itérations successives, en scénarios spécifiques aux PSAN, sans qu'ils soient nécessairement individualisés par PSAN, en fonction des retours d'expérience et de résultats du contrôle interne de la banque.

4.4 L'examen renforcé

Dans le cadre de son obligation de vigilance constante qui implique une surveillance des opérations, si une banque identifie une opération atypique ou suspecte nécessitant un examen renforcé, elle doit se renseigner « *auprès du client sur l'origine des fonds et la destination de ces sommes ainsi que sur l'objet de l'opération et l'identité de la personne qui en bénéficie* » (article L. 561-10-2 du CMF).

Conformément à l'article L. 561-10-2 du CMF, la banque doit se tourner vers son client (le PSAN) afin de recueillir les informations de nature à lever le doute ou le soupçon, notamment concernant l'origine et la destination des fonds. Dans ce cadre, la banque peut être amenée à recueillir des informations sur le client du client, c'est-à-dire les clients du PSAN[23]. La banque peut par exemple recueillir auprès du PSAN des analyses issues d'un outil d'analyse transactionnelle.

Ces dispositions ne font pas obstacle à ce que la banque conduise elle-même sa propre analyse ce qui nécessite de disposer des informations nécessaires à cette fin (comme l'adresse publique des crypto-actifs du client du PSAN par exemple).

Pour les membres du groupe de travail, un tel échange d'information avec les banques ne soulève *a priori* pas de difficulté, les PSAN conservant la relation exclusive avec leurs clients.

Ces pratiques reflètent le cadre légal : dans le cadre d'un examen renforcé d'une transaction, la loi impose qu'un organisme financier (ici la banque) se tourne vers son client pour exercer l'examen renforcé (ici le PSAN). Le groupe de travail n'a pas identifié de cas où une banque doit entrer en contact direct avec le client de son client. Cependant l'échange entre la banque et le PSAN peut aller assez loin en profondeur et la banque doit pouvoir obtenir de son client PSAN toutes les informations nécessaires pour lever le doute. Cela peut comporter les résultats fournis par des outils d'analyse transactionnelle ou des informations sur le client ou le bénéficiaire de l'opération. Une banque pourrait également, si elle le souhaitait, développer une capacité d'analyse transactionnelle, en s'appuyant sur les données fournies par son client PSAN, à savoir les adresses des portefeuilles de crypto-actifs impliqués dans la transaction ou toute autre information nécessaire pour réaliser ces analyses.

Dans ce contexte, la question se pose de la profondeur des diligences à réaliser – et donc des informations à collecter - en vue de répondre aux besoins de l'examen renforcé. Si la réponse à certaines questions relatives aux crypto-actifs sous-jacents ne semble pas poser de problème particulier (par exemple : s'agit-il d'un transfert issu d'une autre plateforme en crypto-actifs ? d'une

[23] Il revient au PSAN, le cas échéant, de transmettre ces informations à l'établissement bancaire dont il est le client, lorsque l'établissement bancaire lui en fait la demande.

opération de paiement ou une donation ? le produit d'une opération de minage ou de *staking*[24] ?), la question plus générale de la traçabilité des crypto-actifs - et de la profondeur de recherche requise à cette fin – reste en partie ouverte.

Le groupe de travail note toutefois que le GAFI, dans ses travaux récents, a réaffirmé le principe de l'approche par les risques ; en ce sens, l'analyse pourrait être considérée comme complète si le flux était remonté jusqu'à un prestataire réglementé (sans couvrir l'historique complet des transactions, i.e. qu'il soit nécessaire de remonter jusqu'au minage par exemple).

[24] Voir glossaire

5 Les opérations bancaires des clients bancaires lors d'achat ou de vente de crypto-actifs

5.1 Les constats

5.1.1 Les difficultés rencontrées par les particuliers à l'occasion de vente ou d'achat de crypto-actifs

Des enquêtes réalisées en ligne par une association de défense des utilisateurs de crypto-actifs et un média d'information spécialisé[25], témoignent de difficultés sensibles pour l'achat de crypto-actifs par des particuliers via leur compte bancaire. Ces difficultés concernent aussi bien les virements bancaires que les paiements par carte, majoritairement utilisés pour les opérations d'un montant inférieur à 200€.

Dans un contexte où de nombreuses plateformes ou structures frauduleuses (et souvent éphémères) proposent l'achat de crypto-actifs sur internet, les échanges au sein du groupe de travail mettent en avant que ce type de blocages, qui ne sont pas réalisés à des fins de LCB-FT, pourraient avoir comme effet de protéger les consommateurs des escroqueries.

Toutefois, il apparaît que les plateformes les plus souvent bloquées par les établissements bancaires sont des plateformes pérennes, non répertoriées comme frauduleuses et généralement populaires auprès des acheteurs. La concentration des blocages sur les plateformes les plus connues risque dans les faits d'être contreproductive dans le domaine de la lutte contre les escroqueries, en conduisant les clients à se déporter vers d'autres plateformes potentiellement mal intentionnées.

Enfin les témoignages de clients révèlent une grande disparité dans la communication effectuée par les banques vis-à-vis des clients dont les opérations sont bloquées.

Les justifications apportées au blocage semblent variées : plusieurs banques rappellent ainsi leur devoir de vigilance quant aux opérations menées par leurs clients et préfèrent s'assurer, via la signature par le client d'une lettre de décharge de responsabilité, qu'il s'agit bien de la volonté de ce dernier. Plusieurs acteurs bancaires mettent enfin en avant les multiples décisions de justice condamnant les teneurs de compte pour devoir de « conseil » non suivi.

Certaines pratiques apparaissent toutefois problématiques, en ce qu'elles mentionnent par exemple une interdiction de mener de telles opérations par l'ACPR ou l'AMF (ce qui est une information inexacte) : des exemples de ces pratiques ont été portés à la connaissance du groupe de travail.

En tout état de cause, il convient de rappeler que le client doit être informé des opérations qu'il peut réaliser sur la base du fonctionnement normal du compte et des éventuels blocages concernant ses fonds.[26]

---

[25] Il s'agit essentiellement de l'enquête réalisée par l'association AssoCryptoFR pour la défense des usagers des crypto-actifs et du sondage périodique du site spécialisé bitcoin.fr.

[26] Il s'agit d'une obligation légale qui figure à l'article L. 312-1-1 du code monétaire et financier.

5.1.2 Les procédures mises en œuvre par les établissements bancaires

Les premiers échanges du groupe ont montré que les procédures mises en place par les banques pour effectuer ces blocages (critère de détection des virements inhabituels, actions déclenchées, communication au client) n'étaient pas harmonisées au niveau de la place et qu'ils ne semblaient pas l'être non plus au sein même de chaque groupe bancaire. Une importante liberté d'action serait parfois laissée aux agences locales dans le traitement de ces problématiques.

Pour étayer et préciser ce premier constat, un rapide questionnaire a été diffusé auprès des représentants du secteur bancaire présents au groupe de travail sur les thèmes suivants :

- sur l'analyse des risques (hors LCB-FT) réalisée par l'établissement bancaire à l'égard des opérations sur actifs numériques conclues par les clients de l'établissement. Sur l'existence éventuelle de procédure écrite dédiée à ce type d'opérations ;

- sur les critères de vigilance (hors LCB-FT) utilisés par l'établissement bancaire (ex. : montant ou récurrence de l'opération, identité ou localisation géographique de la contrepartie). Sur les actions mises en œuvre en cas de déclenchement de ces critères (ex. : investigations complémentaires, information ou avertissement du client, courrier de décharge de responsabilité, blocage de l'opération) ;

- sur la disponibilité d'information statistique sur le recours à ces différents critères ainsi que sur le volume et la proportion d'actions subséquentes déclenchées ;

- sur le contenu et le format de l'information transmise au client concernant la politique de l'établissement en matière d'opérations en lien avec des actifs numériques.

L'absence de réponse n'a toutefois pas permis au groupe de poursuivre ses travaux sur ce thème.

5.2 Les pistes d'amélioration

Une première piste d'amélioration de la situation consisterait à établir soit une « liste blanche » de plateformes reconnues, ne présentant pas de risques spécifiques, enregistrées et supervisées, soit une liste de plateformes considérées comme « sûres ». Cette liste comprendrait également les coordonnées bancaires de ces plateformes (IBAN) afin de pouvoir identifier les transactions. Le principe d'une telle liste semble soutenu par les associations professionnelles représentant l'industrie bancaire et l'industrie des crypto-actifs.

Une telle liste, qui pourrait être construite par une collaboration entre les deux secteurs, est de nature différente de celle évoquée dans la partie 4 relative à la surveillance des opérations ; car il s'agit de qualifier des plateformes sûres, dans un contexte où la fréquence de création de ces plateformes est élevée (comme pour les listes noires déjà constituées). L'association représentative de l'industrie bancaire souligne cependant la charge inhérente de maintenance et de diffusion de cette liste entre les acteurs concernés ; par ailleurs elle s'interroge sur les possibilités de mise en œuvre au regard du droit de la concurrence.

Dans tous les cas, la création d'un canal d'échange entre PSAN et banques sur cette question serait profitable à l'ensemble du marché – et les clients - car il pourrait également servir à faire remonter aux banques les éventuelles faiblesses observées par les PSAN dans leurs systèmes de lutte contre les fraudes ou le blanchiment (par exemple : absence de seuil d'alerte concernant les paiements cumulés).

En matière de listes, le groupe de travail rappelle par ailleurs la publication sur le site de l'AMF[27] de la liste noire des sites proposant des produits dérivés sur crypto-actifs. Celle-ci ne prétend pas à l'exhaustivité (*« de nouveaux acteurs non autorisés apparaissant régulièrement »*), mais elle peut être utilisée par les établissements bancaires pour déclencher une alerte.

Les autres pistes identifiées relèvent davantage du seul secteur bancaire.

Il s'agit d'une part d'améliorer, parfois d'harmoniser au sein de groupes bancaires, les procédures de blocage pour s'assurer que celles-ci sont pertinentes, proportionnées aux risques et justifiées.

Il s'agit d'autre part de travailler sur l'information délivrée au client :

- *Ex ante*, sur les risques encourus lors de l'achat de crypto-actifs en distinguant bien le risque d'escroquerie du risque inhérent au caractère spéculatif de certains crypto-actifs courants. Des initiatives pourraient être prises au titre des actions d'éducation financière du secteur bancaire et par les acteurs du secteur des crypto-actifs.
- En cas de blocage de l'opération, lorsque celui-ci se justifie : dans ce cas, il conviendrait que les dispositifs de formation des agents et de traitement de l'opération garantissent une information claire, exacte et non trompeuse du client.

[27] Relayée sur le site commun Assurance Banque Épargne Info service qui recense les différentes listes noires des sites interne et entités non autorisés

6 Annexes

6.1 Glossaire

Terme	Description
TRD, *blockchain*	La Technologie des registres distribués ou TRD (Distributed Ledger Technologie, DLT, ou par substitution *blockchain*) décrit un dispositif électronique sécurisé par cryptographie, permettant le partage et la validation par consensus des données de transactions au sein d'un réseau.
PSAN	Selon la réglementation française, les prestataires de services en actifs numériques (PSAN) fournissent l'un des services suivants : 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.
LCB-FT, BC-FT	Lutte contre le blanchiment des capitaux et le financement du terrorisme, Blanchiment des capitaux et financement du terrorisme
Smart contract	Un *smart contract* désigne une fonctionnalité des *blockchains* 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.
Actif numérique, Crypto-actif	Les crypto-actifs sont un terme générique désignant l'ensemble des actifs émis et échangés sur la *blockchain*. 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.
CMF	Code monétaire et financier
Minage, *staking*	Le minage est le processus technique nécessaire de validation des transactions sur *blockchain*, assorti d'une récompense pour les acteurs de ce processus. Le minage est associé historiquement aux *blockchain* dont le protocole est basé sur le consensus par preuve de travail (*Proof of Work*) et d'autres mécanismes de consensus ont émergé comme la preuve d'enjeu (*Proof of Stake*). À cet égard l'activité de *staking* contribuant à ce processus en immobilisant des crypto-actifs,

	appartenant éventuellement à un tiers, et générant en contrepartie des récompenses potentielles dont le taux est fluctuant.
AEC, Privacy coin	Les *AEC* (*Anonymity-Enhanced Cryptocurrencies*) désignent une classe de crypto-actifs 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*.

6.2 Références documentaires

COLB (Conseil d'orientation de la LCB-FT)	Analyse nationale des risques de blanchiment de capitaux et de financement du terrorisme en France	septembre 2019
ACPR	Analyse sectorielle des risques de blanchiment de capitaux et de financement du terrorisme en France	décembre 2019
AMF	Analyse sectorielle des risques de blanchiment de capitaux et de financement du terrorisme en France	décembre 2019
Forum Fintech ACPR-AMF	Rapport du groupe de travail du Forum Fintech sur l'application des règles de LCB-FT au secteur des crypto-actifs	septembre 2020
ADAN	État des relations entre le secteur bancaire et financier et l'industrie des actifs numériques	octobre 2020
GAFI	Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing	septembre 2020
ASB	Guide pratique de l'ASB concernant l'ouverture de comptes d'entreprise pour des sociétés TRD (seconde édition, communiqué de presse)	août 2019
ACPR	Lignes directrices de l'ACPR en matière d'identification, de vérification d'identité et de connaissance de la clientèle	Décembre 2018
ACPR	Lignes directrices de l'ACPR sur les obligations de déclaration et d'information à Tracfin	Novembre 2018
ACPR	Lignes directrices de l'ACPR sur les Personnes politiquement exposées (PPE)	Mai 2018
ACPR	Lignes directrices de l'ACPR sur le gel des avoirs	Juin 2019
AMF	Questions réponses relatives au régime des prestataires de services sur actifs numériques *(en cours de révision)*	Juillet 2020
Commission européenne	Analyse supranationale des risques (*Report from the Commission to the European parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*); annexe	Juillet 2019
Joint Committee of the European supervisory authorities	Avis conjoint des autorités européennes de surveillance sur les risques de BC-FT affectant le secteur financier européen (*Joint Opinion of the European Supervisory Authorities on the risks of money laundering and terrorist financing affecting the European Union's financial sector*) *(en cours de révision)*	Octobre 2019
Tracfin	Rapports annuels et rapports « Tendances et analyse des risques de BC-FT »	
US DoJ	Cryptocurrency enforcement framework (report of the attorneys general's cyber digital task force)	octobre 2020

6.3 Description sommaire des travaux de l'ASB

Extrait du communiqué de l'Association suisse des banquiers du 21/09/2018 :

https://www.swissbanking.org/fr/medias/positions-et-communiques-de-presse/ouverture-de-comptes-entreprises-pour-des-societes-blockchain-guide

Ouverture de comptes d'entreprises pour des sociétés blockchain

L'Association suisse des banquiers publie un guide pour ses membres

Bâle, 21 Septembre 2018 – Le nombre de sociétés blockchain a fortement augmenté en Suisse. L'ASB salue cette évolution et estime que cette forte dynamique de marché est positive parce qu'elle renforce l'attrait de la place financière suisse. Les banques considèrent la technologie blockchain comme un potentiel avec diverses possibilités pour la place technologique et financière suisse. Dans le cadre de ses priorités, l'ASB encourage et demande des conditions-cadres qui favorisent concrètement l'innovation numérique. Cela inclut entre autres des conditions-cadres qui soutiennent le développement durable des sociétés ayant une connexion blockchain.

Avec la croissance des sociétés blockchain, la demande de comptes d'entreprises de leur part a augmenté auprès des banques en Suisse. L'ouverture de tels comptes pose plusieurs défis aux banques car les nouvelles technologies blockchain peuvent induire des risques, notamment dans le domaine du blanchiment d'argent. En Suisse, les opérations financières sont soumises à une réglementation légale et à des obligations de diligence strictes. Les banques sont ainsi obligées de procéder à un examen minutieux lors de l'ouverture d'un compte.

L'ASB a déjà reconnu en amont les difficultés liées à l'ouverture de comptes pour des sociétés blockchain et communiqué les intérêts et les questions en suspens de ses membres aux différentes autorités. De plus, dans le cadre d'un groupe de travail interne composé de représentants des banques membres et auquel la Crypto Valley Association (CVA) a été associé, l'ASB a examiné en détail les défis possibles et les conditions concernant l'ouverture de comptes pour des sociétés liées à la blockchain et aux ICO. Le guide publié aujourd'hui est le résultat de cette analyse.

Le guide fait des distinctions en fonction du financement des entreprises

Le guide publié permet aux banques de procéder à l'ouverture d'un compte de manière différenciée selon le type de rattachement de l'entreprise à la technologie blockchain. Le guide répartit dans différentes catégories les rattachements des sociétés concernées en termes d'émission de jetons (ICO) ou de financement d'entreprise. Il précise notamment en détail les exigences de documentation à l'égard des sociétés qui financent un ICO avec des cryptomonnaies.

- ***Sociétés blockchain sans ICO**: les sociétés dont le rattachement à la technologie blockchain n'intervient pas dans leur financement d'entreprise doivent en principe être traitées comme tout autre client PME qui souhaite ouvrir un compte. Les dispositions légales strictes qui régissent habituellement l'ouverture d'un compte doivent être appliquées. Les sociétés ont une obligation de coopérer lors de l'ouverture de relations bancaires. Elles doivent pouvoir montrer qu'elles connaissent et respectent toutes les règles pertinentes à leur modèle d'affaires. Elles le démontrent entre autres avec un business plan pertinent ou des processus et ressources appropriés.*
- ***Sociétés blockchain avec ICO**: les sociétés qui effectuent une levée publique de capitaux, à des fins entrepreneuriales, en émettant des jetons basés sur la technologie blockchain peuvent le faire sous forme de monnaies fiduciaires ou de cryptomonnaies. Les sociétés dont l'ICO est financé par des cryptomonnaies doivent être soumises à des exigences supplémentaires et plus*

strictes - indépendamment de leur assujettissement à la Loi sur le blanchiment d'argent. Le guide recommande que l'organisateur d'un ICO applique les normes suisses pertinentes concernant l'origine des fonds (KYC) et le blanchiment d'argent lors de l'acceptation de cryptomonnaies dans le cadre d'un ICO. En outre, il propose que l'acceptation de cryptomonnaies dans le cadre d'un ICO soit en principe traitée au minimum comme une opération au comptant.

Guide pour la pratique

Le guide reprend la terminologie et la classification des jetons du guide pratique sur les ICO de la FINMA daté du 16 février 2018 et repose sur la Convention relative à l'obligation de diligence (CDB) de l'ASB, complétée par des aspects spécifiques à la blockchain.

Le guide ne définit aucune norme minimale contraignante à cet effet. Dans tous les cas, les directives spécifiques à chaque établissement membre de l'ASB priment sur le guide. Chaque banque est responsable de ses activités.

Avec ce guide, l'ASB soutient des conditions-cadres optimales pour un écosystème technologique et financier varié. Les comptes commerciaux représentent une importante prestation d'infrastructure. Les banques ont un intérêt pour des relations d'affaires dans ce secteur de croissance. Il convient par ailleurs de souligner que les obligations de diligence applicables sont contraignantes et qu'il n'existe aucun droit à l'ouverture d'un compte. L'intégrité et la réputation de la place financière suisse doivent rester l'objectif premier de tous les acteurs du marché.

6.4 Composition du groupe de travail

Organisme	Représentant
ACPR – Direction des affaires juridiques	Yvan Bazouni
ACPR – Direction des affaires juridiques	David Sabban
ACPR – Direction du contrôle des banques	Philippe Ruez
ACPR – Direction du contrôle des banques	Laurent Clerc
ACPR – Direction du contrôle des banques	Arnaud Le Teurnier
ACPR – Direction du contrôle des pratiques commerciales	Stéphanie Machefert
ACPR – Direction du contrôle des pratiques commerciales	Maud Brassart
ACPR – Pôle Fintech innovation	Olivier Fliche
ACPR – Pôle Fintech innovation	Timothée Dufour
ACPR – Pôle Fintech innovation	Laurent Camus
Association pour le développement des actifs numériques (ADAN)	Simon Polrot
Association pour le développement des actifs numériques (ADAN)	Faustine Fleuret
AMF – Division Fintech innovation	Alexandre Barrat
AMF – Division Fintech innovation	Louis Charpentier
Arkéa	
Arkéa Direct Bank	
AssoCryptoFR	Quentin de Beauchesne
Banque de France – Direction de la transformation digitale	Andrés Lopez Vernaza
BNP Paribas	
Boursorama	Moncef Maghraoui
Coinhouse, Coinhouse Custody Services	Nicolas Louvet
Coinhouse, Coinhouse Custody Services	Sandrine Lebeau
DG Trésor – MULTICOM	Pierre Offret
DG Trésor – FINENT	Timothée Huré
Fédération bancaire française (FBF)	
HSBC	
LGO Europe	Alizée Rebeyrol
Office de coordination bancaire et financière (OCBF)	Carole Delorme d'Armaillé
Qonto	Alexandre Dressayre
Société Générale	
TRACFIN	

6.5 Note annexée au présent compte-rendu à la demande de la FBF

FÉDÉRATION BANCAIRE FRANÇAISE

La FBF et les banques qui ont participé aux réunions du Pôle Fintech sur l'accès des prestataires de services sur actifs numériques (PSAN) aux comptes bancaires et sur le fonctionnement des comptes de clients bancaires lors d'achat ou de vente d'actifs numériques saluent l'initiative du Pôle Fintech. Même si le compte rendu des travaux n'a pas de valeur juridique contraignante, la FBF et les banques participantes aux travaux ne peuvent, toutefois, s'associer au compte rendu des discussions qui se sont tenues dans ce cadre pour les raisons suivantes :

- Les constats ne prennent pas en compte l'historique de l'évolution de l'encadrement des prestatataires de services en actifs numériques, et notamment l'ordonnance n°2020-1544 du 9 décembre 2020, ni le fait que cet encadrement ne soit pas encore abouti tant sur le plan national, qu'au niveau européen et au niveau international (GAFI[28]). Les constats ne prennent pas non plus en compte les difficultés d'articulation des contraintes réglementaires des banques avec le développement de l'écosystème des PSAN dont la maturité en termes d'appréhension des risques de blanchiment de capitaux et de financement du terrorisme est inégale en fonction des acteurs.

- En conséquence de ce qui précède, les pistes de solutions proposées ne répondent pas aux interrogations du secteur bancaire en termes d'évaluation des risques de BC/FT présentés par chaque service en actifs numétiques ni en termes de surveillance des opérations réalisées par les différents PSAN. Il est rappelé, à cet égard, la nécessité que des lignes directrices soient adoptées par l'ACPR comme le suggère, d'ailleurs, le GAFI.

- En ce qui concerne les difficultés rencontrées par les particuliers à l'occasion de la vente ou de l'achat d'actifs numériques, les constats ne prennent pas en compte le besoin de clarification des banques en termes de surveillance des opérations de ces derniers et n'apportent donc pas de pistes de solution à cet égard. Les pistes de solution proposées qui consistent à améliorer l'information au client ne peuvent répondre qu'à des situations marginales.

[28] http://www.fatf-gafi.org/fr/publications/?hf=10&b=0&q=VIRTUAL+ASSET&s=desc(fatf_releasedate)