

Lithuania

Ieva Dosinaite

Ellex Valiunas, Vilnius

ieva.dosinaite@ellex.legal

Gabrielė Mačerauskaitė

Ellex Valiunas, Vilnius

gabriele.macerauskaite@ellex.legal

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

There are no specific laws or regulations for fintechs in Lithuania. Nevertheless, there are certain pieces of regulations that indirectly relate to technology applied to financial innovation, the most relevant of which are summarised below.

Law on Electronic Money and Electronic Money Institutions

This law applies to persons entitled to issue electronic money in the Republic of Lithuania and establishes conditions for the issuance and redemption of electronic money; the procedure for the licensing, operation, termination and supervision of electronic money institutions (EMIs); and branches of EMIs in foreign countries, in order to ensure that the system of EMIs is stable, reliable, efficient and secure.

Law on Payment Institutions

This law lays down the procedures for the licensing, operation, closure and supervision of payment institutions (PIs) in order to ensure that the system of PIs is stable, sound, efficient and safe.

Law on Financial Institutions

This law establishes what services are considered to be financial services; the requirements for the founders, participants and managers of financial undertakings and credit institutions engaged in the provision of financial services; their rights and obligations; the conditions, procedures and peculiarities for the establishment, operation, termination and resolution of financial institutions; and the conditions, procedures and specifics of the supervision of the activities of financial institutions licensed as providing financial services. This law applies to all financial institutions – legal entities of Lithuania and branches of foreign financial institutions operating in Lithuania and engaged in the provision of financial services set out in this law.

Law on Payments

This law regulates the activities and responsibilities of payment service providers and payment services; the conditions for their provision and the informational obligations related thereto; execution of payment transactions; authentication, operational and security risk management; the rights and obligations of users of payment services and providers of payment services in relation to payment services where the provision of payment services is a business; the rules on transparency and comparability of fees charged to natural payment service users for payment accounts; the rules on the transfer of payment accounts; the rules and conditions for the opening and use of a basic payment account; and the rights and powers of the supervisory authority in the supervision of compliance with the provisions of this law and the out-of-court settlement of consumer disputes.

EU MiCA Regulation and Lithuanian Law on Markets in Crypto-Assets

The European Union Regulation on Markets in Crypto-Assets, Regulation (EU) 2023/1114 (MiCA), discussed in Question 2, provides a uniform, direct regulation across all EU Member States by setting the overarching, directly applicable legal framework for crypto assets, whereas Lithuania's Law on Markets in Crypto-Assets, also discussed in more detail in Question 2 *et seq*, implements specific national requirements, designating local supervisory roles and setting out precise national requirements for implementing the EU regulation, transitioning the industry from simple registration to a supervised licensing regime. The Lithuanian Law on Markets in Crypto-Assets law complements MiCA by establishing the legal framework for the issuance, offering and admission to trading of crypto assets in the Republic of Lithuania; the licensing, operation and supervision of crypto asset service providers; and the protection of investors and market integrity. It defines the requirements for issuers of crypto assets, including those offering asset-referenced tokens (ARTs) and e-money tokens (EMTs), as well as the rules governing crypto asset service providers (CASPs) engaged in custody, trading, exchange, advisory and other activities. The law aims to ensure transparency, financial stability, technological neutrality and consumer protection in the Lithuanian crypto asset market, in line with the principles of MiCA.

Law on the Prevention of Money Laundering and Terrorist Financing

The purpose of this law is to establish measures for the prevention of money laundering, including certain requirements for institutions, inter alia, fintechs, and/or terrorist financing and the institutions responsible for the implementation of measures for the prevention of money laundering and/or terrorist financing.

Bank of Lithuania positions and guideline

The Bank of Lithuania, when needed, releases positions, guidelines, opinions and explanations of relevant local legal acts and decisions on the application of EU guidelines, all of which are relevant for supervised financial market participants.

Open banking

In the EU, of which Lithuania is a member, the existing Payment Services Directive ('PSD2') requires banks to enable authorised third-party providers to access the accounts maintained by those banks in order to provide account information and payment initiation services. Please see Question 5.

Other Fintech-related laws at the EU Level

There is no piece of EU legislation that covers all aspects of fintech. Fintech companies providing financial services (eg, lending, financial advice, insurance or payments) must comply with the same laws as any other companies offering such services. Therefore, different laws apply depending on the activity (eg, payment services or crowdfunding), such as Directive 2000/31/EC (ecommerce), Directive 2002/65/EC (distance marketing of consumer financial services), Directive 2009/110/EC (electronic money) and Directive (EU) 2015/2366 (payment services).

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

The regulation of crypto assets in Lithuania is established in MiCA and the Law on Markets in Crypto-Assets of the Republic of Lithuania. These legal acts create a uniform regime for the issuance, offering and admission to trading of crypto assets, and the authorisation and supervision of CASPs.

MiCA applies to crypto assets not already covered by existing EU financial legislation, such as Directive 2014/65/EU, that is, Markets in Financial Instruments Directive II ('MiFID II'); the E-Money Directive; and the Securitisation Regulation. It distinguishes three categories of regulated assets: (1) ARTs are designed to maintain stable value by referencing a basket of assets, currencies, commodities or rights; (2) EMTs are stablecoins pegged to a single official currency and primarily intended for payments; and (3) a residual category captures other crypto assets, including utility tokens, which do not fall within the definitions of ARTs or EMTs. Financial instruments, deposits, structured deposits and securitisations remain outside MiCA's scope and continue to be regulated under sector-specific EU frameworks.

Issuers of crypto assets must comply with obligations tailored to the token type. For crypto assets other than ARTs or EMTs, the central requirement is to publish a crypto asset white paper with prescribed disclosures. The Bank of Lithuania must be notified of the white paper, together with any marketing materials, and an explanation showing why the asset is not an ART or EMT, at least 20 working days before operations begin, and all this information must be made publicly available on the issuer's website.

ART issuers face more extensive obligations. They must obtain authorisation from their home competent authority (in Lithuania, the Bank of Lithuania). In addition to white-paper approval/notifications applicable to ARTs, they must meet capital requirements, maintain a reserve of backing assets, comply with liquidity standards, safeguard client funds and prepare a redemption plan to protect holders in case of issuer failure.

EMT issuers are subject to requirements broadly similar to those for ARTs; however, notification of EMT white papers must be provided at least 20 working days before publication, and an EMT issuer must be authorised as an EMI or a credit institution. Holders of both ARTs and EMTs benefit from a statutory right of redemption at par value.

Alongside issuers, MiCA regulates CASPs, which include services such as the custody and administration of crypto assets; operation of trading platforms; exchange of crypto assets for funds or other crypto assets; transfer services; execution of orders; and the provision of advice or portfolio management. CASPs are subject to prudential and organisational requirements, including initial capital (typically €50,000–€150,000 depending on the services offered); fit-and-proper requirements; risk management; safeguarding and segregation of client assets; and robust conflict-of-interest frameworks. Authorisation in Lithuania is granted by the Bank of Lithuania and can be passported across the EU.

CASPs are subject to ongoing conduct-of-business duties requiring them to act honestly, fairly and professionally, and to maintain systems that ensure sound governance, effective risk management and proper record-keeping. In addition, according to the Bank of Lithuania, CASPs engaging in

certain EMT transactions that qualify as payment services will also need separate authorisation to provide payment services.

From an investor protection perspective, MiCA establishes a comprehensive set of safeguards aimed at protecting clients and strengthening operational resilience. These include the segregation of client assets from the CASP's own funds to ensure clients retain access even in the event of insolvency, and prudential requirements obliging CASPs to hold adequate capital and liquidity buffers. MiCA also requires clear and transparent disclosures on services, risks, fees and procedures, and imposes strict governance and internal control standards, including fit-and-proper tests for management, robust risk management frameworks and independent control functions.

MiCA entered into force on 29 June 2023. Provisions applicable to ART and EMT issuers have applied since 30 June 2024, while the remainder of the framework, including CASP rules, applied from 30 December 2024. Lithuania set a national deadline, requiring CASPs to be authorised by 1 January 2026.

It is important to note that, until the end of the transitional period for applying for a CASP licence, the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania (the 'AML Law') governed virtual currency exchange and custodian wallet service providers by including them in the list of undertakings that are subject to anti-money laundering (AML) requirements. Currently, the AML Law applies to CASPs, which are treated as financial institutions for AML/counter-terrorist financing (CFT) purposes and are subject both to general AML obligations and specific requirements addressing risks inherent to crypto asset services. In particular, CASPs must identify, assess and manage money laundering and terrorist financing risks related to crypto asset transfers, including transfers to or from self-hosted addresses, and implement appropriate internal policies and control measures. CASPs are also subject to reporting and record-keeping obligations under the AML Law, including the obligation to provide transaction and customer information to the Financial Crime Investigation Service (FCIS) and to retain relevant records for statutory periods. Strong customer authentication requirements apply to international correspondent relationships involving crypto asset services, and the AML Law expressly prohibits the provision of services on an anonymous basis.

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

In Lithuania, payment services may be provided by several categories of entities as defined by applicable legal acts. There are two main non-bank payment service providers as defined by legal acts (in general, the Law on Electronic Money and Electronic Money Institutions and the Law on Payment Institutions): (1) PIs; and (2) EMIs.

A PI is defined by the acts as a market participant providing payment services and licensed by the Bank of Lithuania with an unrestricted, restricted or account information service licence.

An unrestricted PI may carry out money transfers, payment operations, cash deposits or withdrawal services, direct debit or credit transfers and so on, but may not accept deposits from retail market participants or issue electronic money. In addition to payment services, it is entitled to provide ancillary services closely related to main payment services, such as foreign exchange. A PI may hold a restricted licence. With a restricted licence, a PI is subject to lighter requirements for

management, that is, no capital and shareholder eligibility requirements apply, but it is subject to restrictions on the turnover of payment transactions laid down in the Law on Payment Institutions; such an institution may only operate in Lithuania. Alternatively, a PI may hold a licence providing an account information service. This licence is valid in other EU Member States, but is not subject to capital and shareholder eligibility requirements, requirements for the protection of funds, intermediaries and the transfer of operational functions. A PI holding an unlimited licence may operate throughout the EU.

On the other hand, an EMI is defined by the acts as a company that has been issued an EMI licence or an EMI limited activity licence granting the right to issue electronic money in the Republic of Lithuania and/or other EU Member States. An EMI may also carry out money remittances, payment transactions, cash deposit and withdrawal services, direct debit and credit transfers, and so on.

The Lithuanian financial market and its participants are supervised by the Bank of Lithuania. In Lithuania, financial market supervision is based on a risk-based supervisory model. This means the Bank of Lithuania focuses its resources on the most systemically important financial market participants, and financial services and products that pose the greatest risk to consumers. The Bank of Lithuania periodically carries out examinations (inspections and investigations) of financial market participants. The Bank of Lithuania, when needed, releases positions, guidelines, opinions and explanations of relevant local legal acts, decisions on the application of EU guidelines, all of which are relevant for supervised financial market participants.

Furthermore, on 28 June 2023, the European Commission published a legislative package proposing to amend and modernise PSD2. The package consists of a new Payment Services Directive ('PSD3') and a directly applicable Payment Services Regulation, both expected to enter into force by the end of 2027. Together, these instruments aim to establish a harmonised and technology-neutral framework for payment and electronic money services across the EU. PSD3 updates and clarifies the rules governing PIs and fully integrates EMIs as a sub-category of PIs, thereby repealing the Electronic Money Directive (2009/110/EC). As a result, all entities currently licensed as EMIs will be required to transition and obtain a PI authorisation under the new regime, with specific permissions for e-money issuance.

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

In 2018, the Bank of Lithuania launched its own regulatory sandbox, which was meant to facilitate the introduction of financial innovation in the Lithuanian financial market, especially where regulation of financial innovation is insufficient or unclear. It was also intended to enable the Bank of Lithuania to understand in advance the potential impact of financial innovation on consumers and the financial system; to identify emerging risks and potential regulatory gaps in the financial market related to the application of financial innovation; and to seek to address or mitigate, within the scope of its competence, such regulatory gaps and the potential negative impact of financial innovation.

The sandbox allows potential and existing fintech companies to test financial innovations in a live environment under the guidance and supervision of the regulator. Participation in the sandbox has

many advantages, such as continuous consultation with the regulator; access to real consumers for testing new products and services; exemptions from certain regulatory requirements during participation (ie, no obligation to have a licence in hand); and, except when necessary, no enforcement measures under legal acts applicable either to the participant or its managers.

Fintech companies may enter the regulatory sandbox if their financial innovation meets the following criteria: (1) it is new to Lithuania's market; (2) if implemented, it would bring more convenient, safer and cheaper financial services or other identifiable benefits to consumers; (3) its testing in a live environment is objectively necessary and may contribute to the implementation of the said financial innovation; (4) the financial market participant has carried out an assessment of its adaptability, allocated sufficient resources and carried out a risk analysis; and (5) it will be further developed in Lithuania.

The sandbox was conceived as a horizontal framework applicable to fintech innovations across traditional financial services, and its core rules and objectives have remained unchanged since its introduction in 2018. While, in practice, crypto asset use cases have been limited, the sandbox regime could also be used to test innovative crypto asset-related services, provided that the relevant eligibility criteria are met and that live testing is objectively justified.

Furthermore, the Bank of Lithuania's Newcomer Programme helps potential financial market participants evaluate their opportunities in Lithuania, and provides insight into legislative and licensing requirements for businesses aiming to start their activities in the country. It is a one-stop shop for meetings and consultations with potential financial market participants; basic information about licensing and financial services opportunities in Lithuania; requesting meetings; consultations via email or phone on launching a business or a new product; and checking whether your future plans are in line with legislative and licensing requirements.

Lastly, the Bank of Lithuania provides practical infrastructural support to fintech companies through CENTROLink, its 24/7/365 retail payment system. Through CENTROLink, participating payment service providers are able, under a 'single access point' model, to offer their clients the full range of Single Euro Payments Area (SEPA) payment services, including SEPA Credit Transfers, SEPA Direct Debits and SEPA Instant Credit Transfers. The system is directly connected to the main European instant payment infrastructures: RT1 and the TARGET Instant Payment Settlement system.

From a tax perspective, Lithuania offers tax incentive schemes for small and medium-sized businesses, and tech/fintech businesses.

- Entities whose income during a tax period does not exceed €300,000 are exempted from corporate income tax during the first tax period. These companies are taxed at a rate of seven per cent during other tax periods compared to the standard rate of 17 per cent. In order to benefit from such a tax incentive, the shareholders of an entity should be natural persons.
- Lithuania promotes alternative financing by exempting collective investment undertakings, private equity and venture capital undertakings from corporate income tax – that is, income, dividends and other distributed profits are not taxed. It should also be noted that legal entities' incomes from the increase in the value of assets, dividends and other distributed profits, received from units, shares or contributions held by collective investment undertakings, are also not taxed.

There is also a plethora of both national and EU-wide public and private accelerators that startups may freely apply to. The fintech community is quite unified: Fintech HUB LT unites fintech industry participants in Lithuania, helping them to create the best conditions for their activities, while FINTECH Lithuania also brings together fintechs, developers of IT solutions, service providers for fintechs, legal, licensing and regulatory compliance consultants, banks and other ecosystem participants.

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

In the EU, of which Lithuania is a member, PSD2 requires banks to enable authorised third-party providers to access accounts held by banks in order to provide account information and payment initiation services. However, the framework does not define a single standard for achieving this.

Because open banking operates by allowing third-party financial service providers access to consumer financial data through application programming interfaces (APIs), different API standardisation groups across Europe are working towards harmonisation of the PSD2 API standard, such as the Berlin Group, PolishAPI and STET. The Berlin Group is the leading API standardisation group. It unites almost 40 banks, associations and payment service providers. The majority of banks in Lithuania have also decided to develop the PSD2 API in accordance with the Berlin Group standard that will enable access to customer data for all participants.

6. Regulation of virtual asset service providers.

Until 1 January 2026, virtual asset service providers (VASPs) in Lithuania were regulated under the AML Law. That regime required VASPs to provide notification of their activities to the Register of Legal Entities, but did not provide for a prudential licensing framework. Two categories of VASPs were defined: (1) virtual currency exchange operators, meaning legal persons or branches providing exchange, purchase or sale of virtual currencies for remuneration; and (2) custodian wallet operators, meaning legal persons or branches providing custodial wallet management services. This national notification-based regime was phased out and replaced by the MiCA Regulation, together with the Law on Markets in Crypto-Assets of the Republic of Lithuania, which supplements MiCA at the domestic level. From 1 January 2026, only duly licensed CASPs may provide such services in Lithuania.

The Bank of Lithuania is the competent authority responsible for licensing and supervision. The Bank of Lithuania has indicated that only transparent, well-governed and AML/CFT-compliant companies will be granted authorisation. Applicants must demonstrate that members of the management body and qualifying shareholders are of good repute, possess appropriate knowledge and skills, and can dedicate sufficient time to their duties. They must also show that the institution will implement sound governance (including conflict of interest management and separation of control and operational functions), maintain honest cooperation with the supervisory authority and establish an effective operational presence in Lithuania rather than operating as an 'empty shell'. The Bank of Lithuania also assesses the origin of funds used to finance the business or acquire qualifying holdings in CASPs, and expects applicants to demonstrate familiarity with both MiCA and the Lithuanian regulatory environment.

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

Background of Lithuania's Travel Rule adoption

On 26 June 2015, Regulation (EU) 2015/847 of the European Parliament and of the Council on information accompanying transfers of funds entered into force. Among other objectives, the Regulation aimed to align European legislation with Recommendation 16 of the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, adopted by the Financial Action Task Force (FATF) in 2012. Regulation (EU) 2015/847 defined the information that must accompany fund transfers executed by payment service providers, thereby establishing the so-called 'Travel Rule'. Following its adoption, the FATF extended Recommendation 16 to include VASPs, recognising that transfers of virtual assets present similar money laundering and terrorist financing risks.

In July 2023, Regulation (EU) 2023/1113 (TFR) of the European Parliament and of the Council on information accompanying transfers of funds (recast) entered into force, superseding Regulation (EU) 2015/847 and extending its application to transfers of crypto assets (Transfer of Funds Regulation or TFR). The Regulation extended the definition of 'financial institution' in Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing to encompass CASPs regulated under MiCA. As a result, CASPs are now subject to the same AML/CFT obligations and standards as other credit and financial institutions within the scope of Directive (EU) 2015/849.

In Lithuania there is no separate legislation regulating Travel Rule obligations for VASPs. Instead, AML/CFT and Travel Rule requirements are enforced through the AML Law applicable to all obliged entities, including VASPs. Since TFR is directly applicable, separate transposition into national law is not required.

In addition, the updated European Banking Authority (EBA) Guidelines on the Travel Rule have been in effect since July 2024 (the 'Guidelines'). The Guidelines provide clearer guidance for CASPs on how to collect, hold and transmit originator and beneficiary data when required under the TFR.

General requirements under the TFR: Regulation (EU) 2023/1113

Under the TFR, which is enforced in Lithuania, CASPs must collect, verify, and transmit originator and beneficiary information for crypto asset transfers. Specifically, CASPs are obliged to:

- collect and verify originator and beneficiary information for all qualifying crypto asset transfers: Article 14(1)(2) of the TFR obligates the VASP of the originator to ensure that crypto asset transfers include specific information on the originator and beneficiary. The accuracy of this information must be verified by the provider before making the crypto assets available to the beneficiary;
- detect and handle missing or incomplete information, potentially rejecting or suspending transfers if necessary: Article 16(1) of the TFR stipulates that the beneficiary CASP must take appropriate measures to detect missing or incomplete originator or beneficiary information. Article 17 of the TFR obligates the CASP of the beneficiary to implement effective risk-based

procedures for determining whether to execute, reject, return or suspend crypto asset transfers lacking mandatory information on the originator and beneficiary, as well for taking appropriate follow-up actions. If required information is incomplete or missing, the provider must, on a risk-based approach and without delay, either reject and return transferred crypto assets to the originator's crypto asset account or request the missing information before making the crypto assets available to the beneficiary;

- transmit this information to the recipient's CASP or financial institution during or before the transaction: Article 19 of the TFR requires intermediary CASPs to ensure that all information received on the originator and beneficiary accompanying a transfer of crypto assets is transmitted with the transfer, and that records of such information are retained and available upon request to the competent authorities; and
- retain records of the information for at least five years: Article 26(1) of the TFR states that information on the originator and beneficiary (or payer and payee) shall not be retained for longer than strictly necessary. CASPs of the originator and beneficiary shall retain records of the information referred to in Articles 14–16 for a period of five years.

It must be noted that CASPs must collect and verify information for transactions involving self-hosted wallets, especially for high-value transfers. According to Article 14(5) of the TFR for crypto asset transfers over €1,000 between a CASP and a self-hosted wallet, the CASP of the originator or beneficiary must verify the identity of their own customer or whether the transfer involves a self-hosted wallet of the customer. CASPs must also verify ownership of the self-hosted wallet using cryptographic proof or other effective methods.

These obligations apply to both domestic and cross-border crypto asset transfers, that is, transfers within Lithuania, and between Lithuania and other jurisdictions involving CASPs. Article 2(1) of the TFR covers not only transfers of monetary funds by payment service providers or intermediary payment service providers in the EU but also crypto asset transfers, including those executed via crypto-ATMs, where the CASP, or the intermediary CASP, of either the originator or the beneficiary has its registered office in the EU.

To date, there are no known sanctions from supervisory authorities in Lithuania specifically targeting Travel Rule implementation.

Supervisory authorities in Lithuania

In Lithuania, oversight of AML/CTF obligations on CASPs, including compliance with the Travel Rule under the TFR, is shared between two supervisory authorities: the Bank of Lithuania and the FCIS.

The Bank of Lithuania is the main supervisory body in Lithuania responsible for licensing and full scope monitoring of CASPs under MiCA. The Bank of Lithuania oversees conduct and prudential standards, and ensures that CASPs maintain adequate governance, risk management and compliance systems, according to AML/CFT and TFR requirements. In addition, it is mandated to conduct inspections and impose sanctions, in cooperation with FCIS issue guidance for CASPs, and jointly work on other AML/CFT matters affecting financial market participants, including the implementation of the Travel Rule within the broader AML/CTF framework.

FCIS was the competent authority responsible for the AML/CFT supervision of VASPs throughout the transitional period of implementing MiCA in Lithuania until 31 December 2025. From 1 January 2026, FCIS's main responsibilities towards CASPs are the same as for other financial institutions, including handling suspicious transaction reports and reports on virtual currency transactions equal to or exceeding €15,000 (or the corresponding amount in foreign or virtual currency),¹ issuing instructions in coordination with the Bank of Lithuania. In addition, FCIS supervises CASPs' implementation of the obligations set out in the TFR, that is, collect and verify originator and beneficiary information as required under Articles 14–21 of the TFR.

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

Structuring of financial instruments for tokenised assets

The legal framework applicable to tokenised financial instruments in the EU primarily derives from MiFID II; Regulation (EU) No 600/2014 on Markets in Financial Instruments (MiFIR); and Regulation (EU) 2022/858 on a pilot regime for market infrastructure based on distributed ledger technology (the 'DLT Pilot Regime'). In addition, depending on the nature of the tokenised asset, the MiCA Regulation may also be relevant, although its scope expressly excludes crypto assets qualifying as financial instruments under MiFID II. These EU-level instruments are implemented in Lithuania through the Law on Markets in Financial Instruments, alongside sectoral acts.

Under MiFID II, financial instruments encompass a wide range of assets, including transferable securities, money-market instruments, units in collective investment undertakings and derivative instruments. The decisive factor in determining whether a token qualifies as a financial instrument is the legal nature of the rights it represents, rather than its technological form. Therefore, if a token embodies rights or obligations equivalent to those of a share, bond or derivative contract, it is treated as a financial instrument and remains within the MiFID II/MiFIR regulatory perimeter.

Conversely, MiFID II does not apply to crypto assets that do not display the characteristics of financial instruments. The qualification of a crypto asset therefore requires a case-by-case assessment focusing on the substance of the rights conferred by the token, including whether it constitutes a class of securities; whether it is negotiable on the capital market; whether it primarily serves as an instrument of payment; or whether it mirrors the economic features of shares, bonds, collective investment units or derivative contracts. Where such characteristics are present, the crypto asset is subject to MiFID II rather than MiCA.

In practice, tokenised assets are often structured in two main ways. First, tokens may represent natively issued financial instruments recorded directly on a distributed ledger. This model can be used, for instance, for digital bonds or tokenised shares issued under the DLT Pilot Regime, which allows regulated entities to experiment with DLT-based issuance and trading infrastructures, while maintaining compliance with MiFID II requirements. Second, tokens may represent rights

¹ In addition, from 2 January 2026, all VASPs, which have not obtained a license from the Bank of Lithuania under MiCA, are unregistered from the Register of Legal Entities. Although they will no longer be permitted to carry out activities, FCIS granted an additional three-month period to submit suspicious activity reports and reports on virtual currency transfers equal to or exceeding €15,000 relating to client activity up to 31 December 2025.

to an underlying financial instrument or asset held off-chain, as is often the case with tokenised derivatives or tokenised real estate. In such cases, the token itself is not the financial instrument but serves as a digital record or derivative that reflects the value or performance of the underlying asset. Tokens that do not confer MiFID II type financial rights, such as EMTs or ARTs, may instead fall within the scope of the MiCA Regulation.

Collateral to secure tokenised asset transactions

From practice, most obligations arising from digital asset transactions are generally unsecured. In cases where collateral to secure the obligation is desired, standard methods of securing obligations are used in accordance with the Civil Code of the Republic of Lithuania (the 'Civil Code'), as there is no special regime governing the securing of obligations related exclusively to digital assets. The usual methods of securing obligations include a guarantee, surety, mortgage or pledge.

Legal formalities for securing tokenised asset transactions

Pledge or mortgage

If a pledge (a limited proprietary right over another person's movable property and property rights) or mortgage (a proprietary right over another person's immovable property) is used as security, the Civil Code requires that the agreement be made in writing and specify the secured assets, the underlying obligation, and the terms of the pledge or mortgage. For the security to be valid, perfected and enforceable under Lithuanian law, the agreement must be notarised, and the pledge or mortgage must be registered in the relevant public register (eg, the Register of Contracts, Mortgages or Securities) to ensure its enforceability against third parties. Only Lithuanian citizens with a qualified electronic signature can conclude a pledge agreement via the self-service part of the Centre of Registers of the Republic of Lithuania. There is no stamp duty, but small registration fees apply. The respective corporate approvals must be obtained for entering into a pledge or mortgage agreement in accordance with applicable laws and the by-laws of the companies involved in the transactions.

Both pledges and mortgages are practically difficult to apply when securing tokenised transactions. A pledge can require the transfer of possession of the pledged asset to the creditor or the third party; however, tokens have no physical form, and legal frameworks do not provide a definitive understanding of what constitutes possession in this context, nor is it possible to determine their specific characteristics that would allow them to be pledged. Mortgages generally require asset registration in a recognised public registry, yet tokens exist outside traditional asset registers. Without such asset registration, a mortgage is neither legally valid nor enforceable, which makes the instrument unusable for securing tokenised asset transactions. Also, as mentioned above, pledges and mortgages require notarisation, and notaries in Lithuania do not have experience in certifying tokenised asset transactions, making it difficult to implement this security measure. At present, there is no clear regulation in Lithuania on how enforcement against crypto tokens should be carried out.

Guarantee

When a guarantee (a unilateral commitment by the guarantor to compensate the creditor if the debtor fails to fulfil its obligation) is used to secure obligations, the Civil Code requires a written agreement specifying the principal obligation, the secured amount and the parties. No notarisation or public registration is required. The respective corporate approvals must be obtained in accordance with applicable laws and the by-laws of the companies involved in the transactions.

A guarantee provides the creditor with a personal claim against the guarantor, but it creates no proprietary right in the tokens and offers no mechanism to prevent their transfer or disappearance. Since crypto tokens are not defined as tangible property or as being located in a specific place, enforcement against them is complicated and, in practice, impossible. Furthermore, most guarantees are drafted with conventional financial assets in mind and do not account for the complexity of tokenised assets. As a result, guarantees are generally considered inefficient for securing tokenised asset transactions.

Surety

When a surety (a commitment by the surety to cover the debtor's obligation if it is not fulfilled) is used to secure obligations, the requirement set out in the Civil Code is a written agreement specifying the secured obligation, the principal debtor and any limits of the surety's liability. No notarisation or public registration is required. The respective corporate approvals must be obtained for entering into security agreements in accordance with applicable laws and the by-laws of the companies involved in the transactions.

A surety is a form of personal security that relies entirely on the solvency and creditworthiness of the surety rather than on any direct control over the assets themselves. Enforcement of a surety requires notices, evidentiary procedures and, potentially, litigation against the surety. There is no established practice in Lithuania where crypto tokens are secured by a guarantee and/or surety; therefore, it is difficult to predict whether such a claim would be properly enforced and how it would be enforced, other than by relying on the general principles set out in the Civil Code and the Code of Civil Procedure of the Republic of Lithuania (the 'Civil Procedure Code'). Such jurisdiction-dependent mechanisms are incompatible with tokenised transactions and face disproportionate risks.

Recognition of foreign law contracts in Lithuania

Under Regulation (EC) No 593/2008 (Rome I), which applies in Lithuania as an EU Member State, parties are free to choose the governing law of their contract, that includes contracts involving crypto assets. Lithuanian courts will uphold this choice unless it violates Lithuanian public policy or circumvents mandatory Lithuanian or EU rules (eg, consumer protection or AML).

Enforcement of security interests upon the event of default

Secured lenders have several legal procedures to enforce their security interests in the event of a default. The procedures and rights available depend on the type of collateral and the

nature of the security instrument. If the security agreement includes a notarial deed with an enforcement clause, the lender can bypass court proceedings and enforce the claim through a bailiff, a procedure set forth under the Civil Procedure Code. If the creditor does not have a notarial enforcement deed, it must go through court proceedings to obtain a judgment and then proceed to enforcement.

In Lithuania, public auction is generally required when enforcing security interests through judicial procedures, especially for immovable property or high-value movable assets. This is handled by a bailiff under the Civil Procedure Code. However, a public auction is not required in non-judicial enforcement cases, where the creditor may appropriate the collateral directly or sell it privately, when the legal conditions are met.

Direct appropriation of collateral

Under Lithuanian law, appropriation of collateral is permitted in limited circumstances and subject to strict conditions. It is allowed only where such a right is expressly provided for in the pledge agreement; is not applicable to mortgaged immovable property; and may be exercised only if the debtor does not object to the appropriation.

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

Under Lithuanian law, disputes involving crypto assets are generally treated as contractual commercial disputes, unless they fall under specific categories, such as administrative or criminal law. As of now, there is no special procedural framework governing jurisdiction in disputes specifically related to crypto assets. Accordingly, questions of jurisdiction are determined by the same rules and principles that apply to other civil and commercial disputes.

In cross-border cases within the EU, the principal instrument governing jurisdiction is Regulation (EU) No 1215/2012 ('Brussels Ia'). Where a dispute involves non-EU international elements or is purely domestic, jurisdiction is determined by the Civil Procedure Code and applicable international treaties. Under both Brussels Ia and the Civil Procedure Code, the general rule of jurisdiction is based on the defendant's domicile, providing that actions must be brought before the courts of the defendant's place of residence or registered office. In addition, both EU and national frameworks establish an alternative (special) rule to the general jurisdiction, allowing an action to be brought in the state where the obligation was or should have been performed.

Parties may, however, derogate from the general jurisdictional rules by concluding an agreement designating the courts of a specific state to hear their disputes. Brussels Ia expressly permits such agreements, provided that they are concluded in writing or in a form that satisfies the requirements of established commercial practice. The Civil Procedure Code likewise recognises agreements allowing the parties to alter the territorial jurisdiction of the dispute. Lithuanian law expressly provides that parties engaged in commercial or professional activities may, by written agreement, stipulate that disputes arising from their contractual legal relationships shall be heard by foreign courts, provided that such an agreement does not contravene the law of the state whose courts are designated.

Where no prior jurisdiction agreement exists, but a party brings an action before a court other than that provided for under the general or special rules of jurisdiction, that court may nevertheless proceed to examine the case on the merits if the defendant enters an appearance and does not contest the court's jurisdiction. In situations where the case is heard by a court that is not competent, Brussels Ia provides that if the defendant does not raise any objection to jurisdiction and participates in the proceedings, the defendant is deemed to have tacitly accepted the jurisdiction of the court. Lithuanian courts apply a corresponding principle: even where a court would not otherwise have jurisdiction based on general or special jurisdiction rules, if the defendant participates in the proceedings and fails to object to jurisdiction, and the defendant's conduct can reasonably be interpreted as acquiescence, the court's jurisdiction is deemed validly accepted.

There are, however, certain exceptions to the general possibility of concluding jurisdiction agreements, one of which concerns consumer disputes. Under Brussels Ia, in addition to the defendant's domicile, a consumer has the right to bring an action in the courts of the defendant's place of residence, even if the business is established in another EU Member State. Parties may only depart from these provisions by an agreement concluded after the dispute has arisen. Another exception relates to exclusive jurisdiction, which is recognised under both Lithuanian law and EU procedural law – in such cases, jurisdiction is reserved for specific courts, irrespective of the parties' agreement. Finally, in purely domestic proceedings, specific jurisdiction provided for in the Civil Procedure Code also constitutes an exception, allowing certain categories of disputes to be heard exclusively by designated Lithuanian courts.

The grounds on which a Lithuanian court may refuse recognition or enforcement are listed exhaustively and interpreted narrowly. Importantly, a judgment issued by a non-EU or Member State court cannot be refused enforcement merely because the proceedings were brought in contravention of the general or special jurisdictional rules. Among the limited exceptions listed in EU and national rules are cases where the judgment infringes the rules on exclusive jurisdiction, or where enforcement would be manifestly contrary to the public policy (*ordre public*) of Lithuania. However, the latter exception is applied narrowly: not every infringement of national law amounts to a breach of public policy, which is reserved for cases that would clearly undermine the fundamental principles of the Lithuanian legal order. Finally, under Brussels Ia, enforcement may also be refused in consumer cases, where mandatory jurisdictional protections apply to ensure that consumers are sued only in the courts of their domicile.

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

At present, there are no specific national laws or case law that deal directly with crypto assets in the field of IP. Nevertheless, there are certain pieces of IP law that could provide a useful basis for addressing certain issues related to crypto assets.

Copyright

Under the Law on Copyright and Related Rights of the Republic of Lithuania ('LCRR'), copyright protection applies to original literary, scientific and artistic works that are expressed in an

objective form. Accordingly, for a creation to qualify as a copyright-protected work, it must satisfy two cumulative requirements: (1) originality, reflecting the author's intellectual and creative contribution; and (2) objective form, meaning that the work must be expressed with sufficient precision and objectivity. Therefore, under Lithuanian law, due to their nature, crypto assets, such as cryptocurrencies or non-fungible tokens (NFTs), cannot per se be considered subject matter protected by copyright. However, their constituent elements – for example, an original computer program or the artwork embedded in an NFT – may qualify for such protection.

The copyright owner, as defined in the LCRR, may be: (1) the author; (2) another natural or legal person holding the author's exclusive economic rights in the cases stipulated by LCRR; or (3) a natural or legal person to whom the author's exclusive economic rights have been transferred. It must be emphasised that the status of 'author' is invariably vested in the natural person who has created the work, and such a person enjoys the fullest scope of rights thereto, encompassing both economic and moral rights from the moment of creation of such works. Conversely, other persons may only acquire the author's economic rights (moral rights cannot be transferred) explicitly transferred to them by contract, through inheritance or in any other manner prescribed by law.

Industrial property: patent law

Similarly to copyright, it is not possible to obtain patent protection for a crypto asset itself. Moreover, the European Patent Convention (EPC) and Patent Law of the Republic of Lithuania ('PL') exclude the patenting of computer programs *as such*.

However, this exclusion does not apply to computer programs that possess a technical character. To be considered to have a technical character, and thus fall outside the exclusion from patentability, a computer program must produce a 'further technical effect' when run on a computer.

Given that blockchain operates on a decentralised computer network, blockchain-related subject matter may, under certain circumstances, fall within the concept of a computer-implemented invention in the meaning of the EPC. Accordingly, if such an invention exhibits the requisite technical character and the remaining statutory conditions are satisfied, namely, that the invention is novel, involves an inventive step and is capable of industrial application, such an invention may, in principle, be deemed to meet the criteria for patentability and thus be eligible for patent protection.

Under PL, only a natural person who has conceived the invention may be recognised as the inventor; however, the right to the patent may vest in a broader range of persons, including a successor in title or the employer. Any transfer of such a right shall only become effective upon its registration in the Register of Patents of the Republic of Lithuania.

Trademarks

Trademark protection applies to signs that meet the statutory criteria for registrability. Signs containing verbal, graphical or other distinctive elements that satisfy these legal requirements may be registered as trademarks. In this context, the names and logos of crypto assets may qualify for trademark protection if they consist of signs that: (1) are capable of distinguishing the goods or services of one person from those of other persons (capable of fulfilling the function of origin); (2)

can be entered in the Register of Trade Marks of the Republic of Lithuania in such a way that the competent authorities and the public can clearly and precisely identify the subject matter of the protection afforded to the proprietor of the mark; and (3) do not fall within the absolute grounds for refusal or invalidation.

Under the Law on Trade Marks of the Republic of Lithuania (LTM), any natural or legal person may apply for a trademark. The right to the mark applied for or registered may be transferred in respect of all or some of the goods or services for which it has been registered.

Enforcement

IP enforcement depends on the type of right. Available remedies include provisional measures, civil and administrative procedures, border measures and criminal sanctions. In case of infringement, rights holders may seek judicial protection, for example, through the recognition of rights, injunctions, damages or removal of infringing goods from the market.

Foreign protection

IP rights are inherently territorial and enforceable solely within the jurisdiction in which they have been granted by the competent foreign IP authority. Consequently, rights holders seeking protection beyond Lithuania must obtain registration and enforce their rights in each jurisdiction where they intend to carry out commercial activities or foresee exploitation of their IP.

Monetisation

While there are no absolute prohibitions on the monetisation of IP rights, any disposition or transfer thereof must comply with statutory procedures.



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