ACPR-AMF Fintech Forum

Work report of the working group on the application of AML-CFT rules to the cryptoasset sector

Sep 2020, 29th

This work report retraces the deliberations of the working group bringing together the *Autorité de Contrôle Prudentiel et de Résolution* (APCR, the French prudential supervision and resolution authority), the *Autorité des Marchés Financiers* (AMF, the French financial markets authority), the *Direction Générale du Trésor* (the French Treasury General Directorate), Tracfin (the French National Financial Intelligence Unit) and the stakeholders of the both the cryptoasset sector and financial institutions[1]. This document shall not engage the responsibility of the ACPR or the AMF.

Table of contents

1 Summary ... 3

2 Introduction ... 5

3 Reminder on the AML-CFT framework applicable to cryptoasset-related activities ... 7

3.1 The work of the FATF ... 7

3.2 The French legal framework ... 8

3.2.1 The DASP status (*PSAN*) ... 8

3.2.2 Initial coin offerings (ICO) ... 8

3.3 The main money laundering and terrorism financing risks posed by cryptoasset activities ... 9

3.3.1 Money laundering ... 9

3.3.2 Terrorism financing ... 10

3.3.3 Characteristics of ML-TF and practices conducive to ML-FT risks ... 10

4 Inventory of current practices ... 11

4.1 Assessing exposure to ML-TF risks ... 11

4.2 Identification and knowledge of the customer base ... 12

4.2.1 Identification and identity verification when entering into a business relationship ... 12

Authentication of the customer during a transaction ... 12

4.2.2 Customer knowledge and transactional analysis ... 13

4.3 Due diligence ... 14

4.3.1 Split transactions and multiple public addresses ... 14

[1] See annexed composition of the working group.

4.3.2 Technologies facilitating anonymity on the internet 14
4.3.3 Unhosted wallets 15
4.3.4 Technologies enhancing the anonymity of cryptoasset holders 15
4.3.5 Blockchain and geographical origin and destination of funds and cryptoassets 16
4.3.6 Blockchain and asset freezing 16
4.4 Implementation of the travel rule 17
5 Identified technological leads 18
5.1 Transactional analysis tools for blockchains 18
5.1.1 Brief operational description 18
5.1.2 Issues identified by the working group 19
5.2 Communication standardisation initiatives 20
5.2.1 The industry has taken up the subject 20
5.2.2 Challenges and opportunities in the implementation of the travel rule 21
6 Annexes 25
6.1 Glossary 25
6.2 Documentary references 27
6.3 Composition of the working group on the application of AML-CFT rules to the cryptoasset industry 28

1 Summary

Within the framework of the ACPR-AMF Fintech Forum, **a working group** has been created with market players and the relevant public authorities **to study the application of the rules on the fight against money laundering and terrorist financing (AML-CFT) to the cryptoasset sector**.

The aim of this working group was twofold: on the one hand, **to raise awareness in a recently regulated industry** (French PACTE law of 2019, extension of the FATF Recommendations to cryptoassets in 2018 and 2019), and on the other hand, **to make an initial inventory of the AML-CFT practices** of the stakeholders as well as the specificities and prospects opened up in this area by the exploitation of blockchain technologies.

This report reflects the work of this group, carried out between late November 2019 and early July 2020.

This shows that **the most experienced French players in the cryptoasset sector have already been able, to a large extent, to adapt the general AML-CFT principles to the technical and operational context of their activity** (entry into business relations and remote operations, identification mode for wallets on the blockchain disconnected from the notion of client, *etc*.)

Blockchain technologies generally allow transactions to be traced, with the exception of products or transaction modes specifically designed to enhance anonymity. Using this traceability feature, **transactional analysis tools** have been developed by specialised service providers, using network analysis techniques and studying a long-term history of blockchain transactions in order to characterise potentially suspicious behaviour and wallets. **Some digital asset service providers (DASPs, PSAN in French) use these tools, supplemented by their knowledge bases,** on a daily basis **to monitor their transactions and control their money laundering and terrorism financing risks (ML-TF)**.

These tools, which are inherent to the ecosystem of public blockchains, **usefully strengthen customer knowledge and the investigations carried out on transactions**. Even if their recent development requires improvements in order to address the few limitations (cost, scope of cryptoassets covered) identified in the report, **they nevertheless represent a key focus for the prevention of ML-TF**. Moreover, **ensuring a good grasp of these tools, as well as an in-depth understanding of how they operate** is essential both for the stakeholders in the industry, in terms of implementation of their risk policy, and for the authorities, as regards their supervisory role.

The application of **electronic funds transfer transparency (*travel rule*)** to the transfer of virtual assets, however, remains a major challenge for providers of services linked to virtual assets throughout the world. The aim is to establish the minimum conditions required for both the fast and secure communication of information and trust between stakeholders. The **main standardisation initiatives underway at a global level** (message standardisation, communication protocols) were examined by the working group, which also endeavoured to identify and discuss the **complementary actions** to be undertaken (register of service providers, security, data storage and retention, etc.) to achieve a satisfactory implementation of the travel rule from a technical point of view.

This analysis showed the **necessity of mobilising the French ecosystem** and integrating it into the transnational reflections that are underway, otherwise compliance with the transparency rule will only be costly and flawed for each stakeholder. In this respect, **the European legislative work on cryptoassets** could be an opportunity for the French financial centre to become part of a **European momentum** in order to support the regulatory aspect by **developing** the corresponding **technical solutions**.

2 Introduction

At the request of the G20, in October 2018 and June 2019, the Financial Action Task Force (FATF) amended its Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Recommendations to include certain players in the cryptoasset sector, referred to as Virtual Asset Service Providers (*VASP*)[2]. These service providers must be licensed or registered, subject to supervision by the authorities, and are required to set up effective due diligence systems using a risk-based approach (customer knowledge, transaction monitoring, etc.) and suspicious transaction reporting.

In June 2019, the FATF also published guidance detailing and clarifying the implementation of its recommendations on *virtual assets*[3] and virtual asset service providers.

The implementation of and follow-up on the FATF Recommendations on virtual assets were evaluated twelve months after their adoption[4]. In addition, a Contact group under the aegis of the FATF, bringing together several AML-CFT auditors, monitors developments in the cryptoasset sector, the implementation of its obligations as regards AML-CFT and the development of technical solutions aimed at strengthening the sector's compliance with FATF recommendations.

At the same time, the French PACTE Law of 22 May 2019 created the status of service provider for digital assets (*DASP*, PSAN in French). Providers offering virtual asset safekeeping services for third parties or buying and selling virtual assets in legal tender must be registered with the AMF, subject to the ACPR's approval. Registration as a DASP presupposes the implementation of an organisation, of procedures and an internal control system that is able to ensure compliance with the requirements as regards AML-CFT[5]. The definition of DASP activities and their registration procedures have been specified by way of Orders[6], as well as through the General Regulations of the AMF[7] and an Instruction published by the same Authority[8].

Against the background of the ongoing registration of players in the cryptoasset sector, a market working group was set up at the end of 2019, under the aegis of the Fintech ACPR-AMF Forum, bringing together, *inter alia*, the supervisory authorities and representative players in the cryptoasset sector in France.

---

[2] See [1] of the glossary.
[3] See [2] of the glossary.
[4] The twelve-month evaluation report following the FATF Recommendations on virtual assets was published in July 2020, see [4] of the documentary references.
[5] Article L. 54-10-3 of the French monetary and financial Code.
[6] Orders No. 2019-1213 of 21 November 2019 and No. 2019-1248 of 28 November 2019.
[7] Title II of Book VII of the General Regulation of the *Autorité des marchés financiers* approved by the Order of 5 December 2019.
[8] Instruction DOC-2019-23 of the *Autorité des marchés financiers* on the regime applicable to virtual asset services providers.

The objectives of this working group were the following:

- Raising awareness, within the industry, of both AML-CFT issues and the recommendations of the FATF;
- Identifying the technical solutions available to the stakeholders in the sector, especially regarding the enforcement of the 16th FATF Recommendation on wire transfers including the respect of customer privacy (as well as the potential locks hindering the development of these solutions);
- Identifying risk factors and the impact of the FATF Recommendations on the industry;
- And, more broadly, fostering discussion, upward reporting and experience feedback from the financial community on the enforcement of the new recommendations to the FATF.

This document compiles the main lessons, analyses and paths identified by the working group.

3 Reminder on the AML-CFT framework applicable to cryptoasset-related activities

3.1 The work of the FATF

The increasing use of cryptoassets for money laundering and terrorist financing purposes in recent years has highlighted the need to subject the cryptoasset sector to the AML-CFT regulations.

Mandated by the G20 for that purpose, the FATF amended its 15th Recommendation in October 2018 to provide for the implementation of its standards to the virtual asset sector and adopted an interpretive note in June 2019 specifying their implementation terms and conditions, especially with regard to the registration and supervision of virtual asset service providers and the transparency of virtual asset transfers. These requirements were also detailed in guidelines published in June 2019.

The FATF Recommendations now provide for virtual asset service providers to be subject to international standards as regards the fight against money laundering and terrorist financing. These service providers must as a minimum be licensed or registered in their country of establishment (or in the country where their activity is located if they are natural persons) and set up an appropriate anti-money laundering mechanism. States must sanction natural or legal persons carrying out activities on virtual assets without prior approval or registration.

In addition, the FATF has extended the scope of transfer transparency (or *travel rule*) to the virtual asset sector. This rule aims to ensure the integrity of the system for transferring virtual assets, in particular by allowing the freezing of assets, and to ensure the transparency and traceability of such transfers.

The 16th FATF Recommendation notably requires the collection and transmission of basic information on the originator and beneficiary for any transfer of virtual assets involving at least one VASP. The transmission of this information must be immediate and secure, but it is not necessary for this information to be directly attached to the transfer of virtual assets, or even for the transmission of the information to be carried out using a blockchain.

The FATF published initial conclusions of the implementation of the travel rule following its June 2020 plenary session. While there is currently no technological solution enabling the implementation of the transparency of virtual asset transfers on a global scale, a technical standard enabling the transmission of information between VASPs has been developed by private sector stakeholders. Several challenges have also been identified, such as the interoperability of the various information transmission systems, the identification of the VASP of the counterparty to a transaction, or the securing of the transmitted information. The FATF will conduct a new review two years after the adoption of its Recommendations on virtual assets.

3.2 The French regulatory framework

3.2.1 The DASP status (*PSAN*)

(i) Mandatory registration

Pursuant to Article L. 54-10-3 of the French Monetary and Financial Code ("CMF"), applicants for registration as a DASP[9] must put in place an organisation, procedures and an internal control mechanism that are appropriate and conducive to ensuring compliance with the provisions relating to the fight against money laundering and terrorist financing and the implementation of asset freezing measures.

AMF Instruction DOC-2019-23 on the regime applicable to providers of digital asset services sets out the list of documents required for this purpose, including the development of a classification of risks and the implementation of an AML-CFT system adapted to this classification. The applicant's AML-CFT system must include internal procedures including customer due diligence, procedures for monitoring customer transactions and a system for implementing asset freezing measures. The applicant is also required to set up an internal control mechanism.

Once the DASPs are registered with the AMF, subject to prior approval by the ACPR, they are subject to permanent control by the ACPR.

(ii) Optional licensing

Some virtual asset-based services, including the exchange of digital assets for other digital assets and the operation of a digital asset trading platform, may be offered by DASPs without mandatory registration[10]. They have the option of applying to the AMF for optional licensing in order to be subject[11] to the AML-CFT[12] and asset freeze regulations.

3.2.2 Initial coin offerings (ICO)

The PACTE Law created an optional visa regime for initial coin offerings (ICO) awarded by the AMF. The latter analysed the applicability of the AML-CFT regulations to initial coin offerers in view of their specific features (subscription in cryptoassets, small structures, occasional customers) and summarised on its website the main obligations of coin offerers[13].

---

[9] For services involving the custody of virtual assets for third parties and the purchase and sale of digital assets in legal tender (see [1] of the glossary).

[10] The description relates to the regulatory framework in force at the time this report was written. Changes may be made to this framework in the near future.

[11] Optional approval also implies compliance with obligations that are not linked to AML-CFT (professional insurance, or own funds, commercial policy, etc.).

[12] Optional licensing for services on virtual assets that are also subject to mandatory registration (Article L. 54-10-5 of the French monetary and financial Code) will not be discussed in the remainder of this report.

[13] Document available online: https://www.amf-france.org/sites/default/files/2020-02/ico_va_obligations_lutte-contre-le-blanchiment_5edirective.pdf

3.3 The main money laundering and terrorism financing risks posed by cryptoasset activities

Various analyses at the national (COLB, Tracfin)[14] and supranational (European Commission, European supervisory authorities) levels confirm that the ML-TF risk with regard to cryptoassets is proven. Under current regulations, the intervention of third parties subject to AML-CFT is limited to the *placement* and/or *layering* phases of the laundering proceeds into cryptoassets, i.e. the conversion between legal tender and cryptoassets[15]. Once the conversion has been carried out, cryptoassets make it possible to transfer funds in an efficient, secure, fast, inexpensive and cross-border manner under cover of relative anonymity or pseudonymity, without the intermediation of a third party subject to AML-CFT.

These features can make cryptoassets attractive for the hidden financial flows inherent in the practice of money laundering or terrorism financing.

While it is possible to observe flows for a selected asset, and thus for a given blockchain, the use of platforms that allow for the conversion from one asset to another without these transactions being recorded in the blockchain contributes to the fragmentation of the holding chain and complicates the work of analysts.

3.3.1 Money laundering

There are two distinct trends in money laundering techniques involving cryptoassets. On the one hand, the latter may be the object, the medium, or the proceeds of the crime; on the other hand, they may be used independently of the original crime, as a simple money laundering instrument.

(i) Criminality specific to cryptoassets

Cybercrime is an area particularly conducive to the use of cryptoassets. Many modus operandi make use of them, either as a tool of the crime or as a product of it. Examples include cryptojacking, ransomware or the hacking of trading platforms.

(ii) Common law crime using cryptoassets

The emergence of new technologies and their democratisation allow criminals to develop new methods for money laundering. For example, drug trafficking and money laundering on the dark web, as well as the buying and selling of illicit products or illegal services such as the sale of weapons, stolen bank details, child pornography, etc., are on the rise.

Apart from the dark web, common law criminals also use cryptoassets for scams and cross-border movements of funds linked to any type of financial or organised crime.

[14] See [6] and [5] of the documentary references

[15] These are the phases of money laundering, see [3] of the glossary.

3.3.2 Terrorism financing

The use of cryptoassets by terrorist groups is also documented. Several organisations have used calls for donations made on social networks, forums or private groups disseminating cryptoasset addresses to which funds are sent to finance their criminal activities.

3.3.3 Characteristics of ML-TF and practices conducive to ML-TF risks

In addition to the characteristics mentioned above, cryptoassets offer the possibility of carrying out transactions without the intervention of a trusted third party or third party subject to AML-CFT regulations. One way of limiting the ML-TF risks is to regulate the entry and exit points of this economy, i.e. the purchase or sale of cryptoassets for legal tender.

The working group's work has shown that such control is necessary to circumscribe the ML-TF risk specific to cryptoassets, but that such control does not make it possible to grasp the full extent of that risk. Indeed, many practices exist that make it possible to circumvent these controls.

One of the main shortcomings of this system is the lack of subjugation of exchanges between cryptoassets to AML-CFT regulations. It is therefore possible for an offender to change one asset for another without having to declare his or her identity, fragmenting the holding chain through the practice of *chain swapping*[16]. Combined with the use of privacy coins, this technique, known as *obfuscation*, makes it impossible to trace funds and identify the user.

The work of the various actors involved in the working group has converged towards the same solution concerning these practices, namely:

- Taking into account cryptoasset exchanges in the AML-CFT regulation.
- The reinforcement of due diligence measures for players subject to these regulations when they are confronted with anonymity-enhanced cryptocurrencies (AECs).

[16] See [9] of the glossary.

4 Assessment of current practices

In December 2019, a questionnaire was sent to the members of the working group as well as other market players in order to gain a better understanding of their business and their exposure to ML-TF risks. The main results are analysed below, following the structure of the questionnaire.

4.1 Assessing exposure to ML-TF risks

The main risk criteria identified by the respondents to assess their risk exposure, with regard to the focuses of risk classification provided for in the regulations[17], are summarised below.

The following are therefore assessed, with a view to identifying the high ML-TF risks associated with a customer:

- The customer's location or his or her residing in a high-risk country, such as those on the FATF or European Commission lists;
- Potentially risky behaviour (such as connections to a virtual private network or "VPN", use of a *Tor*-like[18] browser);
- A poor transactional analysis score of the customer's wallet;
- The total amount of transactions carried out by the customer (abnormally high amount compared to the customer's profile or habits, without economic justification or apparent lawful purpose);
- An abnormally high frequency of transactions in relation to the customer's profile or transaction history;
- The use of means of payment considered to bear risks.

In order to identify the high ML-TF risks associated with a transaction:

- Splitting transactions ;
- Suspicious links between several customers;
- Identity theft
- A large or abnormally high transaction amount compared with the customer's profile;
- An abnormal frequency of transactions with regard to the customer's profile or transaction history;
- Carrying out of cryptoasset exchange ("crypto-to-crypto") transactions - in particular when the transaction is carried out outside the blockchain - insofar as they do not involve legal tender and make it more difficult to assess the ML-TF risk[19];
- The history of the cryptoassets involved as well as the wallets concerned, where the cryptoassets' holding chain has been altered (for example through the use of *mixers* or *tumblers*[20], or by passing through exchange platforms), assessed in particular through the use of transactional analysis tools.

[17] Article L. 561-4-1 of the French monetary and financial Code (in French).
[18] See [5] of the glossary.
[19] One respondent moderates this criterion on the basis of a thematic report by the association representing the sector (ADAN) on activities between digital assets carried out from France (in French).
[20] See [4] of the glossary.

4.2 Identification and knowledge of the customer base

4.2.1 Identification and identity verification when entering into a business relationship

Firstly, the regulations require the implementation of customer due diligence measures for business relationships, which relate to the identification and verification of the customer's identity, theoretically before entering into a business relationship[21].

In the case of remote entry into a business relationship, specific identity verification measures are provided for[22]. Previous work by the Fintech Forum has also dealt with the issue of the remote identity verification of natural and legal persons[23].

One respondent noted that "in the world of digital assets, remote business relationships are the norm. Consequently, the implementation of additional due diligence measures cannot be systematic". However, since Order No. 2020-115 of 12 February 2020, remote business relationships are no longer considered to present a high risk of money laundering requiring the systematic implementation of additional due diligence measures. The practical implementation of the new regulatory texts has not been the subject of specific work by this working group.

Secondly, the occasional customers of a DASP must be identified and their identity verified, either in the event of suspicion of ML-TF, regardless of the amount of the transaction, or when the customer carries out one or more transactions exceeding the EUR 1,000 threshold provided for in point 5, section II of Article R. 561-10 of the French monetary and financial Code. The issue of the relevance of this threshold -below which customer identification is not mandatory- was the subject of discussions within the working group. In fact, a DASP engaged in activities that are riskier from a ML-TF perspective (such as automated cryptoasset vending machines[24] for example) may find it relevant to identify all its customers, from the first euro, in order to mitigate its risks.

Authentication of the customer during a transaction

Beyond the tools and techniques used in the traditional financial sector, solutions more specific to the blockchain ecosystem could be used to strengthen customer authentication when executing transactions. However, these mechanisms should not be confused with identification in the sense of compliance, and it applies *de facto* to a customer that has been previously validated through the KYC due diligence applied by the DASP.
The solutions mentioned are essentially prospective and could rely, for example, on *self-sovereign identity architectures*[25] or services provided by technical service providers such as regtech. In addition to the direct authentication purpose itself, these solutions would provide additional opportunities to

[21] I of Article L. 561-5 of the French monetary and financial Code (in French).
[22] Article R. 561-5-2 of the French monetary and financial Code (in French).
[23] Refer to the summaries of the Fintech Forum working group on the remote identity verification of natural and legal persons (in French).
[24] For a reminder on the AMF registration requirement for ISPs deploying cryptoasset vending machines in France, see the joint press release issued by ACPR and the AMF on 27 July 2020, https://acpr.banque-france.fr/communique-de-presse/lamf-et-lacpr-rappellent-leurs-obligations- aux-operateurs-de-distributeurs-automatiques-de-crypto (in French).
[25] See [8] of the glossary.

strengthen compliance by offering new use cases[26].

4.2.2 Customer knowledge and transactional analysis

As with any organisation subject to AML-CFT regulation, DASPs must, depending on risk exposure, gather customer knowledge to better understand the nature of the business relationship and establish a ML-TF risk profile[27].

The method used to gather the information required to obtain this knowledge is not always linked to the technology specific to cryptoassets, and sometimes requires methods comparable to those used in other regulated sectors. For example, the geographical address of the customer or the origin of the funds (with the particularity that cryptoasset funds may come from mining activities and not just from purchases or exchanges).

However, in terms of cryptoassets, the public blockchain economy allows this knowledge to be improved and verified using transactional analysis tools (Know Your Transaction or "KYT").

These computer tools exploit the characteristic of public blockchains to trace all cryptoasset transactions and movements. Through the analysis of these transactions, they make it possible to highlight potential risks as to the origin or destination of digital assets by assigning a score (scoring) to the client's cryptoasset wallet.

Transactional analysis tools can be used to determine whether cryptoassets have passed through public addresses associated with criminals or hackers. Data analysis and cross-checking can, in some cases, reveal the origin, destination and parties involved in a transaction. These tools also make it possible to reconciliate some addresses with an owner (exchange platform, online shopping website). However, these tools are still perfectible and do not allow for the analysis of transactions linked to anonymity-enhanced cryptocurrencies: in addition to this tool, DASPs must also be able to draw on their experience, consolidated using the knowledge bases acquired, and turn to their customers for additional information (transaction counterparty, purpose and nature of the planned transaction, supporting documents). These tools are discussed in more detail in Part 5 of this document.

[26] For illustrative purposes, one respondent mentioned a solution allowing for the generation of a customer-specific cryptographic identifier that could be attached to transactions -thus enhancing the traceability of operations- once the KYC process has been completed and approved; this identifier could also be technically exploited as a precondition for the execution of transactions.

[27] Article L. 561-5-1 of the French monetary and financial Code (in French).

4.3 Due diligence

Due diligence, and in particular the monitoring of cryptoasset transactions and flows, is a key element in the AML-CFT mechanism of DASPs. In this regard, the use of the public blockchain has distinctive features that lead to the consideration of very specific methods of transaction monitoring.

4.3.1 Split transactions and multiple public addresses

Transactions that are split by the same customer for fraudulent purposes can be detected using the cryptographic identity or nominative account attached to each user.

In this respect, the use by a single customer of multiple public addresses on the blockchain may cause difficulties. Any customer can generate an almost infinite number of cryptographic wallet addresses from an initial wallet (either physical or software), even though a respondent indicates that this use "does not match the vast majority of malicious uses". In fact, the use of several addresses on a public blockchain may be aimed at preserving the privacy of the users of this blockchain.

In order to mitigate the negative effects of the use of multiple addresses on customer knowledge, some respondents noted that DASPs may request the disclosure of all public addresses controlled by a given customer. Some also limit the number of wallets associated with a single customer. However, some challenges were identified. The destination addresses provided by the customer for digital assets may not be the property of the customer. Conversely, a customer may have control over several withdrawal addresses[28] and disclose only a limited number of them to the DASP that person is the customer of.

4.3.2 Technology facilitating anonymity on the internet

Technologies that enhance online anonymity (using a VPN or a Tor-like browser) can be indicators of suspicion regarding the customer, leading to enhanced due diligence in terms of the supporting documents collected from the customer. However, the working group noted that the use of private networks is common among experienced users in the cryptoasset sector. According to the members of the working group, these tools are of interest from the customer's standpoint (encrypting information when connecting to a public Wi-Fi network, securing the sending and receiving of personal data) but also involve risks (bypassing embargo measures). Other DASPs allow the use of a VPN which can be used to ensure the security of a customer by avoiding being traced by a third party[29] as long as the customer is known to the DASP through customer knowledge mechanisms and the use of own IT equipment for authentication purposes.

[28] The diversity of offers available for the creation of wallets, in terms of service provider as well as wallet types (online or mobile, computer-based, protected physical medium, etc.) and their ease of use, makes it easy for DASPs customers to create multiple wallets.

[29] The use of VPNs is widespread among professionals and frequent for individuals (within the gaming community for example). Therefore, VPN use needs to be compared with other clues in order to refine a user's profile, in addition to the lists differentiating VPNs intended for non-professional use.

4.3.3 Unhosted wallets

Concerning flows of digital assets from unhosted wallets[30], DASPs may request from a customer using an unhosted wallet that the customer provide them with that wallet's public address in order to use a transactional analysis tool to recreate the history of movements that have taken place in this wallet since its creation (amounts, dates, origin and destination wallets).

DASPs can also use a transactional analysis tool to assess whether a public address cryptoassets pass through has been generated by another DASP: if not, it may be a private wallet. However, since not all DASP addresses are identified and some DASPs generate a new address for each transaction, this information is not sufficient to determine whether the flow comes from an unhosted wallet.

4.3.4 Technologies facilitating the anonymity of cryptoasset holders

Theoretically, it is possible to analyse all flows (amount, sender and receiver address, time stamp) for a given a digital asset. However, some digital assets are intended to enhance the anonymity of their users: the FATF refers to these as *AEC* or *privacy coins*[31] (see 3.3.3. above). These are an obstacle to risk analysis prior to a transaction with a VASP.

French regulations do not prohibit AECs. However, DASPs that wish to sell or buy such cryptoassets must have in place an AML-CFT mechanism that is sufficiently effective to analyse and mitigate the risks inherent in these cryptoassets.

To a certain extent, blockchain transactional analysis tools can help to address these risks relating to technologies that make it possible to conceal the identity of the sender, recipient, holder or beneficial owner (AEC, tumblers, etc.). It is thus possible to identify whether cryptoassets come from an exchange, a tumbler, a transaction on the dark web or from other processes that make it possible to cover the origin of digital assets. Some of these tools also allow for the issuance of "certificates of compliance" aimed at confirming the traceability of operations to DASPs. The recovery of these certificates or other supporting information from the customer is, however, a costly and complex process, which will only be carried out when there are other indications that the transaction under review bears a risk.

To provide a reference for the market, a list of high-risk digital assets implying an increased risk for ML-TF and therefore requiring enhanced due diligence on the part of a VASP could be drawn up in collaboration with market participants through their representative associations.

[30] In the case of the unhosted wallets, the holder of the cryptoassets keeps his keys himself and does not use the storage service of a VASP.
[31] See [6] of the glossary.

4.3.5 Blockchain and geographical origin or destination of funds and cryptoassets

In the case of the purchase or sale of digital assets against legal tender, the location of the customer's or counterparty's bank account makes it possible to determine the geographical origin or destination of the funds.

The question arises differently when it comes to determining the geographical origin or destination of digital assets. This notion is in fact foreign to the underlying principles of a blockchain. Indeed, no geographical data is attached to a cryptoasset address. The information may therefore be difficult to obtain, given that the assets are under the control of the private key holder of each address.

4.3.6 Blockchain and asset freezing

In practice, a DASP that holds the digital assets of its customers must be able to proactively apply appropriate asset freezing measures to block access to an account and temporarily store the related digital assets in an escrow account (or quarantine wallet). This aims to prevent the customer concerned from moving his or her digital assets to another public address[32].

It would be technically feasible to automatically filter wallets subject to asset freezing measures using *smart contracts*[33] based on a regularly updated blacklist of addresses. These technical possibilities would also pave the way towards shared lists of wallets subject to restrictive measures, and such lists would allow for wallets to be easily detected in order to follow an audit trail and retrospectively assess the implementation of asset freezing measures.

[32] However, it is by design not possible to prevent a digital asset transfer to a public address on a blockchain. Therefore, the volume of digital assets in a wallet subject to freeze measures may increase during the freeze period if transfers are made to credit that wallet; however, these funds will be blocked by the measures applied by the holding DASP.

[33] See [7] of the glossary.

4.4 Implementation of the travel rule

In 2019, the FATF extended the application of its 16th Recommendation on the transparency of wire transfers to virtual asset transfers. As indicated in its 12-month assessment, the FATF invites industry participants to intensify their efforts to develop a solution to allowing for the implementation of transparency to virtual asset transfers.

To this end, market participants have been asked about possible technologies and potential obstacles identifiable.

Respondents unanimously stressed the need for a coordinated development of solutions, at a supranational level, to implement transparency for virtual asset transfers or interoperable solutions. One of the prerequisites for building an efficient technical solution for information sharing would be the establishment of a messaging standard, or of an agreement on the content and structure of messages between virtual asset service providers.

In this regard, respondents cited the initiatives undertaken towards a standardisation approach (see 5.2).

Projects based on self-sovereign identity[34] were also cited as a potential decentralised technical lead for exposing identity information while strengthening risk control in terms of individual data confidentiality and cybersecurity.

As for access to data for supervisory bodies, the working group did not identify any technological obstacles *a priori*. For illustrative purposes, one member of the working group described a potential solution based on the implementation of APIs that would make transfers transparent and make information available to the authorities in real time.

[34] See [8] of the glossary.

5 Identified technological leads

5.1 Transactional analysis tools for blockchains

5.1.1 Brief operational description

Transactional blockchain analysis tools are used by many DASPs to facilitate the implementation of their obligations under the AML-CFT regulations.

They use a node from one (or more) blockchain(s), that gives them access to data in real time and allows them to track and analyse transactions involving cryptoassets as they occur. Based on transactions recorded over a long period of time and using artificial intelligence techniques, these tools can also carry out the behavioural analysis of an address linked to a cryptoasset wallet. These tools can therefore identify a wallet that is at risk by analysing its incoming or outgoing flows of cryptoassets. From a wallet reported as being at risk, the tools can also escalate alerts, helping to trace the path of funds of suspicious origin.

Concretely, for any given transaction, the tool provides its user with the origin or destination addresses of cryptoassets and assigns a risk score (scoring)[35] to the analysed addresses.

In addition, these tools contribute to the partial de-anonymisation of the blockchain. The practice of clustering allows for the identification of all the addresses linked to a customer wishing to carry out a transaction. These tools also allow for the association of an identity with public addresses, by detecting whether addresses or wallets belong to companies by matching them with natural persons or legal entities (exchange platforms, marketplaces, etc.)[36]. To that end, several complementary techniques are used through test transactions with targeted actors, relying on the screening of accessible internet resources (including social networks or the use of the dark internet) and making it possible to locate or identify suspicious addresses.

Lastly, some transactional analysis tools also integrate public databases[37], allowing for the partial automation of manual identification investigations.

These tools are developed by a small number of specialised service providers: they operate using APIs that can be interfaced with DASP trading software. The development of tools of this kind by the DASPs themselves would, in the opinion of the working group members, be time-consuming, costly and require significant technical skills. One advantage of the external development of these tools is that the feedback from their users leads to a *de facto* cooperation between all these users to report suspicious activities. However, an excessive standardisation of the approaches of all market players may constitute a potential drawback.

Yet, these tools offer considerable configuration freedom for the benefit of their users, which may mitigate this disadvantage. Moreover, depending on the settings and clustering algorithms, the results rely on name matching probabilities: as with other warning tools, stakeholders therefore make the distinction themselves between false positives and cases where it is necessary, for example, to stop

[35] The calculated risk score is the weighted result of several risk categories, including exchange, mixing, gambling, darknet, ransomware, hacking, Ponzi or terrorism.
[36] For example, web scraping and open source intelligence techniques are used.
[37] Such as OFAC sanctions lists.

transactions.

These tools are still relatively recent and present a number of technical limitations. Indeed, it is impossible to trace the history and monitoring of transactions involving cryptoassets with enhanced anonymity (AEC, privacy coins). The same applies to second-level protocols such as *Lightning Network*, *SKALE*, *Loopring*, etc. Lastly, the anteriority of these tools is still limited to ensure a good assessment of their performance with regard to the identified use cases.

5.1.2 Issues identified by the working group

The issues faced by market participants and the authorities all relate to the appropriateness of adopting these transactional analysis tools and their systematic use for AML-CFT purposes. In this respect, the working group has identified the following issues.

Firstly, the cost of these solutions (subscription on a case-by-case basis, permanent solution) may represent a significant financial burden for DASP players with a limited volume of activity and justify, for these players and depending on their level of risk, the use of alternative, less sophisticated analysis techniques.

Secondly, the scope covered by these tools is not exhaustive. More specifically:

- It may be necessary for a DASP to use several complementary tools depending on the cryptoasset wallets covered by the scope of its business;
- As mentioned earlier in the report, some cryptoassets are not covered by transactional analysis tools because they are recent or seldom used[38]; on the other hand, these tools are not adapted to certain cryptoassets developed on private blockchains or specifically designed not to be traceable (AEC, privacy coins)[39].

Finally, the market and the authorities have yet to acquire a more precise appraisal of the performance of these tools and their configuration.

Indeed, the level of performance of these tools depends on the exhaustiveness and quality of the data collected on the web, as well as on the efficiency of the clustering models used, whether they are deterministic or probabilistic.

Configuration, on the other hand, raises the question of the comparative advantages of the various approaches currently encountered on the market: some DASPs rely on the tool's default settings, while others modify them either for tool testing purposes or for better integration into processes. In both cases (default setting, customisation), the question that arises for the authorities is that of the quality of these settings, with regard to the regulations and the user's risk-based approach.

[38] In fact, a significant number of cryptoassets are not covered by these tools, but they represent a small proportion of the volumes of cryptoassets exchanged.

[39] The use of these cryptoassets is however limited in the activities of DASPs, particularly in view of the enhancement of the due diligence measures applied by the DASPs.

5.2 Communication standardisation initiatives

5.2.1 The industry has taken up the subject

The work of the working group made it possible to identify initiatives for a standardisation approach as well as solutions from regtech players based on these initiatives. As a priority, this work focuses on defining and implementing a communication protocol to enable VASPs to exchange the required information. The work on dealing with the issue of the mutual identification of VASPs ("Know your VASP"), which should be distinguished from the standardised technical codification of VASP identifiers, seems less advanced, even though it is paramount for the overall process of the travel rule.

In the course of its work, the working group discussed more particularly the interVASP and OpenVASP initiatives. InterVASP is an initiative to standardise the message format[40] of the travel rule, led by international experts in an international working group. OpenVASP aims to design and develop a protocol solution for the exchange of these messages; the work is being carried out by a group of Swiss stakeholders in the blockchain and cryptoasset industry, with an open and collaborative approach.

Generally speaking, the various initiatives under way, whether in terms of developing standards[41] or protocols[42], guiding the development of *ad hoc* solutions, open source[43] solutions or commercial[44] solutions ready for use or integration and based on the above-mentioned standards or protocols, demonstrate the willingness of the cryptoasset industry to take into account the requirements of the travel rule and to suggest practical solutions.

However, this multiplicity of products raises the issue of interoperability, which must be ensured in order to avoid the fragmentation of cryptoasset flows gathered by the same travel rule tool between different VASP communities. In this respect, regulations in separate jurisdictions should avoid contributing to the perpetuation of a fragmented situation, even though technical solutions may converge in the medium term[45].[46]

Finally, some members of the working group emphasise the business and competitiveness related issues that must be addressed to ensure that VASPs are free to choose when adopting a travel rule tool, meaning without necessarily having to depend on the dominant players in the ecosystem or on specific regional areas.

The definition of interoperable standards therefore appears to be a necessary condition for the effective and widest possible enforceability of the travel rule; its success should depend on the

[40] In other words, the specifications that define the specific format of the message (or payload) exchanged between counterparties applying the travel rule; the task force's work has resulted in a standard called IVMS101, which seems to be gaining ground among players implementing travel rule solutions.
[41] For example, the Joint working group *interVASP* or the Travel rule working group.
[42] For example, *Open VASP* or the *Travel Rule Protocol*.
[43] For example, TRISA.
[44] For example, Shyft or Sygna Bridge.
[45] By way of illustration, the work of the OpenVASP communication protocol is now based on the standardised interVASP messaging format.
[46] This problem is referred to in English as the sunrise issue, describing jurisdictions that transpose the travel rule successively but not concomitantly, which complicates the enforceability of the travel rule to a VASP carrying out a transaction with a counterparty under another jurisdiction that does not apply this rule yet.

broadest possible involvement among representatives of the VASP and DASP industry in the discussion and definition of these standards.

5.2.2 Challenges and opportunities in the implementation of the travel rule

The work of the working group made it possible to highlight the following challenges and perspectives.

(i) The finding: a momentum that needs to be materialised

The assessment made by the FATF in June 2020 on the implementation of the travel rule has not changed significantly since May 2019 (during its session open to the industry), especially regarding the lack of a ready-to-use technical solution for VASPs.

In this respect, few initiatives for discussion on the subject of the travel rule between VASPs have been identified by the working group at national and European levels, as well as low involvement in international initiatives. This state of affairs may be due to a lack of collective awareness on these subjects, or a lack of availability or resources on the part of the stakeholders. The anticipated difficulty in implementing the required data exchange may also be a hindrance to the involvement in collective initiatives.

At this point, stakeholders are able to collect the (incoming and outgoing) data necessary for the travel rule, but the veracity of the collected data remains an issue, especially for non-professional customers that are natural persons. The analysis tools available do not currently incorporate the protocols required to implement the travel rule.

Above all, the critical issue of trust within the VASP community is raised, especially taking into account the increased pace at which new platforms are created that operate from abroad. The main current difficulty lies in the impossibility of identifying with certainty the players carrying out VASP activities around the world and their addresses on the blockchain.

In this context, communication between VASPs is an essential practice for the implementation of compliance rules. Such interactions are notably carried out using restricted and secure online discussion groups, or they take place within representative associations[47], and enable the sharing of best practices. However, these means of information exchange are limited by their network effect (e.g. compliance officers for a given geographical area) and by confidentiality restrictions which do not allow for the transmission of individual data, particularly for the purposes of the travel rule.

The platform registration mechanisms in some jurisdictions[48] are an important factor in establishing the necessary trust between VASPs and facilitating identification and communication between stakeholders, but the scope of VASPs concerned remains limited and geographically fragmented. The issue of the meaning of registrations according to jurisdictions and the difference in the associated requirements also arises.

Some French stakeholders are now showing their openness to broadening the discussion on the subject: for example, within market associations, with European contacts, with representatives of international standardisation initiatives, by participating in test procedures or experiments if the opportunity arises, or by setting up a thematic task force. However, this approach can only be developed by ensuring that a shared dynamic is created and by taking into account the resource

[47] Such as the ADAN (*Association pour le Développement des Actifs Numériques* - French Association for the Development of Digital Assets).
[48] For example, in France, the registration created by the PACTE Law.

constraints of the stakeholders involved. This dynamic could also be extended by integrating actors from other jurisdictions, accustomed to operating with the French DASPs.

(ii) The issue of identifying counterparty VASPs

The proper implementation of the travel rule requires a minimum level of trust between the two VASPs that may be concerned by a transfer of cryptoassets: if one of the two VASPs defaults on its obligations, the other VASP involved will not be able to perform its compliance task in a truly satisfactory manner.

This trust can be facilitated by mechanisms that allow for the identification of VASPs. In this respect, there are several possible options, and on the basis of these mechanisms, several practices can be envisaged for VASPs.

In the current environment, where registration systems or mechanisms for identifying VASPs remain fragmented and poorly harmonised or coordinated, one possible solution for VASPs is the establishment of a white-listing system: in other words, the VASP would only allow the transfer of digital assets between certified addresses. This procedure would, however, be harder to implement in the context of a "retail" activity than in the context of a "BtoB" activity.

Other prospects would naturally be opened up by the creation of a global register of VASPs, possibly relying on registrations made by the various jurisdictions responsible[49]. The establishment of such a register would require a minimum degree of harmonisation between jurisdictions in order to guarantee the symmetry and quality of the information required for the proper application of the travel rule.

The members of the working group are particularly mindful of this last point. Failing this, the creation of a global VASP register could have the adverse effect of authorising -or even encouraging- registered VASPs to operate regardless of their actual level of compliance with the regulatory AML-CFT principles. Furthermore, the registration of a VASP should be considered on a long-term basis; its continued inclusion in the register should provide sufficient assurance that its level of compliance is not significantly lower than it was at the time of registration.

Therefore, a global VASP register should not be considered as a sufficient tool for building trust in itself, but rather as an aid in the assessment that a VASP can make of a counterparty VASP, ensuring its identification and providing information on its jurisdiction and possible supervisory authority. The use of other methods, such as the transactional analysis tools mentioned, should enable VASPs to complete their risk assessment.

The establishment of a global VASP register could be encouraged at the level of the European Union by the current discussions of the European legislator aimed at harmonising the virtual asset sector[50]. The harmonisation process mentioned above goes beyond AML-CFT concerns, covers the entire legal framework applicable to the digital assets industry, including registration and control requirements, which could increase the relevance of a registry.

[49] The question of identifying a counterparty's VASP is a topic included in the FATF's scope of discussion.

[50] The European Commission's action plan proposes to set up a travel rule standard. This integration of the travel rule into the European legal framework could take place on the occasion of legislative proposals relating to cryptoassets (end of 2020) or to the fight against money laundering (beginning of 2021).

Finally, it should be recalled that transactions are not always carried out between two VASPs: the counterparty of a VASP may, for example, be an unlisted platform (e.g. a gaming platform) or an unhosted wallet ("self custody"). In these circumstances and in application of the travel rules, the VASP must request the counterparty's identification information from its customer, which raises the issue of the level of trust to be placed in the information provided by the customer (errors made either inadvertently or with intent to conceal). VASPs must therefore verify their customer's statements. This problem has been clearly identified by the FATF. It is not fundamentally different from other situations, within the traditional financial sector, where information is reported. However, it is true that, for VASPs, these verifications can be technically complex or complicated to carry out depending on the situation.

(iii) The mobilisation required to implement an operational solution

The operational implementation of the travel rule requires a certain amount of collaboration between VASPs: at the national, European and international levels; one of the related challenges is ensuring that this collaboration includes all the stakeholders.

Indeed, an infrastructure or protocol likely to facilitate the travel rule can only be the result of a collective approach, integrating not only the identification issues already mentioned, but also those of security, sovereignty, data storage and management. VASPs can contribute to the definition of these processes and their implementation, especially those relating to obtaining information from customers. Other actors, such as blockchain analysis providers (see 5.1. in particular) could have a role to play, by providing components of a solution, notably through their ability to trace part of the flows.

Such a collective approach implies a clearly understood and shared identification of roles, as well as a consensus on the technical means to be retained to ensure the required operations. In particular, French and European stakeholders would benefit from positioning themselves more clearly vis-à-vis the international initiatives identified and, if they consider them to be a useful starting point, identifying the additions or adjustments to be made to achieve a shared operational process that rises to the challenges posed by the travel rule. Finally, the launch of similar initiatives or projects among the actors of the French or European ecosystem could provide an alternative.

It emerged from the working group's discussions that there is room for improvement in the level of information of the French VASP sector on the travel rule. This report is likely to renew their awareness. Other approaches, such as the testing of travel rule solutions by French VASPs, could help raising awareness within the financial centre and identifying operational issues. Finally, in order to be integrated into existing projects, the French financial centre could profitably intensify its interactions with the leaders of ongoing international initiatives. Discussions or actions towards that goal have been undertaken by some VASP market participants and by the association representing the industry.

At the European level, a think tank representing the interests of the blockchain and cryptoasset industry (The Blockchain and Virtual Currencies Working Group, BVC WG) has been mentioned and aims to put these issues forward with the legislator. This working group has not identified any other European forum that would have made significant progress in its work on the implementation of the travel rule. A dynamic must therefore be created on that level as well, to provide operational support for the regulatory work in progress.

(iv) The question of temporary or "transitional" solutions

The time needed to develop a shared tool on a significant (at least European) scale led the working group to quickly mention the existence of alternative or transitional solutions.

In addition to the above-mentioned technical standards, alternative or transitional technical solutions do indeed exist, such as messaging solutions with an asymmetric encryption feature (such as "PGP"). The challenge for VASP users of these solutions is to be able to integrate them into their information systems in order to automate actions with no added value. Moreover, these alternative solutions do not seem likely to solve the general issues that have already been raised (implementation of a shared tool, which presupposes that a basic consensus be reached between the stakeholders).

More generally, the risk that different jurisdictions might adopt a different pace and a more or less proactive approach to meeting the requirements of the travel rule was raised by some members of the working group. These potential discrepancies in terms of requirements over time could be a competitive disadvantage for VASPs, who would have to bear the increased burden of compliance and the costs of the potential temporary solutions sooner than their counterparts.

6 Annexes

6.1 Glossary

[1]	VASP, DASP	The FATF defines virtual asset service providers (VASP) as any person engaged in any of the following activities in a business capacity in relation to virtual assets: the exchange of virtual assets for legal tender; the exchange between virtual assets; transfer; custody and/or administration; participation in the provision of financial services in connection with an offering of an issuer and/or a sale of a virtual asset. French regulations introduce the notion of providers of digital asset services (DASPs) whose scope of regulated activities applies to digital assets (refer to the following note) and covers: on the one hand, on behalf of third parties, the custody, exchange for legal tender, exchange for digital assets, the reception and transmission of orders, the provision of various financial services (wallet management, advice to subscribers, underwriting, guaranteed and non-guaranteed investment); and on the other hand, the operation of a trading platform.
[2]	Virtual assets, Digital assets, Cryptoassets	The FATF defines virtual assets as any digital representation of value that can be digitally traded, transferred or used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already subject to other provisions of the FATF Recommendations. French regulations use the term "digital asset" to refer to: a token (any intangible asset representing, in digital form, one or more rights that can be issued, registered, retained or transferred by means of a shared electronic recording mechanism), with the exception of financial instruments and savings certificates; or any digital representation of value that is not issued or guaranteed by a central bank or public authority and that does not have the legal status of a currency but is accepted as a means of exchange and can be transferred, stored or exchanged electronically. Cryptoassets are a generic term for all assets issued and exchanged on the blockchain: they include virtual assets and digital assets.
[3]	Money laundering phases	Money laundering is characterised by three phases: an initial placement phase which is the introduction of illegal profits into the financial system; a layering phase which consists of a series of conversions or movements of funds

		to distance them from their source; a integration phase that aims to reintroduce the funds into legitimate economic activities.
[4]	Mixers, Tumblers	Mixers or tumblers are services that make it possible to enhance the anonymity of digital assets by mixing flows of the same type of traceable digital asset (e.g. Bitcoin) from various wallets for the purpose of distributing them to the desired cryptographic addresses, thereby breaking the chain of traceability of these digital assets in the history of the various holding wallets.
[5]	Tor browser	Tor browsers exploit the Tor decentralised computing network for the anonymous browsing of web resources. Several software solutions have been developed to take advantage of the Tor network, including platforms, operating systems, and messaging modules in addition to web browsers.
[6]	AEC, Privacy coins	Anonymity-Enhanced Cryptocurrencies (or AECs) refer to a type of virtual assets designed to enhance the anonymity of its holders by relying on untraceable blockchains: Monero, Zcash, Grin or Dash are commonly used examples of AEC. Their use allows the counterparties to a transaction to ensure their anonymity while allowing for the configuration of the level of confidentiality. The commonly employed term Privacy coin is equivalent to AEC.
[7]	*Smart contracts*	A smart contract is a blockchain feature allowing for the deployment and execution of autonomous and specific programs on a given blockchain; they are triggered automatically when predefined conditions are met.
[8]	Self Sovereign Identity	A Self Sovereign Identity System (SSI) allows a person or an organisation to retain control over the elements that prove their identity by allowing the person or organisation to disclose, with their consent, the appropriate characteristics of their identity. Its operation can be explained by analogy with that of a wallet from which the owner extracts the required supporting documents upon request. Self-sovereign identity emancipates itself from intermediaries and can be based on a decentralised architecture, such as a blockchain.
[9]	*Chain swap*	Chain swapping is a process allowing for the movement of one virtual asset from one blockchain to another blockchain. It thus enables the holders of the moved assets to extend the scope of use of their funds.

6.2 Documentary references

[1]	FATF	FATF Recommendations (updated in June 2019)
[2]	FATF	*Guidance for a risk-based approach Virtual assets and Virtual asset service providers* (June 2019)
[3]	FATF	*Public Statement on Virtual Assets and Related Providers* (June 2019)
[4]	FATF	*12-month review of the revised FATF Standards on Virtual Assets and Virtual Asset Service Providers* (July 2020)
[5]	FATF	*Virtual Assets Red flag indicators of money laundering and terrorist financing* (September 2020)
[6]	TRACFIN (French National Financial Intelligence Unit)	*Rapports « Tendances et analyse des risques de BC-FT »* (reports on ML-TF risk analyses and trends) [in French]
[7]	COLB (French guidance council on AML-CFT)	*Analyse nationale des risques de blanchiment de capitaux et de financement du terrorisme en France* (national risk assessment on AML-CFT in France) [in French]
[8]	JWG interVASP	IVMS101 interVASP data model standard - Issue 1 Final (May 2020)
[9]	OpenVASP	OpenVASP : an open protocol to implement FATF's Travel rule for Virtual assets (white paper, November 2019)
[10]	Travel Rule Protocol (TRP)	*TRP specifications*

6.3 Composition of the working group on the application of AML-CFT rules to the cryptoasset industry

The following were represented as members of the working group and took part in the discussions or contributed to the work:

- Public authorities:
  - The ACPR
  - The AMF
  - The French Treasury General Directorate
  - Tracfin

- Cryptoasset industry and the blockchain:
  - Bitit
  - Coinhouse
  - Consensys
  - Ledger
  - LGO markets
  - Thesaur.io
  - Woorton

- Banking financial institutions industry:
  - BNP Paribas
  - CACEIS
  - SG Forge