Fatemeh Fannizadeh
ff@geneva-legal.ch
Vladimir Moshnyager
vladimir.moshnyager2@gmail.com
Thomas Shababi
thomas@shababi.net

Par courriel uniquement

Groupe de travail sur la technologie blockchain et les ICO
Secrétariat aux questions financières internationales (SFI)
fin@sif.admin.ch

Genève, le 20 septembre 2018

Concerne : Prise de position sur les questions du groupe de travail sur la technologie blockchain et les ICOs

Madame, Monsieur,

Les soussignés, Me Fatemeh Fannizadeh et Messieurs Vladimir Moshnyager et Thomas Shababi, souhaitent intervenir spontanément dans le cadre de la procédure de consultation relative à la blockchain et les ICOs.

Me Fatemeh Fannizadeh, avocate indépendante active dans le domaine de la blockchain et la crypto, Monsieur Vladimir Moshnyager consultant en blockchain et crypto, Monsieur Thomas Shababi, développeur informatique et fondateur de la société TrueLevel SA à Neuchâtel, tous trois interessés par l'innovation et son impact sur la société, souhaitent apporter une vision pluridimensionnelle aux questions soulevées par la procédure de consultation.

Nous n'avons répondu qu'aux questions auxquelles notre expertise nous permettait d'apporter des réponses substantielles.

Nous vous remercions par avance de l'accueil que vous réserverez aux présentes et nous tenons à votre disposition pour répondre à toute question éventuelle.

Soyez assurés, Madame, Monsieur, de notre considération respectueuse.

Fatemeh Fannizadeh Vladimir Moshnyager Thomas Shababi

PRISE DE POSITION

Lutte contre le blanchiment d'argent et le financement du terrorisme

1. La demande de consultation du groupe de travail sur la technologie blockchain et les ICOs soulève à son chapitre 4 la problématique de la lutte contre le blanchiment d'argent et le financement du terrorisme. Elle relève à juste titre que la LBA est neutre sur le plan technologique et englobe de nombreuses activités crypto, notamment les plateforme de négoce centralisée et les *custodial wallet*.

2. L'écosystème crypto connaît des outils qui n'entrent pas – à l'heure actuelle – dans le champ d'application de la LBA. Le chapitre 4.2 s'interroge sur la nécessité d'imposer de nouvelles obligations de diligence aux plateformes de négoce décentralisée (ci-après : « DEX »), aux *non-custodial wallet*, ainsi qu'aux personnes morales émettant des jetons.

3. Notre postulat est qu'il n'est pas nécessaire de modifier la LBA pour étendre son champ d'application à ces nouveaux outils :

    - la neutralité technologique de ladite loi lui permet déjà de s'appliquer aux cas de figure pertinents et d'atteindre largement le but souhaité par le législateur ;
    - elle lui permet d'être parfaitement en conformité avec les recommandations du GAFI ; et
    - le marché des DEX et des *non-custodial wallets* est aujourd'hui encore relativement mince.

4. Par ailleurs, alourdir la réglementation à ce sujet aurait des conséquences importantes sur la capacité d'innovation en Suisse :

    - ces technologies (DEX et *non-custodial wallets*) constituent aujourd'hui la partie la plus innovante technologiquement parlant de la « révolution » blockchain, et sont à même de permettre l'émergence d'usages radicalement nouveaux tout en introduisant des gains d'efficience significatifs dans certains usages actuels ;
    - l'augmentation des coûts engendrée par les obligations de diligence additionnelles nuiraient significativement à des entreprises souvent petites et dont l'effort doit rester concentré sur les développements technologiques ; et
    - de nombreuses juridictions à travers le monde, voyant le potentiel important et les risques faibles présentés par ces outils au regard de la LBA, construisent des régimes juridiques favorables et un environnement propice à la recherche et l'innovation.

Question 4.2.1 ***Plateformes de négoce décentralisées sans pouvoir de disposer et LBA***

A. Caractéristiques pertinentes

5. Fondamentalement, la différence entre les DEX et les plateformes de négoce centralisées est la réduction du risque de disparition des avoirs des utilisateurs (que ce soit en cas de *hack*, vol, faillite, etc.)[1].

6. Les DEX ne prenant pas la « *custody* » des assets et n'intervenant pas dans l'exécution proprement dite des échanges (qui ont lieu directement sur les blockchain ouvertes et publiques), l'utilisateur réduit considérablement son risque tout en échangeant directement et sans intermédiaire avec sa contrepartie. Ils répondent ainsi à un réel besoin accru de sécurité des détenteurs de crypto, tout en désintermédiant le négoce, ce qui en diminue les coûts.

7. Enfin, les DEX ne permettent ni d'entrer, ni de sortir de l'univers crypto (de et vers les monnaies fiat comme le CHF). Nous pensons en conséquence que les DEX doivent être considérés comme des entités « *pass-through* » : les contrôles (KYC et AML) doivent être effectués au niveau de la connexion avec le système financier classique (soit au niveau des exchanges centralisés).

8. Nous sommes de ce fait d'avis que l'importance des DEX va continuer à s'accroître et qu'il est nécessaire de l'intégrer constructivement dans l'environnement règlementaire.

B. Absence de mélange

9. Etant donné que les DEX ne prennent pas possession des avoirs des utilisateurs, aucun mélange des avoirs n'est créé au sein de la plateforme. Chaque utilisateur demeure détenteur de ses propres avoirs. L'échange a lieu directement avec la contrepartie et ne passe donc pas par un pot commun. L'absence de mélange a pour conséquence que chaque transaction peut être aisément tracée, de l'acheteur au vendeur. Cette possibilité de traçage des transactions, soit par le biais de la blockchain directement, soit par consultation du registre des ordres passés sur la plateforme – par opposition à l'opacité des plateforme de négoce traditionnelle ou des exchanges centralisés (*black box*) – signifie que les DEX ne sont en principe pas convoités pour le blanchiment d'argent et n'offrent pas une solution le facilitant. Partant, ils ne devraient pas être soumis à des obligations de diligences similaires aux plateformes d'échanges centralisée.

C. Contrôles existants suffisants

10. Par ailleurs, les utilisateurs doivent dévoiler leur identité, à des degrés divers en fonction des montants en jeu, lors de leur entrée en crypto (achat de crypto-monnaie sur une plateforme centralisée convertissant des fiat à de la crypto) ainsi que lors du cash-out (sortie de la crypto vers le fiat). Partant, l'état dispose déjà d'un contrôle aux frontières de la crypto, ce qui suffit à atteindre l'un des principaux buts de la LBA et du législateur (identité

[1] Cf. liste : https://github.com/distribuyed/index/blob/master/README.md, consulté le 17 septembre 2018.

du cocontractant). Il n'est donc pas nécessaire d'imposer une obligation de diligence financièrement lourde à une DEX qui, en soi, ne permet pas d'éluder le système de protection contre le blanchiment d'argent et le financement du terrorisme en vigueur.

D. Différents types de DEX

11. Les plus de 200 DEX existant aujourd'hui ont pour l'essentiel en commun de permettre à des contreparties d'effectuer des transactions crypto-à-crypto directement et sans intermédiaire. Il faut cependant distinguer plusieurs types de DEX selon le degré d'intervention et/ou selon la palette de service offerte aux utilisateurs afin de concevoir une régulation efficace et juste :

    - les DEX simples et complètement décentralisés (type : Etherdelta) ;
    - les DEX qui centralisent certaines fonctions comme l' « *order book matching* » (type: IDEX);
    - les protocoles pour la construction de DEX (type : 0x) ; et
    - les relayeurs qui utilisent des protocoles DEX comme 0x (type : RadarRelay).

E. En conséquence

12. Nous proposons qu'à partir du moment ou la plateforme d'échange décentralisée ne prend aucune possession des fonds et que les échanges ont lieu directement entre l'acheteur et le vendeur, la plateforme soit considéré comme un DEX, quelles que soient les facilités qu'elle peut offrir en terme d'expérience utilisateur.

13. En conséquence, à partir du moment où les échanges entre utilisateurs sont transparents, il ne conviendrait pas d'ajouter des obligations réglementaires supplémentaires aux DEX.

Question 4.2.2 Fournisseurs de non-custodian wallet et LBA

A. Caractéristiques pertinentes

14. Nous avons identifié quatre catégories de non-custodial wallets :

1. Un logiciel simple (*pure wallet software*)

Il s'agit de *wallet* tel que Bitcoin Core. Ce type de « *portefeuille est un nœud complet qui valide et relaie les transactions sur le réseau. Cela signifie qu'aucune confiance en un tiers n'est requise afin de vérifier les paiements. Les nœuds complets offrent le plus haut niveau de sécurité et sont essentiels afin de protéger le réseau* ». Ces logiciels sont le plus souvent *open-source* et non liés à un service ou à une entreprise ou organisation spécifique.

2. SPV wallet (*Simple Payment Verification wallet*)

Il s'agit d'un *wallet* qui participe directement au réseau de la blockchain concernée. En plus d'être *non-custodial*, il ne dépend ni d'un service externe, ni d'une maintenance externe pour fonctionner. Autrement dit, une fois installé, il n'a plus besoin de maintenance ou de support tout en offrant la possibilité et la sécurité à son utilisateur.

3. Un logiciel, application, service avec une connexion au réseau et les *hardware wallets*

Tout en laissant à l'utilisateur le contrôle total et non-partagé de ses avoirs (via la possession de ses clés privées, les fonctionnalités offertes par ces solutions sont plus développées dans le but de fournir une meilleure facilité d'utilisation. Par exemple, certains de ces *wallets* fournissent une interface où il est possible de voir le solde de ses avoirs et leur évolution, ou de diffuser des transactions via un ou plusieurs services spécifiques, ou d'accéder facilement à des services d'échanges.

Il s'agit de *wallets* tels que Copay, Jaxx, Edge (anciennement Airbitz), ainsi que Bread ou Ledger, Trezor ou DigitalBitbox en ce qui concerne les *hardware wallets* (ce dernier est une entreprise Suisse).

Ces wallets n'ont aucune custody des avoirs de ceux qui les utilisent, mais les utilisateurs dépendent dans certains cas d'un service annexe fourni par le fournisseur.

4. Fournisseur de canaux de paiements (*payment channel wallet provider*)

Les fournisseurs de payment-wallet sont principalement de deux types :

- les payment channels à sens unique qui sont non-custodial et stables ;

- les payment channels à double sens, dans certains cas nécessitant soit une maintenance de l'utilisateur pour conserver ses fonds, soit de la déléguer à un tiers de confiance.

En termes pratiques et régulatoire, cela signifie que les payment channels peuvent être traités comme des non-custodial wallets, et donc ne nécessitent pas d'être régulés

B. En conséquence

15. Ces services, ou applications ne fonctionnent pas différemment d'un coffre-fort ou d'un portefeuille physique. L'utilisateur est en tout état de cause en pleine possession de ses avoirs (via le contrôle de ses clés privées), et il nous semble qu'il n'y a pas de raison particulière d'assujettir les *non-custodial wallets* à des obligations de type KYC / AML.

Question 4.2.3 Art. 697i CO et émetteurs de jetons

A. Caractéristiques pertinentes

16. Il existe plusieurs types de jetons, selon la classification de la FINMA : *security*, *utility* et *payment*. Lesdits jetons sont aussi différents les uns des autres qu'un billet de loterie, une action dans une entreprise ou un ticket de transport en commun. Il convient donc évidemment de distinguer les jetons qui potentiellement pourraient devoir être soumis à des obligations de transparence, de ceux pour lesquels cela n'aurait pas de sens.

17. Par ailleurs, la forme de la personne morale qui émet des jetons n'influence guère le type de jeton qu'elle émettra lors de son ICO : une fondation, comme une entreprise ou même un individu pourraient chacun émettre des jetons de types susmentionnés.

18. Enfin, il est intéressant de souligner que l'obligation de la personne morale émettrice est de tenir un registre, mais il est de la responsabilité du possesseur d'actions de signaler à l'entreprise les changements de sa situation.

B. En conséquence

19. Il nous semble qu'il n'y a pas lieu d'imposer des obligations de transparence semblables à celles définies à l'article 697i CO aux personnes morales qui émettent des jetons autres que des security tokens.

20. Seules les personnes morales qui émettent des security tokens, qui donnent explicitement droit à une partie de l'*equity* de cette personne morale ainsi qu'à des droits patrimoniaux (par ex. dividendes, votes) devraient y être soumises.

21. Dans ce cas, ces obligations devraient être déployées différemment qu'ainsi qu'il est décrit à l'art 697i CO :

    - à l'émission, le registre est tenu de manière similaire au droit de la SA ;
    - postérieurement le registre n'est actualisé qu'aux occasions auxquelles l'exercice des droits patrimoniaux est proposé aux actionnaires : ainsi, ce n'est qu'au moment de réclamer leurs dividendes ou d'exercer leur droit de vote que les propriétaires de jetons doivent effectuer une mise à jour de leur inscription, sous peine de ne pas pouvoir exercer leurs droits patrimoniaux ou que ces droits s'éteignent après un certain laps de temps.

22. Ainsi, un registre est établi à l'émission et mis à jour lors de l'exercice de droits patrimoniaux. Par conséquent, si la nature du security token évolue avec le temps et se transforme, par la suite, à une autre forme de jeton, il n'y aura plus de droits patrimoniaux à exercer et le registre ne devra plus être mis à jour.

23. En cas d'obligation de tenir un registre, il serait utile d'en identifier les modalités de telle sorte à s'assurer de l'intégrité et de la confidentialité des données collectées par l'émetteur des jetons. La centralisation d'information personnelle aux mains d'une entité la rend par définition vulnérable et va à l'encontre des courants actuels en lien avec la protection des données (GDPR).

* * * * *

Nous nous permettons par ailleurs de porter à votre attention les documents suivants qui nous paraissent propre à nourrir la réflexion sur différents aspects :

- *Decentralized exchanges*

September 2018 - List of DEX's
https://github.com/distribuyed/index/blob/master/README.md

January 2018 - Consensys - « State of Decentralized Exchanges, 2018 » - https://media.consensys.net/state-of-decentralized-exchanges-2018-276dad340c79

Opinion on DEX : https://decentralizedlegal.com/dex/

- *AML et régulations dans d'autres juridictions*

July 2018 - European Parliament - « Cryptocurrencies and blockchain : Legal context and implications for financial crime, money laundering and tax evasion » - http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

May 2018 - European Parliament - « Virtual Currencies and terrorist financing: assessing the risks and evaluating responses » - http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf

July 2018 - Malta - « Bill No. 43 - Innovative Technology Arrangements and Services Bill » : http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29078&l=1

June 2018 - Abu Dhabi - « Guidance – Regulation of Crypto Asset Activities in ADGM » : https://www.iosco.org/library/ico-statements/Abu%20Dhabi%20-%20FSRA%20-%20Guidance%20-%20Regulation%20of%20Crypto%20Asset%20Activities%20in%20ADGM.pdf

June 2018 - US - « Regulation of Cryptocurrency in Selected Jurisdictions » (Argentina, Australia, Belarus, Brazil, Canada, China, France, Gibraltar, Iran, Israel, Japan, Jersey, Mexico, Switzerland) : http://loc.gov/law/help/cryptocurrency/regulation-of-cryptocurrency.pdf

June 2015 - GAFI - « Guidance for a Risk-Based Approach - Virtual Currencies » : http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

September 2018 - US - Office of the New York State Attorney General - « VIRTUAL MARKETS INTEGRITY INITIATIVE REPORT » - https://virtualmarkets.ag.ny.gov/

*