ADAN

L'ASSOCIATION POUR LE DÉVELOPPEMENT DES ACTIFS NUMÉRIQUES

ADAN's position paper

Towards a suitable AML/CFT regime for markets in crypto-assets

Consultation on EC's action plan for a comprehensive Union policy on preventing money laundering and terrorist financing

Paris, 29 july 2020

Introduction

Adan is a 1901 non-profit organisation whose mission is to bring together and animate the digital assets industry in France and in Europe. With 40+ corporate members, including Ark Ecosystem, Blockchain Partner, Coinhouse, Coinhouse Custody Services, ConsenSys France, iExec, Kaiko, Ledger, LGO Markets, Nomadic Labs and Woorton, Adan is the most important French organization in the digital assets field.

Adan is thankful to the European Commission for allowing the expression of industry players in this open consultation. The Association's objectives are to help create the more favourable environment in the EU for the development of a crypto-asset industry competitive with other regions of the world.

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

Towards a suitable AML/CFT regime for markets in crypto-assets

Context

For the purpose of this paper, "crypto-assets" / "crypto activities" / "crypto actors" refer to "virtual assets" / "virtual asset services" / "virtual asset service providers" under the FATF's terminology.

Enforcing the application of the existing AML/CFT framework to the crypto-asset industry is not a recent question. For years, both EU institutions and global bodies (FATF, FSB, etc.) have been taking this stance. Even at a local level, national authorities found the temptation to follow this trend: for example, France implemented a dedicated regime for crypto-asset service providers through which actors must comply with the full AML/CFT package to be registered and/or licensed.

If an 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, 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.

Through this paper, Adan wishes to explain which misconceptions about crypto-assets have encouraged most authorities to consider the application of "raw" AML/CFT analytical framework and regulatory requirements, and why this is not the right solution. Instead, **Adan highlights the necessity to tailor current AML/CFT schemes in order to design an adapted and proportionate AML/CFT regime for markets in crypto-assets**. It is of utmost importance to understand that only this approach can ensure an efficient combat against ML/FT threats while preserving both the potential for innovation and competition of the EU crypto ecosystem.

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 first reaction of regulators has been to apply the same analyses as for the financial sector. Notably, transfers of crypto-assets are often equated to transfers of money.

However, financial actors and flows are very different from crypto-assets ones:

- **The foundation of the crypto-asset ecosystem lays in blockchains**, which present innovative and singular technological characteristics compared to the tools traditionally used in the financial world, in terms of: decentralisation, transparency, immutability, auditability, smart contracts, IT resilience, governance, etc. **Such features make crypto-asset transactions executed on blockchains very different at their core**.

- **The profile of a typical "crypto user" strongly differs from bank clients and financial investors**:
  - The clientele of crypto players is specific, mostly knowledgeable and experienced in terms of

blockchain and crypto-assets.
- Business relationships are almost entirely remote.
- Retail crypto clients are more active in terms of transaction frequency, but transaction amounts are much lower.
- Clients can settle their transactions in both legal money or other crypto-assets.
- They can hold their crypto-assets on their own wallet or store their assets with a third party.

- **Crypto entities share specific characteristics that distinguish them from financial companies:**
  - Crypto players use blockchain technology at the core of their business processes.
  - As a nascent industry, the majority of crypto actors are still small, with very little interconnection between them and narrow geographical expansion (in part due to regulatory uncertainties around the world).
  - Their staff is smaller, self-trained by nature and often multi-skilled.
  - Their financial efforts are massively focused on their development and consolidation in an industry under construction and under strong competitive pressure, so it is very difficult for them to tie up resources or redistribute them (shareholdings, profit-sharing, dividends, bonuses, etc.).
  - According to the five criteria established by the Basel Committee, they are not systemic entities whose failure would have repercussions on the rest of the financial system.

- **Indeed markets in crypto-assets are not to be equated to financial ones**:
  - When referring to FATF's virtual assets, **crypto-assets are not considered as financial instruments**. This is a very wide and dynamic range of assets with multiple use cases, given the quickly evolving crypto-asset landscape and the speed of innovation in this sector.
  - Exchange volumes are still very small compared to those of traditional markets (market and payment). At the current stage of maturity of blockchain technologies, decentralized networks cannot process significant transaction flows.
  - At the end of the day, **ML/FT risks raised by crypto-assets are of smaller importance that those posed by the traditional financial activities.**

Thus, **applying blindly the regulatory requirements that were designed for financial entities omits all these fundamental differences**.

Such misconceptions nurture stereotypes about ML/FT risks raised by crypto activities

Temptation to model the AML/CFT framework for crypto actors on the one for financial actors has been fed with confusion and many misunderstandings. **Some long-standing stereotypes about "oversized" ML/FT risks raised by crypto-assets must be challenged**. If ML/FT risks exist in the crypto universe, the true level of such risks is often overstated.

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

This deeply rooted view comes from 2011, at the very beginning of the crypto world when bitcoin still was the first and single "cryptocurrency". Bitcoin gained this "ML/FT label" when it became the only means of payment accepted on the Silk Road website that allowed for buying/selling anything on the darknet. 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 allow 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 2020 State of Crime Report which reveals that illicit transactions is "a small share of all cryptocurrency activity at just 1.1%" and that the overwhelming majority of such transactions (90%+) consists in payments related to scams, 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[1] and FATF[2], 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 BC-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[3].

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**

[1] https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf

[2] FATF guidelines, point 48.

[3] https://adan.eu/rapports

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[4].

Stereotypes about ML/FT risks raised by crypto activities have very detrimental side effects for the development of the crypto industry

The combination of the commingling of financial markets and crypto markets on the one hand, and the misunderstanding of real ML/FT risks posed by crypto-assets on the other hand, led regulators and supervisors to apply the same analyses on crypto actors as for the financial sector.

Such an approach implies harmful direct and indirect consequences.

Direct consequences

While crypto-assets do require an appropriate level of ML/FT regulation, **applying existing rules to them is quite inefficient** as this prompts to:

- **Ill-estimate the risks of crypto-assets in general.** As an example, traditional money transfers require the collection and transmission of information that are impossible to replicate 1-to-1 on the crypto-assets transactions. This is notably due to the bearer nature of those assets, that by definition can be transferred between individuals without supervision. When applying traditional ML/FT lenses to those transactions, one could conclude that all those transactions are high risk. However, applying an indistinct "high risk" label to all the transactions has the detrimental effect of making the whole risk analysis useless.

- **Leave the areas where risks could have been identified - as they were not captured by the traditional financial analysis schemes - out of the scope of the supervision**. This includes activities specific to the sector, that would be ill-covered or not covered at all, and more broadly an incomplete use of information available - e.g. transaction history.

- **Fail to prevent illegal activities**. While the general public and companies will reduce their activities on crypto-assets as a side effect of a stringent regulation that nullifies the interests of crypto-assets, criminals - that do not respect laws anyways - will use the crypto-assets quite freely because the regulator will be looking somewhere else.

- At the very end, **prevent innovation** by placing the burden of the costs associated with an inefficient framework on companies with nascent activity.

Indirect consequences on the relations between the crypto industry and the financial system

Aforementioned direct consequences create a deleterious environment of distrust between financial and crypto industries : **today, the most significant obstacle to the development of the crypto-assets sector is the difficult relations between the actors and banking institutions.**

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

Longstanding deadlocks between the established players in the banking system and the new entrants materialise at different levels:

- **At the level of companies operating an activity related to crypto-assets and blockchain**.

When a company wishes to open a bank account with an institution, due to aforementioned stereotypes, words like "blockchain", "cryptocurrencies" or even "crypto-assets" in the applicant's name or corporate purpose are systematically prohibitive for their interlocutor who then refuses to open an account (both payment and escrow). If the account is finally opened, the slightest transaction that leads the bank to suspect that the company is buying, selling or acting as an intermediary in the purchase or sale of crypto-assets leads to a warning or closure of the bank account without prior notice. This makes it all the more difficult for businesses to find another bank, often within a very short period of time and with all the suspicions that a previous closure would place a burden on the business at the start of the new banking relationship.

In practice, this leads to a situation where actors pass through an account established with a foreign bank. This causes many practical problems: customers have trouble issuing payments or transfers to foreign bank accounts, administrations usually do not allow to enter foreign IBANs, this raises suspicions when entering into relations with partners, etc.

This situation was also very damaging during the COVID19 crisis. Indeed, State-guaranteed loans were *de facto* inaccessible for these "unbanked" entities.

In addition, and for similar reasons, crypto/blockchain companies are faced with the refusal of financial players when they wish to access their payment services. This refusal to deal with companies using crypto-assets is sometimes written in the Terms of Sales of the companies (e.g. Qonto[5]) and send warnings to their clients when flows are going to or coming from crypto-assets-related accounts (e.g. the account of an exchange).

Last but not least, some crypto/blockchain entrepreneurs have seen their personal accounts closed for the entire household.

- **At the customer level**.

Users of crypto/blockchain products and services are also affected and are partially or entirely prevented from using them. As an example, when a client wants to transfer funds to a crypto-asset exchange platform, it very regularly happens that his bank simply blocks the payment or asks the customer to sign a release whose content intends to discourage the operation by providing partial information, exaggerating the risks encountered. When he receives funds from a platform, the consequences are even more dire as the account to which they are credited is often closed by the bank, as of the first transaction and without giving the client the opportunity to transmit any information relating to the origin of these funds.

In conclusion, both in the normal conduct of their business and in a context of economic crisis, the banking sector's opposition in principle to the emergence of new crypto/blockchain players is jeopardizing this young and therefore fragile ecosystem, which must rely on established players to prosper. **This situation is very detrimental for the competitiveness of the EU crypto ecosystem**, even

[5] https://support.qonto.eu/hc/fr/articles/115000510385--Quelles-entreprises-peuvent-ouvrir-un-compte-courant-chez-Qonto-

more in a current context when American and Asian governments financially and regulatory support the development of their actors.

Indirect consequences on the competitiveness of the EU crypto ecosystem

Aside from a lack of support from financial institutions to allow the novel crypto-assets industry to develop, the current inadequate AML/CFT regulatory approach harms the competitiveness of crypto companies within the EU.

Undoubtedly the cost of implementing an extensive LCB-FT policy is likely to nip the emergence of a strong EU crypto-asset industry in the bud. As a sector that is already underfunded in Europe compared to the USA or Asia, it would exacerbate their financial difficulties and prevent them from hiring and investing: they simply do not have access to the same resources as incumbents.

Faced with the burden of the cost associated with this inadapted ML-FT regulation, market players would not be able to compete with the very low commissions applied by the main foreign trading platforms (whose operational and compliance costs would be lower). This is critical as the assets are quoted worldwide and the foreign platforms accept EU-based clients without limitations.

Finally, any additional AML/CFT procedures involve a certain amount of work in the customer's onboarding process, a critical stage for which each additional step is an opportunity for the customer to give up the process.

Conclusion: AML/CFT risk analysis and prevention mechanisms should be adapted to crypto activities

Based on previous findings, the AML/CFT regime for crypto-assets should be designed through three major pillars:

- **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. **Efficient requirements - meaning that they meet financial security challenges - are antagonistic with overloaded obligations**. This is actually consistent with recital 2 of the AMLD5 stating that "It is important to note that the measures taken should be proportionate to the risks".

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. Indeed the following (but non-exhaustive) difficulties and incompatibilities can already be outlined:

- ❏ Risk mapping based on criteria that are not representative of crypto-asset markets: this means that customer due diligence measures that are *complementary* in the traditional financial world are systematic in the crypto world.

❏ The identification of the geographical origin of a crypto-asset is technically impossible.
❏ Constant due diligence measures towards traditional investors are not adapted to crypto-crypto trading.
❏ Regarding asset unfreezing, unlike banks, crypto actors cannot check whether clients actually have to meet a compelling expense (such as paying their rent).
❏ Regarding asset freezing, it is technically impossible to stop the execution of a transaction once it has been validated on the blockchain.

- **Implement ad hoc AML/CFT risk analysis and prevention mechanisms for crypto activities**

A dedicated analysis framework for crypto actors should be implemented for a fair estimation of their ML/FT risks.

Indeed 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. Blockchain proved its relevance to help dismantle entire networks of criminals, for example at the time of the Silk Road affair or, more recently, the dismantling of a network of 300 paedophiles located in 38 countries[6].

For instance, additional information provided through KYT tools should be integrated to allow for a more refined risk analysis that helps identify the transactions that have a high risk of being associated with a ML/FT activity (however KYT must be supplemented with other tools). In addition, removing inadapted or inefficient arrangements would prevent from ill-estimating ML/FT risks raised by crypto activities.

Blockchain could also support authorities in the exercise of their supervisory role. For example, they could issue ID certifications allowing them to carry out unique AML/CFT procedures whose validity would be recognised by everyone on the blockchain. One prerequisite is that authorities start developing specific expertise on crypto-assets. **With this in mind, having a new EU AML/CFT body with a specific team for crypto topics would be a compelling solution. Another solution would be to create a dedicated regulatory body for the supervision of the crypto-asset industry.**

- **Assess competitiveness impacts for the industry when regulating**

The risk emerging from inadapted risk analysis schemes and legal requirements is to jeopardise the emergence of EU crypto-asset champions. Though even more in the current difficult economic context, attractiveness of the EU crypto industry must be carefully kept in mind in regulatory debates.

Therefore, as the AML/CFT regime for markets in crypto-assets is being built, **efforts should be made to rationalise the compliance costs that this nascent industry should bear**.

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

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

Contacts

Simon Polrot, President: simon.polrot@adan.eu
Faustine Fleuret, Head of Strategy and Institutional relations: faustine.fleuret@adan.eu

Website: www.adan.eu

Twitter: @adan_asso

Media Kit: https://adan.link/presskit