

Spain

José F Canalejas Merín*
Gómez-Acebo & Pombo, Madrid
jfcanalejas@ga-p.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

Fintech is not expressly regulated in Spain and a neutral technology principle has been adopted, following the European approach. Therefore, fintech is only currently subject to any laws of general application and certain pieces of regulation that have been passed in recent years to update and adjust the legal framework. Within these regulations, different measures have been adopted to promote and enable fintech to develop its activities, as well as to address the challenges and risks connected with digital transformation.

After the 2018 Fintech Action Plan, in September 2020 the European Commission adopted a comprehensive package on digital finance, including several strategies and legislative proposals on crypto assets and digital resilience. The implementation of the financial package has been a major step towards the comprehensive regulatory framework for financial services that will support the rise of fintech and the modernisation of the European economy across all activity sectors.

Digitally active users, market conditions and an innovation-friendly environment allow the Spanish market to be considered very attractive for the development of fintech businesses. As stated above, steps towards the due implementation of a legal framework that will foster these activities have already been taken. For instance, crowdfunding activities have been regulated in Spain since the approval of Law No 5/2015 of 27 April on Promotion of Business Finance, and a regulatory sandbox was implemented by Law No 7/2020 of 13 November on Digital Transformation of the Financial System.

Furthermore, in December 2022, Law No 28/2022 to promote the startup ecosystem was approved. After the approval of the mentioned startup law, measures and incentives to promote the competitiveness of the Spanish economy have been incorporated into the Spanish legal system, including simplified procedures for the creation of new companies and tax incentives to attract entrepreneurs and highly qualified employees.

Finally, it is important to bear in mind the draft bill on the digitalisation and modernisation of the financial sector, which aims to ensure that the Spanish legal framework remains at the forefront of financial regulation. The fundamental objective of this law will be to maintain Spain's position as a leader in financial regulation by adapting to technological advances and fostering innovation. The draft bill proposes actions in four main areas: cyber resilience, crypto assets, payment services and the regulatory sandbox.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

As indicated, Spanish and European law on financial services are guided by the principles of 'same activities, same risks, same rules' and of technology neutrality. Therefore, crypto assets that fall under existing regulation on financial services are subject to such rules, regardless of the technology used for their issuance or their transfer.

* José is a counsel in the Banking and Finance Department at Gómez-Acebo & Pombo. His practice focuses on structured finance, capital markets, financial regulation and fintech. José works on a regular basis with local and international credit institutions, e-money institutions, payment institutions, investment funds and other financial institutions in Spain, having participated in some of the most important and complex transactions in recent years.

Crypto assets that do not qualify as financial instruments are subject to Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets (MiCAR), which provides a new bespoke regime for all crypto assets not covered in EU financial services legislation and crypto asset service providers. The entry into force of MiCAR has marked a turning point in these markets.

Please note that MiCAR applies, among other, to certain stablecoins, specifically those classified as asset-referenced tokens (ARTs) and e-money tokens (EMTs).

- ARTs are stablecoins that maintain their value by referencing a basket of assets, such as several fiat currencies, commodities, or other crypto assets.
- EMTs are stablecoins that maintain their value by referencing a single official currency, such as the euro or the US dollar.

According to a No Action letter issued by the European Banking Authority (EBA), it is necessary to avoid a dual authorisation under two pieces of EU law for the activity of transacting EMTs. While the existing Payment Services Directive 2 (PSD2) still applies, national competent authorities should enforce authorisation of PSD2 for a specified subset only of crypto asset service providers that transact EMTs.

MiCAR explicitly excludes central bank digital currencies (CBDCs) from its scope. Therefore, the prospective digital euro is not subject to this regulation. The digital euro project is a strategic initiative by the Eurosystem to safeguard the role of central bank money in a rapidly digitalising economy. In 2021, the Eurosystem embarked on the investigation phase which it developed a high-level product design and the related functional and non-functional user requirements for a digital euro. The issuance will depend on the outcome of such phase and require a formal decision by the European Central Bank's Governing Council, as well as the adoption of the necessary legal framework at the European level. The European Commission has proposed a legislative framework for the digital euro, but it is still under discussion within the EU legislative process

The EU DLT Pilot Regime Regulation also establishes the conditions for permission to operate a distributed ledger technology (DLT) market infrastructure, the DLT financial instruments that can be admitted to trading and settled on the DLT, and cooperation between the DLT market operators, competent authorities and the European Securities and Markets Authority (ESMA). Since the approval of the EU DLT Pilot Regime Regulation did not imply a modification of book entry form requirements applicable in Spain, the Spanish government approved a new securities markets law (Law No 6/2023) which includes, among others, the rules applicable to registration, transmission and representation of DLT securities.

After the registration in the administrative records of the Spanish National Securities Market Commission (CNMV) of the first entities responsible for the management of the registration and record-keeping of negotiable securities in systems based on DLT, the first issuances of bonds and shares using these technologies have taken place, in accordance with the provisions of Law No 6/2023.

Once all the tests of the project in the regulatory sandbox created by Law No 7/2020 were completed, the authorisation of a trading and settlement system (SNL) based on DLT in Spain

represents a highly significant milestone, as it is one of the first market infrastructures of this kind to be authorised in the EU.

Finally, Spanish tax authorities have outlined the tax treatment of activities related to crypto assets; the Spanish Finance Ministry has also approved the form to be filled in by Spanish taxpayers who hold crypto assets – with a minimum value of €50,000 – abroad (Form 721). Please note that the disclosure obligation applies from 1 January 2024.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets

The legal framework applicable to payment institutions and service providers operating in Spain mainly comprises Royal Decree-law No 19/2018 of 23 November on payment services and other urgent financial measures, and Royal Decree No 736/2019 of 20 December on the legal regime of payment services and payment institutions. These Spanish payment regulations implemented PSD2 which, among other things, aims to make payments more secure in Europe, to boost innovation and to adapt payment services to newly developed technologies.

Likewise, Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009, on the taking up, pursuit and prudential supervision of the business of electronic money institutions (E-money Directive) was implemented by Law No 2/2011 of 26 July on e-money, and Royal Decree No 778/2012 of 4 May on the legal regime of e-money institutions. Payment institutions and e-money institutions ought to be authorised by the Banco de España (BdE), as the competent authority in Spain to carry out their activities.

For this purpose, the relevant application shall be submitted to the BdE together with:

- a programme of operations;
- a business plan;
- evidence of the initial capital;
- a description of the measures taken for safeguarding payment service users' funds;
- a description of the governance arrangements and internal control mechanisms;
- several procedures; and
- information on the management bodies and the shareholders.

Please note that the BdE follows the EBA Guidelines on the information to be provided for the authorisation of payment institutions and e-money institutions, and for the registration of account information service providers (EBA-GL-2017-09).

4. Special support for fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

In 2016, the CNMV created an 'innovation hub' under the name of Portal Fintech on its official webpage. This innovation hub aims to: (1) provide support to developers and financial institutions on regulatory aspects of securities markets that might affect their projects; (2) create an informal space where developers and financial institutions can share their initiatives in this field; and (3) generate criteria on certain relevant fintech issues in the securities markets.

Furthermore, the regulatory sandbox allows companies to test innovative products, services and business models in a live market environment while ensuring that appropriate safeguards are in place under the supervision of competent authorities. This tool deals with the issue posed by the most innovative financial companies: the complexity of financial regulations.

The sandbox operates under a cohort system, with two calls per year: one in March and the other one in September. The cycle of each of the cohorts involves a total of five phases:

- Presentation of requests for access: the Spanish Treasury shall convene a cohort by means of publishing a resolution on the same web page. Once the application period is opened, promoters have 30 business days to submit their projects.
- Prior evaluation: once the deadline for submitting applications has expired, the supervisory authorities will carry out a preliminary evaluation of the applications, for which they will have one month – a period that may be extended for an additional month.
- Negotiation of the test protocol: the list of projects temporarily admitted to the sandbox will be published. The promoters and the supervisory authorities shall agree on the conditions under which the activity will be carried out in the sandbox.
- Test period: it will begin once the protocol has been signed, the consent of participants in the test has been obtained and the guarantee system has been put in place.
- Exit from the sandbox: at the end of the testing period or during it, if necessary, promoters may request an authorisation to start the tested activity. Likewise, promoters are required to prepare a report evaluating the results of the test and the competent supervisory authority will publish a report of conclusions in this regard.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

European law has established an international regulatory framework and standard for the promotion of an open banking model. Consequently, Spanish law supports the transformation of retail banking from a vertically integrated model in which each credit institution performs all the activities comprising the value chain in an independent manner, into an open model in which credit institutions and other institutions work together and compete in each activity.

Payment initiation services (PISs) and account information services (AISs) are regulated under the Spanish legal framework within which: (1) users have the right to make use of services enabling access to account information to stimulate competition; (2) the development of new products and innovative offerings is enabled; and (3) customers may obtain high-value services.

Nonetheless, the European Commission was required to evaluate PSD2, in particular concerning charges, scope, thresholds and access to payment systems. The evaluation took place in 2022, including advice from the EBA, a general and targeted public consultation, and a report from an independent consultant. Following such evaluation, the European Commission decided to propose amendments to PSD2. The amendments will improve the functioning of EU payment markets by improving the functioning of open banking, especially as regards the performance of data interfaces, removing obstacles to open banking services and consumer control over their data access permissions. Therefore, further measures will be adopted to ensure the expansion from access to payment accounts data towards access to other types of financial data, moving from 'open banking' to 'open finance'.

6. Regulation of virtual asset service providers.

As indicated, MiCAR introduced a harmonised legal framework across the EU, requiring any legal person or undertaking whose occupation or business is the provision of one or more crypto asset services to clients on a professional basis – crypto asset service providers (CASPs) – to obtain prior authorisation from the competent national authority of their home Member State.

The following services and activities relating to any crypto asset are crypto asset services under MiCAR:

- providing custody and administration of crypto assets on behalf of clients;
- operation of a trading platform for crypto assets;
- exchange of crypto assets for funds;
- exchange of crypto assets for other crypto assets;
- execution of orders for crypto assets on behalf of clients;
- placing of crypto assets;
- reception and transmission of orders for crypto assets on behalf of clients;
- providing advice on crypto assets;
- providing portfolio management on crypto assets; and
- providing transfer services for crypto assets on behalf of clients.

Crypto asset service providers that provided their services in accordance with applicable law before 30 December 2024 may continue to do so until 1 July 2026 or until they are granted or refused an authorisation pursuant to Article 63 of MiCAR, whichever is sooner.

Nonetheless, Member States may decide not to apply the transitional regime for CASPs or to reduce its duration where they consider that their national regulatory framework applicable before 30 December 2024 is less strict than MiCAR.

The CNMV is the competent authority for supervising compliance with MiCAR in Spain. However, the Bank of Spain exercises supervisory, inspection, and sanctioning functions in relation to the obligations set out in MiCAR regarding issuers of EMTs and ARTs, in accordance with the 23rd additional provision of Law 10/2014, of 26 June, on the regulation, supervision and solvency of credit institutions.

7. AML and the Travel Rule in crypto asset transactions.

Under Spanish Law 10/2010 of 28 April on the prevention of money laundering and terrorist financing, virtual asset service providers (VASPs) are considered subject entities. Consequently, they must comply with all applicable anti-money laundering and counter-terrorist financing (AML/CFT) regulations in Spain. Key obligations include the following.

Risk-based approach

Subject entities must assess and document AML/CFT risks (by business line, product, channel, geography and customer) and calibrate controls accordingly, including the risk classification of customers and transactions.

Customer due diligence measures

- Identifying and verifying customer identity using reliable, independent sources. Due diligence levels (standard, simplified, or enhanced) are applied based on the customer or transaction risk profile.
- Identifying and verifying the ultimate beneficial owner (UBO), understanding the ownership and control structure of legal persons, and identifying any person on whose behalf a customer may be acting.
- Understanding the purpose and intended nature of the business relationship by obtaining sufficient information.
- Conducting ongoing monitoring of the business relationship and transactions, which includes scrutinising for consistency with the customer's risk profile and ensuring documents and data are kept up to date.

Reporting obligations

Subject entities must report suspicious transactions (STRs) to Sepblac (Spanish AML/CFT supervisor) on their own initiative and without delay. This obligation covers any act or transaction, including attempts, where a special review indicates potential money laundering or terrorist financing. Reports must be submitted using prescribed electronic formats.

Record-keeping

All customer due diligence files, transaction records, and supporting documents must be retained for a period of ten years.

Internal controls and organisation

Governance framework

- AML/CFT policies and procedures proportionate to risk, approved by the governing body.
- A designated representative to act as the point of contact with Sepblac.
- An internal control body or committee responsible for the implementation and oversight of AML/CFT controls.
- A technical prevention unit is also required if annual turnover exceeds €50m or the annual balance sheet total exceeds €43m. This unit must have specialised, exclusively dedicated personnel with appropriate analytical training.
- Group-wide controls and information sharing, consistent with data protection and AML rules.

Manual and risk catalogues

Maintain a written AML/CFT manual aligned with legal and regulatory requirements. This manual must include a catalogue of risk indicators, typologies, and procedures for detection, review, escalation, and reporting.

Training

Implement an annual training plan approved by the internal control body to ensure staff understand their obligations, and can detect and escalate unusual or suspicious activity. Evidence of participation must be kept.

Independent review

Conduct periodic internal audits of AML/CFT controls and compliance. Additionally, an annual external expert's review and report on the adequacy and effectiveness of these controls is required, including follow-up on remediation actions.

Regulation (EU) 2023/1113 introduced the 'Travel Rule' for crypto assets. As this is a directly applicable EU regulation, VASPs must incorporate its requirements into their AML/CFT policies. These policies must include procedures for collecting, verifying and sharing originator and beneficiary information for all crypto asset transfers to ensure traceability.

8. Enforcement and cross-border recognition of tokenisation and structuring of secured transactions involving crypto assets.

While there are contradictory doctrinal positions, it is not possible to link a crypto asset to another asset in such a way that transactions involving the underlying asset are automatically effected by the transfer of the crypto asset, unless this is expressly provided for by law.

Under Spanish law, security interests over movable assets must be created and perfected in accordance with the legal regime of the state where the asset is physically located. However, the *lex rei sitae* principle and territorial approach presents significant challenges when applied to crypto assets. Unlike traditional movable assets, crypto assets such as cryptocurrencies or tokens are inherently digital and decentralised. While Spanish law has been modified to allow the tokenisation of financial instrument and accommodate the existing frameworks, certain matters regarding property law, enforcement mechanisms and insolvency law may require further adjustments.

Spanish courts generally uphold the parties' choice of a foreign governing law in contracts involving crypto assets, in accordance with the EU Rome I Regulation. Nonetheless, this freedom is limited by mandatory local laws and public policy considerations, normally applying to mortgages on immovable assets and consumers. Foreign governing law clauses should be recognised for contractual obligations but cannot override Spanish property rules or procedural requirements.

Please be informed that direct appropriation of collateral by creditors, known as *pacto comisorio*, is prohibited under Article 1859 of the Spanish Civil Code. However, certain cases have allowed enabling the creditor to retain the collateral provided that an independent valuation is made and any excess value is returned to the debtor.

9. Litigation and jurisdiction on crypto assets: legal implications of disputes involving crypto assets.

Please note that Spanish courts apply the procedural rules in any litigation, which creates challenges and recurring issues related to crypto assets: choosing of court, evidence, and enforcing rulings on assets controlled by private keys.

Against that practical backdrop, the rules applicable to jurisdiction are set up in Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments (Brussels I bis) and the Organic Law No 6/1985 on Judiciary (LOPJ).

As general rule, a Spanish party's submission to a foreign court is legally binding and enforceable, provided it is validly agreed and does not trespass on exclusive fora. However, Brussels I bis and Spanish consumer law restrict pre-dispute forum selection. A standard clause in the platform's terms that forces all legal claims to a non-Spanish court will not deprive a Spanish consumer of the right to sue in Spain. Therefore, a jurisdiction clause may be binding for two companies in a issuance, but it may be ineffective against a Spanish consumer.

For judgments in civil and commercial matters from non-EU countries, recognition and enforcement is governed by applicable international treaties or, in their absence, by Spanish domestic law. Under Spanish law, these judgments require a formal proceeding (*exequatur*) before a Spanish court.

Normally, recognition of foreign judgement will be granted unless there are specific grounds for refusal, such as the judgment being contrary to Spanish public policy, a violation of fundamental procedural rights (such as the right to a defence), or if it conflicts with a prior Spanish judgment or Spain's exclusive jurisdiction.

10. Intellectual property and crypto assets: legal protection, ownership, enforcement and monetisation of IP rights related to digital and virtual assets.

In Spain, innovations related to crypto assets can be protected primarily through two intellectual property avenues: software and patents.

Software protection

From a copyright law perspective, software (computer programs) is protected in Spain through the Spanish Intellectual Property Law, which implemented the EU Software Directive. Under Spanish and EU law, software as such is not patentable; instead, it is protected as a literary work.

The source code, object code and documentation of a computer program are protected automatically upon creation, without requiring registration or other formalities. However, voluntary registration with the Spanish Intellectual Property Registry can serve as prima facie evidence of authorship and ownership in the event of a dispute.

Patent protection

From a patent law perspective, crypto-related technologies may be protected as computer-implemented inventions (CIIs) – inventions with features realised wholly or partially by a computer program – provided they meet the eligibility test under Article 52 of the European Patent Convention (EPC) and other patentability criteria such as novelty and inventive step.

For CIIs, the European Patent Office (EPO) has developed a 'two-hurdle approach' to assess patent eligibility and inventive step, which consists of three main steps:

- assessing the invention's eligibility under Article 52 EPC;
- determining whether a feature contributes to the invention's technical character; and
- assessing whether the invention involves an inventive step over the closest prior art.

Ownership of IP over crypto assets

In Spain, the determination of IP rights ownership varies slightly depending on the type of IP involved.

Ownership of software

For software, copyright initially belongs to the author: the individual who created the program. If a program is developed jointly, all co-authors hold the rights in common, unless otherwise agreed. These rights are transferable or licensable. In a dispute, the person or entity whose name appears on the work or in the Spanish Intellectual Property Registry is presumed to be the owner, unless proven otherwise.

A specific regime applies to software created by employees. When a program is developed by an employee or contractor in the course of their duties under an employment or service contract, the employer is generally entitled to the economic rights in the software, unless the contract specifies otherwise. The moral rights, such as the right to be recognised as the author, remain with the individual creator.

If the program is created outside the scope of employment, the author retains ownership. However, the employer may, in certain cases, claim a right of use if the software is closely related to the employee's professional activity and was developed using the employer's resources.

Ownership of patents

For patents, the right belongs to the inventor or, in the case of a joint invention, to all inventors in common. This right is transferable. If the same invention is made independently by multiple parties, priority is given to the first to file a patent application, provided it is published.

During the registration process, the applicant is presumed to be entitled to the patent.

A specific regime governs employee inventions. If an invention is developed by an employee or service provider in the course of their duties as a result of research explicitly or implicitly required by their contract, the employer is legally entitled to the patent. In such cases, the employee is generally not entitled to additional remuneration.

If these conditions are not met, the invention belongs to the employee. However, the employer may claim ownership or a right of use if the invention relates to the employee's professional activity and was developed predominantly using the employer's knowledge or resources.

Enforcement and defence of IP over crypto assets

IP enforcement

The enforcement mechanisms for IP rights in Spain are broadly similar for both software and patents.

In cases of unauthorised use, the rights holder may bring a civil infringement action. Available remedies include injunctive relief to cease or prevent the infringing activity, removal of infringing products, compensation for damages, and publication of the judgment.

Given the technical nature of both software and patent rights, expert evidence is almost always essential in these proceedings.

The rights holder may also request preliminary injunctions, either with the main claim or in advance if urgent. These measures are granted if two conditions are met:

- Urgency (*periculum in mora*): a risk that the final judgment would be ineffective if interim relief is not granted.
- *Prima facie case (fumus boni iuris)*: a preliminary assessment indicating that the right is valid and has likely been infringed.

To prepare for litigation, the rights holder may also request fact-finding proceedings – available specifically for patents but potentially extendable by analogy to software – to verify infringement when it cannot otherwise be proven. Additionally, preliminary proceedings are available for both patents and software to gather information on the identity of infringers and the scale of infringement to prepare a claim.

Although less common, criminal actions may also be pursued, typically in cases of counterfeiting or for strategic purposes, such as to facilitate evidence gathering or to emphasise the seriousness of the claim.

IP defence

SOFTWARE

The validity and ownership of software copyrights may be challenged in court in several ways:

- By way of counterclaim in response to an infringement action: the alleged infringer may argue that the claimant is not the rightful owner or author of the software, or that the work lacks originality, and may file a counterclaim seeking a declaration of non-infringement or invalidity.
- By direct action: a party may initiate a standalone claim seeking a declaration of authorship, ownership or invalidity, for instance, on the grounds that the program is not an original creation or that the claimant has no legitimate title to the rights.

In either scenario, the rights holder or alleged author can respond to the allegations and provide evidence of authorship, originality and ownership. Common grounds for disputing software copyright include lack of originality or creative expression, unauthorised transfer or assignment of rights, or plagiarism or misappropriation claims.

Given the technical nature of software, expert evidence is often critical in assessing the originality of the program's code, structure, and design, as well as to determine whether alleged similarities constitute infringement or independent development.

PATENTS

The validity of a patent can be challenged in court in two main ways:

- by way of counterclaim in response to an infringement action: the alleged infringer may argue that the patent is invalid and file a counterclaim seeking its revocation. Alternatively, invalidity may be raised as a mere defence (exception), in which case it will only have effect within that specific proceeding and will not result in the patent being formally revoked;
- by direct action, through a standalone claim for patent invalidity.

In either scenario, the patent holder can respond to the invalidity allegations. Grounds for invalidity include failure to meet patentability requirements – particularly novelty and inventive step – as well as insufficient disclosure or the inclusion of subject matter beyond the scope of the original application.

Given the technical nature of patent rights, expert evidence plays a crucial role in these proceedings.

Patent validity may also be challenged through administrative proceedings before the granting authority:

- For Spanish patents and utility models, an opposition may be filed before the Spanish Patent and Trademark Office within six months of publication of the grant.
- For European patents, oppositions may be filed before the EPO within nine months of grant publication.

The decision to seek protection in foreign jurisdictions depends on the type of intellectual property right involved.

Software protection in foreign jurisdictions

The decision to seek protection in foreign jurisdictions is generally less complex than for patents or trademarks, since copyright protection arises automatically under international treaties such as the Berne Convention and the World Intellectual Property Organization (WIPO) Copyright Treaty, to which Spain is a signatory. Overall, this means that software created in Spain is automatically protected abroad in all member countries without the need for separate registration.

However, companies may still choose to register software copyrights or related rights (such as trade secrets or trademarks associated with the software) in specific jurisdictions based on strategic factors, including:

- Commercial relevance: markets where the software will be distributed, licensed or commercialised.
- Risk of infringement: countries with higher piracy rates or weaker enforcement may warrant proactive registration or additional legal measures.

- Contractual and licensing arrangements: jurisdictions where key partners, users or clients are located.
- Tax and corporate structure considerations: where IP holding or licensing entities are established.

In summary, while Spanish software authors benefit from automatic international copyright protection, active protection strategies abroad are guided by commercial presence, enforcement needs, and market priorities.

Patent protection in foreign jurisdictions

Patent rights are territorial in nature. Therefore, it is generally advisable to seek the broadest possible territorial protection from the outset. This is particularly important because, once a patent application is filed in any jurisdiction (including regional offices such as the EPO), the applicant has a 12-month window to file in other jurisdictions while claiming the priority of the first filing. After this period, the initial application will destroy the novelty of the invention, making further filings – in any jurisdiction – impossible.

Given this, and the fact that future commercial interests may evolve (eg, a company initially focused on the Spanish market may later expand internationally), it is generally advisable to adopt a forward-looking strategy and seek protection in all jurisdictions where commercial exploitation is either planned or reasonably foreseeable. Although broad territorial protection is ideal, it must be balanced against cost and administrative complexity. In practice, companies tend to prioritise jurisdictions with strong market potential, effective enforcement systems, or a high concentration of potential clients. Common target jurisdictions include the United States, countries covered by the EPO – including EU Member States and the United Kingdom – China and Japan.

To simplify the process of seeking protection in multiple jurisdictions, applicants often rely on the Patent Cooperation Treaty, which allows for a single international application and defers the selection of national or regional offices for up to 30 or 31 months, depending on the jurisdiction.

IP rights over crypto assets – whether protected as software or patents – can be monetised in Spain through standard mechanisms such as assignment or licensing. There are no legal restrictions, to our knowledge, that apply specifically to technologies related to crypto assets.



the global voice of
the legal profession®

International Bar Association

Chancery House
53-64 Chancery Lane
London WC2A 1QS
United Kingdom
Tel: +44 (0)20 7842 0090
Fax: +44 (0)20 7842 0091
Email: editor@int-bar.org
www.ibanet.org