ADAN

L'ASSOCIATION POUR LE DÉVELOPPEMENT DES ACTIFS NUMÉRIQUES

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities

Adan's comments on the Commission Staff Working Document

Introduction

Adan is an industry body that brings together and represents crypto-asset and blockchain professionals in France and Europe. Our members cover a wide range of activities, including market makers, custody providers, payment service providers, investment management, analysis tools, events and marketing, and security. We are dedicated to all the companies that are interested in crypto-assets and are targeting the French market.

We believe that crypto-assets represent a transformational shift in finance and economics. Crypto-asset technologies challenge centuries-old foundations of economics and monetary theory and offer the potential to create a new social contract built on the principles of inclusion and openness.

Our mission is to be a pragmatic voice for the French and European crypto-asset industry, contributing to its growth and development through constructive dialogue and education.

The Association is available for any additional commentary or work related to digitalisation and crypto-assets.

1. General comments

Adan would like to thank the European Commission for this opportunity to share comments and suggestions on their Report on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities.

Adan also welcomes the huge work conducted by the European Commission in 2020 to integrate crypto-assets in the EU Digital Finance Strategy, to design a dedicated framework for such assets as well as their constant willing to listen to the industry through consultation processes, webinars and bilateral contacts with representative bodies like Adan.

Before going into details of this report, Adan would like to share its general comments and 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[1].

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

[1] 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

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 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[2] and FATF[3], 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[4].

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 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

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

funds on the Bitcoin blockchain enabled the takedown of the largest darknet child pornography website, covering over 38 countries[5].

➢ **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 Report 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)**.

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

2. General description of the sector and related product/activity concerned - Adan's comments

In this paper we will commonly use the CSWD acronym to refer to the Commission Staff Working Document.

Stakeholders (p98)

Exchange platforms

Under the new categorisation of crypto-asset service providers (CASPs) introduced by the MiCA proposal for regulation, it should be noted that:

- Exchange platforms encompass both exchanges of crypto-assets for fiat currency that is legal tender and exchanges of crypto-assets for other crypto-assets (defined in article 2.12 and 13).
- But they exclude multilateral venues that the MiCA proposal for regulation refers to as trading platforms for crypto-assets (defined in article 2.11).

Therefore under this new taxonomy, AMLD5 currently covers CASPs that provide the exchange of crypto-assets for fiat currency that is legal tender. The AML framework review is likely to extend to other trading modalities.

Adan's recommendation for the SNRA review: The new vocabulary introduced by MiCA and the pilot regime proposals should be used in the CSWD to replace undetermined ones:

- "Virtual currencies", "virtual assets", "coins" are not MiCA concepts and should be replaced by "crypto-assets".
- "Initial coin offerors" should be replaced by "issuers of crypto-assets".
- "exchange platform" is not precise enough.
- "exchanges from VCs or VAs to other VCs or VAs" should be replaced by "the exchange of crypto-assets for other crypto-assets".
- etc.

This list is likely not exhaustive.

Miners

Miners are only one type of block validators that verify transactions and add blocks on the chain.

Miners are validators on proof-of-work (PoW) blockchains: they contribute their computing power to solve cryptographic hashing problems associated with blocks.

Clarifications on PoW should be bring in the current CSWD:

- Contrary to what is stated, miners do not tend to operate anonymously. They increasingly operate within mining pools.
- "*When a group of miners controls more than half the total computational power used to create VC units, it is in a position to interfere with transactions*": therefore it should be explained that a high level of decentralisation ensures cyber-resilience and the integrity of the ledger.

However, on proof-of-stake (PoS) blockchains, there are no miners. Validators do not contribute their computing power: they are randomly selected to validate blocks based on the amount of crypto-assets that they lock in ("stake") in the blockchain. The more they stake, the more likely than can be selected. PoW and PoS mechanisms are not the only consensus algorithms but the most common ones.

Under both mechanisms, block validators are usually rewarded by crypto-assets automatically created according to the protocol rules (bitcoins on Bitcoin, ethers on Ethereum) and transaction fees paid by users (gas on Ethereum).

Adan's recommendations for the SNRA review:

- Not only refer to miners but validators.
- Provide relevant clarifications.

Initial coin offerors

Coin offerors are now defined in the MiCA proposal as issuers of crypto-assets (defined in article 2.6).

Adan's recommendations for the SNRA review: The new vocabulary introduced by MiCA and the pilot regime proposals should be used in the CSWD to replace undetermined ones (see above).

The VC/VA market in the EU (p99)

Adan's recommendations for the SNRA review: Figures in the table should be updated. Please find below some relevant data gathered by the Adan:

Metrics	Figures
Total VC wallets worldwide	According to Cambridge Center for Alternative Finance (CCAF), 101 million unique crypto-asset users across **191 million accounts** opened at service providers in Q3 2020. This does not include self-hosted wallets.
VC wallets in the EU	
VC users worldwide	According to CCAF, **101 million unique crypto-asset users** across 191 million accounts opened at service providers in Q3 2020. This does not include self-hosted wallets.
VC users in the EU	According to CCAF, **63 %** of users in Europe are retail investors while **30 %** are business and institutional ones.
VC miners worldwide	In 2020 Genesis Mining surveyed 750 US bitcoins owners: **293 respondents (39.1 %) are bitcoin miners**. Chainalysis identified 11 mining pools in bitcoins (89 % of hashers surveyed by the CCAF indicated that they mine it).
VC miners in the EU	According to CCAF, **25 % of respondents to their Mining Survey were from Europe**. According to Statista, Europe hosts 25 % Bitcoin mining pools and 49 % Ethereum mining pools.
VC software wallet providers worldwide	
VC custodians worldwide	Digital Assets Custody reports a list of **74 custodians** (excluding tech providers).
VC custodians in the EU	In the Digital Assets Custody list, **46 custodians are European**.
Exchange platforms worldwide	433 (whatever the platform is: centralised, decentralised, OTC). Kaiko collects data on 89 centralised exchanges but has identified **more than 100**.
Exchange platforms in the EU	It has to be noted that some exchange platforms operate in several countries but depending on the users' nationality they are

	not allowed to trade all pairs (e.g on some exchanges EU citizens cannot trade BTC against USD).
Cashpoint machines worldwide	Fundera reports that there are **5,041 bitcoin ATMs** around the world.
Cashpoint machines in the EU	It should be noted that there is **none in France**.
Daily VC transactions	According to Kaiko, on average on the January 2018-January 2021 period: ● **250,137 daily BTC-USD trades** ● **82,876 daily BTC-EUR trades** Based on Kaiko's data on centralised exchanges
Merchants accepting bitcoins	Fundera finds that **15,174 businesses worldwide accept bitcoin**. An online map is available on coinmap.org
Market capitalisation of VCs	**$1,606,328,362,674** on 22 February 2021.

3. Description of the risk scenario - Adan's comments

Both Money laundering and Terrorist financing paragraphs state that transactions in crypto-assets are anonymous. However **transactions on crypto-assets are not anonymous.** Even on so-called privacy coins - which are a minority of crypto-assets - transactions are not fully anonymous. **Transactions on most crypto-assets are pseudonymous and easily traceable thanks to a combination of both on-chain and off-chain information available.**

Crypto-assets are represented on the blockchain as a balance allocated to a public key (or address). It is therefore literally a record of balances and all the transactions affecting these balances. As the blockchain is public, this information can be collected and processed by any interested party.

Each transaction processed by public blockchains usually contains the following information:

- Sender's address;
- Recipient address;
- The corresponding type of transaction: transfer, deployment of a smart contract, interaction with a smart contract, creation of a new crypto-asset, etc. ;
- The amount of transaction fees paid by the initiator of the transaction;
- The execution date of the transaction;

- The number of the block in which the transaction was validated;
- For transactions involving a transfer of value: the crypto-asset concerned and the amount processed.

It is possible to establish the transaction history of each blockchain address by browsing all the transactions that affected the address. In addition, on programmable blockchains, addresses can reveal additional information when they correspond to smart contracts. Even when clusters of addresses carry out a multitude of transactions between them (with sometimes the aim of masking the real destination of the funds exchanged), transactional analysis tools (like Chainalysis, Elliptic, e-NIGMA, Scorechain, etc.) are able to identify multiple transaction patterns and assess their level of risk.

When they are not sufficient, such on-chain information can be crossed with complementary "off-chain" information (available outside the blockchain) to identify the owners of certain key addresses, as for instance: exchange platforms, brokers and other companies using the blockchain; well-known personalities who have disclosed their addresses; products using crypto-assets; addresses that store crypto-assets which have been stolen; addresses used on illicit sales sites (including the dark web); services used to mask the origin or destination of transactions, etc. This information may be collected on the open web, the dark web or directly from law enforcement agencies when they collaborate with actors.

Therefore the common misconception that transactions on crypto-assets are anonymous must no longer be promoted.

Adan's recommendations for the SNRA review:

- Instead of "anonymous", usually refer to "pseudonymous" transactions in crypto-assets.
- Explain how transactions in crypto-assets are traceable.
- Provide examples to illustrate that traceability of crypto-assets already proved useful to fight against illicit transactions (e.g NetWalker operations). Many cases are listed and described in dedicated Crypto Crime reports such as the ones of: Chainalysis, CipherTrace, Scorechain, etc.).

Those recommendations are relevant on other occasions in the CSWD.

4. Threat - Adan's comments

Adan's recommendation for the SNRA review: The new vocabulary introduced by MiCA and the pilot regime proposals should be used in the CSWD to replace undetermined ones (see above).

Introduction

"*VC/VA-related activity represents a growing money laundering/terrorist financing threat*": This affirmation is not substantiated by any data within the related paragraph. On the contrary, **recent analyses prove 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[6] which is corroborated by Ciphertrace's research (57 %)[7]. **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[8]. 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.

---

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

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

[8] 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/

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.

"*Financial intelligence units (FIUs) across the FATF global network have seen a rise in the number of suspicious transaction reports that relate to VC/VAs*" must be recontextualized. At the time of this SNRA, this increase could be explained as **such reports were not mandatory** before the AMLD5 has covered some crypto-asset activities. In 2020, 3 % of KYC checks led to the closure or refusal to open an account for non-FATF-incorporated countries, 8 % for FATF-incorporated entities[9].

"*anonymity-enhanced VAs, which offer greater privacy, faster transaction times, lower transaction fees and less price volatility*" is a fallacious assumption. Please refer to our comments on *3. Description of the risk scenario*.

"Exchangers can now offer VC/VA to VC/VA transactions that obfuscate the transaction trail and decentralised mixers have also been used": Clarifications should be provided regarding the term "exchanger". If referring to exchange platforms, stating that they offer VC/VA to VC/VA transactions that obfuscate the transaction trail and use decentralised mixers is wrong. As aforementioned, **97 % of all crypto-asset service providers perform KYC checks**.

Adan's recommendation for the SNRA review: Update the analysis on the current state and past evolution of crypto-asset-related crime based on quantitative evidence and examples of how blockchain technologies help in the fight against terrorism.

Terrorist financing (p101)

Adan would like to outline the lack of evidence and precise explanations in this paragraph - no data, "*A limited, but growing number of cases related to VCs have been reported*" and various conditional assumptions ("*may have an interest*", "*may be using*"). However, surprisingly, this allows to conclude "*Consequently, the terrorist financing threat related to virtual currencies is considered significant (level 3)*". **Several analyses - presented above - provide concrete information to challenge this conclusion.**

[9] Ibid

Adan's recommendations for the SNRA review: Avoid leaps of logic by basing the ML/FT risk analysis on the current state and past evolution of crypto-asset-related crime based on quantitative evidence and examples of how blockchain technologies help in the fight against terrorism.

Money laundering (p101)

Similarly, Adan would like to emphasize the lack of evidence and precise explanations in this paragraph - no data, various conditional assumptions ("*may use*", "*may acquire*") - associated with the wrong statement that "*VCs/VAs allow such groups to access cash anonymously and hide the transaction trail*" is a wrong affirmation (please refer to *3. Description of the risk scenario* for our comments).

Despite this limited argumentation, the conclusion states that "*Consequently, the level of money laundering threat related to virtual currencies is considered significant (level 3)*". **Several analyses - presented above - provide concrete information to question it**. The last paragraph in page 103 of the SNRA even signals that "*there is little evidence of VCs being misused for money laundering*".

Adan's recommendations for the SNRA review: Avoid leaps of logic by basing the ML/FT risk analysis on the current state and past evolution of crypto-asset-related crime based on quantitative evidence and examples of how blockchain technologies help in the fight against money laundering.

5. Vulnerability - Adan's comments

Adan's recommendation for the SNRA review: The new vocabulary introduced by MiCA and the pilot regime proposals should be used in the CSWD to replace undetermined ones (see above).

Terrorist financing (p101)

a) risk exposure

"*When used anonymously, VCs make it possible to conduct transactions speedily without having to disclose the identity of the 'owner'*": We welcome this sentence as, while many others in the CSWD wrongly stated that all crypto-assets allow anonymity, this one better reflects the crypto-asset market reality. Indeed not all crypto-assets allow anonymous transactions to be executed: the creation of

so-called "enhanced-anonymity crypto-assets" (AEC) was motivated by "*the growing awareness traceability of transactions on public blockchains and de-anonymization technologies*"[10].

While they already represent a very marginal share of all existing crypto-assets, several trends allow to predict that the use of AECs will either decline or be appropriately managed: blockchain analytical tools are improving in dealing with AECs, exchanges tend to de-list spontaneously those who pose the most significant risk (like the Singapore branch of OKEx, Upbit, Shapeshift, etc.) and evolution in regulatory frameworks worldwide (coming implementation of travel rule, coming AMLD review, etc.).

Adan's recommendation for the SNRA review:

- Distinguish enhanced-anonymity crypto-assets from other crypto-assets.
- Assume that crypto-assets have a pseudonymous (not anonymous) nature.

b) risk awareness

"*competent authorities and financial intelligence units have noted in their contacts with the sector that the level of awareness of terrorist financing risk is still rather low, although the sector is calling for the adoption of an appropriate AML/CFT legal framework.*": The French and European industry of crypto-assets were in favour of the implementation of an adapted AML/CFT framework precisely because they knew about such risks and needed a regulation to guarantee their awareness and their credibility then distinguish themselves - as trustable and serious actors - from malefactors.

"*VAs are among the most important emerging risks in almost all sectors (...)*": Please refer to our comments above (see *4. Threat*).

"(...)

- *a lack of knowledge and understanding, which prevents firms and competent authorities from carrying out a proper impact assessment;*
- *gaps or ambiguities in the application of existing regulation';*
- *potential exposure of financial and credit institutions to increased risks of money laundering and terrorist financing related to VCs/VAs where they act as intermediaries or exchange platforms between VCs/VAs and fiat currencies (in the absence of a proper risk assessment); and*

[10] Ciphertrace, *Q3 2019 Cryptocurrency Anti-Money Laundering Report*: https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/

- *in the investment sector, online processing of transactions with only limited customer identification and verification checks."*

Points 2 and 4 from this list are no longer valid. A dedicated regulatory framework for crypto-asset service providers has been built in France which requires that they comply with the EU AMLD5 to be authorised to operate, FATF standards are being implemented progressively (coming travel rule) and the AMLD review will soon cover markets in crypto-assets. Furthermore as detailed above, 97 % crypto-asset service providers do conduct KYC checks as of today.

Point 1 is about to evolve as authorities and financial/banking institutions are more and more knowledgeable about crypto-assets and the true level of ML/FT risks. In France, the French banking supervisor (ACPR) created an *ad hoc* working group gathering professionals from the crypto and traditional industries to help answer pending questions about ML/FT risks raised by crypto-assets, the level of compliance of crypto-asset actors with the EU AMLD, arrangements set by them to fulfill their requirements, etc. Adan is also deeply committed in pedagogic efforts about markets, risks and opportunities of crypto-assets.

Therefore financial and credit institutions have little exposure to ML/FT risks (point 3). First, crypto-asset service providers are managing such risks. Second, very few traditional actors in the EU (none in France) act as intermediaries or exchange platforms: for now they barely refuse any type of relations with the crypto-asset sector. In the EU, this starts when new firms wish to open a banking account: a survey conducted by the Adan revealed that 68 % of participants were denied an account and/or their bank closed it afterwards[11]. More relevant figures on the difficulties that the industry experiences with the banking industry are available in the Adan's survey report.

"*The sector is not well organised yet*": **In 2021, the crypto-asset industry in the EU and in the United States of America is very well organised** as regulation has paved the way to a great structuration and sanitization of markets (the French PACTE Law, the US statements and actions, the EU MiCA and regime pilot proposals).

Adan's recommendation for the SNRA review: Provide the appropriate updates.

[11] Adan, *État des relations entre le secteur bancaire et financier et l'industrie des actifs numériques*, October 2020: https://adan.eu/en/actualite/compte-rendu-relations-secteur-banque-finance-industrie-crypto-blockchain-france ; https://adan.eu/rapport/relations-secteur-bancaire-financier-industrie-actifs-numeriques

c) legal framework and checks

"There might be gaps to be filled as regards various activities of VA service providers that are not covered by the EU framework:

- *custodian wallet providers that do not safeguard keys on behalf of their customers, but merely provide them with tools to safeguard their cryptocurrencies themselves, like hardware wallet providers and software wallet providers"*
- *exchanges from VCs or VAs to other VCs or VAs"*

The first type of actors should remain out of the scope of regulation. First, they never hold crypto-assets which never pass through such providers. Second, they cannot get any information from holders of crypto-assets. Third, they do not control crypto-assets of their clients, as they safeguard them by themselves.

The second type of actors could be covered by the EU framework but this one should be adapted to the reduced risks that they bear and the technological specificities of full on-chain transactions.

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

[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]. Other examples have been provided above.

Adan's recommendation for the SNRA review: Assume the different level of ML/FT risks within all crypto-asset activities, and explain why pure crypto transactions raise lower risks and which opportunities they offer for the fight against ML/FT.

Conclusion box (p103)

Adan's recommendation for the SNRA review: Update the content of this box based on the aforementioned remarks.

Money laundering (p103)

Introduction

"there is little evidence of VCs being misused for money laundering": Adan welcomes this adequate analysis which should be also restored in part *4. Threat* of the CSWD.

Adan's recommendation for the SNRA review: Harmonise ML/FT risk analysis in the whole document.

a) risk exposure

"As mentioned above, when used anonymously, VCs make it possible to conduct transactions speedily and without having to disclose the identity of the 'owner'": Please refer to our explanations in *5. Vulnerability*.

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

It should be noted that transactions in AECs are not specially faster than others.

"*The new AMLD5 rules will address this by extending the AML/CFT framework to 'providers engaged in exchange services between virtual currencies and fiat currencies'*": This led to the drastic drop of ML/FT crimes using this vector.

"*However, the delivery channels remain decentralised, which increases the risk exposure (in particular, cashpoint machines make it possible to withdraw or convert VCs)*": Cashpoint machines are covered by AMLD5. In December 2020, several Shitcoins ATMs were seized in France[14].

Adan's recommendation for the SNRA review:

- Distinguish enhanced-anonymity crypto-assets from other crypto-assets.
- Assume that crypto-assets have a pseudonymous (not anonymous) nature.
- Update the content when necessary.

b) risk awareness

"*The sector is in more and more need of a legal framework in which VCs are subject to AML/CFT requirements*": This should be updated regarding regulatory evolutions.

Adan's recommendation for the SNRA review: Update the content according to the 2021 landscape.

Conclusion box (p104)

Adan's recommendation for the SNRA review: Update the content of this box based on the aforementioned remarks.

Mitigating measures (p104)

"In the context of the supranational risk assessment report, the Commission will continue to monitor the risks posed by (...) the use of VCs/VAs for the purchase of high-value goods": Adan would appreciate further details on the special ML/FT risks raised by this type of operations.

[14] France Info, *Justice : des distributeurs de bitcoins saisis, une enquête préliminaire est ouverte pour blanchiment aggravé*, 20 December 2020: https://translate.google.com/translate?sl=fr&tl=en&u=https://www.francetvinfo.fr/economie/bitcoin/justice-des-distributeurs-de-bitcoins-saisis-une-enquete-preliminaire-est-ouverte-pour-blanchiment-aggrave_4227417.html (translated version)

Adan's recommendation for the SNRA review: Adan would like to suggest the following additional measure: **the European Commission should guarantee the consistent and harmonised implementation of the coming revised AML framework across all EU Members states**.

~

Adan is available for any question and further discussions related to this document.