SwissBanking

Août 2019, 2e édition

Guide pratique de l'ASB concernant l'ouverture de comptes d'entreprise pour des sociétés TRD

Table des matières

Avant-propos	**3**
1. Contexte et structure du guide pratique	**4**
2. Due diligence concernant la clientèle institutionnelle liée à la TRD	**6**
3. Attentes générales concernant l'émetteur de jetons	**8**
4. Attentes envers l'émetteur de jetons en cas de financement par des cryptomonnaies	**11**
5. Obligations de diligence en cas de financement par des monnaies fiat	**14**
6. Modèles d'affaires spécifiques	**14**
Appendice – Glossaire	**16**

Avant-propos

Le nombre des entreprises liées à la technologie des registres distribués (TRD) (ci-après les « sociétés TRD ») a nettement progressé en Suisse ces dernières années. L'Association suisse des banquiers (ASB) salue cette évolution et considère qu'il s'agit là d'une dynamique de marché positive, dans la mesure où elle rend la place financière et économique suisse plus attrayante. Les banques voient en la technologie de la *blockchain* une opportunité aux multiples facettes pour la place financière et technologique suisse.

La multiplication des sociétés TRD va de pair avec une hausse de la demande de comptes d'entreprise auprès des banques en Suisse. Si l'évolution technologique en elle-même ne constitue pas un risque particulier et peut être qualifiée de neutre, l'ouverture de comptes d'entreprise pour des sociétés TRD comporte plusieurs spécificités pour les banques. En effet, les applications propres à la TRD ne sont pas exemptes de risques, notamment des risques de blanchiment d'argent en cas d'utilisation de cryptomonnaies, ou des risques de fraude. En Suisse, les opérations financières sont soumises à des dispositions légales et des obligations de diligence strictes. Les banques sont donc tenues de procéder à des contrôles méticuleux lors de l'ouverture d'un compte.

Sous la direction de l'ASB, un groupe de travail a remanié le « Guide pratique pour l'ouverture de comptes d'entreprises pour des sociétés *blockchain* », publié en 2018, afin de le mettre à jour quant à la terminologie et au contenu. Ce guide pratique de l'ASB vise à soutenir les banques membres dans leurs relations avec les sociétés concernées ainsi qu'à faciliter la gestion des risques dans ce cadre. Le Département fédéral des finances (DFF) et l'Autorité fédérale de surveillance des marchés financiers (FINMA) saluent la publication de ce guide pratique. Par ailleurs, la Crypto Valley Association (CVA) a contribué à son élaboration sur le fond et soutient sa mise en œuvre dans la pratique.

1. Contexte et structure du guide pratique

Ce guide pratique examine les exigences susceptibles d'être imposées par les banques aux sociétés TRD lors de l'ouverture d'un compte d'entreprise. Ces exigences potentielles vont parfois au-delà des obligations légales minimales en vigueur pour les sociétés TRD, mais n'ont cependant pas pour but de remplacer les dispositions légales applicables ou les directives des autorités en vigueur.

Ce guide repose sur le principe que la réglementation visant à lutter contre le blanchiment d'argent et le financement du terrorisme, comme toute réglementation transversale, s'applique à tous les intermédiaires financiers impliqués dans le domaine TRD. Les obligations en matière de lutte contre le blanchiment d'argent (obligations *anti money laundering*, AML) qui incombent généralement à la banque à l'ouverture de comptes d'entreprise résultent donc des versions en vigueur de la Convention relative à l'obligation de diligence des banques (CDB), de l'ordonnance de la FINMA sur le blanchiment d'argent (OBA-FINMA), de la loi sur le blanchiment d'argent (LBA) et du code pénal (CP), ainsi que des directives internes propres à chaque établissement. Le présent guide pratique s'inspire de la CDB et traite, à titre complémentaire, de problématiques liées à la TRD. Cette nouvelle version tient compte, dans la mesure du possible, des recommandations du Groupe d'action financière (GAFI) publiées en juin 2019. Ce guide sera mis à jour selon les développements qui pourront intervenir, si nécessaire.

Ce guide tient compte des spécificités propres aux sociétés TRD. Selon la maturité et la stratégie commerciale de la société concernée, toutes les recommandations ne sont pas forcément pertinentes pour l'ouverture ou la tenue d'un compte. Ainsi, une start-up financée de manière traditionnelle peut demander à ses débuts l'ouverture d'un compte d'entreprise, mais procéder au bout d'une ou deux années seulement à une émission de jetons. Inversement, des sociétés clientes de longue date peuvent décider de proposer des prestations sur la *blockchain*, d'accepter les cryptomonnaies comme moyen de paiement, voire d'émettre, elles aussi, des jetons. Dans ce dernier cas, il peut s'agir de sociétés dont le modèle d'affaires est sans lien avec la TRD, mais qui souhaitent se financer par ce biais.

Ce guide examine donc non seulement les éléments spécifiques à la TRD dans le cadre du processus *know your customer* (KYC), mais intègre également des exigences concrètes concernant les émetteurs de jetons. Il distingue dès lors les sociétés présentant des points de contact généraux avec la TRD, d'une part, et celles qui présentent des points de contact spécifiques AML (crypto-avoirs et émission de jetons notamment), d'autre part.

S'agissant de l'émission de jetons, le présent guide pratique établit une distinction entre financement par des cryptomonnaies (le plus souvent bitcoin ou ethereum) et financement par des monnaies fiduciaires (monnaies fiat).

Ce guide ne porte que sur les émissions de jetons effectuées par une société opérationnelle domiciliée en Suisse et basées sur le Guide pratique de la FINMA pour les questions d'assujettissement concernant les *initial coin offerings* (ICO) du 16 février 2018. En cas d'élément d'extranéité, par exemple lorsque des participants à une émission de jetons ou d'autres parties prenantes sont domiciliés à l'étranger, les risques résultant de l'application des dispositions légales étrangères (droit fiscal, droit pénal, lutte contre le blanchiment d'argent, droit des marchés financiers, etc.) doivent être répertoriés, limités et contrôlés de manière adéquate.

La présente version du guide pratique ne couvre pas la gestion des crypto-actifs déposés en compte par les clients.

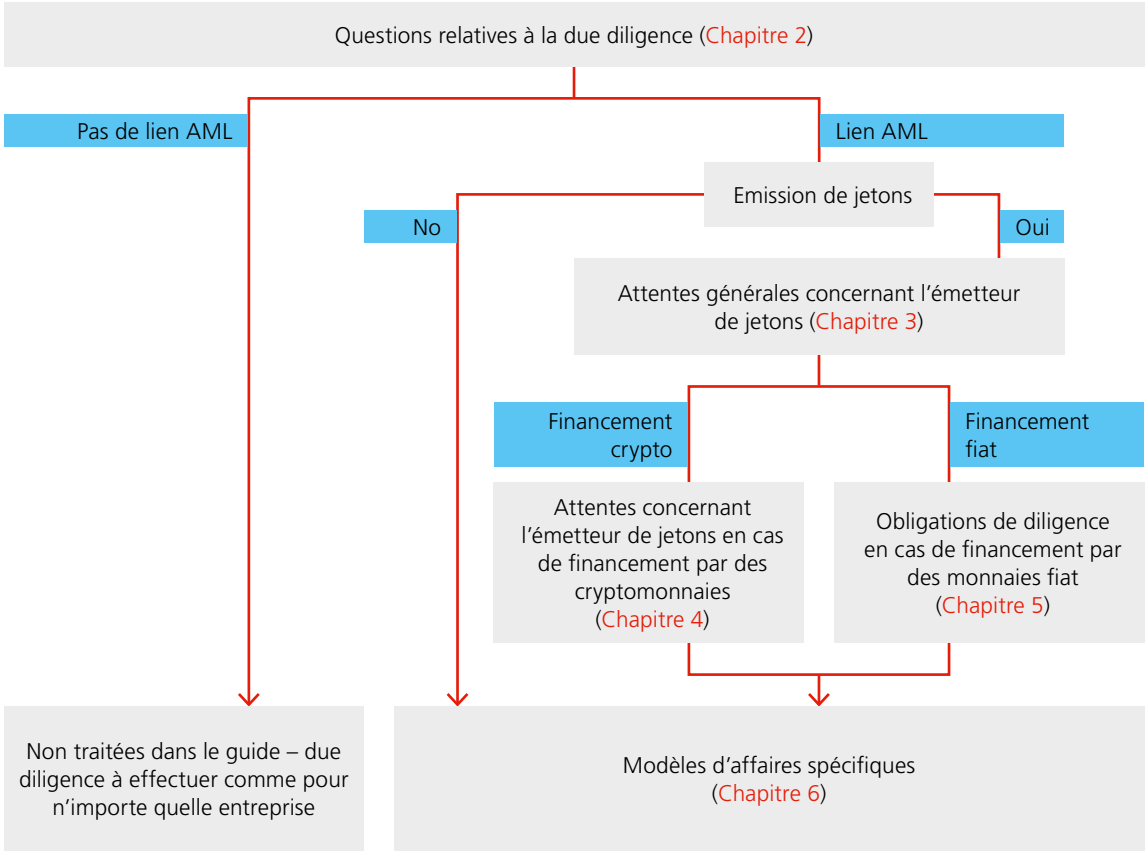
Ce guide s'adresse uniquement aux membres de l'ASB, dont les directives internes prévalent dans tous les cas. Il n'entend pas définir des normes minimales valables pour l'ensemble de la branche. Chaque établissement est libre de l'interpréter et/ou de l'appliquer en fonction de sa propre propension au risque.

Il n'existe pas de droit à l'ouverture d'un compte opposable aux membres de l'ASB.

Le présent guide sera régulièrement mis à jour et complété en fonction des évolutions à venir.

Graphique 1

Structure du guide pratique



Source: ASB

2. Due diligence concernant la clientèle institutionnelle liée à la TRD

Ce chapitre traite des attentes spécifiques qui, dans le cadre du processus KYC, résultent de points de contact généraux avec la TRD (avec ou sans émission de jetons).

Il est recommandé de se faire remettre les documents indiqués avant l'ouverture du compte d'entreprise. Les mesures ci-après valent également en cas de conversion d'un compte de consignation en compte commercial opérationnel dans le cadre d'une constitution de société.

Mesure / contrôle	Recommandation
2.1 Lien avec la TRD	Description précise des points de contact
2.2 Description du modèle d'affaires	• Description exhaustive et claire, sur la base de documents fiables (par ex. un livre blanc) • Description des flux de paiement attendus • Description des processus prévus • Dans la langue du pays/la langue de travail • Indication de la forme juridique • Pour les jetons existants, description des éventuels *smart contracts* et rapport d'audit indépendant afin de réduire les risques
2.3 Exclusion des sociétés de domicile	• La société prouve qu'elle est opérationnelle (CDB 16) et qu'elle a une substance locale. • En cas de constitution d'une société: la société communique ses intentions, son objet ainsi que les recettes et dépenses courantes attendues.
2.4 Compétences réglementaires	La société dispose d'un interlocuteur dédié pour l'ensemble les questions de compliance et d'assujettissement. Elle dispose notamment: • de connaissances sur les réglementations et prescriptions pertinentes; • d'un descriptif de la manière dont elle applique les réglementations pertinentes (directives internes).
2.5 Validation du modèle d'affaires après l'ouverture du compte	Les titulaires de comptes sont tenus d'informer la banque de tout changement pertinent concernant le recours à la technologie *blockchain*, ainsi que de toute émission de jetons prévue.
2.6 Hypothèses	Si la société ne présente pas de points de contact spécifiques AML (émission de jetons, crypto-actifs): ouverture du compte conformément aux directives internes, comme pour les autres sociétés. • Si la société prévoit d'émettre des jetons dans les 12 mois à venir: voir chapitre 3 (Emission de jetons) • Si la société n'émet pas de jetons mais présente des points de contact spécifiques AML: voir chapitre 6 (Modèles d'affaires spécifiques)

Les sociétés ayant déjà procédé à une émission de jetons avant l'ouverture du compte sont tenues, sur simple demande de la banque, de lui remettre une documentation complète sur le processus KYC / AML au sens des chapitre 3 et chapitre 4 ainsi que de prouver que ce processus est conforme à la réglementation suisse.

3. Attentes générales concernant l'émetteur de jetons

Ce chapitre porte sur l'émission de jetons, fréquemment appelée *token generating event* (TGE), quel que soit le mode de financement. Il ne concerne que les émissions de jetons dont l'émetteur est une société opérationnelle domiciliée en Suisse.

Préserver la réputation et l'intégrité de la place financière et économique suisse est une priorité absolue. Les recommandations formulées aux chapitre 3 et chapitre 4 visent à atteindre cet objectif, mais aussi à protéger l'émetteur de jetons lui-même.

Il est possible d'ouvrir un compte selon les modalités indiquées au chapitre 2 avant même de prendre les mesures et de procéder aux contrôles liés à l'émission de jetons décrits au chapitre 3 Un compte d'entreprise classique peut ensuite être converti en « compte TRD » (par ex. pour recevoir des fonds lors d'une émission de jetons et/ou pour des modèles d'affaires spécifiques au sens du chapitre 6), sous réserve que les obligations de diligence décrites dans les chapitres ci-après soient respectées. Si le compte d'entreprise existant est aussi utilisé dans le cadre du financement et de l'émission de jetons, il appartient à la banque de prendre des mesures opérationnelles pour que les fonds issus de l'émission de jetons ne puissent être mis à la libre disposition du client qu'après un contrôle exhaustif.

La banque ne procède à aucune analyse juridique concernant la nature et la maturité des jetons et considère a priori que l'émetteur est assujetti à la LBA. Si tel n'est pas le cas, il incombe à l'émetteur de le faire savoir et de le justifier. En cas de doute, un moyen de preuve peut être la réponse de la FINMA à une question d'assujettissement.

Diverses obligations de diligence découlent de la LBA, telles que l'obligation soit de s'affilier à un organisme d'autorégulation (OAR), soit de déléguer l'acceptation des valeurs patrimoniales à un intermédiaire financier assujetti à la LBA en Suisse.

Les directives internes des établissements peuvent imposer des exigences supplémentaires. Elles priment dans tous les cas le présent guide pratique.

Mesure / contrôle	Recommandation
3.1 Description (jetons)	• Description détaillée des jetons à émettre selon annexe du Guide pratique de la FINMA pour les questions d'assujettissement concernant les *initial coin offerings* (ICO) du 16 février 2018 ainsi que de l'état d'avancement du projet (maturité du marché, date d'émission) • Avant de procéder à l'émission de jetons, l'émetteur confirme que le projet à financer existe, que les fonds comptabilisés au crédit du compte proviennent de l'émission et qu'ils seront affectés à l'objet prévu. • La documentation concernant les jetons, qui revêt le plus souvent la forme d'un livre blanc, constitue un élément essentiel de la due diligence de la banque qui tient le compte. Elle doit donc lui être remise dans les meilleurs délais. • Lors de l'émission de jetons, l'émetteur communique son mode de fonctionnement ainsi que les données de suivi liées à l'application TRD. • Un éventuel *smart contract* peut faire l'objet d'un rapport d'audit technique indépendant, contribuant ainsi à réduire les risques.
3.2 Planification des liquidités	Avant de procéder à l'émission de jetons, l'émetteur transmet à la banque qui tient le compte des informations sur: • la répartition attendue entre monnaie fiat et cryptomonnaies dans le cadre d'une levée de fonds (scénario: par ex. 50 % fiat, 25 % bitcoin, 25 % ethereum); • le montant et la fréquence prévus des virements de fonds convertis en monnaie fiat à la banque qui tient le compte; • le schéma de remboursement si le montant cible n'est pas atteint (en annexant la clause contractuelle correspondante); • les entreprises chargées de changer les cryptomonnaies (voir point 4.7).
3.3 Gestion des risques résultant du droit étranger	L'émetteur de jetons dispose de directives à cet égard et met en œuvre des mesures visant à exclure les investisseurs issus des pays définis par la banque. En cas d'émission de jetons dans le cadre d'un *security token offering* (STO), l'émetteur met une liste des pays cibles à la disposition de la banque qui tient le compte et justifie de ce que les prescriptions locales en matière de STO sont respectées à tout moment. Il communique ces informations à la banque sur simple demande de cette dernière.

3.4 Assujettissement à la LBA	La banque considère a priori que l'émetteur de jetons est assujetti à la LBA. L'assujettissement à la LBA s'établit exclusivement au regard du Guide pratique de la FINMA pour les questions d'assujettissement concernant les *initial coin offerings* (ICO) du 16 février 2018. S'il n'est pas assujetti à la LBA, l'émetteur de jetons doit le prouver. En cas de doute, il lui incombe de fournir notamment la réponse de la FINMA à une demande d'assujettissement. S'il est assujetti à la LBA, l'émetteur de jetons fournit les éléments de preuve suivants: • nom de l'OAR et attestation de son affiliation à cet OAR, ou • en cas de délégation: nom de l'intermédiaire financier, attestation de son affiliation à un OAR et attestation de délégation; • documentation complète conformément au règlement interne de la banque qui tient le compte en matière de compliance.
3.5 Obligations après l'émission	• Les obligations légales résultent de la LBA. • Sur demande de la banque, l'émetteur de jetons confirme que l'affectation courante des fonds correspond à l'objet annoncé. • Sur demande de la banque, l'émetteur de jetons confirme également que les restrictions décrites au point 3.3 ont été respectées en ce qui concerne les investisseurs étrangers. • Fondamentalement, toute mesure visant à créer la transparence quant aux transmissions (de jetons) à l'issue de l'émission contribue à réduire les risques, de sorte que la banque qui tient le compte ne peut qu'y être favorable. Constitue une telle mesure, notamment, la communication d'informations relatives aux transmissions (de jetons) sur demande de la banque. • Pour les modèles d'affaires présentant des points de contact avec la LBA, l'affiliation à un OAR est obligatoire.
3.6 Catégorisation des modes de financement	• Si l'émetteur de jetons assure partiellement ou totalement le financement via la *blockchain* ou des cryptomonnaies: voir chapitre 4 (Emission de jetons en cas de financement par des cryptomonnaies) • Si le financement est assuré exclusivement par une monnaie fiat: voir chapitre 5 (Obligations de diligence).

4. Attentes envers l'émetteur de jetons en cas de financement par des cryptomonnaies

Le tableau ci-après décrit le financement d'entreprise effectué partiellement ou totalement au moyen de cryptomonnaies. La présente version du guide pratique présuppose que la banque qui tient le compte n'accepte pas directement de cryptomonnaies.

L'émetteur de jetons veille à convertir les cryptomonnaies en monnaie fiat par le biais d'un bureau de change (*exchange*) réglementé selon le droit suisse ou un droit équivalent, ou d'une banque tierce réglementée selon le droit suisse ou un droit équivalent. Il transfère ensuite les fonds correspondants à la banque qui tient le compte.

Ce guide recommande d'exiger de l'émetteur de jetons, qu'il soit ou non assujetti à la LBA, d'appliquer les normes KYC et AML pertinentes en Suisse lorsqu'il accepte des cryptomonnaies

Par ailleurs, l'acceptation de jetons de paiement dans le cadre d'une émission peut en principe être traitée comme une opération de caisse. Il convient toutefois de noter que toutes les transactions en cryptomonnaies passent par la *blockchain* et qu'indépendamment de leur montant, un risque de violation de sanctions demeure. Le type de jeton et/ou l'assujettissement à la LBA peuvent donner lieu à d'autres obligations.

Les directives internes des établissements peuvent imposer des exigences supplémentaires ou fixer des seuils différents de ceux du présent guide pratique. Elles priment ce dernier dans tous les cas.

Mesure / contrôle	Recommandation
4.1 Réduction de risque tolérée	La cryptomonnaie doit en principe permettre une analyse de portefeuille (*wallet*). Si tel n'est pas le cas, il convient de le justifier.
4.2 Emetteur de jetons (aspects généraux)	De manière générale, les données à collecter par l'émetteur de jetons concernant chaque souscripteur résultent des exigences des textes applicables (par ex. CDB, OBA-FINMA, règlements des OAR, circulaire « Identification par vidéo et en ligne » de la FINMA). Dès lors, il appartient à l'émetteur de se faire communiquer les informations suivantes: nom, adresse (y compris pays), date de naissance, nationalité et lieu de naissance. Parmi les informations collectées devraient figurer également les adresses des *wallets* (clés publiques) à partir desquelles les investisseurs effectuent le versement. Que l'émetteur soit ou non assujetti à la LBA, il est censé procéder à l'identification et à la vérification de l'identité des ayants droit économiques conformément à la LBA / à l'OBA-FINMA / à la CDB, au minimum lorsque le montant souscrit est égal ou supérieur à CHF 15 000. Toute autre mesure visant à améliorer la transparence permet d'atténuer les risques, en particulier au regard du risque de violation de sanctions. Si la banque a l'intention d'exiger de l'émetteur qu'il lui communique de la documentation sur les investisseurs, celle-ci doit être définie dans le contrat qui la lie à lui. La banque est alors tenue de protéger les données personnelles des investisseurs (souscripteurs, participants, bénéficiaires de jetons) de manière appropriée. Il est recommandé de documenter l'ayant droit économique conformément aux processus en vigueur dans l'établissement concerné. Le contrôle de l'ayant droit économique sur les valeurs patrimoniales peut être confirmé par le fait qu'une transaction est signée numériquement ou qu'une microtransaction est envoyée à partir de la clé publique / de l'adresse publique de l'émetteur. L'émetteur peut faire consigner le processus et / ou la réalisation d'une microtransaction dans un acte authentique.
4.3 Emetteurs de jetons de paiement (aspects spécifiques)	Les émetteurs de jetons de paiement sont assujettis à la LBA. Pour pouvoir accepter des valeurs patrimoniales d'investisseurs, ils sont donc tenus de respecter les prescriptions en vigueur en matière de lutte contre le blanchiment d'argent, lesquelles sont précisées notamment dans la LBA, dans la Circ.-FINMA 16 / 07 « Identification par vidéo et en ligne » ainsi que dans les règlements des OAR. S'agissant des transactions portant sur un montant inférieur à CHF 3 000, les émetteurs de jetons de paiement sont tenus de respecter les obligations de diligence simplifiées prévues à l'art. 12, al. 2, let. d, OBA-FINMA en vertu duquel ils n'ont pas à faire authentifier les copies des documents d'identification des investisseurs.

4.4	Contrôle dans les bases de données sur les risques	L'émetteur de jetons vérifie que les souscripteurs ne figurent pas dans les bases de données usuelles sur les risques (en particulier listes de personnes politiquement exposées ou PPE, de personnes liées au terrorisme, de sanctions). Le résultat de ce contrôle est mis à la disposition de la banque sur simple demande de cette dernière, de même que les directives internes concernant la surveillance des PPE et des clients soumis à un régime de sanctions.
4.5	Clarification de l'arrière-plan économique (origine des fonds) et évaluation des risques inhérents aux adresses des *wallets* utilisées par les investisseurs (AML)	De manière générale, il est recommandé à l'émetteur de jetons d'adopter une approche basée sur les risques lors de la clarification de l'arrière-plan économique de la transaction. Il n'est pas exigé, à ce jour, de procéder à un traçage général de l'origine des fonds sur la *blockchain*. Néanmoins, toute mesure prise par l'émetteur en vue d'améliorer la transparence contribue à atténuer les risques. Dans des cas spécifiques ou en présence de soupçons concrets, il est recommandé de procéder à un contrôle approfondi au moyen d'une analyse de *wallet* ou d'une documentation complémentaire (par ex., en cas d'investissement important ou de domiciliation du souscripteur dans un pays à risque, une due diligence approfondie est préférable à un simple contrôle des bases de données). Un contrôle approfondi par l'émetteur de jetons est conseillé dans tous les cas dès lors que les souscriptions excèdent CHF 100 000 (individuellement ou cumulativement). Ce contrôle approfondi implique la vérification de la concordance entre adresses de portefeuille et investisseurs, ainsi que la documentation y relative. La banque qui tient le compte se réserve le droit de demander les informations concernant les investisseurs avant la réception des fonds. En cas de soupçons concrets de sa part, elle peut demander à l'émetteur de jetons de procéder à des clarifications complémentaires et de lui en communiquer les résultats (par ex. analyses de *wallets* spécifiques).
4.6	Qualité des contrôles KYC / AML	Les résultats de ces contrôles sont communiqués à la banque qui tient le compte sur simple demande de cette dernière. Ils doivent documenter également le respect des directives internes en matière de PPE.
4.7	Bureau de change (*exchange*) pour la conversion de cryptomonnaie en monnaie fiat	Les bureaux de change de cryptomonnaies et la conversion de cryptomonnaies en monnaie fiat représentent un risque particulier pour les banques, dans la mesure où ils concentrent des risques au sens de la LBA. Les banques doivent ainsi prendre des mesures propres à atténuer les risques: par ex. un bureau de change réglementé selon le droit suisse ou un droit équivalent, ou une banque tierce réglementée selon le droit suisse ou un droit équivalent. L'« équivalence de la réglementation » doit être définie conformément aux directives internes de la banque concernée.

4.8	Soupçon de blanchiment d'argent	L'investisseur est exclu de l'émission (sous réserve que l'opération doive être exécutée en raison de l'interdiction du *tipping-off* suivant une communication au Bureau de communication en matière de blanchiment d'argent [MROS], art. 9a LBA). La responsabilité de l'exclusion incombe à l'émetteur de jetons. Afin de procéder aux clarifications requises dans le cadre du processus KYC et de la due diligence, la banque qui tient le compte peut se libérer du secret bancaire, sous réserve d'avoir obtenu l'accord correspondant de son client dans le contrat ou au moyen d'une clause séparée (*waiver*). Il incombe à la banque de rendre le client attentif à ce cas de figure et il est recommandé à l'émetteur de jetons de le déclarer en toute transparence dans les conditions générales (*Terms & Conditions*).
4.9	Dispositions en matière de sanctions	L'émetteur de jetons respecte les dispositions en matière de sanctions (par ex. loi sur les embargos).

5. Obligations de diligence en cas de financement par des monnaies fiat

En cas de financement par des monnaies fiat, il convient de respecter les seuils indiqués au chapitre 4 ainsi que les obligations d'identification et de vérification de l'identité des ayants droit économiques résultant de la LBA, de l'OBA-FINMA et de la CDB.

6. Modèles d'affaires spécifiques

Dans son rapport « Bases juridiques pour la *distributed ledger technology* et la *blockchain* en Suisse » du 14 décembre 2018, le Conseil fédéral souligne que les activités TRD suivantes (outre l'émission de jetons, qui fait l'objet des chapitre 3 et chapitre 4) sont soumises à la LBA dès lors qu'elles sont exercées à titre professionnel (art. 7 LBA):

- Les fournisseurs de *wallets* qui conservent les clés privées des clients et leur permettent d'envoyer et de recevoir des cryptomonnaies ont un pouvoir de disposition sur les valeurs patrimoniales de tiers et sont donc assimilables à des intermédiaires financiers soumis aux prescriptions AML. Pour l'heure, il n'est pas prévu de réglementer les fournisseurs de *wallets* non dépositaires, qui n'ont aucune possibilité d'intervention dans la transmission des jetons.

- Les exploitants de plateformes de négociation qui ont accès aux clés privées des clients et donc au pouvoir de disposition sur les valeurs patrimoniales de tiers, ou qui travaillent sur la base de *smart contracts* et ont un tel pouvoir de disposition par confirmation, validation ou blocage des ordres, font office d'intermédiaires entre clients dans le cadre d'une relation tripartite. En conséquence, ces plateformes de négociation centralisées sont soumises aux prescriptions AML. Les plateformes de négociation qui ne présentent pas les caractéristiques susmentionnées et fonctionnent de manière complètement décentralisée, c'est-à-dire sans possibilités d'influence de la part du développeur de la plateforme, ne sont pas soumises aux prescriptions AML.

L'évaluation du risque inhérent aux clients institutionnels qui fournissent des prestations en relation avec des cryptomonnaies ou des jetons via des bureaux de change ou des plateformes de négociation centralisées peut être facilitée par la prise en compte des éléments suivants:

Mesure / contrôle	**Recommandation**
6.1 Conversion d'une cryptomonnaie en monnaie fiat	Via un bureau de change *(exchange)* réglementé selon le droit suisse ou un droit équivalent, ou via une banque tierce réglementée selon le droit suisse ou un droit équivalent. L'« équivalence de la réglementation » doit être définie conformément aux directives internes de la banque concernée.
6.2 Conformité AML/sanctions	Programme AML/sanctions conforme aux prescriptions suisses en matière d'*onboarding* et de surveillance courante des transactions.
6.3 Programme AML	Interlocuteur dédié et qualifié en matière de compliance.
6.4 Positions de négoce	Sur demande de la banque qui tient le compte, la plateforme de négociation confirme que les valeurs patrimoniales échangées répondent aux exigences des pays concernés en matière d'enregistrement (par ex. valeurs mobilières américaines).
6.5 Surveillance	Le prestataire est soumis aux règles AML dans leur version en vigueur.
6.6 Autorisation	Selon les modèles de licence existants (par ex. licence Fintech).
6.7 Segmentation de clientèle	Sur demande, le système de négociation TRD met à disposition des informations complémentaires sur la structure de la clientèle, par exemple une classification par montant ou par origine géographique.

- Bureaux de change: l'achat et la vente à titre professionnel de cryptomonnaies ou de jetons en échange de monnaies fiat ou d'autres cryptoplacements constituent une activité de change bipartite soumise aux prescriptions AML.

- Les cryptofonds, c'est-à-dire les placements collectifs qui investissent leurs capitaux principalement ou exclusivement dans des cryptomonnaies ou d'autres crypto-actifs, sont traités comme les autres placements collectifs du point de vue des prescriptions AML.

S'agissant des entreprises qui offrent la possibilité d'acquérir leurs produits et services contre des cryptomonnaies, il leur est recommandé de se baser sur les contrôles approfondis détaillés au point 4.5 et/ou sur les seuils recommandés au point 4.2.

Appendice – Glossaire

Jeton (*token*)
Formulé simplement, un jeton est une unité de données numérique et cryptée qui est stockée dans un registre basé sur la TRD. La FINMA classe les jetons sur la base de leur fonction économique et distingue entre jetons de paiement, jetons d'investissement et jetons d'utilité. Voir le Guide pratique de la FINMA pour les questions d'assujettissement concernant les *initial coin offerings* (ICO) du 16 février 2018.

Distinction entre ICO, ITO, TGE, STO et IEO

La définition des notions d'*initial coin offering* (ICO), *initial token offering* (ITO), *token generating event* (TGE), *security token offering* (STO) ou *initial exchange offering* (IEO) ne fait pas encore consensus. Ces notions ont en commun l'émission d'unités informationnelles et/ou fonctionnelles uniques, numériques et transmissibles (jetons) susceptibles de représenter des droits très divers: droits de créance et de participation envers une entreprise, droits réels ou autres droits absolus ou relatifs.

Un jeton peut servir exclusivement de moyen de paiement (jeton de paiement, *payment token*), sans conférer d'autres droits spécifiques à son titulaire. Dès lors que des jetons matérialisent explicitement des droits envers l'émetteur, on parle plutôt aujourd'hui de STO (*security token offering*). Un ICO (*initial coin offering*), ou plus précisément un ITO (*initial token offering*), est une méthode de financement consistant, pour une entreprise, à lever des fonds par une *première* émission de jetons. Selon la configuration de l'opération, les jetons peuvent représenter un droit-valeur TRD et/ou être assimilés à des effets au sens de la législation sur les marchés financiers.

Un IEO est une levée de fonds qui s'effectue exclusivement via un bureau de change (*exchange*), lequel prend en charge la réception des fonds et l'émission des jetons pour le compte de l'émetteur.

Le présent guide pratique considère que les notions d'« émission de jetons » et de « TGE » sont synonymes et emploie la première en lieu et place de la seconde.

Analyse de chaîne *(chain analysis)*

L'analyse de chaîne vise à déterminer l'origine des crypto-actifs. Elle peut prendre en compte de multiples critères, comme les entrées et sorties de paiements dans certains *wallets*, les liens avec le *darknet*, les mixers et les *tumblers*, les sites *scam* et/ou les sites de paris en ligne, ou encore les transactions émanant de ou effectuées dans des pays à haut risque. Elle peut également s'appuyer sur une classification par niveaux de risque des places de négoce à partir desquelles les portefeuilles en question ont été alimentés.

Technologie des registres distribués (TRD) / *blockchain*

La technologie des registres distribués (TRD, en anglais *distributed ledger technology*, DLT) permet la gestion commune et sécurisée de données dans le cadre d'un réseau informatique (décentralisé). Formulé simplement, un registre distribué est une base de données gérée sur un grand nombre d'ordinateurs en réseau, qui synchronise et valide de manière autonome et continue les données / transactions enregistrées par les participants. Ces derniers disposent à tout moment d'un historique non manipulable et vérifiable de toutes les informations stockées dans un bloc de données particulier. La notion de « TRD » est plus large que celle de *blockchain* et intègre d'autres applications.

***Blockchain* (application de la TRD)**

Une *blockchain* ou chaîne de blocs est une forme particulière de registre distribué. Il s'agit d'un ensemble de registres numériques ou de bases de données extensibles à tout moment et infalsifiables. Un réseau d'ordinateurs, dont chacun constitue un nœud (*node*), exécute le protocole du logiciel de manière autonome: les transactions – ou d'autres données – sont vérifiées et groupées à intervalles de temps réguliers en blocs, lesquels sont ajoutés à la chaîne existante de blocs déjà validés. La *blockchain* est utilisée, par exemple, pour les transactions en bitcoin, ethereum et autres cryptomonnaies. Afin de permettre le chaînage des blocs, la *blockchain* utilise une signature cryptographique appelée hash. Cette signature résulte d'un processus (asymétrique) de cryptage, qui comprend pour chaque utilisateur une clé publique (*public key*) et une clé privée (*private key*). Les utilisateurs gèrent cette paire de clés dans le cadre de *wallets* qui peuvent être disponibles sur différents médias (portefeuilles en ligne, sur ordinateur, sur smartphone, papier ou matériel). Une *blockchain* publique fonctionne de manière décentralisée, elle est accessible à tous et exploitée sans intermédiaire par un grand nombre de participants anonymes (par ex. bitcoin et ethereum). Inversement, une *blockchain* privée est gouvernée par un ou plusieurs administrateurs de réseau et n'est accessible qu'à des participants identifiés et autorisés. Il existe par ailleurs des formes mixtes de *blockchain* ainsi que des *blockchains* de consortium: dans ce cas, seuls certains acteurs valident les transactions mais le protocole peut être public.

Bureau de change (*exchange*)
Les cryptomonnaies peuvent être converties en monnaies fiat conventionnelles comme le franc suisse, ou en d'autres cryptomonnaies, dans des bureaux de change (*exchanges*).

Crypto-avoirs / actifs numériques (*digital assets*)
Les crypto-actifs sont des valeurs patrimoniales numériques enregistrées dans le cadre d'une application TRD et sécurisées par un système cryptographique, dont le contenu est clairement documenté (par ex. cryptomonnaies ou droits-valeurs numériques). Chaque jeton représente les informations enregistrées dans le registre correspondant, dont le titulaire peut disposer à l'aide d'un code d'accès. En tant que moyens de paiement, les cryptomonnaies ne sont disponibles que sous forme numérique, contrairement aux monnaies fiat ordinaires émises par une banque centrale comme le dollar américain ou le franc suisse. Les cryptomonnaies les plus connues actuellement sont le bitcoin et l'ethereum. Chacune dispose de son propre système de paiement. Selon les configurations, les jetons peuvent être liés à d'autres valeurs (par ex. monnaie, matière première, titre) et les représenter sous forme de crypto-avoirs (par ex. *asset backed token*).

Smart contract
Un *smart contract* (contrat intelligent) est un protocole informatique auto-exécuté qui repose sur une *blockchain* et qui réplique des clauses contractuelles prédéfinies dans le code logiciel. Une transaction qui passe par un *smart contract* est automatiquement exécutée dès lors que toutes les parties impliquées remplissent les conditions prédéfinies. Un *smart contract* permet de répliquer et vérifier techniquement le contenu d'accords contractuels ou d'en assurer l'exécution. Le protocole informatique surveille automatiquement les conditions enregistrées et, en présence d'un événement donné (*trigger event*), il exécute de manière autonome les opérations convenues entre les parties. Selon les configurations, les *smart contracts* peuvent être eux-mêmes des contrats juridiquement contraignants.

SwissBanking

Schweizerische Bankiervereinigung
Association suisse des banquiers
Associazione Svizzera dei Banchieri
Swiss Bankers Association

Aeschenplatz 7
Case postale 4182
CH-4002 Bâle

office@sba.ch
www.swissbanking.org