ADAN

L'ASSOCIATION POUR LE DÉVELOPPEMENT DES ACTIFS NUMÉRIQUES

Draft updated Guidance for a risk-based approach to virtual assets and VASPs

FATF public consultation

Adan's contribution

20 April 2021

The Association pour le Développement des Actifs Numériques ("ADAN") is an industry body with 70+ members operating in France in the crypto-assets field. ADAN's objective is the development of the industry in France and Europe and takes all necessary actions to attain this objective.

We appreciate the opportunity to submit comments in response to the public consultation on FATF draft guidance on a risk-based approach to virtual assets and virtual asset service providers. Our response is detailed in the document below.

We look forward to continuing the discussion with the FATF and other interested parties on those matters.

~

General Comments

ADAN strongly supports the development of appropriate KYC-AML measures to prevent to the most extent possible money laundering and financing of terrorism-related risks ("ML/FT risks") and more broadly any illicit use of crypto-assets (or so-called "Virtual Assets" or "VAs").

We are generally in line with the Recommendations published in June 2019 that mandates crypto-assets service providers (or "Virtual Assets Service Providers", or "VASPs") to implement measures to mitigate those risks. The implementation of the Recommendations is currently ongoing, notably in France. The effect of those guidelines will not be visible for a few years, as most countries have not implemented the Recommendations yet.

We are also in agreement with the fact that the development of "decentralized" use cases creates new ML/FT risks that have to be properly addressed.

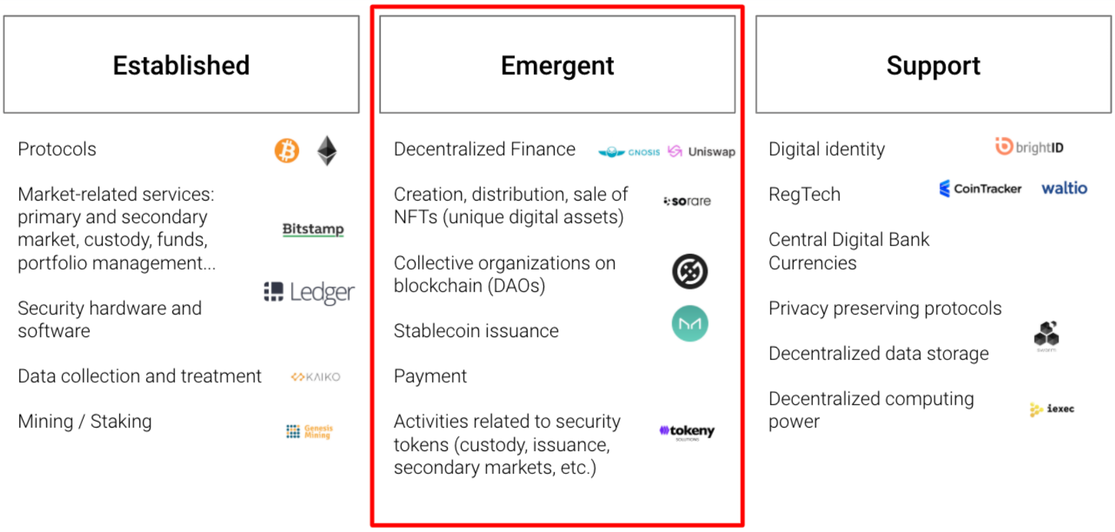
However, the proposals for changes that have been open to comment in March 2021 are, in general, very concerning as they effectively expand the KYC-AML supervision obligations in ways that are neither practical nor desirable.

I. Preliminary remarks

a. Features and interest of emerging crypto-asset uses case

So-called "P2P transactions" are booming. The development of programmable public blockchains have greatly expanded the development and use cases of VAs. We have witnessed the development of innovative use cases that we refer to as "emergent" (e.g. Decentralized Finance (DeFi), digital items (NFTs), collective organizations (DAOs), stablecoins). These emergent use cases use the full potential of VAs and open publicly accessible blockchain networks. Their success and their value hugely depends on key characteristics: openness, trustlessness, transparency and interoperability. They aim at being universally accessible:

- for users, as anyone can interact with the protocols, and ;
- for developers/project owners as the networks on which protocols are deployed are "permissionless" and most bricks and apps are open source.



Established

Protocols

Market-related services: primary and secondary market, custody, funds, portfolio management...

Security hardware and software

Data collection and treatment

Mining / Staking

Emergent

Decentralized Finance

Creation, distribution, sale of NFTs (unique digital assets)

Collective organizations on blockchain (DAOs)

Stablecoin issuance

Payment

Activities related to security tokens (custody, issuance, secondary markets, etc.)

Support

Digital identity

RegTech

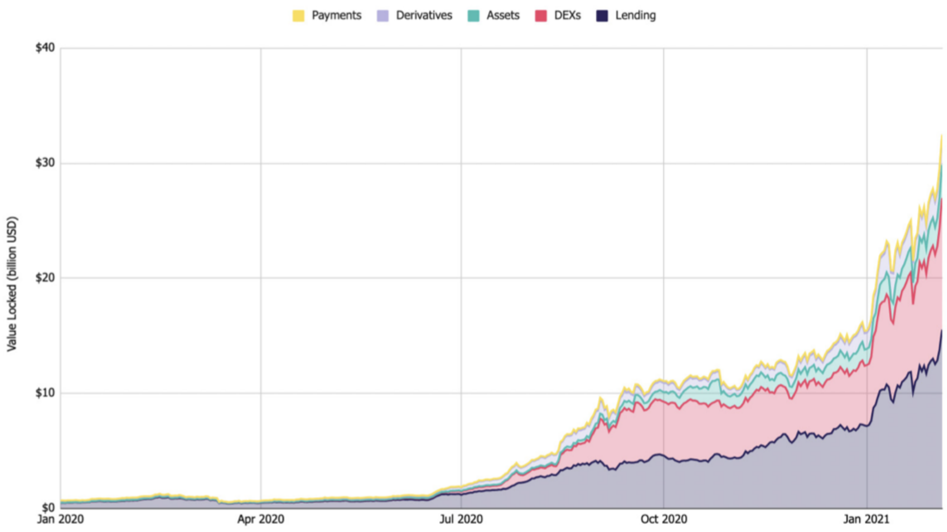
Central Digital Bank Currencies

Privacy preserving protocols

Decentralized data storage

Decentralized computing power

The value proposition of these innovative use cases is attracting novel users, investors and sparkling interest from technologists, financial institutions and the general public. We see this happening with so-called Decentralized Finance (DeFi), a field that comprises hundreds of projects, attracts hundreds of millions of dollars of investments each month and manages more than 50 billion in assets today, with strong development happening in the last year. Decentralized Finance already provides access to new financial service today and the long-term potential of such developments with respect to financial inclusion, efficiency of financial services and more broadly the fluidity of the economic systems are more and more broadly recognized.



(source: The Block)

The entire decentralized finance industry is made up mostly of so-called "*P2P transactions*" as defined in Paragraph 34 "*without the use or involvement of a VASP or other obliged entity*". They play an important role in the growing digital asset ecosystem.

b. ML/FT risk analysis and additional elements to be considered

The ML/FT risks created by P2P transactions are overstated by FATF. The Guidelines imply that widespread illicit finance abuse needs to be curtailed in the sector and that such illicit activities are of particular significance with actors utilizing personal ("unhosted") wallets, engaged in P2P transactions or otherwise without a regulated financial intermediary such as an exchange.

However, the concentration of illicit activities have shown to be primarily with a "*small group of shady cryptocurrency services, mostly operating on top of large exchanges, [who] conduct most of the money laundering that cybercriminals rely on to make cryptocurrency-based crime profitable*"[1]. A significant share of money laundering is being actively facilitated by organizations that are deliberately engaged in 'money laundering services' and incorporating capabilities such as mixers and/or 'nested services' - rather than large amounts going undetected by a wide-range of actors.[2]

This would seem to call for more targeted efforts by law enforcement to concentrate investigations of criminals by identifying owners of these deposit addresses and the organizations that are conducting deliberate money laundering operations (among otherwise legitimate activities). Increased targeted enforcement and requirements for transaction monitoring would strengthen law enforcement regulatory intentions with the rule vs a more wholesale application of AML controls across the VA sector.

[1] Chainalysis, *Crypto Crime Report 2021*, February 2021: https://go.chainalysis.com/2021-Crypto-Crime-Report.html
[2] Ibid

Generally speaking, if ML/FT risks do exist in the crypto universe, the true level of such risks is often overstated.

Recent analyses indicate that the share of transactions in crypto-assets associated with illicit activities has sharply decreased over the past years: by 53.6 % between 2019 and 2020 in terms of transaction volume according to Chainalysis[3] which is corroborated by Ciphertrace's research[4] (57 %). In 2020, the illicit share of all activities on crypto-assets dropped from 2.1 % to 0.34 % representing $10.0 billion of total cryptocurrency value sent and received by illicit entities. More importantly, such illicit activities are mainly scams (53.8 %), darknet markets (37 %) and ransomware (7.1 %) leaving terrorism financing accounting for a very marginal share.

This is probably correlated with the falling number of crypto-asset service providers that do not perform KYC checks: only 3 % in 2020[5]. When dealing with service providers supporting both legal currencies and crypto-assets, this share slumpes to 1 %. It should be highlighted that nearly 100 % of European and North American firms do verify the identity of accounts' owners.

In 2019, in their "National Analysis of Money Laundering and Terrorist Financing Risks in France", the French Treasury already outlined that the illicit use of crypto-assets for ML/FT purposes was not a preferred option by criminals. Indeed, some factors - such as the specific knowledge and technical expertise required to use them, as well as their volatility - deter them from using these assets. Moreover, in many scenarios, the information stored on and off chain allows for the identification of customers and the monitoring of transactions. For these reasons, very few cases where crypto-assets were used for illicit purposes have been reported.

This latest assumption is corroborated by the recent analysis led by the former Deputy Director of the CIA which reports that criminals are increasingly aware that illicit activities can be easily identified and disrupted as "blockchain analysis is a highly effective crime fighting and intelligence gathering tool"[6]. Therefore, while this report shows the share of ML/FT activities using crypto-assets is already overstated today, it also highlights that criminals will continue on flowing away from crypto-assets (at this time, the risk is mainly related to anonymity-enhanced crypto-assets).

Regarding blockchain analysis, it has to be noted that the sophistication and efficiency of transactional analysis tools (like Chainalysis, Elliptic, e-NIGMA, Scorechain, etc.) are permanently improving with uses and experience. In 2020, they helped authorities to trace and dismantle several criminal networks like the Harrod's drug ring in 2019, ISIS-related individuals in France and in the UK in 2020, and more recently the identification of donors who helped plan the US Capital riot in January 2021.

[3] Ibid

[4] Ciphertrace, *Cryptocurrency Crime and Anti-Money Laundering Report*, February 2021: https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report/#trends

[5] Cambridge Centre for Alternative Finance, *3rd Global crypto-asset benchmarking study*, September 2020: https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/3rd-global-cryptoasset-benchmarking-study/

[6] M. Morrell, J. Kirshner, T. Schoenberger, *An Analysis of Bitcoin's Use in Illicit Finance*, April 2021: https://cryptoforinnovation.org/resources/Analysis_of_Bitcoin_in_Illicit_Finance.pdf

II. Comments on Current FATF approach

We recognize that the increasing development of P2P networks could however be cause of concerns with respect to ML/FT risks. Should a significant development of those novel modes of operation occur, they will require new and adapted methods for properly and efficiently monitoring and preventing those risks.

Unfortunately, the revised Guidelines take a less ambitious and therefore unadapted approach, merely aiming at expanding existing obligations to new entities. This is neither sufficient nor desirable.

The current approach taken by the FATF is an extreme extension of captured entities' definitions and operations **(a)** without adaptation to surveillance obligations **(b)**, which creates legal uncertainty, detrimental to an effective surveillance and prevention of ML/FT risks **(c)**.

a. The revised Guidelines make (almost) everyone a VASP

Although the revision of the Guidelines is presented as a clarification, it effectively extends the definition of VASP to such extent that **every single individual or company involved in the development, deployment, use or governance of such a use cases could be considered as a "VASP"**, i.e. an entity that has to implement KYC-AML preventive measures.

This is shown in §47 to §79 and aptly summarized end of §75 and beginning of §76: "*The FATF takes an expansive view of the definitions of VA and VASP and considers most arrangements currently in operation, even if they self-categorize as P2P platforms, may have at least some party involved at some stage of the product's development and launch that constitutes a VASP. The expansiveness of these definitions represents a conscious choice by the FATF.* [...] *Where customers can access a financial service, it stands to reason that some party has provided that financial service, even if the act of providing it was temporary or shared among multiple parties.*"

The last statement indicates that FATF conscientiously chooses to ignore the innovative ways of operating a service that VAs allow, i.e. operations that function without any party interfering at the execution stage.

Other expansive interpretations include:

- §59: ***For example, the owner/operator(s) of the DApp likely fall under the definition of a VASP,*** *as they are conducting the exchange or transfer of VAs as a business on behalf of a customer;*
- §60: ***Any entity that provides or facilitates control of assets or governs their use*** *may qualify under part (iv) as this is the conceptual meaning of the words "administration" and "safekeeping";*
- §73: ***If one or more parties have decision-making authority over structures that affect the inherent value of a VA****, such as changing reserve requirements or monetary supply for a so-called stablecoin, they are likely to be VASPs as well;*
- *§74: Only entities that provide very limited functionality falling short of exchange, transfer, safekeeping, administration, control, and issuance will generally not be a VASP.*

- §75: *Launching a service as a business that offers a qualifying function, such as transfer of assets,* ***may qualify an entity as a VASP even if that entity gives up control*** *after launching it. Some kinds of "matching" or "finding" services may also qualify as VASPs* ***even if not interposed in the transaction.***
- §77*: When there is a need to assess a particular entity to determine whether it is a VASP or evaluate a business model where VASP status is unclear, a few general questions can help guide the answer. Among these would be* ***who profits from the use of the service or asset, who established and can change the rules, who can make decisions affecting operations, who generated and drove the creation and launch of a product or service, who possesses and controls the data on its operations, and who could shut down the product or service****.*
- §79*: Launching a service that will provide VASP services, for instance, does not relieve a provider of VASP obligations,* ***even if those functions will proceed automatically in the future****, especially but not exclusively if the provider will continue to collect fees or realize profits, regardless of whether the profits are direct gains or indirect. The use of an automated process such as a smart contract to carry out VASP functions does not relieve the controlling party of responsibility for VASP obligations. For purposes of determining VASP status,* ***launching a self-propelling infrastructure to offer VASP services is the same as offering them****, and similarly commissioning others to build the elements of an infrastructure, is the same as building them.*

This last sentence is particularly worrying. **It is a mistake to think that launching a self-propelling infrastructure to offer VASP services is the same as offering them, from a functional point of view**. The ML/FT risks borne by those two ways of offering VASP services are entirely different.

While we understand that the Recommendations aims to cover every entity that retains a meaningful control on the assets and the operations, **the current definition encompasses entities or even natural persons that have no meaningful control on such operations.**

Indeed, some of those new captured persons:

- **do not and can not have access to any specific information regarding the users or the funds** (in addition to information that is already available on chain due to the transparent nature of most public networks);
- **do not and can not have any meaningful control** on the persons that have access to the application, nor the functioning or the funds managed by the application;
- **are not properly trained and do not have the financial means to conduct such analyses** and submit to reporting obligations mandated by FATF guidance.

The mismatch between obligations that the extension of the definition and the real level of control exercised by those actors is illustrated in the table below with topical examples when analysed in light of to §47-79:

	Decentralized exchange (e.g. Uniswap)	**Decentralized stablecoin (e.g. Maker)**	**Liquidity aggregators (e.g. Paraswap, 1inch)**	**Issue identified**
Developer	***Captured****. Launching a service as a business that offers a qualifying function, such as transfer of assets, may qualify an entity as a VASP even if that entity gives up control after launching it (§75)*	***Captured.*** *Developers are VASPs if they deploy programs whose functions fall under the definition of VASP and they deploy those programs as a business on behalf of customers. (Box 4)*	***Captured.*** *Some kinds of "matching" or "finding" services may also qualify as VASPs even if not interposed in the transaction. (§75)*	The developer's control on the users of the protocol is dependent on the use case implementation. He can always deploy new versions of the smart-contract. He has no access to information regarding users that are not already available on-chain.
Deployer of the smart-contract	***Captured.*** *Launching a service as a business that offers a qualifying function, such as transfer of assets, may qualify an entity as a VASP even if that entity gives up control after launching it (§75)*			The deployer of the smart-contract may be an anonymous individual. He usually retains no controlling power on the operations. He has no access to information regarding users that are not already available on-chain.
Governance token holder (UNI, MKR, 1INCH)	***Captured.*** *When there is a need to assess a particular entity to determine whether it is a VASP or evaluate a business model where VASP status is unclear, a few general questions can help guide the answer. Among these would be who profits from the use of the service or asset, who established and can change the rules, who can make decisions affecting operations.*	***Captured.*** *If one or more parties have decision-making authority over structures that affect the inherent value of a VA, such as changing reserve requirements or monetary supply for a so-called stablecoin, they are likely to be VASPs as well,*	***Captured.*** *When there is a need to assess a particular entity to determine whether it is a VASP or evaluate a business model where VASP status is unclear, a few general questions can help guide the answer. Among these would be who profits from the use of the service or asset, who established and can change the rules, who can make decisions affecting operations.*	Token holders do not have access to any relevant information nor have the means to implement any form of anti-ML/FT procedure on transactions.

From a practical and technical point of view, it is uneven to ask all the persons that play a role in the operation of a VASP as being themselves fully-fledged VASPs, regardless of their level of intervention and activities, to comply with the same obligations. An advertising company has no access to the accounts of the clients unlike the custodian. These two activities cannot be subject to equal obligations.

Similarly, a governance token holder has and cannot have any information on the governed product and should not be subject to KYC obligations.

Extensive definition of control. This objective to cover every single case where ML risks are identified with the "VASP" status is also visible in changes that aim to cover personal wallets (so-called "unhosted wallets") or multisignature schemes. It is indeed desirable that multisignature schemes do not help malicious actors to avoid liability. However, **the amendments proposed are so broad that they are capturing every single participant to a multisignature scheme as being a fully-fledged VASP,** making multisignature arrangements entirely impractical even though those arrangements are vital to the security of VA operations (see notably §55, "*A user, for example, who owns a VA, but cannot send it without the participation of others in a multisignature transaction, likely still controls it for the purposes of this definition.*").

The modifications that have been published for comments therefore create an environment of legal uncertainties and risks where every user of public blockchain deploying or interacting with a smart-contract or any multisignature scheme could be analysed as operating a VASPs, not complying with regulation and therefore facing extreme sanctions, even though the vast majority of such individuals are merely interacting with an innovative protocol in good faith to finance new activities, buy digital items or speculate on future of VAs prices.

b. The revised Guidelines do not provide with new actionable options for mitigation of ML/FT risks for newly captured persons

Such extensive definitions, potentially capturing every active user of public blockchains, are already problematic. But this is aggravated by the fact that this extension is proposed without any adaptation to the measures that have to be implemented by targeted entities. We believe that such adaptations would be required to monitor effectively ML/FT risks created by the development of those use cases without hindering the development of P2P innovative use cases.

With respect to P2P activities in general, the options for mitigation of ML/FT risks do **not** mirror the options that are suitable for more traditional VASPs. Those use cases cannot, by definition, require prior identification of clients (KYC), because the clients directly interact with each other. **The upside is that those interactions are happening on public and auditable networks, allowing for detailed analysis of transactions and implementation of adapted monitoring and reporting**.

c. The revised Guidelines create legal uncertainty for the crypto-assets industry and will likely have a net negative effect on the effectiveness of supervision and mitigation of ML/FT risks

The elements above create an environment where peer-to-peer use cases, using a variance of smart-contracts, a form of multisignature scheme or personal wallets could not operate with sufficient legal certainty in countries that apply those Recommendations to the letter.

This risks nullifying the whole value proposition of decentralized use cases and, more broadly, what constitutes the underlying value of VAs, as:

- One of the main value proposition of the “decentralized” application is the lack of a manual validation or operation of the use case, the business logic being executed by the public network;
- Another significant value proposal is that each application can be used as an open service (equivalent to an “API”), allowing for the creation of complex use cases that bring together more than one product.
- More generally, VAs' whole value proposal is due to the fact that they allow for direct apprehension of digital assets by consumers, enterprises and other persons, without the need for intermediaries.

We consider this extensive coverage of natural and legal persons that are linked to decentralized use cases or personal wallets to be a net negative for both the smooth operation of the markets and the supervision of those operations. Analyzing all the legitimate use cases as potentially illegal and threatening their developers and users with extreme sanctions is not a reliable way to address money laundering and terrorism financing risks.

There is a significant chance that those revised Guidelines lead innovative companies to move their activities to unregulated or underregulated markets, creating a place for illicit activities to thrive. This is a very real risk, accentuated by the fact that regulators will likely find it difficult to track and take action against decentralized use cases that facilitate peer to peer transactions in the industry.

We conclude that the approach taken by the FATF-GAFI is not proportionate, impractical, and in opposition with the developing trends of the ecosystem. **We consider this approach to be counterproductive for avoiding ML/FT risks in crypto-assets and propose other solutions to reach the same objectives.**

On this basis, we provide a suggested approach for adaptation of Recommendations below.

III. Suggested approach and recommendations

ML/FT risks should be properly addressed by FATF Guidelines, including risks created by "decentralized" use cases. In consideration of the very specific nature of VAs, the public blockchains on which they are created, transferred, exchanged and the functioning of smart-contracts that are executed directly by the community participating in the networks, we suggest the following approach.

As a preliminary remark, we would like to point out that those risks have not materialized so far. Therefore, we recommend first and foremost that the period for observation and appropriate study of relevant options for mitigating future ML-FT risks related to P2P transactions is extended. More time is needed to create rules that appropriately cover all the issues at hand without hindering the development of VAs.

1. **The most effective way to mitigate P2P transactions-related ML/FT risks is to ensure that law enforcement and financial intelligence agencies use the latest tools to analyse those transactions, update and publish relevant lists of "tainted" addresses and assets on public blockchains and effectively arrest criminals using those networks.** This will ensure that such activities are discouraged very efficiently. This has already been proven efficient, as the share of illicit transactions on public blockchains decreased from multiple percents to less than 1 percent in the last few years.

   Indeed, when crypto is used for ML/FT transactions, they can be traced. In many scenarios, the information stored on and off chain already allows for the identification of customers and the monitoring of transactions using the existing VASP definition.

   As acknowledged in Michael Morrell's analysis, "*Blockchain technology is a powerful but underutilized forensic tool for governments to identify illicit activity and bring criminals to justice*". Several people that were questioned (among them officials at the CFTC and the US Treasury) promote a greater use of blockchain analytics: thanks to the transparency inherent to blockchain networks, with the help of such tools, crypto-asset transactions would be more traceable and ML/FT risks much more easily manageable than in the traditional financial and banking system.

2. **Obligations set forth with regards to P2P exchanges, decentralized products and "unhosted" wallets should be first and foremost applied to the VASPs already covered by the regulation, not by the means of extending the existing definition of VASPs to entities that do not control meaningfully the operation of the product and the VAs.**

   In this respect, the Guidelines should clarify that only the entities that would effectively operate a service and have an effective means to control it should be targeted as VASPs. We therefore recommend that the definitions are reworked to clarify the exact entities covered, considering the existence of actually decentralized use cases and the level of control that those use cases allow for each kind of participant. **FATF should ensure that the qualification of VASP does not apply to entities that have no effective control on assets or products targeted**.

Existing VASPs could be liable to implement relevant KYC-AML procedures on the clients, but also additional AML-CFT diligences on the "decentralized" products themselves when necessary. They could ensure that the product provides a sufficient degree of transparency and auditability that allows for a sufficiently reliable assessment of the ML/FT risks associated with their use. This is proposed by the Guidelines in §35 ("*Countries should also consider how ML/TF risks of P2P transactions for some VAs may be mitigated through, for example, blockchain analytics, which may provide greater visibility over P2P transactions.*") but this should be emphasized and generalized.

3. **Other participants should not be considered as fully-fledged VASPs but could eventually be covered by another, adapted status that would come with adapted AML-CFT obligations.**

The list below is not exhaustive and that we highly recommend that the FATF assesses more reliably the actual risks posed by crypto-assets. Latest elements provided by ML/FT risks specialists in the crypto-assets space indicate that such risks are generally low[7]. Imposing new AML-CFT obligations to entities should therefore only be considered where actual risks have been identified and observed.

In all cases, the ideals of decentralization that the sector aims to achieve include transparency and openness. In consideration of this, the most efficient way to ensure that decentralized products are not used for money laundering or financing of terrorism would be to **encourage high information and transparency standards for developers / deployers of decentralized products**.

This could be done in multiple ways, some of them listed below:

a. Create "DeFi AML-CFT Standards". Those standards could include transparency and auditability requirements that would help blockchain transaction analysis companies to identify ML-FT risks born by P2P transactions facilitated by those products. Products that would respect such standards would be considered "lower risk". This would allow VASPs to operate with them or to accept the proceeds of their use with lower diligence.

b. Define reporting and information gathering standards that would be required from entities that benefit from the operation of decentralized use cases. Those entities could register to their local authorities with a specific status and report atypical financial operations, hacks and malfunctionings to the relevant agencies. These surveillance obligations should be limited to relevant information and, in any case, not include prior identification of clients nor any form of prior authorization to ensure a smooth functioning of markets.

[7] https://www.coindesk.com/ex-cia-director-says-criminals-will-move-away-from-bitcoin-in-new-lobbying-groups-first-report

c. Create a form of liability after deployment imposed on the developer / deployer that would apply to cases where the developer and / or deployers did not ensure that the use case operates with the most extent possible with full transparency and auditability. **This option should however be treated with extreme caution, they should not block the deployment and use of privacy-preserving products. The liability should only be qualified when a clear intent to facilitate ML-FT risk can be identified.**

In line with our preliminary recommendation, this should probably justify taking some more time to refine the risk analysis led by the FATF and design and implement aforementioned proposals accordingly.

We hope that those comments provide relevant information to the FATF and remain available for any further questions.

Answers to FATF questions

1. Does the revised Guidance on the definition of VASP (paragraphs 47-79) provide more clarity on which businesses are undertaking VASP activities and are subject to the FATF Standards?

- *Is further guidance needed on how the FATF Standards apply to various business models, as stated in paragraphs 56-59? How should the Guidance further address the challenges in applying the definition of VASP to businesses which decentralize their operations across multiple parties?*

  Yes. The FATF Guidelines should either not cover those businesses or cover them with proper functional analysis methods. As discussed in General Comments, the approach taken by the FATF is too broad and does not capture the subtleties of decentralized use cases governance and operations. The result is unadapted and impractical obligations.

  We therefore recommend that the definitions are reworked to clarify the exact entities covered. This rework should consider the existence of actually decentralized use cases and the level of control that those use cases allow for each kind of participant. FATF should ensure that the qualification of VASP does not apply to entities that have no effective control on assets or products targeted.

- *Is more guidance necessary on the phrase 'for or on behalf of another natural or legal person' in the FATF definition of VASP? What are the challenges associated with applying the business-customer relationship concept in the VASP context?*

  /

- *Do the clarifications on the 'expansive' approach to the definition of VASP in identifying and policing the 'regulatory perimeter' for VASPs provide countries and the private sector with enough guidance? What additional clarity can be given to make the perimeter clearer?*

The perimeter is not clear and creates legal uncertainties. It has to be redefined to clarify both the scope and the obligations, as described in the General Comments.

2. What are the most effective ways to mitigate the money laundering and terrorist financing (ML/TF) risks relating to peer-to-peer transactions (i.e., VA transfers conducted without the use or involvement of a VASP or other obliged entity, such as VA transfers between two unhosted wallets) (see paragraphs 34-35 and 91-93)?

- *How are peer-to-peer transactions being used for ML/TF purposes and what options are available to identify how peer-to-peer transactions are being used? What role and implications (e.g., benefits) do peer-to-peer transactions and unhosted wallets have in VA ecosystems?*

  Peer-to-peer transactions and personal wallets are the epitome of "VA" ecosystems. Crypto-assets have been created to allow for such use cases and they provide the most value to the market. We see this happening with so-called Decentralized Finance, a field that comprises hundreds of projects, attracts hundreds of millions of dollars of investments each month and manages more than 50 billion in assets today, with strong development happening in the last year. Decentralized Finance already provides access to financial services to new populations that have been banned from accessing traditional financial products.

  As with any financial product, those can be used for ML/FT purposes. However, the transparent nature of the P2P transactions registered on a public blockchain provides powerful tools for mitigation of ML/FT risks. In practice, the use of such schemes for ML/FT purposes has been observed as low[8].

  The most effective way to mitigate those risks is to ensure that law enforcement and financial intelligence agencies use the latest tools to analyse those transactions, update and publish relevant lists of "tainted" addresses on public blockchains and effectively arrest criminals using those networks. This will ensure that such activities are discouraged very efficiently. This has already been proven efficient, as the share of illicit transactions on public blockchains decreased from multiple percents to less than 1 percent in the last few years (please refer to our summary of various analysis in I.b).

  In addition, VASPs (old definition, not including P2P networks, unhosted wallets and multisignature schemes that do not exercise meaningful control) should implement relevant surveillance mechanisms for P2P transactions.

- *What specific options are available to countries and VASPs to mitigate the ML/TF risks posed by peer-to-peer transactions?*

  The tools used should be adapted to the public and transparent nature of those networks.

[8] https://ciphertrace.com/wp-content/uploads/2021/01/CipherTrace-Cryptocurrency-Crime-and-Anti-Money-Laundering-Report-012821.pdf

- **Blockchain analytics;** those tools are extremely useful and allow for development of comprehensive maps of wallets and transactions engaged in illicit activities, attribution of specific identities to such wallets, identification of suspicious transactions and red flag indicators...

- **Information collection from the client** (origin of funds, transactions, motivations…) for centralized entities;

- **Implementation of additional rules mandating from the developer / deployer of the business logic (point of contact)**:
    - Surveillance of use;
    - Reporting of any:
        - suspicious transaction;
        - hack, thief or other illicit operation;
        - malfunction.

- *Are the risk mitigation measures proposed in the Guidance in paragraphs 91-93 appropriate, sufficient and feasible?*

    In general, measures proposed make sense. Some of them are however not appropriate. **Notably, the mitigation method that is, in substance, a ban of P2P and decentralized use cases (§91, c)**. The denial of licencing to VASPs seems excessive, as the equivalent in traditional finance would be denial of licencing to financial institutions that provide cash to customers. We want to emphasize that P2P use cases are the most innovative and where the market interest has been developing. They could ultimately provide huge benefits to society as a whole. Rather than hindering or banning licit uses of such products, FATF should aim to provide for suitable guidance for adapted surveillance and mandate the adequate level of transparency and information reporting to the creators / deployers. **We would therefore prefer that this paragraph be removed**.

    Conversely, recommendations of §92 are very welcomed and should be further encouraged. **The emphasis should be placed on those measures that are required as soon as possible.**

3. Does the revised Guidance in relation to the travel rule need further clarity (paragraphs 152-180 and 256-267)?

- *Are there issues relating to the travel rule where further guidance is needed? If so, where? Please provide any concrete proposals.*

    The clarification provided is welcomed by the industry. To the best of our understanding, the Guidance provided is sufficient.

- *Does the description of counterparty VASP due diligence clarify expectations, while remaining technology neutral and not prescribing how VASPs must undertake this process (see paragraphs 172-177 and 261-265)?*

  The final word in Paragraph 179, "limitations" infers that countries should consider limiting unhosted wallet transactions, with the consequence that this may drive more business underground (that is, larger transactions may simply move peer-to-peer or be split into smaller transactions across multiple exchanges), or it may result in VASPs being unable to continue with operations. When considered as a risk-based approach, a more suitable wording may be "appropriate risk mitigations" that will allow for the size, nature, and complexity of the individual industry sector, national risk assessment, and other factors to be considered.

4. Does the revised Guidance provide clear instruction on how FATF Standards apply to so-called stablecoins and related entities (see Boxes 1 and 4 and paragraphs 72-73, 122 and 224)? ***Is the revised Guidance sufficient to mitigate the potential risks of so-called stablecoins, including the risks relating to peer-to-peer transactions?***

The General Comments provide with specific comments with regards to stablecoin arrangements.

In addition to those comments, we would like to point out that some wording on those paragraphs and Boxes seems to illustrate some misunderstandings with regards to how those stablecoin arrangements operate.

The most obvious mismatch is on the **purpose of stablecoins**. Box 1 states that such stablecoins are created solely to overcome price volatility issues with regards to VAs. While correct, this statement is incomplete. The stablecoins were primarily created to bring the advantages of VAs (direct apprehension, transparency, programmability) to legal currencies. This should be reflected in the Recommendations.

Another issue that can be identified **is the broad VASP qualification capture**. In this regard, §72 notably states that "*If one or more parties have decision making authority over structures that affect the inherent value of a VA, such as changing the reserve requirements or monetary supply for a so-called stablecoin, they are likely to be VASPs as well, depending on the extent of the influence*". This is not a good criterias as it does not allow to capture any activity that could be associated with actual functions operated by VASPs. This article should be redrafted or erased.

In addition to those comments, we would like to refer to and support comments submitted by Global Digital Finance on the matter, that provide additional clarifications and justified criticism of the Guidance with regards to stablecoins.

5. Are there any further comments and specific proposals to make the revised Guidance more useful to promote the effective implementation of FATF Standards?

Our additional comments are provided in the beginning of this response.

We would like to express again our gratitude for this opportunity to present detailed comments on the proposed revision of the Guidance.

Appendix: Adan's general analysis on the crypto-asset ecosystem and their ML-FT risks

In this section, Adan would like to provide with some additional useful elements regarding the current situation of the crypto-asset ecosystem and risks.

According to Adan and its members, AML/CFT regime for markets in crypto-assets is a matter of absolute necessity in order to guarantee financial security and confidence within crypto markets. However, the biggest fallacy would be to model analytical assessments and rules applicable to this novel industry on the current AML/CFT framework designed for financial entities.

➢ **Current AML/CFT risk analysis and prevention mechanisms were designed for financial entities which are very different from crypto players.** Due to the fact that the use of crypto-assets can, at a first glance, be likened to financial activities (money, investment vehicles, trading, etc.), the same analyses as for the financial sector have been applied to crypto-asset markets. Notably, transfers of crypto-assets are often equated to transfers of money. However, the financial sector (actors, clients, transactions, technology used, etc.) is very different from the crypto-assets one. For more details, please refer to Adan's position paper sent to the European Commission in the context of the consultation on their action plan for a comprehensive Union policy on preventing money laundering and terrorist financing[9].
This comparison explains why at the end, ML/FT risks raised by crypto-assets are of smaller importance than those posed by the traditional financial activities. That is why applying blindly the regulatory requirements that were designed for financial entities would omit all these fundamental differences and appear disproportionate for crypto-actors.

➢ **Based on this partially unadapted risk analytical framework, misunderstandings and stereotypes about ML/FT risks raised by crypto activities are persisting.** If ML/FT risks do exist in the crypto universe, the true level of such risks is often overstated. Two fundamental factual realities must be widely acknowledged:

- **Crypto-assets do not raise *substantial* ML/FT risks.**

This deeply rooted dates back at the very beginning of the crypto world when bitcoin still was the first and single "cryptocurrency". Bitcoin, a quasi-financial object that was not borne in the financial world, was viewed with suspicion and gained a "ML/FT label" when it became the only means of payment accepted on "Silk Road", a dark web market that allowed the purchase or sale of anything, including

[9] Adan, *Contribution to the consultation of the European Commission on its AML/CFT Plan*, 3 August 2020: https://adan.eu/en/testimony/european-commission-mla-cft-plan

illegal goods and services. Since then, many other crypto-assets and related use cases emerged, the ecosystem structured itself with serious and solid actors, and markets in crypto-assets self-sanitized. However, this outdated vision remains.

In their "*National Analysis of Money Laundering and Terrorist Financing Risks in France*" published in September 2019, the French Treasury outlines that the illicit use of crypto-assets for ML/FT purposes is not a preferred option by criminals. Indeed, some factors - such as the specific knowledge and technical expertise required to use them, as well as their volatility - deter them from using these assets. Moreover, in many scenarios, the information stored on and off chain allows for the identification of customers and the monitoring of transactions. For this reason, very few cases where crypto-assets were used for illicit purposes have been reported.

This analysis is corroborated by the 2021 Crypto Crime Report published by Chainalysis which reveals that illicit transactions represent 0.34% of all transactions in crypto-assets and that the overwhelming majority of such transactions consists in payments related to scams and ransomware, not ML/FT issues *per se*.

- **All the crypto-asset activities do not bear the same level of ML/FT risks.**

First of all, it is of utmost importance to distinguish crypto market players (exchanges, brokers, custodians, etc.) from other companies dealing with crypto-assets (e.g. as a product, means of payment or investment) when defining the scope of AML/CFT requirements. For example, as already set very clearly by the European Parliament[10] and FATF[11], non-custodial wallets are pure technical providers who should be excluded from the lists of VASPs: as they do not function as intermediaries, it does not make much sense to target them for AML/CFT purposes. Similar reasoning should be led regarding other actors that develop blockchain products and services and are not market players.

Within market-related activities, "crypto-crypto" exchanges are deemed to raise lower ML/FT risks. In their analysis, the French Treasury attributes a "moderate level of risk" (on a scale of "low" to "high") to crypto-assets and precise that "crypto-crypto" activities are less exposed to ML/FT threats than "crypto-fiat" activities. The conclusions of a public consultation led by Adan on the crypto-crypto activities carried out from France corroborate this analysis[12].

Several tangibles reasons can be outlined:

❏ Crypto-crypto activities do not imply the re-injection of funds into traditional economic channels. Yet potential ML/FT risks materialise at the time of the purchase or sale of the asset against legal money.
❏ Crypto-crypto transactions can be monitored thanks to "Know your Transactions" (KYT) processes. It is possible for companies to directly or indirectly (through blockchain analysis service providers) audit transactions on public blockchains. It is therefore possible to analyse in near-real time the transactions executed on the blockchain and, thanks to databases that are updated very regularly and machine learning algorithms, assign a suspicion score to the

[10] https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf
[11] FATF guidelines, point 48.
[12] Adan, *Activités "crypto-crypto" en France*, March 2020: https://adan.eu/rapport/activites-crypto-crypto-france-recommandations-encadrement-acteurs

transactions in the chain. Therefore actors can use these analyses in their AML/CFT arrangements.

❏ Where those tools are not used during any transaction (e.g. because the risk analysis of this transaction deemed it less risky), all the history of those past transactions remains accessible on the blockchain forever. This means that police departments, financial and tax authorities can use this powerful tool to catch fraudsters and criminals after the fact and incriminate them with one of the most strong forms of proof available ; and they do. In 2019, following the flows of funds on the Bitcoin blockchain enabled the takedown of the largest darknet child pornography website, covering over 38 countries[13].

➢ **Such stereotypes about ML/FT risks raised by crypto activities have very detrimental side effects for the development of a safe crypto industry.** The main one is that applying existing rules to crypto-assets appears quite inefficient, while crypto-assets do require an appropriate level of ML/FT regulation. Other indirect consequences lay in the difficult relations between the crypto industry and traditional actors among first the banking system. At the end, an inadequate AML/CFT regulatory approach will harm the competitiveness of crypto companies within the whole EU. For more details, please refer to the aforementioned Adan's position paper.

➢ That is why Adan's additional recommendations to be considered in this Consultation are:

- In accordance with recital 2 of the AMLD5 stating that "*It is important to note that the measures taken should be proportionate to the risks*", **adapt AML/CFT requirements for crypto actors when they are identified as unsuitable**. The underlying principles of any regulation that is efficient but compatible with the economic development of a sector are pragmatism and proportionality. Therefore, AML/CFT rules that would apply to crypto players, whether they operate exclusively with crypto-assets or with legal money, should follow such principles meaning that they should be tailored to their specific features and the real level of ML/FT risks that they pose. In the aforementioned position paper, Adan has already identified some areas where adjustments would be necessary to better reflect the reality behind the functioning of crypto-markets while fighting against ML/FT threats.
- **Implement *ad hoc* AML/CFT risk analysis and prevention mechanisms for crypto activities**. The public nature of transactions executed on blockchain could be a powerful AML/CFT support for *a priori* analysis of incoming flows to identify risk accounts, but also *a posteriori* monitoring of flows that could be performed by law enforcement agencies.
- **Assess competitiveness impacts for the industry when regulating.**
- For European institutions and regulatory/supervisory bodies, as well as national competent bodies and finance intelligence units, **engage into specific training efforts to better understand crypto-assets, the specific functioning of markets, their risks and opportunities, and growing trends on markets (such as decentralized finance)**.

[13] https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child