BLOCKCHAIN INTELLIGENCE

Abogacía Española
CONSEJO GENERAL

www.blockchainintelligence.es

Doctrinal article

THE ROLE OF COMPLIANCE IN BLOCKCHAIN, CRYPTO ASSETS AND THE NEW DIGITAL ECONOMY

AN APPROACH TO THE IMPACT OF BLOCKCHAIN TECHNOLOGY ON THE COMPLIANCE PROFESSION

ALMUDENA DE LA MATA MUÑOZ

UNIVERSITY PROFESSOR & PHD,
MANAGING PARTNER OF BLOCKCHAIN INTELLIGENCE AND
PRESIDENT OF BLOCKCHAIN INTELLIGENCE LAW INSTITUTE

JANUARY 2023

ARTICLE PUBLISHED IN AEAEC JANUARY 2023

The role of compliance in blockchain, crypto assets and the new digital economy.

An approach to the impact of blockchain technology on the compliance profession.

Dr. Almudena de la Mata Muñoz
CEO of Blockchain Intelligence and Blockchain Intelligence Law Institute.
Corresponding Academician of the Royal Academy of Jurisprudence and Legislation.
Director of Legal Expert and Compliance Certifications in Blockchain, Crypto Assets and Metaverses

---

Table of Contents

1. Blockchain and compliance today

1.1. The dual impact of Blockchain on the compliance function

The compliance function is being strongly affected by Blockchain technology. This impact is manifested in two very different ways. On the one hand, Blockchain has created new economic and social operations and generated new digital assets (crypto assets, cryptocurrencies, NFTs, etc.) and new contracting spaces such as metaverses, which must comply with the applicable regulations and be subject to control by compliance units.

On the other hand, Blockchain offers very valuable tools for exercising the compliance function itself. It is an optimal technology for reliable management of records and databases and improving the traceability and auditability of actions and processes that help to identify non-compliance and define responsibilities. Blockchain also enables the development of multiparty processes based on decentralised trust and the automation of processes via smart contracts and tokenisation. In this way, the involvement of various business units in compliance processes is encouraged.

In addition, this technology enables the creation of incentives to encourage internal compliance with regulations, internal policies and whistle blowing through tokenisation systems.

1.2. The new digital operations on Blockchain, subject to control by regulatory compliance units.

Since the founding of the Blockchain Intelligence Law & Compliance Institute more than 5 years ago, we have witnessed a growing demand for specialised personnel and knowledge of Blockchain in the field of regulatory compliance.

Undoubtedly an important sector of activity takes place in the financial environment, in both traditional and technological entities and FinTechs and companies related to crypto activity such as exchanges, investment funds or NFTs platforms or DEFI (decentralised finance) investment products. As operations in this field have increased, there has also been growing concern about the possible use of these financial products and operations for the development of criminal activities or financial crime.

This concern has attracted the attention of regulators and supervisors in the different jurisdictions and has given a certain legal framework to the prevention activities of compliance units. Thus, an important part of

this operation is framed in the establishment of KYC processes and prevention of money laundering and the financing of terrorism (AML/CFT) as well as compliance with financial sanctions. In short, risk-based control structures (risk-based approach) are established in constant collaboration with supervisors.

The high proportion of Blockchain-based projects that have been admitted to the various editions of the Spanish financial sandbox is striking, as it is indicative of the real and growing use of this technology in Spanish industry and the interest of public institutions in understanding its operation and encouraging the development of innovation in a controlled and sustainable manner.

In addition, compliance units have often been responsible for managing the relationship with the respective supervisors (Bank of Spain, CNMV or Directorate General of Insurance (DGS)).

But these are not the only compliance units that are specialising in Blockchain. Traditional companies in a wide variety of sectors are also training their staff in this technology for the management of related risks and the implementation of new systems adapted to their digital processes. Since the launch of the Blockchain Intelligence Legal and Compliance Expert Certification in Blockchain and Crypto Assets with the General Council of Lawyers, representatives of the compliance units of companies operating in the fields of insurance, retail, construction, real estate, energy, management, consultancy, the automotive industry, agricultural production, art galleries, football clubs, etc. have passed through our classrooms. The compliance control needs in these cases are very varied. Some companies operate with crypto assets or have invested in NFTs. Others use digital identity systems on Blockchain in their KYC processes. Some have chosen to seek funding through STOs or use Blockchain networks to better manage some of their multiparty processes. Several of them are using blockchain systems to enable remote participation and decision-making in

corporate governance bodies. Internal multiparty processes have also been developed on distributed databases, for example for treasury management or processes in which several companies are involved and whose data are managed in Blockchains or DLTs that facilitate traceability and control of the process. All this activity based on Blockchain technology requires control and compliance management. Still incipient, but of key importance, is the development of Blockchain-based metaverses in which an important digital contractual activity takes place and to which the European Union is devoting a significant effort to determine and mitigate the possible related risks.

In addition, Blockchain projects have been developed in the field of public administration to make its services more transparent and efficient. The use of Blockchain in the development of digital public administration solutions has made it necessary to involve the intervention and some internal compliance units of public bodies. An interesting example is the development of digital procurement systems on Blockchain, as is the case of the one implemented in the Autonomous Community of Aragon. On the other hand, there are numerous examples of public-private partnerships based on Blockchain applications, as is the case of the Cartagena port project.

1.3. Institutional support for the use of Blockchain technology to boost the economy and improve society.

This increase in activity on Blockchain technology in both the private and public spheres is being driven by the activity of European institutions. Since 2017, the European Union has implemented a roadmap with the aim of promoting the development and use of this technology as a key element for maintaining European competitiveness on an international level. This institutional activity is structured in three main lines of work:

- Development of specific regulations and criteria for legal interpretation, which we develop in the following section;
- Development of European Blockchain infrastructure laying the technological and regulatory foundations for the development of a fully secure digital society. In this sense, progress has been made in: a) the development of the European Blockchain network (EBSI), b) the creation of a digital means of payment issued by the European Central Bank (digital euro / cryptoeuro / CBDC) and c) progress in digital identity models and the creation of the EU ID Wallet or European digital identity wallet.
- Supporting the development of blockchain applications in the private sector through project funding mechanisms.

Already in October 2017, the Council of Europe asked the European Commission to take action on blockchain in order to better position the

EU geopolitically and economically on a global level. With this mandate, in February 2018 the Commission launched the European Blockchain Observatory and Forum[1] in order to identify relevant actors, technical, legal and market barriers and to foster the development of blockchain in the European environment[2]. In April 2018, 22 European countries, including Spain, signed a Declaration of Cooperation establishing the European Blockchain Partnership which aims to create a European Blockchain Services Infrastructure (EBSI) to facilitate cross-border exchange. Today, 30 countries (all EU countries plus Norway and Liechtenstein) are signatories to this declaration. Since then, important steps have been taken in the creation of this EBSI infrastructure, where relevant use cases are being implemented, such as projects aimed at achieving a common self-managed digital identity, facilitating the issuing of university degrees in blockchain or the development of a common social security number, the management of the recognition of the right to asylum for cross-border purposes also linked to the digital identity system, or the generation of a financing system for SMEs.

But the European institutions also strongly support private initiatives in Blockchain by investing through funding programmes and working to develop a clear legal and regulatory framework to enable the development of blockchain networks as well as blockchain-based products and services.

2. The evolving regulatory framework specific to blockchain, DLTs and crypto assets and its impact on the compliance function.

Regulators and supervisors have worked incessantly in recent years both to create a specific regulatory corpus and develop a supervisory activity appropriate to the new reality. In contrast to the legal vagueness of the early days in relation to the blockchain/crypto phenomenon, we now have greater regulatory clarity and clear obligations for compliance and registration in ad hoc authorised units.

The speed of the regulatory approach to Blockchain/DLT has been dizzying. In our European jurisdiction alone, important rules have been developed on crypto assets, money laundering and terrorist financing, securities regulation and tokenisation of financial instruments, regulation and development of digital identity and tax regulation. In this regard, it should be noted that we already have a specific regulatory

[1] EU Blockchain Observatory and Forum https://www.eublockchainforum.eu/
[2] Montaña Merchán and Angel Martín, The European Blockchain Service Infrastructure y el Desarrollo blockchain en el marco institucional europeo. Casos de uso [https://blockchainintelligence.es/the-european-blockchain-service-infrastructure-ebsi-y-el-desarrollo-de-blockchain-en-el-marco-institucional-europeo-casos-de-uso/].

body that helps to define concepts and taxonomy and understand the legislator's will regarding the protection of markets and social operations linked to the crypto and Blockchain phenomenon.

Thus, we already have explicit regulations, among which we highlight: (a) the Crypto Asset Markets Regulation (MiCA) (not in force), (b) EU Regulation 2022/858 on a pilot scheme for market infrastructures based on decentralised registry technology (Pilot Scheme) and its impact on the draft Securities Market and Investment Services Law, (unanimously approved in the Spanish Parliament last December), c) Regulation on digital operational resilience (DORA Regulation), d) the 5th Directive 2018/843 on the prevention of money laundering and its transposition into Law 10/2010 on the prevention of money laundering and terrorist financing (LPBC) through Royal Decree Law 7/2021 or e) the tax regulation of crypto assets accompanied by the Tax Agency's responses to consultations. Special mention should also be made of the publication of the EiDAS2 Regulation and the package of technological measures with which the EU aims to provide citizens and entities with digital identity tools such as the EU ID Wallet.

We also have guidelines, criteria and alerts from regulators and supervisors such as the CNMV, the European Securities Markets Agency (ESMA), the Bank of Spain, the European Banking Agency (EBA), EIOPA and the Data Protection Agency, and the creation of national and international standards related to Blockchain networks and applications continues. In this regard, it is worth highlighting the guides that European regulatory authorities have been producing for years on the adaptation of the regulation and supervision of certain phenomena, products or markets that have arisen as a result of the use of Blockchain. For example, the European Securities and Markets Authority (ESMA) published a document on the application of securities market regulations to crypto assets.

For its part, the European Banking Authority - EBA - in its report from 9 January 2019 also addressed the issue of crypto assets from the perspective of the application of financial regulations (e.g. on electronic money, payment services, prevention of money laundering and other regulations applicable to credit institutions).

Moreover, certain working groups are reflecting on the appropriate application of European legislation to this new phenomenon. One example is the effort that several groups are making on the application of the General Data Protection Regulation to the Blockchain reality. This is the case of the Art. 29 Working Party, Opinion 04/2014 on Anonymisation Techniques, 0829/14/EN, 20 which concluded that transactional data encrypted with hashing processes could be considered personal data in accordance with the Data Protection Regulation (GDPR).

At the international level, there is also collective work to develop common visions and coordinated activity to control the risks arising from the use of crypto assets. Thus, there is significant activity within structures such as the G20, the FSB, the BIS and, due to its particular impact on the compliance function, the role of the Financial Action Task Force (FATF), an intergovernmental body that establishes international standards with the aim of preventing global money laundering and the financing of terrorism, should be highlighted. FATF has been working on the phenomenon of virtual assets (VA) since 2014, issuing various recommendations and guidelines. On 28 October 2021 it published an updated Guidance to encourage the application of a risk-based approach in the treatment of VAs and virtual asset service providers (VASPs). It emphasises the need for countries, VASPs and other entities involved in virtual asset (VA) activities to understand the money laundering and terrorist financing risks arising from such activities and to take appropriate mitigation measures to manage those risks. The Guidance further discusses how AV activities and VASPs fall within the scope of the FATF Standards. It describes the types of activities included in the definition of VASPs and provides examples of such activities that would fall within that definition, as well as those that would potentially be excluded. In addition, the Guidance highlights the elements necessary to qualify as a VASP, which are (a) acting as a business for or on behalf of another person and (b) actively providing or facilitating activities related to virtual assets.

It thus provides the public and private sectors with guidance focused on six key areas: (1) clarifying the definitions of VA and VASPs to make clear that these definitions are expansive and there should not be a case where a relevant financial asset is not covered by the FATF Standards (whether as a VA or as another financial asset), (2) providing guidance on how the FATF Standards apply to stablecoins and clarifying that a number of entities involved in stablecoin arrangements could qualify as VASPs under the FATF Standards, (3) provide additional guidance on the risks and tools available to countries to address ML/TF risks in peer-to-peer transactions, which are transactions in which no obliged entity is involved, (4) provide updated guidance on the licensing and registration of automated payment service providers, (5) provide additional guidance to the public and private sectors on the application of the "travel rule", and (6) include principles for information sharing and cooperation between supervisors of automated payment service providers. This is a key document for the definition of internal control structures but also for the development of supervisory activity.

In short, at international, European and national level, a regulatory corpus and a taxonomy have been gradually shaped and they facilitate and justify the work of compliance officers in relation to DLT

infrastructures, crypto asset activity, the use of smart contracts and tokenisation, and the establishment of crypto asset service providers.

3. The relationship of compliance units with supervisors and specific records relating to blockchain / crypto operations.

Operations involving crypto assets (digital assets or virtual assets) are relatively recent and constantly evolving. Therefore, the prevention of risks related to these operations requires the cooperation of the actors involved with the supervisory bodies.

Within the framework of the applicable regulations, compliance and registration obligations have already been established, such as registration in the Bank of Spain's Register of virtual currency for fiat currency exchange and electronic wallet custody service providers, in accordance with the provisions of the Second Additional Provision of Law 10/2010 on the prevention of money laundering and terrorist financing (LPBC). Entry in this register is possible on two conditions: (i) the existence of adequate procedures and bodies for the prevention of money laundering and terrorist financing, and (ii) compliance with the requirements of commercial and professional integrity.

Until now, compliance units have generally been responsible for ensuring compliance with the obligations and managing access to this register. The establishment of procedures as well as the definition of decision-making bodies and structures in relation to the objectives of money laundering prevention have been the responsibility of compliance professionals who have been carrying out their task in collaboration with the business and internal technological units on the one hand and with the supervisory bodies on the other.

4. Risks, practices and compliance processes arising from blockchain and crypto use.

As we have seen, activity on Blockchain networks is very diverse. Each application will have its own compliance requirements and will generate specific risks that will be the focus of the compliance function.

In terms of regulatory risks, it is necessary to make an interpretation of the legal nature of the application in question in order to properly identify the associated risks and the applicable regulations. In this regard, it is advisable to be aware of the possible evolution of the legal nature of digital assets or legal transactions, in which case different rules will apply to them over time. This is specified by the EBA in its 2019 guidance. This implies that the compliance function should remain active throughout the life of the legal business or technological application and be the guarantor of compliance beyond the initial management.

In addition to the management of risks linked to the applicable regulations, there are also reputational risks, and it is necessary to develop procedures to identify and mitigate this type of risk. The decentralised nature of Blockchain operations often makes it difficult for compliance officers.

The first level of risk is linked to the type of Blockchain or DLT network in which the application is developed. There are important differences between public, private or public-permissioned networks with fundamental implications on issues such as: a) sustainability, b) definition of the applicable jurisdiction, c) responsibilities of the parties, d) identification of the nodes that make up the network and e) maintenance of the network's operability and risks linked to the possible termination of the network.

The second level of risks is related to the legal business developed on the Blockchain and its constituent elements (identity, agreement of the parties, electronic contracting and fulfilment of obligations using tokenisation or cryptocurrencies/crypto assets).

Especially financial institutions, FinTechs and crypto companies have developed a compliance control and risk mitigation practice specific to crypto asset activity. The most imminent risks in this environment relate to the use of cryptocurrencies or crypto assets for criminal activities, money laundering or terrorist financing as well as evasion of sanctions compliance or interaction with PEPs. Also recently, the use of cryptocurrencies or crypto assets in the context of international conflicts such as the war in Ukraine has opened up a new area of geopolitical and cybersecurity risks.

To prevent criminal use or non-compliance with applicable regulations, compliance units have been introducing changes to their systems for monitoring money laundering, terrorist financing and sanctions. They have expanded control requirements in their KYC operations and introduced digital tools to control crypto transactions.

One of the biggest challenges for compliance units in the control of crypto assets is the definition of the applicable jurisdiction. Another challenge is the provision of sufficient technological know-how to be able to identify transactions involving digital assets that pose a risk to the institution. For this reason, monitoring is often outsourced to specialised external companies.

5. Fight for compliance-blockchain-crypto talent and new digital tools for the compliance function.

The risks associated with the new digital operations require talent specifically trained in the technologies that are in real use in the business environment. The growing use of digital assets and Blockchain-based applications, far from being an area of high specialisation or a one-off market boom, is evolving into a growing, standardised, and transversal operation. As we have seen, practically all sectors of the economy are affected by the new digital tools. The future of the economy is eminently digital and Blockchain is precisely the technology that makes it possible to create markets without any analogue intermediation in which the parties not only meet and negotiate but also achieve the perfection of the legal business and its automatic and digital execution. Forecasts therefore point to Blockchain, web 3.0 and metaverses as the new contracting environments. With this growth in digital operations, the risks of fraud, regulatory non-compliance and reputational risks are also increasing, and the role of digital compliance is absolutely key to the sustainable development of this new economy.

In case the business is developing a Blockchain application (e.g. issuance of a cryptocurrency, development of a metaverse or international trade management platform, creation and sale of an NFT, etc.), the compliance unit should be integrated in the development team to achieve a "compliant by design" result. On other occasions,

organisations buy or use Blockchain solutions from the market for better business management or use or invest in Blockchain-based assets (crypto assets). In this case, there are also risks that the compliance function must identify and that will help the business to make a decision on the product or negotiate with the suppliers possible adaptations (technical or contractual that mitigate or eliminate the possible risks).

In addition, compliance units are increasingly using Blockchain-based digital tools to improve their own departmental operations. These include:

- Maintenance of databases in blockchain/DLT networks in order to ensure transparency and traceability as well as to be able to share data in multiparty processes. This is the case of tools for storing minutes of meetings or decision-making in order to have clarity on the accountability of the parties involved.
- Use of digital tools for digital participation in decision-making bodies.
- Creation of incentives via tokens to encourage compliance with internal policies.
- Specific tools for compliance with regulatory obligations, such as the establishment of whistle blowing channels.

We are currently in a fierce search for digital compliance talent. Our job board and Head Hunting function receives continuous requests for compliance officers and lawyers with expertise in cryptocurrencies, privacy and money laundering in the crypto environment and digital transformation of compliance units. These professionals work directly with the business in the design of solutions and are also key in the choice of third party applications containing Blockchain elements of automated contracting and maintenance of databases focused on monitoring and auditing.

6. Skills required in digital compliance positions.

Compliance professionals need to understand how blockchain technology works, its uses and applications in order to identify applicable regulations, comply with regulatory requirements, map risks and related mitigants, and use digital tools to improve the efficiency of the unit.

Both in the case of Blockchain application development and in the choice of Blockchain solutions on the market, it is first necessary to understand the different types of networks and how they work (especially the consensus and governance mechanisms of the networks). This will have important implications in terms of the responsibility of the parties, project viability and possible contractual requirements, operational and reputational business risks.

It will also be necessary to understand the possible applications running on these networks (cryptocurrencies or crypto assets, tokenisation, smart contracts, or digital identity) and the specific business operations linked to them (custody, currency exchange, decentralised finance (DEFI), use of tokenisation in metaverses, etc.).

The "new generation" compliance officers must be familiar with Blockchain operations and, of course, know not only the regulations applicable to this reality but also the criteria of regulators and supervisors. Sometimes it is necessary to anticipate solutions to prevent the fast and bold digital market from generating unwanted social risks (risk-based approach). In this sense, compliance units are excellent allies for supervision and are key to the sustainable and solid development of the business.

Beyond the regulatory framework, it is essential that compliance officers use the digital tools that are the object of their control. For this reason, the Blockchain Intelligence certification accompanies all the learning modules with practical laboratories in which compliance officers and lawyers use the Blockchain networks and applications that they will be monitoring. In fact, they use wallets, receive crypto assets, use digital identity wallets and analyse the related privacy issues, program a Smart contract, mine an NFT, etc. We have also developed the first space in the metaverse where students interact and use their avatars, NFTs and wallets. Let's remember that the future of contracting and human relations will happen mainly in metaverses and therefore

they will be spaces in need of identification and risk control. Finally, the students stamp their certificate in Blockchain and obtain the token that proves their attendance (POAP). In this way, we achieve full immersion and understanding of the technology and can identify how to develop a compliance strategy and procedures as well as use the digital tools that facilitate the activity itself.

The future of digital recruitment will definitely be linked to Blockchain technology, and we therefore consider it to be a key element for the development of the profession.