

# The Republic of Ireland

**Josh Hogan**

*McCann FitzGerald, Dublin*

josh.hogan@mccannfitzgerald.com

**John Boyle**

*McCann FitzGerald, Dublin*

john.boyle@mccannfitzgerald.com

**Artur Pokhilo**

*McCann FitzGerald, Dublin*

artur.pokhilo@mccannfitzgerald.com

**Jennifer Ekomaru**

*McCann FitzGerald, Dublin*

jennifer.ekomaru@mccannfitzgerald.com

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

Ireland does not have a regulatory regime that is specific to fintech or fintech companies. In all cases, it is necessary to look to the underlying service provided to determine whether it is subject to Irish financial services regulation.

The main Irish legislation that may typically apply to the activities of fintech companies includes:

- the European Union (Markets in Financial Instruments) Regulations 2017, which implement Directive 2014/65/EU (MiFID II) in Ireland;
- the European Union (Payment Services) Regulations 2018 (the 'Irish Payment Services Regulations'), which transpose the EU's revised Payment Services Directive 2015/2366 ('PSD2') into Irish law; and
- the European Communities (Electronic Money) Regulations 2011 (the 'Irish E-Money Regulations'), which transpose the EU's Electronic Money Directive 2009/110 ('EMD2') into Irish law.

In addition, investment and lending activities of fintech companies may fall within the scope of Irish domestic legislative regimes, including the Investment Intermediaries Act 1995, the Central Bank Act 1997 and the Consumer Credit Act 1995, which set out regulatory regimes for investment business firms, retail credit firms, credit servicing firms and high-cost credit providers.

The above enactments prescribe certain activities as regulated activities, meaning an entity must be appropriately authorised to conduct such activities in Ireland. Typically, this means that an entity must hold an authorisation from the Central Bank of Ireland (the 'Central Bank') or, where the activity is subject to EU passporting rights, from another EU regulator. In all cases, there may be possible exemptions or exclusions available, or methods of structuring activities in order to ensure they do not fall within scope of regulated activity.

In recent years, further regulatory regimes that may govern the activities of fintech companies have been introduced. The EU (Crowdfunding) Regulations 2021 (the 'Irish Crowdfunding Regulations') were transposed into Irish law, which give effect to the EU's Crowdfunding Regulation, and introduce a regulatory regime for crowdfunding service providers. As explained in section 2, crypto assets are regulated pursuant to Regulation (EU) 2023/1114 on markets in crypto assets (MiCAR).

The Central Bank is the entity with principal responsibility for Irish financial services regulation in Ireland (including for fintechs). The Central Bank has a significant role in the conduct of business of regulated entities and has issued a number of codes and regulations, including:

- the Consumer Protection Code 2012 (a revised version of which took effect on 24 March 2026);
- the Central Bank (Supervision and Enforcement) Act 2013 (section 48) (Lending to Small and Medium-Sized Enterprises) Regulations 2015 (commonly known as the SME Lending Regulations); and
- the Minimum Competency Code 2017.

The Central Bank also has significant enforcement powers, both in relation to the prosecution of financial crimes, and under its administrative sanctions procedure (permitting it to carry out investigations and inquiries, and impose sanctions if it determines that firms or individuals have committed a prescribed contravention).

The Central Bank has consistently underscored its commitment to openness and constructive engagement in relation to fintech, a stance reflected in its ongoing interaction with industry stakeholders. It operates an Innovation Hub that provides a central point of contact for fintech firms, as well as an Innovation Sandbox Programme. In addition, the Central Bank permits certain regulated Irish funds – qualifying investor alternative investment funds (QIAIFs) – to hold exposures to crypto-assets of up to 20 per cent for open-ended QIAIFs and up to 50 per cent for closed-ended QIAIFs.

## **Payment services**

In general, fintech companies that provide payment services such as the execution of payment transactions, issuance of payment instruments, acquiring of payment transactions, money remittance, payment initiation services and account information services will fall within the regulatory regime set out in the Irish Payment Services Regulations, and will require authorisation to provide such services unless an exemption is available.

In relation to open banking, under the Irish Payment Services Regulations, payment service providers are required to permit third parties, who are authorised under those regulations, to access relevant account information. There are specific rules governing this activity set out in those regulations.

## **Lending**

Under the Central Bank Act 1997, a person who meets the definition of a retail credit firm, or who performs the regulated activity of ‘credit servicing’, may be required to obtain authorisation from the Central Bank. Similarly, under the Consumer Credit Act 1995, a person who meets the definition of a high-cost credit provider (typically lending at an interest rate of 23 per cent or more), may be required to obtain authorisation from the Central Bank.

However, there may be reasons as to why these particular regimes would not apply in the context of lending (eg, if the lending is to a professional client for MiFID II purposes, or to a regulated financial service provider), and lending activities could be structured, if possible, so as not to fall within these regimes.

## **Buy now, pay later**

The Consumer Protection (Regulation of Retail Credit and Credit Servicing Firms) Act 2022 gave effect to one of the most significant expansions to Irish financial services authorisation requirements for many years. Authorisation from the Central Bank is required in relation to a broader scope of ‘credit’ (which no longer only applies to ‘cash loans’, and which following enactment includes ‘deferred payments’ and ‘other similar financial accommodation’). This broader definition of credit brought buy now, pay later providers within scope of the regulatory regime governing retail credit firms.

## **Deposit taking**

Deposit taking is only permitted by entities that have been authorised as a credit institution by the Central Bank, the European Central Bank or another EU regulator.

## **Crypto assets**

See section 2.

## **Crowdfunding**

Pursuant to the Irish Crowdfunding Regulations, the Central Bank has been designated the national competent authority or crowdfunding regulation in Ireland and is responsible for the authorisation and supervision of crowdfunding service providers (CSPs). CSPs that facilitate either peer-to-peer business lending or investment-based crowdfunding via their platforms need to be authorised by the Central Bank. Once authorised, they are able to provide crowdfunding services across the EU on a cross-border basis in line with the requirements outlined in the EU's Crowdfunding Regulation.

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

Ireland has chosen to follow EU developments relating to crypto rather than create a standalone domestic regulatory regime. Depending on the nature of the activities relating to crypto assets, such activities could fall within scope of: (1) existing Irish financial services regulatory regimes (as set out in section 1); or (2) MiCAR.

## **Anti-money laundering framework**

As an enhancement to the anti-money laundering (AML) framework for crypto assets, the EU enacted Regulation (EU 2023/1113) on information accompanying transfer of funds and certain crypto assets, which has been directly applicable in Ireland since 30 December 2024. This Regulation replaced the existing Wire Transfer Regulation (EU 2015/847) and increases the traceability of crypto asset transfers. The Regulation requires crypto asset service providers to ensure that transfers of crypto assets are accompanied by certain information on the originator and beneficiary of the transfer, for example, the originator's name and address.

The Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (CJA 2010) previously provided for a virtual asset service provider (VASP) regime, under which a person falling within the definition of a VASP was required to register with the Central Bank and comply with AML obligations. Since August 2025, the CJA 2010 no longer provides for a VASP regime. A transitional period was provided by the European Union (Markets in Crypto-Assets) Regulations 2024 ('Irish MiCAR') whereby firms registered and operating under the VASP regime prior to 30 December 2024 were permitted to do so until 30 December 2025 or until they were granted or refused an authorisation pursuant to MiCAR, whichever was sooner. Accordingly, all VASPs that failed to obtain an authorisation pursuant to MiCAR were required to cease VASP operation by 30 December 2025.

## MiCAR

MiCAR is fully in force in Ireland. As an EU Regulation, it required no domestic transposition and has direct effect in Irish law. However, certain national discretions and ancillary matters were addressed through Irish MiCAR, which give effect to those limited areas left to Member States.

MiCAR provides for three types of crypto asset:

- asset-referenced tokens (ARTs);
- electronic money tokens (e-money tokens or EMTs); and
- other crypto assets – neither ARTs nor e-money tokens, including utility tokens.

MiCAR sets out uniform requirements for the offering of, and admission to trading of, these categories of crypto assets, and establishes a comprehensive regulatory framework for crypto asset service providers (CASPs). The regime includes detailed transparency and disclosure obligations for the admission of crypto assets to trading, authorisation and supervisory requirements for issuers and CASPs, protections for holders of crypto assets and CASP clients, and measures aimed at preventing market abuse, including insider dealing and market manipulation.

Under MiCAR, CASPs are entities that provide crypto asset services to clients on a professional basis. They must be authorised by a national competent authority in order to operate in the EU. In Ireland, this is the Central Bank.

MiCAR does not apply to crypto assets that ‘are unique and not fungible with other crypto-assets’ (known as non-fungible tokens or NFTs) or to crypto assets that also qualify as one or more of:

- financial instruments as defined in MiFID II;
- deposits, as defined in the Deposit Guarantee Scheme Directive, and structured deposits, as defined in MiFID II;
- funds (as defined in PSD2) except if they qualify as e-money tokens;
- securitisation positions;
- non-life or life insurance products or reinsurance and retrocession contracts; or
- certain pension products, social security schemes and officially recognised occupational pension schemes.

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

#### **Payment service providers**

Payment institutions are regulated under PSD2, as transposed into Irish law by the Irish Payment Services Regulations, and related measures. Regulation 6(1) of the Irish Payment Services Regulations provides that a person shall not provide a payment service (as set out in Schedule 1 – Payment Services of those Regulations) in Ireland unless that person is authorised, either under Irish law or the law of a member state of the European Economic Area (EEA) as a credit institution, an electronic money institution or a payment institution, subject to certain exceptions.

The Central Bank is responsible for the authorisation, prudential regulation and supervision of payment institutions in Ireland. There are eight payment services under the Irish Payment Services Regulations, reflecting those set out in PSD2.

Where the activities constitute regulated payment services in Ireland, a range of exemptions under the Irish Payment Services Regulations should be assessed. These include, for example, the commercial agent exemption (which may apply where the firm acts solely on behalf of either the payer or the payee) and the limited network exemption. Where appropriate, the activities may be structured to fall within one of these exemptions, thereby avoiding the need for authorisation as a payment institution. However, each exemption is subject to specific limitations, and reliance on them must be approached with care.

On 27 November 2025, the European Council and Parliament announced they had arrived at a provisional political agreement on the final text of the proposals package to create a new PSR and PSD3. The current proposed text narrows the applicability of the 'commercial agent' exemption referred to above and seeks to clarify the applicability of the 'limited network' exemption. The final text will likely be published in the first half of 2026, with the new regulatory regime entering into force after a transitional period.

#### **Digital wallets**

The provision of digital wallet services may fall within the meaning of electronic money services (an 'e-money service') requiring authorisation under the Irish E-Money Regulations. Authorisation as an e-money institution is broader than authorisation as a payment institution, as it permits an entity to provide both payment services and e-money services.

The Central Bank places particular emphasis on the safeguarding of users' funds. E-money institutions (and payment institutions) must maintain a robust safeguarding risk framework, approved by their board, to ensure that relevant client funds are properly identified, managed and protected on a continuous basis. This framework must be subject to effective oversight by the firm's second line of defence (risk and compliance functions) and third line of defence (internal audit).

In Ireland, an e-money institution (and payment institution) would have the choice of safeguarding users' funds in either of two ways: (1) by depositing the funds in a separate bank account in a credit institution or by investing the funds in assets accepted by the Central Bank as secure and

low risk; or (2) by insuring the funds with an insurance company or having them guaranteed by a credit institution. Where the funds are deposited in a separate bank account, the Irish E-Money Regulations provide legal protections for the e-money users in the event of the e-money institution's insolvency.

It is expected that the PSR and PSD3 proposals (referred to above) will merge the e-money institution and payment institution frameworks and align conduct and prudential rules.

#### **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.**

### **Ireland for Finance Action Plan**

Financial innovation remains a key focus of Irish Government attention. The Department of Finance launched the *Ireland for Finance Action Plan* in June 2025, a key objective of which is the continued development of Ireland as a centre for fintech and digital finance.

### **Government agency support**

The Irish Government has two agencies that support the development of business in Ireland, with a particular emphasis on the fintech sector. These are Enterprise Ireland (focused on domestic Irish companies) and IDA Ireland (focused on foreign direct investment into Ireland).

### **Innovation Hub**

The Central Bank has established an Innovation Hub and an industry engagement programme to support fintech firms. The Innovation Hub provides a dedicated channel through which firms can engage with the Central Bank outside traditional supervisory or regulatory interactions. Its purpose is to assist innovators in navigating the regulatory framework by offering guidance on:

- the relevant components of the regulatory regime;
- applicable supervisory rules and policies; and
- how to navigate the Irish supervisory and regulatory landscape.

The Innovation Hub is open to enquiries from individuals, new fintech firms and existing firms that provide – or intend to provide – financial products or services that are both innovative and at a sufficiently developed stage. A product or service will be considered innovative where it is based on new technology that:

- is not currently present in the Irish market or has not been deployed at scale; or
- materially changes the way an existing product or service is structured or delivered.

## **Innovation Sandbox Programme**

The Central Bank's Innovation Sandbox Programme operates on a cohort basis over six months focused on a particular theme for that period. The theme for the H1 2026 Sandbox Programme is 'Innovation in Payments'. The objective is to accelerate solutions that deliver safer, faster, greener and more inclusive payments for households and businesses, while giving the Central Bank early insight into emerging risks and supervisory questions.

## **Advantages to being authorised in Ireland**

Aside from Ireland's position as a fintech hub, there are a number of advantages to being authorised in Ireland, including:

- a strong regulatory framework with a credible and experienced regulator, the Central Bank;
- a favourable passporting regime with the ability to passport to other EEA Member States either on a branch or a cross-border services basis;
- a favourable tax regime, due to a combination of a 12.5 per cent corporate tax rate and an exceptionally extensive and comprehensive set of double tax agreements; and
- access to a sophisticated financial services ecosystem with a deep pool of staff, managers, professional advisers, regulators and service providers including not only native English speakers but a sizeable international population.

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

As noted in section 1, the main legislation relevant to open banking is the Irish Payment Services Regulations. These Regulations do not 'regulate' open banking; rather, they provide the framework within which open banking is facilitated (through the regulation of payment initiation service providers (PISPs) and account information service providers (AISPs)).

Third parties seeking to access account data for open banking purposes must register as an AISP (an entity that collects information on one or more payment accounts and aggregates account details such as balances or outgoings and displays them on a single platform) or be authorised as a PISP (an entity that initiates a payment order for an account held with another provider at the user's request) with the Central Bank. The activities of AISPs and PISPs are highly regulated to ensure consumer protection, and informed consent from consumers is required before data is shared.

While registration as an AISP is considered a lighter form of authorisation than providing some other payment services, an AISP is still undertaking payment services and is supervised by the Central Bank in the same way as firms providing other payment services.

On 23 June 2022, the European Banking Authority (EBA) published an opinion (*Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*) which, among other things, suggested a move from

‘open banking’ to ‘open finance’, meaning an expansion from access to payment accounts data towards access to other types of financial data (such as savings, investments and insurance data).

On 28 June 2023, the EU Commission proposed a package of measures (which are not yet law) relating to payment services. One of these measures was a legislative proposal for a Regulation on a ‘Framework for Financial Data Access’ to establish clear rights and obligations to manage customer data sharing in the financial sector beyond payment accounts. Under the proposal, customers will have the possibility (but no obligation) to share their data with financial institutions or fintech firms in secure machine-readable formats in order for the customers to receive new, cheaper and better data-driven financial and information products and services, such as financial product comparison tools and personalised online advice.

On 4 December 2024, the Council of the EU announced that it had agreed on its position on the proposed framework for financial data access (to be known as the ‘FiDA Regulation’). The FiDA Regulation proposes to establish rules on the access, sharing and use of certain categories of customer data in financial services, as well as rules concerning the authorisation and operation of financial information service providers. The Council’s agreement paves the way for the commencement of interinstitutional negotiations between the Council and the European Parliament.

There has been extensive EU activity on FiDA and open finance throughout 2025. While trilogue negotiations progressed during 2025, the legislative proposal has not yet been finalised (as of January 2026) and, on current indications, is expected to be concluded during 2026.

## **6. Regulation of virtual assets service providers.**

As noted above, the CJA 2010 had previously provided for a VASP regime, where a person falling within the definition of a VASP had to register with the Central Bank and comply with AML obligations. From August 2025, the CJA 2010 no longer provides for a VASP regime.

A transitional period was provided by Irish MiCAR, whereby firms registered and operating under the VASP regime prior to 30 December 2024 were permitted to do so until 30 December 2025 or until they were granted or refused an authorisation pursuant to MiCAR, whichever was sooner. Accordingly, all VASPs that failed to obtain an authorisation pursuant to MiCAR were required to cease VASP operation by 30 December 2025.

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

The ‘Travel Rule’ (ie, the information that should accompany transfers of funds and certain crypto assets) is implemented and enforceable in Ireland via Regulation (EU) 2023/1113 (the ‘Recast Transfer of Funds Regulation’).

The Recast Transfer of Funds Regulation in relation to information accompanying transfers of funds and certain crypto assets, provides that CASPs are obliged to collect and make accessible certain information about the sender and beneficiary of the transfers of crypto assets they operate, regardless of the amount of crypto assets being transacted. This ensures the traceability of crypto asset transfers to more easily identify possible suspicious transactions and block them.

The Recast Transfer of Funds Regulation expressly recognises that certain transfers of crypto assets entail specific high-risk factors for money laundering, terrorist financing and other criminal activities, in particular transfers related to products, transactions or technologies designed to enhance anonymity, including privacy wallets, mixers or tumblers. The EBA has issued 'Guidelines on information requirements in relation to transfers of funds and certain crypto assets transfers under Regulation (EU) 2023/1113' (the 'Travel Rule Guidelines') which set out, inter alia, factors that CASPs should consider when establishing procedures to detect and manage transfers of crypto assets lacking the required information on the originator or the beneficiary.

Further, the EU (Information Accompanying Transfers of Funds) Regulations 2025 (the '2025 Regulations') have amended the CJA 2010 such that the meaning of a designated person now include a CASP. Accordingly, CASPs are required to comply with AML obligations under the CJA 2010. The Central Bank is the regulatory and supervisory authority responsible for overseeing CASPs in Ireland.

In the context of VASPs specifically, please note, as per our responses above, Ireland no longer provides for a VASP regime.

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

### **Tokenised assets: structuring**

The tokenisation of assets is typically understood as involving a digital representation of a physical asset/financial instrument or the issuance of the physical asset/financial instrument in tokenised form to enable them to be issued, stored and transferred on a distributed ledger.

In the context of financial instruments, as per Guideline 5 of the European Securities and Markets Authority (ESMA)'s 'Guidelines on the conditions and criteria for the qualification of crypto assets as financial instruments', the process of tokenisation of financial instruments should not affect the classification of such assets. Accordingly, tokenised financial instruments will continue to be considered as financial instruments for regulatory purposes.

Tokenised assets can be structured as securities tokens (these resemble traditional instruments, such as shares and bonds), NFTs (a unique digital identifier of ownership), stablecoins, tokenised deposits or as a central bank digital currency. One of the benefits of tokenisation includes the ability to turn an illiquid asset into a liquid asset.

### **What types of collateral are typically used to secure obligations arising in such digital asset transactions?**

Depending on the transaction, pledged collateral may include traditional collateral types (eg, bonds, cash and equities), as well as digital assets. As with any collateral, the ability of an asset to be used as collateral will depend on a number of factors such as credit and liquidity risks, its ability to maintain a stable value and whether it correlates to the provider's credit risk.

**Please describe the procedures to create and perfect a security interest in these types of collateral, including any requirements for notarisation, registration, stamp duty or other legal formalities.**

Our response applies to assets that are traditionally used as collateral.

The particulars of charges created by an Irish company over its assets must be registered with the Companies Registration Office within 21 days of the creation of the charge. This registration requirement does not apply where the security constitutes a financial collateral arrangement over cash, money credited to an account, shares, bonds or other financial instruments, provided certain statutory requirements are met.

A charge will be void against any liquidator or creditor of the company where there has been a failure to register it. Further, where the security comprises of a fixed charge over book debts, a notification should also be made to the Office of the Revenue Commissioners within 21 days of the creation of the charge.

Security over Irish real estate must be registered with Tailte Éireann (the property registration authority). Security over certain other assets, such as intellectual property, ships and aircraft, must be registered at applicable registries.

In the context of digital assets, Ireland currently does not have any specific legislation relating to the creation and perfection of security interest in digital assets. Accordingly, careful consideration may need to be given as to whether creating a charge over the specific digital asset would necessitate any registration/perfection requirements. Where the digital asset, by way of an example, is a representation of a physical asset (eg, Irish real estate, intellectual property, a ship or an aircraft), it would be prudent to ensure that any registration requirements that apply in respect of such physical assets are complied with.

**Will the courts in your jurisdiction recognise and enforce a foreign governing law clause in a crypto asset-related contract?**

Yes, a party's submission to the jurisdiction of the courts of another jurisdiction will generally be upheld by the Irish courts. Please see section 9.

**In the case of a default, what enforcement procedures are available to secured lenders to realise their security interest and recover their claims? Is a public auction required for enforcement? Can a secured lender appropriate the collateral directly in certain cases?**

The appointment of a receiver, or receiver and manager (the latter with authority to manage the company's business) is the most common method of enforcement by a holder of a legal fixed or floating charge over the assets of a chargor. The role of a receiver is to realise the secured assets and discharge any unpaid indebtedness from the proceeds of such realisation. A receiver is appointed by way of a deed or instrument of appointment between the secured creditor and receiver in accordance with the terms of the security document and is typically granted broad contractual powers in addition to their statutory powers.

On the appointment of a receiver, the directors' powers cease so far as the receiver is acting and a receiver, under a power of attorney as provided under the relevant security document, is able to execute documents on the company's behalf. A court order, generally speaking, is not necessary for the appointment of a receiver. However, in the case of real property, it may be necessary to obtain a court order for possession if the security holder intends to enter into direct possession.

In the context of digital assets, there are no specific enforcement procedures that relate to digital assets specifically.

Where the digital asset, by way of an example, is a representation of a physical asset, in order to obtain possession of the physical asset it may be necessary to, inter alia, appoint a receiver or obtain a court order.

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

A party's submission to the jurisdiction of the courts of another jurisdiction will generally be upheld by the Irish courts.

The submission by an entity incorporated in Ireland to the jurisdiction of the courts of another EU Member State will be upheld in the Irish courts pursuant to the provisions of Regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (the 'Brussels Recast Regulation'). The Brussels Recast Regulation effectively streamlines the free movement of judgments within the EU, determining which EU Member State's courts can hear a case (usually based on the defendant's home country (domicile), but also other specific rules and criteria), governs recognition and enforcement of judgments in civil and commercial matters across the EU Member States, thus simplifying cross-border litigation. This Regulation is directly applicable in Ireland and has applied to proceedings instituted on or after 10 January 2015.

Further, the Convention of 30 June 2005 on Choice of Court Agreements (the '2005 Hague Convention') and the Convention on jurisdiction and the recognition and the enforcement of judgments in civil and commercial matters of 30 October 2007 (the '2007 Lugano Convention') each have force of law in Ireland.

As per the terms of the 2005 Hague Convention and the 2007 Lugano Convention, a submission by an entity to the courts of a state coming within the scope of those conventions is valid and binding on the entity, subject to and in accordance with the terms of those conventions.

Valid exclusive jurisdiction clauses are generally enforceable in Ireland. Ireland is bound by Article 25 of the Brussels Recast Regulation and the 2005 Hague Convention. Further, exclusive jurisdiction clauses are also generally enforceable at common law in Ireland. Note that, in case of asymmetric jurisdiction clauses that limit one party's ability to bring proceedings before one single court while permitting the other party to bring proceedings before, in addition to that court, any other competent court, special considerations apply as a result of the EU Court of Justice's judgment of 27 February 2025, in the proceeding *Società Italiana Lastre*, C-537/23, ECLI:EU:C:2025:120. Specifically, the jurisdiction clause must designate courts in EU Member States or in states party to the 2007 Lugano Convention, it must identify objective and precise

factors enabling the relevant court to verify its jurisdiction, and it must not conflict with other provisions in the Brussels Recast Regulation.

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

### **IP rights and ownership**

Innovations and inventions would generally be protected by patents. Trade secrets and confidential information can also be protected. Other IP that could be relevant to crypto assets includes copyright and trademarks (and the law of passing off). Such IP could for example protect certain images, graphics, trade and product names.

#### ***Patents***

A patent is an intellectual property right granted with respect to inventions that allows the patent holder to prevent others from using the invention without consent for a proscribed period of time. An invention is patentable if it is susceptible to industrial application, is new and involves an inventive step.

Crypto-related inventions also face challenges in so far as they are computer-implemented inventions. Under the European Patent Convention and the Irish Patents Act computer programs 'as such' are excluded from patentability. There is no Irish case law on the interpretation of this exclusion, though European Patent Office (EPO) examination practice and decisions, as well as jurisprudence from other EPC countries, in particular the United Kingdom, would be influential on the Irish courts.<sup>1</sup> Generally, if a computer program can claim a 'further technical effect' when run on a computer, that is, a technical effect going beyond the 'normal' physical interactions between the software and the hardware, it is not excluded from patentability.

This can be a challenging hurdle for some crypto-related inventions to overcome, as demonstrated by the decision of the EPO Board of Appeal in T 0767/21 (Blockchain generation method/ NIPPON). There, the Board found that a claim to a blockchain consensus protocol that alternated two parameters for approving a block (in particular, alternating between proof of stake and a requirement based on past counterparty interactions, such that at least one in six blocks is generated using either method), in order to mitigate against 51 per cent attacks, did not amount to a further technical effect.

The Board instead found that 'it is a non-technical policy which is based on business and psychological considerations'. The Board also rejected an argument that the technical character of the protocol was inherent from the tamper-proof properties of the blockchain, saying: 'Regardless of its computer implementation, the blockchain is a vehicle for doing business. At a business level,

---

<sup>1</sup> The EPO's Examination Guidelines specifically address computer programs, in particular at Part F, chapter IV, s 3.9 [www.epo.org/en/legal/guidelines-epc/2025/f\\_iv\\_3\\_9.html](http://www.epo.org/en/legal/guidelines-epc/2025/f_iv_3_9.html), Part G, chapter II, s 3.6 [www.epo.org/en/legal/guidelines-epc/2025/g\\_ii\\_3\\_6.html](http://www.epo.org/en/legal/guidelines-epc/2025/g_ii_3_6.html) and in the Index for Computer-Implemented Inventions [www.epo.org/en/legal/guidelines-epc/2025/j.html](http://www.epo.org/en/legal/guidelines-epc/2025/j.html) accessed 15 July 2026.

it is a transaction ledger to which all participants can add blocks of transactions. Contrary to the appellant, the Board considers that deciding who can add transaction blocks to the blockchain is not based on technical considerations.'

The Board further explained its rationale by saying that a consensus protocol 'does not improve the blockchain security, but rather the accuracy of transaction data recorded on the blockchain'. The Board found that a consensus protocols operate at the 'semantic level' and are concerned with ascertaining that the blockchain's business content accurately reflects business reality over time; that stands in contrast to an electronic signature scheme that operates 'at bit level'. The assessment will always be fact-specific: indeed, the Board noted that some consensus protocols could potentially involve a technical effect, giving the example of a proof of work protocol that takes into account specific hardware factors that make it ASIC resistant (referring to T 1358/09 – Classification/BDGB ENTERPRISE SOFTWARE).

In T 0767/21, discussed above, the Board of Appeal also upheld a clarity objection under Article 84 EPC. That was also the case in T 1253/21 (Temporary cryptocurrency issuance/STANDARD TRANSACTION), which concerned an approach to validating cryptocurrency transactions by means of two digital signatures: the first from the issuer, resulting in the issuance of a temporary unit of the cryptocurrency, which is then validated by a second digital signature of a related custodian (the issuer's 'trust bank'), which confirms that the issuer has deposited assets, such as fiat money or gold, sufficient to complete the transaction. In its preliminary opinion, the Board of Appeal indicted that the invention did lack an inventive step over Satoshi's white paper and also lacked clarity under Article 84 EPC. The written decision was limited to the clarity objection, with the Board finding that the application did not provide details on how the temporary cryptocurrency would be issued on the blockchain or indeed set as a valid one once approved.

The right to apply for a patent belongs to the inventor of the invention. If the inventor is an employee the right to a patent shall be determined in accordance with the law of the state in which the employee is wholly or mainly employed or, if the identity of such state cannot be determined, in accordance with the law of the state in which the employer has their place of business to which the employee is attached. In Ireland, an invention would generally belong to an employer if created during the course of employment, absent any agreement to the contrary.

### ***Trade secrets and confidential information***

Information can be protected as trade secrets where it:

- is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
- has commercial value because it is secret; and
- has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

The law of confidence also protects confidential information. This arises where information has the necessary quality of confidence and is disclosed in a situation importing an obligation of confidence.

### *Copyright*

Copyright is an intellectual property right protecting an author's original work. Types of protected works include original literary, dramatic musical or artistic works, sound recording, films, broadcasts or cable programmes, the typographical arrangement of published editions and original databases. Computer programs are protected as literary works. Databases are also protected by a separate database right protecting databases where there has been a substantial investment in obtaining, verifying or presenting the contents of the database.

Generally, the author is the first owner of the copyright. A notable exception is that a work created by an employee during the course of their employment belongs to the employer absent any agreement to the contrary. Any assignment of copyright must be in writing to have legal effect.

### *Trademarks*

A trademark is any sign capable of being represented graphically that is capable of distinguishing goods or services of one undertaking from those of another. It may consist of words, designs, letters, numerals, or the shape of goods or of their packaging. A registered trademark is a property right obtained by the registration of the trademark; the owner of a registered trademark is accordingly afforded rights and remedies in respect of their registered trademark.

Unregistered marks can be protected under the law of passing off. In order to obtain protection, the mark must have acquired goodwill. It prevents any misrepresentation by another party to the public (whether or not intentional) leading or likely to lead the public to believe that the goods or services offered by the third party are the goods or services of the owner of the original mark.

## **Enforcement**

Intellectual property rights are enforced in the courts in Ireland. The High Court has general jurisdiction over IP disputes. It is also the designated court to hear disputes in relation to EU trademarks in Ireland.

IP disputes (other than EU trademarks) can also be heard by the District and Circuit Court. The District Court has a monetary jurisdiction over claims concerning a value of up to €15,000 and the Circuit Court of €75,000. However, these courts do not have jurisdiction over the validity of patents or trademarks.

## **Where to seek IP protection**

Unregistered rights, such as copyright and trade secrets, are generally protected automatically and do not require registration. There are however certain exceptions, such as the United States requiring registration of copyright in order to obtain full protection and damages in case of infringement.

Generally, such IP is recognised and protected in foreign jurisdictions. There are a number of international treaties, including Trade-Related Aspects of Intellectual Property Rights (TRIPS), the Paris Convention and the Berne Convention, ensuring sufficient protections in signatory states.

Registered rights, such as patents and trademarks, are generally only protected in jurisdictions where they are registered. There are a number of considerations when deciding in which jurisdictions to seek registration. These include:

- the residence of the party seeking to protect its rights;
- the main countries where it operates and/or where competitors or potential infringers operate;
- the costs of registration fees; and
- the value that IP protection would provide in each jurisdiction.

In addition to national registrations, trademarks can also be registered EU-wide as an EU trademark. Patents can also be applied for nationally, as well as centrally at the EPO, which covers countries that are signatories to the European Patent Convention. This does not grant one Europe-wide patent, but an applicant can choose to designate only certain countries and/or for the patent to take effect as a unitary patent within the Unified Patent Court system (to which Ireland is not currently a party). Protection and enforcement of patents granted by the EPO is then dealt with at a national level and/or before the Unified Patent Court (though the validity of such patents can also be challenged centrally at the EPO).

## **Monetisation**

IP in respect of any subject matter, including crypto, can be monetised in a number of ways, including licensing or selling the IP. We are not aware of any legal restrictions on monetising IP insofar as it relates to crypto or is linked to decentralised or open-source crypto projects – in theory it can be monetised in the same way as any other IP and the statutory rules governing IP (described above) continue to apply.

Blockchain technologies could also potentially be used to monetise assets, including crypto-related IP, through a process referred to as tokenisation. Broadly speaking, this refers to the concept of having interests in ‘real world’ assets such as securities, real estate and potentially other assets including intellectual property represented as coins or tokens issued on blockchains. Tokenisation may be appealing to IP owners who may see it as having the potential to fractionalise ownership (ie, effectively splitting beneficial ownership into millions of coins or tokens that could each be traded and held by multiple parties); create liquidity in an asset class that would generally be illiquid; or streamline certain commercial processes such as royalty distribution or licensing.

To date, much of the focus of tokenisation has been on real estate and securities – Blackrock’s launch of its BlackRock USD Institutional Digital Liquidity Fund (BUIDL) tokenised investment fund is notable in that regard – with more limited interest in relation to IP assets. For IP assets, the main focus has been on the use of tokens to create fractional economic interests

in revenue streams relating to copyright protected musical works, such as royalties or revenue from online streaming services.

Conceivably, it might also be possible to indirectly tokenise IP assets by tokenising the beneficial interest in a company that holds IP (eg, through a holding company structure). More ambitious tokenisation efforts that purport to address ownership or scope of protection of IP rights inevitably run into difficulty as the legal framework governing the IP in question, which determines title/ownership, validity and infringement, would continue to govern those matters irrespective of what the position is according to any tokenisation structure that may be put in place. Formal requirements such as registration of ownership and exclusive licenses would also cause challenges in so far as the token on the blockchain ledger would not be integrated with government IP registers.

Given the value of IP and legal complexities, both in relation to statutory requirements governing IP but also contract law, investment regulations and other relevant legal areas (often involving multiple jurisdictions), the viability of tokenisation of IP, at least over and above monetising future income streams in conjunction with the existing legal framework, remains to be seen. While there have been some relatively unsophisticated attempts to create decentralised IP networks (eg, Story Protocol, which purports to allow users to register 'IP' on-chain and offer permissionless licensing tools and automated royalty distribution), we are not aware of any that have made serious efforts to address, let alone which have overcome, the legal challenges arising. The prospect of that happening remains highly speculative at this point in time.



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](mailto:editor@int-bar.org)

**[www.ibanet.org](http://www.ibanet.org)**