BLOCKCHAIN INTELLIGENCE

Abogacía Española
CONSEJO GENERAL

www.blockchainintelligence.es

Doctrinal article

CRYPTO ASSETS: THE REGULATORY CHALLENGE REGARDING THE PREVENTION OF MONEY LAUNDERING

MAY 2023

LAURA SCARPELLINI CASANA

AML COMPLIANCE SENIOR MANAGER, BBVA
CERTIFIED LEGAL AND COMPLIANCE EXPERT IN BLOCKCHAIN, WEB 3.0 & METAVERSE (SMART CONTRACTS, TOKENIZATION AND CRYPTOASSETS) FROM BLOCKCHAIN INTELLIGENCE

CELIA HERRERO CANTÓ

AML COMPLIANCE ASSOCIATE, BBVA
CERTIFIED LEGAL AND COMPLIANCE EXPERT IN BLOCKCHAIN, WEB 3.0 & METAVERSE (SMART CONTRACTS, TOKENIZATION AND CRYPTOASSETS) FROM BLOCKCHAIN INTELLIGENCE

Crypto assets: the regulatory challenge in terms of preventing money laundering.

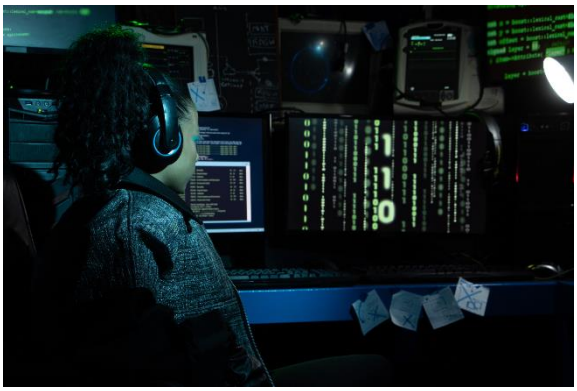
Laura Scarpellini Casana, AML Compliance Senior Manager en BBVA

Celia Herrero Cantó, AML Compliance Associate en BBVA

Introduction

New forms of crime

Technology and its evolution are undoubtedly an opportunity. It improves our quality of life, generates new sectors, generally makes our daily lives easier, but it also represents an opportunity and an innovative avenue for crime. In this sense, the crypto assets[1] were not going to be an exception and criminals know how to jump on the bandwagon.



According to Chainalysis[2], a leading *blockchain* analysis company, in 2021, $11 billion (approximately €9.7 billion) in crypto assets were in the hands of criminals, mostly based in Russia, Iran and North Korea. This is 266% more than in 2020, having multiplied by more than two and a half in just one year.

Most of these funds, that is, 93%, came from theft by hacking. However, there are other crimes involved such as *deep web* transactions, scams, fraud, and *ransomware*[3]. They are also used to evade economic sanctions, or for illicit purposes.

This is greatly aggravated by the slow pace of legislative processes which have taken more months and even years than criminals to understand how crypto assets work and the opportunities and risks they bring. This has caused a legislative vacuum that gave a competitive advantage to criminal groups.

In the latest report of the Financial Action Task Force ("FATF") on financial flows related to ransomware, it was noted that criminals are

[1] For clarification purposes, the term "crypto asset", according to the International Monetary Fund, refers to "a broad spectrum of digital products that are privately issued with similar technology (cryptography and often distributed ledgers) and that can be stored and traded using primarily digital wallets and exchanges." Its main technical characteristics are intangibility (since it is a digital representation), the use of Distributed Ledger Technology (or DLT for its acronym) such as the blockchain, the absence of intermediaries and its decentralization, the use of cryptography or similar technology and immutability.
[2] The Chainalysis 2022 Crypto Crime Report. https://go.chainalysis.com/2022-Crypto-Crime-Report.html
[3] FATF Report - Countering Ransomware Financing (March 2023) - https://www.fatf-gafi.org/en/publications/Methodsandtrends/countering-ransomware-financing.html

exploiting the latest technologies to develop increasingly powerful tools to carry out their attacks.

One of the main risks related to crypto assets is money laundering ("**ML**") and financing of terrorism. ML is the act of concealing the illicit origin of profits obtained from previous criminal activity, introducing said profits under an appearance of legality into commercial traffic. Applied to crypto assets, an example of criminal conduct could consist of converting cash into crypto assets in order to hide their illicit origin.

Given the anonymity they allow (that is, the addresses from which crypto assets are operated do not have associated information about the owner of these addresses), it is more complex than in the traditional banking system to carry out detailed and exhaustive monitoring of the origin and destination of funds, and therefore, crypto assets become an attractive mechanism for ML.

By not being able to control the origin of the funds, it is easier to introduce money from illicit activities into the legal system and, therefore, launder assets. Likewise, by not being able to control the destination of funds, it is more complex to prevent the financing of terrorism.

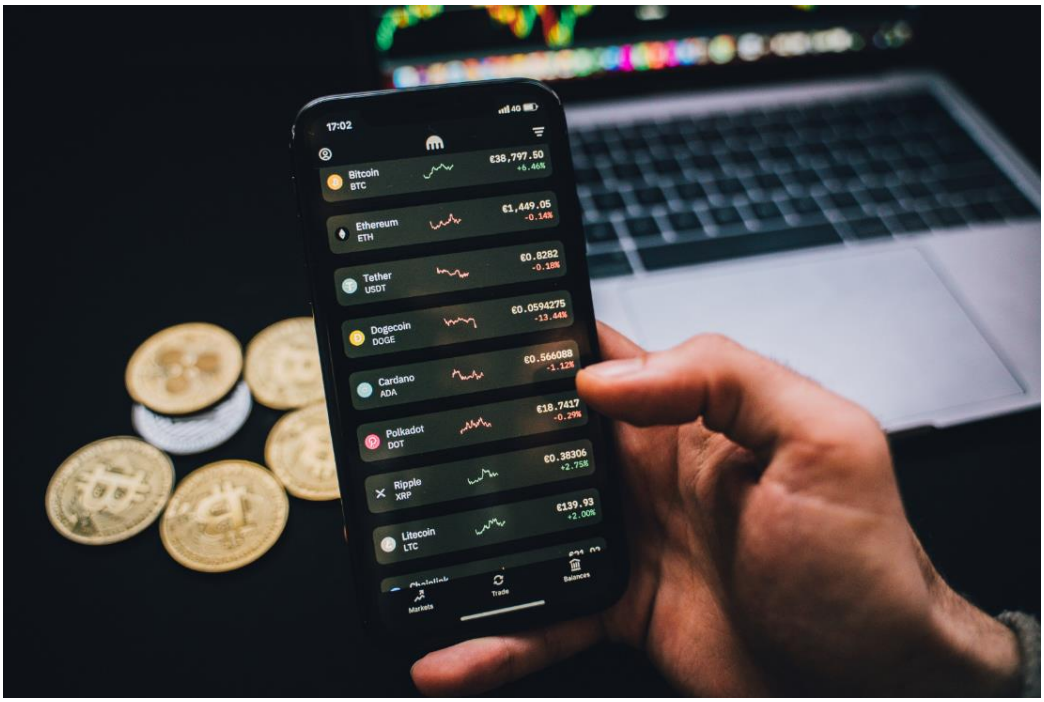
Furthermore, since there are no entities that centralize the activity, as is the case with banks in the traditional financial system, it is more complex to apply the measures usually used to prevent money laundering and financing of terrorism ("**AML**" or Anti-Money Laundering) such as identifying customers or tracking business relationships.

This is clearly seen in the case of *unhosted wallets*. A *hosted wallet* is a digital wallet guarded by a third party, which can still apply these AML measures (providing a partial solution to the challenge represented by the anonymity of crypto assets). However, in *unhosted wallets* there are no intermediaries, with crypto assets being managed solely by the users themselves.

Likewise, operations with crypto assets are much faster than those carried out through the traditional banking system. A cross-border operation can take several business days to execute the traditional bank transfer system, while a transfer of crypto assets can take just minutes. Therefore, the possible deadlines to analyze or detect suspicious operations again are considerably reduced when we use crypto assets, thus favoring the possible commission of ML crimes.

Finally, transactions carried out with crypto assets are irreversible, so classic measures in the field of AML, such as embargoes, are not applicable to this system.

Considering the above, it is of vital importance to apply to AML matters rigorous controls that are appropriately adapted to the particularities and characteristics of this peculiar industry.



This was underlined at the FATF *Virtual Assets Contact Group*[4] meeting in April 2023, which stated that "(i)t is increasingly important to strengthen measures to combat money laundering, terrorist financing and proliferation financing, including the theft and misuse of virtual assets by North Korea" in reference to ML risks arising from the use of digital assets (including crypto assets).

Prevention of money laundering in new technologies

This year will mark 15 years since the publication of the White Paper called "*Bitcoin: a peer-to-peer electronic cash system*", a moment that marked the starting point for the emergence of crypto assets. Therefore, we can affirm that we have had 15 years of constant evolution, development and transformation and the integration of crypto assets and, in general, new technologies in more and more sectors.

[4] https://www.fatf-gafi.org/en/publications/Virtualassets/Press-Release-FATF-VACG-2023.html

Even having had this long period of time, the truth is that legislative and regulatory development has not been able to keep up with the pace set by the technology (as criminals have been able to do, as we have seen in the previous section) in terms of adaptation times. However, there has been awareness at all times of the need to reinforce existing systems and to adapt in the best possible way as threats emerge.

In this way, the obligated entities, supervisors and legislators, as key actors in the AML ecosystem, have been forced to advance by leaps and bounds in the development of new policies and tools that would allow restricting the use of new technologies as tools of money laundering.

Although we will go into detail later, proof of this is that many jurisdictions, to a greater or lesser extent, included crypto asset service providers as obligated subjects (that is, natural or legal persons who are professionally dedicated to certain activities that, due to their characteristics and the risk they entail, must comply with a series of obligations regarding AML such as application of due diligence measures, information obligations, among others).

Likewise, and gradually, the agents involved in AML systems have worked on converting these technologies into allies of AML. Examples of this are the use of disruptive technologies in the tasks of AML teams. For example, in relation to the creation of tools that make use of Big Data or Machine Learning to facilitate the AML obligations of obligated entities.

What's more, PwC[5] stated that AI could be an essential lever to make systems more robust and anti-fragile by managing alerts more efficiently or detecting new patterns of crime commission. And we have also seen how a new sector has been created: RegTech, made up of technology companies that create solutions focused on regulatory compliance (including AML).

Therefore, not only is the creation of threats by new technologies in the field of ML being controlled, but also, new technologies are becoming strategic partners for AML.

On the other hand, the threats that new technologies can cause are better understood than a few years ago, which prevents, on the one

[5] PWC: "Artificial Intelligence: Opportunities & Challenges to Fight Money Laundering and Terrorism" https://www.pwc.fr/en/publications/artificial-intelligence-fight-money-laundering-and-terrorism.html

hand, criminals from using this type of technology to commit crimes and, on the other hand, favors their ethical and responsible use.

For example, this year Eurojust and Europol coordinated an action against a fraudulent online investment platform that had produced 33,000 victims for an approximate amount of 89 million euros[6]. Seventeen countries collaborated in the takedown of Genesis Marketplace, a marketplace selling stolen account credentials to hackers[7]. Europol has issued a report titled "ChatGPT: the impact of Large Language Models on security forces"[8], demonstrating an understanding of the risks of generative AI, to encourage more responsible and ethical use and warn about its possible risks (such as, for example, promoting the financing of terrorism).

In this way, we can see how the agents involved in the system have been aware of the existence of this great challenge and have made efforts to overcome the barriers created. Even so, given the limitation of resources and the characteristic speed of technology, it is undeniable that there is a long way to go, even if the path in the right direction has begun.

[6] https://www.europol.europa.eu/media-press/newsroom/news/further-action-against-fraudulent-online-investment-platform-five-arrests-of-high-value-targets
[7] https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-notorious-hacker-marketplace-selling-your-identity-to-criminals
[8] Europol (2023), ChatGPT - The impact of Large Language Models on Law Enforcement, a Tech Watch Flash Report from the Europol Innovation Lab, Publications Office of the European Union, Luxembourg

In this article, we will go into greater detail into the challenges that crypto assets have posed for AML and how they are being addressed from an international, community and national perspective.

International focus: the Travel Rule

The FATF was the first body to identify the imminent need to establish preventive measures against the risk of money laundering and financing of terrorism and to provide legal certainty to activity with crypto assets.

The most important step in this regard was the modification of FATF Recommendation No. 16[9], with the objective of making financial institutions and payment entities, as well as other regulated entities, share identifying information about the originator and beneficiary of transactions. This information travels in the payment chain, from beginning to end, and is known as the Travel Rule. In 2019, the FATF modified this recommendation to extend its requirement to *Virtual Asset Service Providers* or **VASPs** (including crypto assets)[10]. By sharing information about the identity and knowledge data of the originator and beneficiary of a transfer between VASPs, transparency is increased and the use of crypto assets for illegal activities is made more difficult.

While the *Travel Rule* largely prevents the ML risk associated with crypto asset activity, its implementation presents certain technical and practical challenges for VASPs:

1. **Developing systems and processes to share information securely and efficiently:** VASPs must ensure that information shared between them is secure and protected from cyber-attacks or data breaches.
2. **Complying with personal data protection regulations:** VASPs must comply with data privacy regulations when sharing information about their customers. This can be a challenge, especially if they operate in multiple jurisdictions with different privacy regulations.

[9] International Standards on combating money laundering and the financing of terrorism & proliferation - The FATF Recommendations - https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf

[10] For these purposes, the FATF defines digital assets as "any digital representation of value that can be the object of a digital transaction, transfer, or payment. It does not include the digital representation of fiat currencies".

3. **Verifying the identity of other VASPs:** VASPs must verify the identity of other VASPs before sharing information with them, which is not always a simple task, especially when the counterparty VASP is located in a jurisdiction other than the VASP originating the transfer.
4. **Costs:** Implementation of the Travel Rule may require significant investments in technology and human resources to develop and maintain systems and processes for the secure exchange of information.

Although the FATF Recommendations are not legally binding, many countries adopt them and incorporate them into their national legislation, largely because of the influence that compliance can have on a country's international reputation and its ability to attract investment and do business on an international level.

Likewise, it is worth highlighting the importance of this issue in the debates that are being held today in the FATF plenary sessions, and that it has been agreed to develop an action plan to guarantee greater security in matters of crypto assets by strengthening implementation of FATF standards on *Virtual Assets* and VASPs[11].

[11] https://www.fatf-gafi.org/en/publications/Fatfgeneral/outcomes-fatf-plenary-february-2023.html

Community approach: the regulation of the crypto asset phenomenon

In the European Union, the so-called Fifth AML Directive of 2018[12] introduced a relevant novelty by incorporating virtual currency exchange service providers and electronic wallet service providers as obligated subjects of regulation. Although this represented an important advance in the regulation, providers of exchange services of one virtual currency for another were not included as obligated subjects, so a part of the activities with a high-risk focus were left outside the scope of application of the standard.

After the publication of the Fifth Directive, Member States transposed these new measures into their legal systems. Germany adopted specific provisions in its AML regulation in 2019 aimed at including cryptocurrency service providers[13] in its scope, which must also be registered with the Bundesanstalt für Finanzdienstleistungsaufsicht or the Federal Financial Supervisory Authority (BaFIN). The same is true for France, which also adopted the Fifth European AML Directive and included the obligation to register virtual currency exchange service providers with the Prudential Supervision and Resolution Authority (ACPR). In the case of Spain, like their European counterparts, these entities must process their registration with the Bank of Spain and present documentation accrediting their AML control framework, as we will explain later.

These advances were not, however, sufficient. In 2021, the European Commission presented an ambitious package of legislative proposals to strengthen the European Union's rules on AML. The measures that were proposed and that today continue to be processed in parliament, aim to improve and strengthen the current European framework, and adapt to emerging challenges related to technological innovation and virtual currencies in particular.

The package consists of four legislative proposals:

[12] Directive (EU) 2018/843 of the European Parliament and of the Council, of 30 May 2018, amending Directive (EU) 2015/849 on the prevention of the use of the financial system for money laundering or the financing of terrorism, and which modifies Directives 2009/138/EC and 2013/36/EU.

[13] For these purposes, it should be noted that although there are other types of cryptoassets (such as utility tokens, security tokens, tokens as assets, stock tokens, reward tokens and dividend tokens), the most spread due to their popularity are cryptocurrencies.

- a Regulation creating a new European AML supervisory authority[14];
- an AML Regulation containing rules directly applicable in Member States[15];
- the sixth AML Directive, which replaces the current Directive (EU) 2015/849 (Fourth Money Laundering Directive, as amended by the Fifth Directive), which contains provisions on the organization and functioning of national supervisors and financial intelligence units of member states[16]; and
- an amendment to the 2015 European Regulation on information accompanying transfers[17].

The second legislative proposal, consisting of the issuance of a new Regulation on AML, will bring with it important developments for virtual asset service providers or VASPs (the name is used by the FATF, but called *Crypto-asset service providers* or CASPs in the terminology used by European co-legislators). These developments include the expansion of the scope of application, which will be extended to all crypto asset service providers, including those operating outside the

[14] Proposal for a regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010
[15] Proposal for a regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
[16] Proposal for a directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849.
[17] Proposal for a regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto assets (recast).

European Union, and also to providers of exchange services of one virtual currency for another, covering thus the existing gap in the current European AML regulation.

These modifications will be complemented by those introduced by the modification of Regulation (EU) 2015/847 of the European Parliament and the Council from 20 May 2015, regarding the information accompanying transfers of funds, which aims to guarantee full traceability of transfers with crypto assets through the collection and access for all participants in the payment chain to the identifying data of the payers and beneficiaries in a transfer. During the parliamentary discussions of this text, the European Parliament introduced a ban on anonymous crypto asset transfers above €1,000, unless it is possible to identify the counterparty. Therefore, and in accordance with the European Parliament's proposal, all transfers above the aforementioned threshold that come from or are destined for a self-managed electronic wallet or *unhosted wallet,* in which the identification of the owner is not required, would be prohibited.

Additionally, after the political agreement reached on June 30 of last year, the final text of the Regulation of the European Parliament and the Council relating to crypto asset markets and amending Directive (EU) 2019/1937, commonly known as Markets in Crypto Assets ("**MiCA**") Regulation, was approved by the Parliament of the European Union on April 20, and unofficially agreed with the Council of the European

Union. Following its publication in the Official Journal of the European Union, it will enter into force 20 days later. However, its application will be extended for another 12 months for titles related to the issuance of *stablecoins* and 18 months for the rest of the titles, including obligations for crypto asset service providers.

According to its explanatory statement, it is intended that this regulation, although it does not contain specific AML requirements, does affect the requirements for the prevention of money laundering and financing of terrorism. Providers of certain services included in its scope, who are obligated subjects of AML in accordance with the specific sector regulations of this area, must comply with these requirements. These providers will need to prove compliance with AML requirements (i.e. having an appropriate AML programme) as a prerequisite for granting the European license regulating MiCA.

The truth is that MiCA legislators have opted for a sophisticated and ambitious legislative technique, which aspires to maximum regulation. Although from the point of view of legal certainty, it is possible that this approach adds rigor and security to the system, it also adds a greater degree of difficulty for compliance than if a minimum regulation had been chosen.

Another element to highlight consists of the definition provided by MiCA of the concept of crypto asset. That is, "a digital representation of a security or right that can be transferred and stored electronically, using distributed ledger technology or similar technology." In this case, a broad definition has been chosen, which includes any type of digital representation that can be transferred digitally with the aim that the technological evolution of crypto assets, to the extent possible, remains covered by this definition.

Another thing to note is that even having included different types of crypto assets, the regulatory body focuses mainly on cryptocurrencies and their operations. Even though it is true that these are the most widespread crypto assets, they are not the only type of digital asset that can be used for illicit activities or, specifically, for money laundering.

Therefore, in practice, it is possible that part of the illicit activity is concentrated in other types of crypto assets.

National focus: virtual currencies

Even with the evolution of crypto assets and their regulation at the international and community level, in Spain the regulations that regulate crypto assets in relation to AML are still incipient. And yet Spain is one of the most active countries in this field: according to a report from the Bank of Spain[18], the volume of transactions with crypto assets in 2021 in Spain was 60,000 million euros, being the fifth country with the highest number of transactions after the United Kingdom, France, Germany and the Netherlands, and ahead of Switzerland and Italy. For all the more reason, this regulation is necessary.

The first definition of the term "crypto asset" in Spanish regulations was included in Circular 1/2022 from January 10 of the National Securities Market Commission, which came into force on 17 February 2022, being quite late[19].

However, the community legislator, more alert about the magnitude of this phenomenon, already introduced in 2018, as mentioned above,

[18] Bank of Spain (2022). Financial Stability Report. Spring 2022. Section E crypto assets.
[19] This Circular defines cryptoasset as the "digital representation of a right, asset or value that can be transferred or stored electronically, using distributed ledger technologies or other similar technology".

a mention of virtual currencies in the Fifth AML Directive, thus hoping that countries would transpose it.

The Spanish legislator, through Royal Decree-Law 7/2021 from April 27, transposing European Union directives on competition, prevention of money laundering, credit institutions, telecommunications, tax measures, prevention and repair of environmental damage, displacement of workers in the provision of transnational services and consumer protection, modified Law 10/2010 from April 28 on the prevention of money laundering and the financing of terrorism (the "LAML") indicating that this modification highlighted "the incorporation of new obligated subjects and, in particular, the submission to preventive obligations of people who provide virtual currency exchange services for legal tender."

Therefore, even without addressing the concept of crypto assets, the LAML, by the directive of the European co-legislators, goes ahead of other areas of Law by defining what is the most used type of crypto asset: virtual currencies. This inclusion is significant since it highlights that, rather than regulating its issuance or its nature in general, it was necessary to anticipate this phenomenon in terms of AML given the risk that it could entail in relation to the crimes of money laundering and financing of terrorism.

For these purposes, the LAML indicates that a "virtual currency" is "that digital representation of value not issued or guaranteed by a central bank or public authority, not necessarily associated with a legally established currency and that does not have the legal status of currency or money, but which is accepted as a medium of exchange and can be transferred, stored or negotiated electronically." This definition, unlike those that we have been able to analyze in the first section of this work, is built on negative premises, that is, what a virtual currency is not: it is not guaranteed by an authority, it does not necessarily have a legally associated currency, it does not have the legal status of currency or money...

The elaboration of this definition based on a negative construction provides very little legal security since we cannot know, with the premises provided, what a virtual currency is, only what it is not and given the rapid technological advance, it may become obsolete or cause certain practical inaccuracies that make the practical application of AML regulations difficult.

Likewise, the LAML, after the modification incorporated by Royal Decree-Law 7/2021, introduced "providers of virtual currency exchange services for fiduciary currency and custody of electronic wallets" as obligated subjects for the purposes of complying with the obligations required in terms of AML (identification of clients, application of due diligence measures according to risk...), which reduced the ML risks that may arise from these businesses.

For these purposes, the exchange of virtual currency for fiduciary currency will be understood as "the purchase and sale of virtual currencies through the delivery or receipt of euros or any other foreign currency of legal tender or electronic money accepted as a means of payment in the country in which that has been issued" and for electronic wallet custody services "safeguarding or custody services of private cryptographic keys on behalf of its clients for the holding, storage and transfer of virtual currencies." It should also be added that for the purposes of AML, these suppliers are considered financial entities, thus not being able to benefit from some of the exceptions stipulated in relation to compliance with internal control standards.

Along these lines and with the aim of controlling providers of virtual currency exchange services for fiduciary currency and custody of electronic wallets, the LAML itself requires that the latter, when they want to offer or provide these services in Spain, register in a registry established for these purposes in the Bank of Spain, under penalty of a fine of up to 10 million euros if the corresponding registration is not made.

To grant registration, the Bank of Spain, with the participation of SEPBLAC in the verification procedure, verifies the existence and adequacy of prevention procedures and bodies (including the AML manual, structured procedures, risk analysis), so that, to a certain extent, greater compliance with the AML obligations imposed on regulated entities is being guaranteed.

Taking these instructions into account, the registry of the Bank of Spain, which was enabled at the end of 2021 in compliance with the requirements of the Fifth Directive, should cover all providers who, regardless of the location of the recipients of their services , acted in Spain (with or without establishment) and met the requirements of commercial and professional honorability after the suitability examination. In this way, minimum standards are guaranteed regarding the suppliers that intervene in the Spanish market.

However, the Bank of Spain warns about the depth of this analysis, announcing on its website that "registration in this registry does not imply any approval or verification of the activity carried out by providers of virtual currency exchange services by fiduciary currency and custody of electronic wallets by the Bank of Spain." This is a somewhat more formal examination that does not guarantee the security of the system to investors, not only due to the risk of ML, but also the intrinsic risk of operating with virtual currencies, risks of a technological nature, information transparency, financial supervision, among others.

In relation to the AML requirements for the correct registration of suppliers, in practice it requires the creation of procedures and systems that guarantee the application of enhanced due diligence measures if operating with virtual currencies that, due to their technical characteristics, may particularly favor anonymity. It also requires the implementation of measures that can prevent the use of crypto mixers or cryptocurrency mixers (services that enhance the anonymity of transactions by making it difficult to identify the origin and destination of assets) or special measures that take into account the greater risk that unhosted wallets carry. In this way, and despite the warning included on the Bank of Spain's website and that the latter does not supervise risks of another nature (such as financial or operational or security), we can appreciate how some measures are being implemented and considerable efforts are made to ensure minimum AML compliance. This is easily noticeable since in November 2022 of all the applications submitted more had been

rejected than accepted[20], among other reasons, due to AML issues and on 21 April 2023 there were only 66 registered suppliers[21].

This examination seems to go further, since, in the context of the processing of the bill that creates the Independent Administrative Authority for the Defense of the Financial Client for the extrajudicial resolution of conflicts between financial entities and their clients, an amendment[22] has been registered that proposes adding a new final provision to the LAML indicating that the Bank of Spain will require providers of virtual currencies to present a report from the Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offenses (SEPBLAC) at their registration, thus reinforcing the prominence of AML in the controls carried out on these suppliers. According to the justification provided for including this amendment, it is alleged that the providers of this type of services are not under continuous supervision by the Bank of Spain and that this measure is essential for a correct assessment of AML obligations.

In relation to the activity of providers of virtual currency exchange and custody services in matters of AML once the others are duly registered, in the SEPBLAC report for 2020-2021[23] it is indicated that "(i)n 2021, providers of virtual currency exchange services for fiduciary currency and custody of electronic wallets acquired the status of obligated subjects (new letter z) according to the Law 10/2010 from April 28, introduced by Royal Decree-Law 7/ 2021 from April 27, and they have sent ten communications." It is true that 10 communications are really few compared to more than 5,000 made by banks, more than 1,500 by payment entities or more than 500 made by electronic money entities. However, these providers became obligated subjects that same year, so the figure is not representative of the level of

[20] https://cincodias.elpais.com/cincodias/2022/11/26/mercados/1669463316_436379.html
[21] Data from the Bank of Spain Registry as of April 21, 2023.
[22] Amendment number 257. Official Gazette of the Cortes Generales from 31 March 2023, series A, number 134-5, page 208
[23] https://www.sepblac.es/wp-content/uploads/2022/12/Memoria_Sepblac_2020-2021.pdf

compliance with the obligations of these obligated subjects in matters of AML.

Likewise, and in relation to sanctions, as of today we do not have data available on possible requirements or sanctions imposed on these suppliers by SEPBLAC. However, in the coming years we will be able to have a greater vision of this point. This sanctioning power and the figures that are extracted from it on an annual basis are of great interest to know: firstly, what is the degree of compliance of these obligated subjects and, secondly, what is the degree of pressure that the supervisor is exercising over them to guarantee compliance with their obligations regarding AML. This has been notable in other jurisdictions such as the United States, a country that has used sanctions to prioritize AML compliance among the agents of this phenomenon.

Despite this, Spain (through the Civil Guard) has already participated in some operations to stop criminal activities linked to crypto assets. An example of this is that on January 18, 19 and 20 of this year, a coordinated operation was carried out in France, Portugal, Cyprus, the United States and Spain, led by Europol, in which 18 million euros in cryptocurrencies were seized and accounts associated with Bitzlato were blocked for an amount of more than 50 million euros[24].

Having said all the above, all these measures and legislative reforms are only limited to the providers of two specific services in relation to virtual currencies, excluding many other services (such as, without going any further, the issuance of these currencies) and many other types of crypto assets, so it is a partial response to this phenomenon. However, we cannot help but positively value the legislator's efforts to try to find agile solutions to the ML risks detected in this growing sector.

Even though it is not an AML regulation, it is worth making a brief mention of the new Law 6/2023 from March 17 on Securities Markets and Investment Services, which has significantly established the regulatory landscape of crypto assets in Spain. For these purposes, it is indicated that the CNMV will be the competent authority for supervising compliance with the (EU) Regulation relating to crypto asset markets; a regime of infractions and sanctions for non-compliance is established; and, in addition, registered negotiable

[24] https://www.interior.gob.es/opencms/ca/detalle/articulo/La-Guardia-Civil-participa-en-la-desarticulacion-de-uno-de-los-principales-exchange-de-criptodivisas-utilizado-por-el-cibercrimen/

securities or represented by systems based on decentralized ledger technology are regulated.

In fact, there is more: the CNMV, in its activity plan for 2023[25], has announced that it will create a Money Laundering Prevention Unit, demonstrating that, although it is not a supervisor focused primarily on AML, it has understood the importance of the latter in operations with crypto assets and other negotiable securities.

Finally, it should be noted that in the coming months and years, the national legislative panorama regarding crypto assets, in general and also in particular in relation to AML, will be widely transformed as we must not forget that MiCA is a Regulation (and not a Directive). These types of legal instruments are applied directly in the Member States after their entry into force, without the need to resort to transposition (as was the case with the modification of the LAML in 2021), and an effort must be made in Spain of adaptation at both the regulatory and supervisory levels in the coming months.

[25] https://www.cnmv.es/DocPortal/Publicaciones/PlanActividad/Plan_Actividades_2023.pdf

Conclusions

Great regulatory advances, but are they enough?

European legislators have made a great regulatory effort in recent years to shed light on what until now completely lacked a regulatory framework. However, as is the case in almost all areas, real life almost always moves much faster than any regulatory effort. This implies that the regulation that is being published and is pending issuance in the short term will become obsolete in a short time. The adaptation effort will be continuous and frenetic, but it will reach a certain stability when the time comes.

Until then, we envision a reality divided between those operators who will do their best to scrupulously comply with the regulation, and those who, on the contrary, take advantage of the gaps caused by technological advances to avoid having to make investments in the improvement and implementation of AML programs with a "check-the-box" approach and thus continue operating with lax or non-existent controls.

The fundamental role of the supervisor

The correct implementation of the new regulatory framework for crypto assets in terms of AML must necessarily be accompanied by the *enforcement* of these requirements, precisely to avoid a "check-the-box" approach by market operators. To achieve a true risk-based approach, as required by FATF, it is therefore necessary for AML supervisors to include the phenomenon of crypto assets in their agendas as a priority to supervise.

While it is true that much of the regulation on this matter is recent and that operators will need an adaptation period to implement their AML frameworks, supervisors will have a fundamental role in ensuring that the measures adopted to prevent financial crime are correct and effective for the purpose they pursue. Furthermore, this is reinforced by the fact that, as opposed to lengthy legislative processing processes, the supervisor, within the regulatory framework, can identify and pursue with agility and speed new practices that may threaten the security of the financial system, thus being able to provide a response, at least partial, to technological advance.

Public-private collaboration as a key tool for AML in the blockchain world.

Spaces for collaboration and coordination between public and private operators are one of the topics that has acquired a leading role in the European Commission's legislative package as a mechanism to prevent financial crime. This collaborative model has made great progress in some European countries, such as the Netherlands, but it remains a pending issue in other Western jurisdictions.

If this collaboration is essential in the fiat world, it is even more so in an environment as fast and changing as blockchain. The private sector faces AML threats and risks on a daily basis, but it needs the guidance, focus and panoramic vision that only the supervisor has. This is why it is highly recommended that both sides (public and private) prioritize constant and fluid conversation between them, exchanging good practices and new typologies, so that the prosecution of infractions and criminal operations is truly effective.

Disclaimer: The opinions contained in this article are solely the personal opinions of the authors and do not necessarily reflect the views of their employer.

Executive Summary

The appearance of crypto assets, without a doubt, has caused a true revolution in many industries and has been a turning point for the financial sector. They have generated the emergence of many opportunities, but also some challenges and threats such as the use of this technology by criminals with the aim of money laundering or financing terrorism ("ML").

Some of the intrinsic characteristics of crypto assets facilitate the commission of this type of crime. For example, the anonymity of crypto assets makes it difficult to trace the origin and destination of funds. Decentralization prevents the existence of an entity that applies due diligence measures to users in the crypto world. The irreversibility and speed of transactions carried out with crypto assets can make useless some of the mechanisms, for example, embargoes, usually used in the traditional world to prevent money laundering and financing of terrorism ("AML").

Despite all of the above and even knowing that legislative and regulatory development has not been able to keep up with the pace set by technology in terms of adaptation times, we have been aware at all times of the need to reinforce existing systems and adapt as best as possible as threats emerged.

In this way, the obligated entities, supervisors and legislators, as key actors in the AML ecosystem, have been forced to advance by leaps and bounds in the development of new policies and tools that would allow restricting the use of new technologies as laundering tools.

In this way, not only are the threats that arise from crypto assets being better controlled by better understanding the technology and its implications, but also new technologies are becoming a strategic partner for AML through the use of Machine Learning or Big Data in the creation of tools.

Taking all the above into account, it is worth to briefly analyze what is being done from the international, community and national perspective:

- At the international level, FATF was the first organization to identify the imminent need to establish preventive measures in this area, modifying the so-called *Travel Rule* (Recommendation No. 16) in 2019 to incorporate the so-called Virtual Asset Providers or "**VASPs**" (including crypto assets). The *Travel Rule* implies that identifying information about the originator and beneficiary of the transactions is shared, and that this information travels in the payment chain from beginning to end. Although the FATF Recommendations are not legally binding, many countries adopt them and incorporate them into their national legislation and it is also worth highlighting the importance that this issue has in the debates held today in the FATF plenaries, and that it has been agreed to develop an action plan to guarantee greater security in matters of crypto assets.

- At the community level, the EU modified the so-called Fifth Directive to include as obligated subjects providers of virtual currency exchange services and providers of electronic wallet services (leaving out providers of exchange services of a virtual currency for another). Likewise, currently, a new legislative package on AML is being processed, and it will be extended to all crypto asset service providers, including those operating outside the European Union, and also to providers of virtual

currency exchange services, thus covering the existing gap in the current European AML regulation. Furthermore, in relation to this legislative package, (EU) Regulation 2015/847, relating to information accompanying fund transfers, will be amended, with the aim to guarantee full traceability of transfers with crypto assets through collection and access for all participants in the payment chain to the identifying data of the payers and beneficiaries in a transfer. Finally, it is worth mentioning the approval of MiCA which, although does not contain specific AML requirements, does affect the requirements for the prevention of money laundering and financing of terrorism that providers of certain services must comply with.

- At the national level, the regulations that regulate crypto assets, in general and in particular in relation to AML, are still incipient, even though Spain is one of the most active countries in terms of the volume of transactions with these instruments. In 2021, Law 10/2010 from April 28 on the prevention of money laundering and the financing of terrorism was modified with the objective of including "the incorporation of new obligated subjects and, in particular, the submission to the preventive measures of persons who provide services for exchanging virtual currency for legal tender" thus focusing, as at the European level, on one of the most famous types of crypto assets: virtual currencies. Likewise, these suppliers were required to register in a registry established for these purposes at the Bank of Spain. To grant registration, the Bank of Spain, with the participation of SEPBLAC in the verification procedure, verifies the existence and adequacy of prevention procedures and bodies.

As main conclusions, we can extract the following:

- European legislators have made a great regulatory effort in recent years to shed light on what until now completely lacked a regulatory framework. However, as is the case in almost all areas, real life almost always moves much faster than any regulatory effort. This implies that the regulation that is being published and is pending issuance in the short term will become obsolete in a short time. The adaptation effort will be continuous and frenetic, but it will reach a certain stability when the time comes.
- The correct implementation of the new regulatory framework for crypto assets in terms of AML must necessarily be accompanied by the *enforcement* of these requirements. To

achieve a true risk-based approach, as required by FATF, it is therefore necessary for AML supervisors to include the phenomenon of crypto assets in their agendas as a priority to supervise.

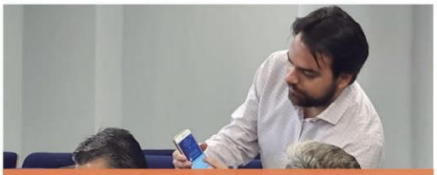
- Spaces for collaboration and coordination between public and private operators are one of the topics that has acquired a leading role in the European Commission's legislative package as a mechanism to prevent financial crime. This collaborative model has made great progress in some European countries, such as the Netherlands, but it is still a pending issue in other Western jurisdictions.

BLOCKCHAIN INTELLIGENCE
BI BLOCKCHAIN LAW INSTITUTE Abogacía Española CONSEJO GENERAL

CURSOS CERTIFICADOS BLOCKCHAIN

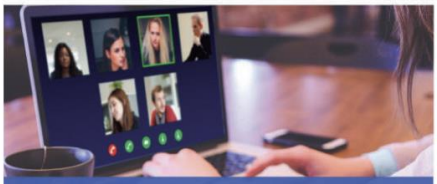
CURSO
EXPERTO LEGAL Y COMPLIANCE
EN BLOCKCHAIN
VER CURSO

CURSO
CRIPTOACTIVOS Y CUSTODIA:
REGULACIÓN Y NEGOCIO
VER CURSO



CURSO
EXPERTO COMPLIANCE
EN BLOCKCHAIN
VER CURSO

CURSO
EXPERTO LEGAL
EN BLOCKCHAIN
VER CURSO



CURSO
BLOCKCHAIN
Y POSIBILIDADES DE USO
VER CURSO

CURSOS Y
WORKSHOPS
INHOUSE
MÁS INFO.

www.blockchainintelligence.es
info@blockchainintelligence.es