

Luxembourg

Marc Moutan

Arendt & Medernach, Luxembourg

marc.mouton@arendt.com

Frédéric Schmit

Arendt & Medernach, Luxembourg

frederic.schmit@arendt.com

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

The Luxembourg fintech regulatory framework has been developing to accompany the continuous digitalisation of the financial sector through legislative measures introduced between 2019 and 2024.

In 2019, Blockchain Law I introduced definitions of blockchain-related concepts and recognised the use of distributed ledger technology (DLT) for the custody and transfer of book-entry securities. Subsequent reforms in the form of Blockchain Laws II and III built on this foundation by modernising the regime for issuing dematerialised securities on a blockchain, authorising European Union and European Economic Area (EEA) credit institutions and investment firms to act as central account keepers for unlisted debt securities, keeping issuance accounts on DLT and confirming that DLT-held instruments benefit from the Luxembourg legislation protecting financial collateral.

On 19 December 2024, Luxembourg adopted Blockchain Law IV, which introduced several innovations that advance the modernisation of the capital markets framework through DLT.

A key innovation introduced by Blockchain Law IV is the creation of the control agent role. The control agent has been conceptualised with the objective to unbundle the functions concentrated in the central account keeper under the pre-Blockchain IV framework. Under that regime, the central account keeper was responsible both for maintaining issuance accounts and for acting as the top tier custodian. Blockchain Law IV seeks to enhance efficiency by reducing intermediaries while preserving the integrity of the issuance and holding process. Therefore, the control agent is granted authorisation to maintain the issuance account, to track the chain of ownership of securities and to reconcile issued securities without itself acting as custodian.

The function of control agent may be entrusted to a Markets in Financial Instruments Directive (MiFID) investment firm, an EU credit institution or a settlement organisation designated by the issuer. Although no authorisation from the national regulator is required, entities intending to assume this role must provide prior notification to the national regulator, Commission de Surveillance du Secteur Financier (CSSF). The notification is to be provided no later than two months before starting the activity; the prospective control agent must provide documentation showing that it meets the relevant prudential standards, including governance, IT and operational requirements.

The second key development introduced by Blockchain Law IV is the extension of the tokenisation framework to unlisted equity securities and thus also to fund units, moving beyond the earlier focus on debt instruments. By expressly allowing these instruments to be issued and recorded on DLT-based infrastructures, the Law enables the tokenisation of fund shares and units, and facilitates their administration through distributed ledger systems. It is worth noting that this is not the only possibility to keep fund shares/units or other securities on DLT under Luxembourg law as there is also the option of keeping registered securities on-chain (an option that is in certain respects more straightforward).

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

The regulatory framework governing crypto assets in Luxembourg is mainly constituted by the Markets in Crypto-assets Regulation (EU) 2023/1114 ('MiCAR'). Local enforcement provisions were incorporated into Luxembourg law by the Law of 6 February 2025, amending the Law of 16 July 2019 on the operationalisation of European regulations in the area of financial services ('Law of 2019').

Under MiCAR, crypto assets are defined as digital representations of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology. Crypto assets are further divided into three types: (1) crypto assets other than asset-referenced tokens (ARTs) or e-money tokens (EMTs) ('Other CA'); (2) EMTs; and (3) ARTs.

Other CA

Under MiCAR, there is no definition for Other CA. Persons interested in offering Other CA to the public must meet specific legal requirements. These include being a legal person, and the requirement of a crypto asset white paper, duly drawn up, notified and published. Furthermore, marketing communications must be drafted and published in accordance with the criteria in MiCAR. Depending on whether the person wishes to offer or trade Other CAs, certain requirements may be subject to exceptions under specific circumstances. These requirements are set out in Article 4 and following of MiCAR.

A crypto asset white paper provides potential holders with valuable information on:

- the offeror, issuer and operator;
- the underlying technology;
- the offer to the public and admission to trading;
- the Other CA itself;
- the rights and obligations attached to it; and
- the risks.

Its purpose is to provide potential holders with all the necessary information to make an informed decision and safeguard their interests. Offerors, operators and persons seeking admission to trading are liable for losses incurred to the holders of Other CA if the information in the corresponding white paper is false, incomplete, unfair, unclear or misleading.

Once a crypto asset white paper has been published, the offeror can offer Other CAs throughout the EU. These Other CAs can be admitted to trading on a crypto asset trading platform in the EU.

Other CA offerors who have not set a time limit on their offer must publish the number of units of the crypto assets in circulation on their website at least monthly. Those who have set a time limit

on their offer must publish the results of the public offer on their website within 20 days of the end of the subscription period.

Retail holders who purchase an Other CA have 14 calendar days to cancel their order free of charge and without giving a reason (cooling-off period). They are also entitled to reimbursement of all payments made in relation to their purchase within 14 days. Reimbursement must be made using the same payment method used by the retail holder for the initial transaction, unless otherwise agreed.

EMTs

EMT is defined as a type of crypto asset that maintains a stable value by referencing the value of one official currency. 'Official currency' is defined as an official currency of a country that is issued by a central bank or other monetary authority.

Persons wishing to issue EMTs must be authorised as a credit institution or as an electronic money institution. They must also have drawn up a crypto asset white paper and marketing communications, and published them in accordance with the specified criteria. Both documents should be communicated to the CSSF.

The content of a crypto asset white paper for an EMT is similar to that of an Other CA, with the difference that it should only include information about the EMT's issuer, and not its offeror and operator. Like Other CA, issuers of EMTs are liable for the losses incurred to the holder of their EMT when the information on their white paper is false, incomplete, unfair, unclear or misleading. Issuers of EMTs have an obligation to notify the CSSF 40 days before the date on which they intend to offer EMTs to the public or trade EMTs. The relevant provisions are set out in Articles 48 and following of MiCAR.

Issuers of EMTs cannot grant interest in relation to EMT and the services connected to them. In other words, it is not possible for the issuer to pay a yield to holders of EMTs.

Issuers of EMTs must abide by specific requirements regarding the issuance, redeemability, as well as recovery and redemption plans of their EMTs.

EMT should be issued at par value and upon the receipt of funds.

As for redemption, issuers of EMTs should be able to redeem at any time, at par value, by paying in funds in the monetary value of the EMTs held by the holder upon their request.

A recovery plan provides measures to be taken by the issuer to preserve its services related to the EMTs, the timely recovery of operations and the fulfilment of its obligations in cases of events posing a significant risk of disrupting operations.

A redemption plan is an operational plan supporting the orderly redemption of each EMT. When the CSSF has doubts as to the issuer's capacity to fulfil its obligations, for example, in cases of insolvency, resolution or withdrawal of authorisation, it can order for the redemption plan to be implemented.

EMTs must be classified as significant by the European Banking Authority (EBA) or on a voluntary basis by their issuer if they exceed certain volumes of holders, values or numbers of transactions. Significant EMTs are subject to heightened supervision by the CSSF, the EBA, the European Central Bank (ECB) and sometimes the Central Bank of Luxembourg (BCL). Issuers of significant EMTs have additional obligations to fulfil.

ARTs

ARTs are defined as: ‘a type of crypto-asset that is not an electronic money token and that purports to maintain a stable value by referencing another value or right or a combination thereof, including one or more official currencies’.

Issuers of ARTs are subject to an authorisation procedure before they can offer their crypto asset. There are specific eligibility criteria for legal persons and credit institutions wishing to offer or trade ARTs. The relevant provisions are set out in Articles 16 and following of MiCAR.

Similarly to Other CA and EMT issuers, ARTs issuers have to prepare a crypto asset white paper, duly drawn up, notified and published, as well as drawing up and publishing marketing communications, all of which should be made available to the CSSF upon request. The content of a crypto asset white paper for an ART is very similar to that of an EMT, with the difference that it should also provide information on the ART issuer’s reserve of assets.

An ART issuer must submit an application for authorisation to the CSSF. The assessment of the application for authorisation by the CSSF is subject to several requirements. The CSSF has the right to grant or refuse the authorisation as well as withdraw it under specific circumstances.

ART issuers are subject to additional obligations such as reporting, own funds and reserve of assets. The prohibition on granting interest also applies to ARTs.

As for recovery and redemption plans, the same rules apply to both ARTs and EMTs, with the only difference that recovery plans for ART should also include measures to restore compliance with reserve of assets requirement.

Like EMTs, ARTs can be classified as significant by the EBA or on a voluntary basis. The criteria are the same as for both types of crypto assets.

MiCAR does not only protect investors via rules applying to issuers of crypto assets, but also via regulatory rules of conduct, organisation and liability applying to crypto asset service providers (CASPs) when providing crypto asset services. Key investor protection rules to be mentioned in this respect include rules applying to custody services and best execution requirements.

With respect to custody services, Article 75 of MiCAR provides for a comprehensive set of requirements including but not limited to:

- the conclusion of a written custody agreement with some mandatory contents;
- the keeping of a register of client positions which needs to be kept up to date;

- the adoption of a custody policy with the aim to minimise the risks of fraud, cyber threats, negligence and losses for clients;
- the reporting to the client on a regular basis of statements of positions;
- the adoption of procedures facilitating the return of crypto assets;
- the segregation of client assets; and
- liability rules for the loss of crypto assets due to incidents attributable to the CASP.

With respect to best execution requirements, Article 78 of MiCAR obliges CASPs, when executing orders for crypto assets on behalf of clients, to take all the necessary steps to ensure the best possible outcome for their clients and implement effective execution arrangements in this context such as an order execution policy. CASPs need to obtain prior consent from clients regarding the order execution policy and must be able, upon request from their clients and from competent authorities, to demonstrate that their orders were carried out according to the order execution policy.

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

Luxembourg regulates payment service providers (PSPs) and digital wallets through a framework centred on the law of 10 November 2009 on payment services (Payment Services Law or PSL), which implements Directive (EU) 2015/2366 on payment services in the internal market ('PSD2') and Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions. The CSSF is the single competent authority for authorisation, prudential and conduct supervision of payment institutions (PIs), electronic money institutions (EMIs) and account information service providers (AISPs).

PSPs

The PSL distinguishes three main categories of regulated PSPs.

- PIs under Article 6 of PSL require prior CSSF authorisation for providing payment services as listed in Annex I (cash services, execution of payment transactions, offering of payment accounts, card acquiring and issuance, money remittance, payment initiation and account information services).
- EMIs are authorised under Article 24-2 of PSL to issue electronic money and to provide payment services alongside e-money services.
- AISPs providing only consolidated account information are subject to a lighter registration regime under Article 48-1a of PSL, rather than full authorisation. Unlike PIs and EMIs they are not subject to own-funds *minima*, but they are required to meet professional indemnity, security and governance standards.

Moreover, credit institutions may engage in the provision of payment services.

For PIs and EMLs, the CSSF operates a structured three-stage licensing process consisting of: (1) a preliminary contact and presentation; (2) pre-instruction review of some key sections of an electronic file and the same in relation to the full file; (3) and formal instruction phase leading to issuance of the licence and inclusion in the CSSF and EBA registers.

The PSL imposes stringent safeguarding obligations. PIs and EMLs must segregate client funds from their own assets or obtain equivalent protection via insurance or comparable guarantees for safeguarding of funds in case of insolvency. These requirements are reinforced by CSSF guidance articulated in expectations on reconciliations and record-keeping.

A recent development is Circular CSSF 26/906, published on 19 January 2026, which enhances the governance and risk management framework for PIs, EMLs and AISP, with a compliance deadline of 30 June 2026. The circular covers the role and responsibilities of the management body, the structure and independence of internal control functions (compliance, risk management, internal audit), conflicts of interest, new product approval process, and detailed organisation of funds safeguarding.

A key aspect of the PSP regulatory framework is security and access-to-account provisions. Commission Delegated Regulation (EU) 2018/389 on strong customer authentication (the 'SCA Regulation') and secure communication is fully applicable in Luxembourg. PSPs must implement SCA based on at least two independent elements (knowledge, possession and inherence) and apply dynamic linking for remote payments with narrowly defined exemptions. In addition, account-servicing PSPs must provide secure interfaces to PISPs and AISPs, offer technical documentation and testing facilities, and maintain a contingency mechanism unless exempted by the CSSF.

Luxembourg PSPs are also fully integrated into the national and EU anti-money laundering/counter financing of terrorism (AML/CFT) framework. They are obliged entities under the Law of 12 November 2004 as amended, applying a risk-based approach to know your customer (KYC), monitoring, reporting and internal controls, guided by the 2025 update of the national money laundering risk assessment and by forthcoming Regulation (EU) 2024/1620 (the 'Anti-Money Laundering Regulation' or AMLR), Directive (EU) 2018/1673 (the 'Sixth Anti-Money Laundering Directive' or AMLD6) and Regulation (EU) 2024/1624 (the 'Anti-Money Laundering Authority' or AMLA) reforms.

Authorised Luxembourg PIs and EMLs benefit from passporting rights under the PSL. They may provide services throughout the EEA via branches or cross-border services upon notification to the CSSF, which coordinates with host authorities. Similarly, EEA-authorised PSPs may passport into Luxembourg following home-state notification.

Several directly applicable EU instruments significantly shape Luxembourg's regime.

- The Instant Payments Regulation (Regulation (EU) 2024/886) has become applicable since 9 October 2025, obliging Luxembourg PSPs to receive and send real-time euro credit transfers with 24/7 availability, settlement within seconds and fee parity with standard credit transfers, up to €100,000 per transaction.
- The Digital Operational Resilience Act (DORA – Regulation (EU) 2022/2554) has come into effect as of 17 January 2025. It covers PIs, EMLs and banks, imposing harmonised obligations

on ICT risk management, major incident reporting, resilience testing and third-party risk oversight. Luxembourg transposed consequential changes via a law of 1 July 2024 and CSSF circulars 25/880–25/883 and 25/885–25/886.

- MiCAR applies to the issuance of e-money tokens and the provision of services in this respect.

A political agreement in relation to the Third Payment Services Directive ('PSD3') and the Payment Services Regulation (PSR) has been reached on 27 November 2025, with formal adoption expected in 2026. PSD3 will recast the licensing and prudential regime, including merging the separate e-money directive into a single regime for PIs/EMIs. PSR will on the other hand directly harmonise conduct-of-business rules on transparency, rights, fraud and open banking.

Digital wallets

Under Luxembourg law, the regulatory characterisation of a digital wallet depends on its functions.

- A wallet that stores monetary value redeemable against the issuer that can be used to pay third parties is typically electronic money, requiring EMI authorisation under the PSL.
- A wallet in which funds can be stored and payments executed would typically fall under the payment institution perimeter, requiring PI authorisation under the PSL.
- A wallet used for custody of crypto-assets or private keys on behalf of clients is within the CASP perimeter under MiCAR and requires CSSF CASP authorisation for the wallet provider.
- A wallet used to for custody of tokenised financial instruments would typically require a credit institution or investment firm licence.

Overall, Luxembourg garners a landscape in which PIs, EMIs and digital wallet providers face a number of requirements on authorisation, internal governance, safeguarding, security, open banking access and operational resilience, against the backdrop of a cross-border passport that allows Luxembourg-licensed entities to scale across the EEA.

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.

The Luxembourg financial sector is a major global hub for banking, investment, insurance and sustainable finance. It brings together a large network of institutions managing over €5tn in assets and serving markets around the world. Luxembourg supports fintech startups through public and private initiatives without a traditional regulatory sandbox.

The CSSF established an Innovation Hub in 2020 providing regulatory guidance and informal consultations within existing financial services regulation, applying a technology-neutral approach where legal qualification is assessed based on services provided regardless of technology used. The Innovation Hub serves as a dedicated point of contact for persons presenting innovative projects or

seeking dialogue on financial innovation challenges, though it does not grant regulatory waivers or lighter supervision.

The Luxembourg House of Financial Technology (LHoFT) is a private-public platform founded in 2016. It operates multiple acceleration programmes targeting sectors including green fintech, banktech and fundtech. As of 2026, the LHoFT has supported 211 fintechs, accelerated 190 startups, and is supported by a network of over 300 mentors and experts. Similarly, Fit 4 Start, managed by Luxinnovation since 2015, targets early-stage ventures in the digital, healthtech and space sectors. Selected startups are provided with up to €150,000 in equity-free funding, six months of intensive coaching and access to co-working spaces under the programme.

The Société Nationale de Crédit et d'Investissement announced €300m in financing over five years in March 2025 targeting cybersecurity, deeptech, sustainable technologies, healthtech, space and fintech. Moreover, the Ministry of the Economy offers research and innovation subsidies up to 50 per cent co-financing, an 18 per cent tax credit for digital innovation, and a spin-off aid programme providing up to 80 per cent co-financing capped at €200,000.

On the regulatory side, while Luxembourg has not established a regulatory sandbox for financial services, it applies Regulation (EU) 2022/858 on a pilot regime for market infrastructures based on distributed ledger technology (the 'DLT Pilot Regime'). The DLT Pilot Regime entered into force on 23 March 2023 as a temporary regime under which market infrastructures can obtain exemptions from applicable financial regulations to use DLT for trading and settlement of securities transactions. The regime introduces three types of market infrastructures: DLT multilateral trading facilities, DLT settlement systems, and DLT trading and settlement systems, which may benefit from temporary exemptions for up to six years from obligations under Directive 2014/65/EU (MiFID II), Regulation (EU) No 600/2014 (MiFIR), and Regulation (EU) No 909/2014 (CSDR) that would otherwise restrict use of DLT. Luxembourg implemented the DLT Pilot Regime through Blockchain Law III, amending the definition of financial instruments to clarify inclusion of instruments issued using DLT.

The CSSF is the competent authority for DLT Pilot Regime applications, whereas early-stage project initiators are encouraged to contact the CSSF Innovation Hub for preliminary guidance.

The DLT Pilot Regime is set to be significantly extended as part of the EU Commissions Market Integration Package/Savings and Investment Union initiative.

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

Luxembourg does not have a standalone legal framework specific to open banking. Instead, Luxembourg open banking requirements derive from PSD2 as implemented into the PSL and PSD 2 implementing regulations such as Commission Delegated Regulation (EU) 2018/389 on strong customer authentication (SCA) and common and secure open standards of communication.

Account-servicing payment service providers (ASPSPs) including credit institutions, EMIs, Post Luxembourg and PIs must grant third-party payment service providers secure access to customer payment account data subject to the customer's explicit consent. ASPSPs must provide at least one secure access interface, either a dedicated application programming interface (API) or an adapted customer interface, make technical documentation available, provide testing facilities and employ

qualified eIDAS certificates for third-party provider (TPP) identification. Where a dedicated interface is offered, a contingency mechanism must be implemented unless the CSSF grants an exemption under the conditions specified in Article 33(6) of the SCA Regulation.

In practice, Luxembourg's banking sector operates LUXHUB, a centralised open banking API platform founded by four major banks and implementing the Berlin Group NextGenPSD2 framework, enabling accredited TPPs to access account information, initiate payments and confirm fund availability. Other private providers also offer solutions in the market.

The Law of 13 June 2017 on payment accounts complements open banking by establishing payment account switching obligations, enabling consumers to facilitate transfers of accounts, and transfer standing orders and direct debits between accounts.

Looking ahead, the regulatory environment for open banking is expected to further evolve at the EU level. The European Commission has made proposals to further broaden open banking (without exact timelines being known at the present time) and to modernise the existing framework under the proposed PSD3 and PSR.

6. Regulation of virtual asset service providers.

The regulatory framework governing the authorisation of CASPs in Luxembourg is MiCAR.

The CSSF is the Luxembourgish competent authority responsible for ensuring the application of MiCAR. The CSSF has the authority to request information, suspend or prohibit services or activities related to crypto assets, order changes to white papers and marketing communications, require the disclosure of important information, make non-compliance public, order the cessation of unauthorised activities, require the transfer of contracts, and protect customers by intervening in offers, negotiations and platforms when violations or risks are identified.

Under MiCAR, there is a single definition for CASPs. They are defined as legal persons or other undertakings whose occupation or business is to provide one or more crypto asset services to clients on a professional basis, and that are allowed to provide crypto asset services.

Crypto asset services are defined as any of the following services and activities relating to any crypto asset (including ARTs, EMTs and Other CA):

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

- providing advice on crypto assets;
- providing portfolio management on crypto assets; and
- providing transfer services for crypto assets on behalf of clients.

Accordingly, all of the crypto asset services enumerated above are regulated activities in Luxembourg.

CASPs are subject to an authorisation procedure under MiCAR. There are specific eligibility criteria for legal persons and certain credit institutions wishing to provide crypto asset services. The assessment of the application for authorisation by the CSSF is subject to several requirements. The CSSF has the right to grant or refuse the authorisation as well as withdraw it under specific circumstances. CASPs wanting to provide an additional crypto asset service to their clients must update their initial application for authorisation and wait for the approval of the CSSF before providing such crypto asset service.

Under the reverse solicitation exemption, third-country firms providing crypto asset services to a client based in Luxembourg can do so without authorisation if this happens at the client's sole initiative.

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

In Luxembourg, the AML/CFT framework is built around the MiCAR concept of CASPs, rather than the VASP category. The AML/CFT legal framework on CASPs in Luxembourg is composed of various laws and regulations supplemented by CSSF and EBA guidance; the most relevant ones being:

- the law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended (the 'AML Law');
- CSSF Regulation 12-02;
- Regulation (EU) 2023/1113 on information accompanying transfer of funds and crypto assets ('Reg 2023/1113'); and
- EBA Guidelines on information requirements in relation to transfers of funds and certain crypto assets transfers under Reg 2023/1113 (EBA/GL/2024/11) (the 'Travel Rule Guidelines').

Both Reg 2023/1113 and AML Law are enforceable; as for the Travel Rule Guidelines, they are non-binding but widely respected. As of 1 January 2026, the EBA has transferred its AML/CFT powers to the new AML authority, AMLA.

As per the AML Law, the CSSF is the competent Luxembourgish supervisory authority for AML/CFT purposes.

CASPs have been added to the scope of the AML Law by the Law of 6 February 2025, which implemented the provisions of MiCAR and Reg 2023/1113 into Luxembourg law. CASPs are required to include specific information on the originator and beneficiary with transfers of crypto assets to make these transfers traceable. CASPs also have to apply specific measures in relation to transfers of crypto assets involving self-hosted addresses.

A 'self-hosted address' means a distributed ledger address not linked to either of the following: (1) a CASP; and (2) an entity not established in the EU and providing services similar to those of a CASP.

In the event of a transfer of crypto assets and of a transfer to or from a self-hosted address, the CASPs from both the originator and beneficiary are obliged to collect information regarding both the originator and the beneficiary. In the event of a transfer of crypto assets being made from a self-hosted address, the CASPs are obliged to obtain and retain the originator's and beneficiary's information, as well as to ensure that the transfer of crypto assets can be individually identified. In principle, CASPs should not be required to verify the information on the user of the self-hosted address. However, in the event of a transfer amounting to more than €1,000 being sent or received on behalf of a client of a CASP to or from a self-hosted address, the CASPs are obliged to verify whether that self-hosted address is effectively owned or controlled by that client. Before transferring crypto assets, the originator's CASP must verify the accuracy of the information on the basis of documents, data or information obtained from a reliable and independent source. The same obligation applies to the beneficiary's CASP before making the crypto assets available.

If a CASP knows or discovers that originator or beneficiary information is inaccurate, or detects unusual, suspicious or high-risk transaction patterns, it should apply, where appropriate, enhanced due diligence measures to manage and mitigate the associated AML/CFT risks. The same applies to transfers from a self-hosted address.

Transfers of crypto assets should be subject to the same requirements regardless of their amount and of whether they are domestic or cross-border transfers.

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

Under Luxembourg law, tokenisation of securities is possible both for registered securities and dematerialised securities. This has been recognised by authorities and in law.

There is a common industry position that the law on commercial companies allows for the tokenisation of registered securities. The tokens taken together need simply to reflect all information required to be included in a securities register, and such information needs to be accessible from the corporate seat of the issuer. The CSSF has already validated a number of fund tokenisation projects under this approach and has enabled regulated registrar agents to keep securities registers on-chain.

Another option is to tokenise securities using dematerialised securities held on DLT under the Blockchain Laws. The latest Blockchain Law also introduced the concept of the 'control agent', which is allowed to hold the issuance account, while securities accounts can be held with multiple custodians throughout the EU.

As previously discussed, Blockchain Law IV expanded the scope of using control agents and central account keepers also to unlisted equity securities. Consequently, the tokenisation of real estate investments held via corporate vehicles, digital bonds and fund units, and other types of securities has been enabled.

For financial instruments within MiFID II scope held on DLT, the Law of 5 August 2005 on financial collateral arrangements (the 'Financial Collateral Law'), amended by Blockchain Law III and adopted on 15 March 2023 applies. The Blockchain Laws confirmed that pledges over such instruments are perfected through control agreements with custodians, account registration or issuer notification, without requiring notarisation, public registration or stamp duty. By contrast, security interests in native crypto assets not qualifying as MiFID II financial instruments fall outside the Financial Collateral Law regime. Instead, they are governed by Luxembourg law pledge provisions under the Commercial Code.

To our knowledge, there is not yet much market experience with secured transactions involving crypto assets. As far as tokenised financial instruments are concerned, we expect the Financial Collateral Law to fully apply, including in respect of the enforcement possibilities foreseen under such law such as appropriation and assignment. The protections of the collateral arrangements in case of insolvency are also expected to apply. As regards crypto assets not qualifying as financial instruments, the more cumbersome enforcement mechanics of the Commercial Code apply which require, for example, a prior notice.

There are no specific private international law rules for crypto assets in Luxembourg, so general intellectual property rights concepts apply.

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

Luxembourg courts generally recognise and enforce parties' submission to foreign jurisdiction and exclusive jurisdiction clauses under Regulation (EU) No 1215/2012 (the 'Brussels I bis Regulation') for intra-EU matters and applicable bilateral treaties or domestic law for third-country jurisdictions.

Under Article 25(1) of Brussels I bis, parties may agree that a court of a Member State has jurisdiction to settle disputes, and such agreement is binding regardless of domicile. The Court of Justice of the EU confirmed in *Società Italiana Lastre SpA v Agora Sarl* (Case C-537/23) that asymmetric jurisdiction clauses are valid provided three conditions are met:

1. the clause must designate courts of one or more EU Member States with certainty;
2. the clause must be clear and comprehensible; and
3. the clause must not violate protective jurisdiction provisions under Articles 10–23 of Brussels I bis.

Where an exclusive jurisdiction clause designates a Luxembourg court, Article 31(2) of Brussels I bis requires other Member State courts to stay proceedings until the designated court declares it lacks jurisdiction.

For jurisdiction clauses designating third-country courts, enforcement depends on applicable bilateral treaties.

Luxembourg is bound by the Hague Convention of 2 July 2019 on the Recognition and Enforcement of Foreign Judgments in Civil and Commercial Matters (entered into force 1 September 2023),

which applies to exclusive choice of court agreements designating contracting state courts. Absent an applicable treaty, Luxembourg domestic law under Article 678 of the New Civil Procedure Code governs recognition, requiring verification of international jurisdiction, procedural regularity and absence of contradiction with Luxembourg public policy.

Arbitration agreements constitute an alternative, especially where institutional counterparties are concerned. Luxembourg courts recognise arbitration clauses and decline jurisdiction where a valid arbitration agreement exists conditioned to verification of the agreement's validity and applicability. Arbitral awards are enforceable under the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards.

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

Luxembourg protects intellectual property related to crypto assets through patent, copyright, and trademark frameworks.

Patents receive protection through three routes: (1) national Luxembourg patents filed with the Intellectual Property Office (OPI); (2) European patents designating Luxembourg via the European Patent Office (EPO); or (3) international applications under the Patent Cooperation Treaty. The EPO classifies blockchain inventions as computer-implemented inventions subject to stringent case law requiring demonstration of a technical effect beyond merely employing a computer to implement a known algorithm. A blockchain invention must solve a technical problem or produce a technical effect tied to the functioning of the technical system itself, rather than merely automating an abstract business method. It must also demonstrate novelty in differing from prior art in at least one technical feature and inventive step.

Copyright protection applies automatically to blockchain software, smart contracts, and original digital content without registration. For non-fungible tokens (NFTs), ownership is distinguished from copyright. Purchasing an NFT typically conveys ownership of the token and a licence to display or resell underlying digital content, while the creator retains underlying copyright unless explicitly transferred through smart contract licensing terms. Trademark infringement applies where NFTs authenticate digital items incorporating protected marks without authorisation.

Enforcement against third-party infringement of IP rights related to crypto assets proceeds through remedies specified in Luxembourg's Patent, Copyright, and Trademark Acts. Patent holders may seek cessation of infringement through provisional or permanent injunctions with daily fines, publication of judgments, damages compensating harm caused, and confiscation or destruction of infringing goods and instruments specifically intended for committing infringement. The *saisie-contrefaçon* procedure constitutes a specialised enforcement mechanism enabling rights holders, after judicial authorisation, to enter alleged infringers' premises to gather evidence and seize allegedly infringing articles within three months from notification.

Patent infringement claims must be initiated within three years from the date the rights holder becomes aware of both the alleged infringement and the infringer's identity. Beyond civil remedies, criminal sanctions range from fines, confiscation or destruction of infringing goods to

imprisonment for bad-faith or fraudulent infringement. For NFT-related trademark disputes, where NFTs authenticate digital items incorporating protected marks without authorisation, trademark owners invoke standard infringement procedures adapted to the digital context.

Assessment of foreign jurisdiction protection for blockchain and crypto asset innovations depends on market importance, likelihood of infringement, enforcement effectiveness and cost considerations. Luxembourg's participation in the European Patent Convention enables applicants to designate all Member States through a single EPO application, while Patent Cooperation Treaty applications enable designation of up to 146 countries, deferring national phase entry costs while preserving priority rights.

Luxembourg imposes no sector-specific prohibitions on licensing or transferring IP rights related to crypto assets, with such transactions governed by general commercial law principles. IP licensing agreements are enforceable under Luxembourg contract law and the Rome I Regulation choice-of-law principles. Smart contracts embedding licensing terms are recognised as valid contractual arrangements, provided they satisfy essential contract formation requirements.



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