

The Netherlands

Roderik Vrolijk

Stibbe, Amsterdam

roderik.vrolijk@stibbe.com

Jibraeel Mussani

Stibbe, Amsterdam

jibraeel.mussani@stibbe.com

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

As a principle, legislation in the Netherlands is technology neutral. Financial regulatory laws are based on the same activity, same risk and the same regulatory principle. Activities are regulated irrespective of the use of technology by the service provider. Accordingly, the Dutch fintech regulatory framework lacks a uniform and harmonised character. To date, the Dutch legislator has mostly adapted the existing rules applicable to traditional banking and financial services and implemented European Union directives directed at particular segments of the fintech industry (eg, crypto asset service providers, electronic money institutions (EMIs) and payment institutions).

The key laws and regulations that apply to fintech companies in the Netherlands are the following directly applicable EU regulations:

- the Markets in Crypto Instruments Regulation (MiCAR), is an EU framework regulating crypto assets and related services. MiCAR promotes innovation, ensures legal certainty, protects consumers and market integrity, and safeguards financial stability through licensing for crypto asset service providers (CASPs), white paper requirements, and anti-money laundering rules;
- the General Data Protection Regulation (GDPR) is an EU regulation that governs the processing of personal data. The GDPR is central for fintechs and payment service providers because their core business is the large-scale processing of highly sensitive personal and financial data, which makes them subject to the full set of GDPR obligations and enforcement risks. For payment institutions and other second Payment Services Directive (PSD2)-regulated providers, GDPR applies alongside sector rules and specifically governs how customer data is processed; and
- the EU Crowdfunding Regulation, which sets a single EU-wide regime for licensed crowdfunding service providers offering business lending and investment-based crowdfunding to project owners.

Additionally, Dutch sectoral legislation (often implementing EU Directives) which, albeit of broader application, applies to the fintech sector, and mainly includes:

- the Dutch Financial Supervision Act (*Wet op het financieel toezicht*, or Wft), which governs the supervision of the entire financial sector in the Netherlands. The Wft sets out rules and regulations for financial markets, including licensing and information requirements, as well as their supervision. The Wft also implements various EU sectoral directives (eg, PSD2, Solvency II, the fifth Capital Requirements Directive (CRD V) and the sixth Capital Requirements Directive (CRD VI));
- the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (*Wet ter voorkoming van witwassen en financieren van terrorisme*, or Wwft) provides rules to prevent the utilisation of the financial system for money laundering or terrorist financing, and provides for a registration requirement for crypto asset services providers; and
- the Dutch Sanctions Act 1977 (*Sanctiewet 1977*), which serves as umbrella legislation under which national and international rules are implemented in compliance with international sanctions regulations.

These laws are supplemented by decrees and guidance of the Dutch financial supervisory authorities the Dutch Central Bank (*De Nederlandsche Bank* or DNB), the Dutch Authority for the Financial Markets (*Stichting Autoriteit Financiële Markten* or the AFM), the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens* or the DPA), and the Netherlands Authority for Consumers and Markets (*Autoriteit Consument & Markt* or the ACM).

The regulation of the financial sector is constantly evolving. Examples of future regulations, applicable in the Netherlands, which are of particular interest to the fintech industry are:

- On 27 November 2025, the European Parliament and the Council reached a provisional agreement on the third Payment Services Directive (PSD3) and the new Payment Services Regulation (PSR).
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (the AI Act).
- The EU Savings and Investments Union.

Given the comprehensive and still-expanding nature of financial regulation, careful analysis of applicable regulatory regimes is indispensable prior to starting any fintech business in the Netherlands.

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

Dutch law treats crypto assets primarily as private law property and taxable assets, overlaid with an EU-driven financial regulatory and AML/investor protection framework (not as legal tender or 'money').

Legal nature of cryptocurrencies

Dutch case law and commentary qualify cryptocurrencies (such as Bitcoin) as 'other property rights' (*overige vermogensrechten*) that are transferable, seizable and have an ascertainable market value.

Depending on their structure, specific tokens may fall under existing regulatory categories (e-money, financial instruments, units in collective schemes), triggering Wft/Second Markets in Financial Instruments Directive (MiFID II)/Alternative Investment Fund Managers Directive (AIFMD)-style licensing, in addition to, or as an alternative to, the MiCAR crypto asset regime.

Pure payment-type cryptocurrencies typically fall outside those legacy product categories but are now in scope as 'crypto assets' under MiCAR, with service providers qualifying as CASPs.

CBDCs, the digital euro and interaction with private crypto

DNB has actively explored a retail central bank digital currency (CBDC) and strongly supports the Eurosystem's work on a digital euro, motivated by declining cash use, resilience of payments and monetary sovereignty.

A digital euro would constitute central bank money in digital form, issued under EU monetary law. It would therefore be categorically distinct from private cryptocurrencies, which are neither central bank liabilities nor legal tender.

In terms of synergies, a digital euro could provide: (1) settlement rails for tokenised assets; (2) safer on- and off-ramps for CASPs; and (3) an anchor for stablecoins that are required by MiCAR to hold reserves in central bank money or high-quality assets.

On the tension side, DNB and the ECB identify risks that largescale private stablecoins could fragment payments and weaken monetary transmission. MiCAR and prospective EU rules on digital euro design therefore seek to limit systemic risks and ensure interoperability, while leaving room for private innovation. Nevertheless, DNB and the ECB also recognise risks in the widespread adoption of stablecoins. Mass use could weaken monetary transmission and lead to fragmented payments. MiCAR and the prospective EU rules on digital euro design therefore aim to balance this tension between the advantages and risk.

Investor protection for crypto asset transactions

Investor and consumer protection is now largely harmonised at EU level through MiCAR, which the AFM and DNB are implementing in the Netherlands.

Since 30 December 2024, CASPs have been required to obtain an AFM licence under MiCAR. CASPs are subject to obligations concerning organisational integrity, conflicts of interest, and the provision of clear, fair and not misleading disclosures to clients.

The explicit objective of the MiCAR is to raise investor protection standards. CASPs must provide standardised risk warnings, inform clients of the absence of deposit guarantee and investor compensation scheme protection, and comply with market abuse rules, including prohibitions on insider dealing and market manipulation in crypto asset markets.

Where a crypto token qualifies as a financial instrument or e-money under the Wft or MiFID II framework, existing EU investor protection rules – including prospectus requirements, MiFID II conduct of business obligations, best execution, and appropriateness or suitability assessments – continue to apply in parallel. When a crypto token qualifies as a financial instrument or e-money token under the Wft or MiFID II framework, traditional investor protection rules (eg, the prospectus requirement and MiFID II conduct of business requirements) are applicable. The AFM supervises conduct of business compliance, while DNB is responsible for prudential supervision.

More generally, Dutch law applies standard civil law principles and unfair commercial practices rules, including those relating to misrepresentation, distance selling and consumer contracts, to crypto transactions. In addition, AML obligations under the Wwft and sanction-screening duties provide a further layer of public law protection against fraud and financial crime.

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

The Netherlands has implemented PSD2 and the second Electronic Money Directive (EMD2). In general, the Dutch implementation of PSD2 closely mirrors the wording of the directive. PSD2 only provided for a few Member State options and the Netherlands opted to use only a few of those. Anyone providing payment services in the Netherlands must have obtained prior authorisation from DNB (or from a competent EU regulatory authority, subject to passporting their licence), must have been exempted from the authorisation requirement, or need to rely on a statutory exception. Authorised banks and e-money institutions are permitted to provide payment services to the extent that this is permitted under the authorisation concerned; they do not require separate authorisation for the provision of payment services. It should be noted that DNB is not the only supervisory authority that supervises compliance with PSD2 in the Netherlands. The DPA, AFM and ACM are also relevant in this regard. The AFM supervises compliance with business conduct rules, the DPA monitors compliance with the GDPR, and the ACM is in responsible for supervision of PSD2 compliance from a competition law perspective. This multi-authority supervisory structure renders compliance with PSD2 particularly complex.

As noted earlier, on 27 November 2025, the European Parliament and the Council reached a provisional agreement on the PSD3 and the PSR. Formal adoption and publication of PSD3 and PSR in the Official Journal of the EU will follow after the technical finalisation of the legal texts in 2026. Following publication in the Official Journal of the EU, there will be a transition period of 18 months before compliance becomes mandatory. Affected institutions are expected to be required to fully comply with the requirements of PSD3 and PSR by the end of 2027 at the latest, following the formal entry into force of PSD3/PSR.

PSD3 will merge PSD2 and EMD2, enhance fraud prevention, simplify licensing, and strengthen supervision for payment institutions. It will be paired with the PSR, which establishes uniform EU conduct rules on authentication, refunds and open banking.

The reform adopts a dual structure. PSD3, as a Directive, focuses on who can provide payment services and how they are supervised. It sets out the rules for authorisation and passporting, governance, and prudential standards such as safeguarding of client funds. It also covers incident reporting obligations and gives supervisors enforcement powers with mechanisms for cross-border cooperation.

PSR, as a directly applicable regulation, harmonises how payment services work across all EU Member States. It mandates strong customer authentication, transaction security and fraud controls, and verification of payee details. PSR also establishes liability rules and refund rights for unauthorised or incorrectly executed payments and requires transparency on fees and foreign exchange rates. For open banking, it sets performance standards for payment account interfaces and governs how consent is managed, including through a new permission dashboard that banks must provide. The rules also embed the EMD2 into PSD3, which brings EMIs fully within the payment institution regime, and opens up payment systems by giving payment institutions direct access to settlement arrangements. EMD2 will be revoked as a separate directive.

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

In July 2020, the former Dutch Minister of Finance presented the FinTech Action Plan to the House of Representatives based on the first Dutch FinTech Census 2019. The action plan contains three different lines of action, which in their turn have been divided into more concrete goals and points of action:

- (1) putting the Dutch fintech sector on the map, both nationally and internationally;
- (2) ensuring adequate access to knowledge and talent for fintech companies; and
- (3) ensuring that regulations are future-proof and offer room for innovation.

The Dutch Government works together with the Netherlands Foreign Investment Agency in order to build a reputation for the Netherlands as global fintech hub. The Action Plan describes that it specifically focuses on possibilities for foreign venture capital funds to invest and relocate to the Netherlands. One way the government aims to make it easier for fintech companies to attract capital is to assist them in their search to acquire funding; The Ministry of Economic Affairs and Climate Policy provides guarantees for bank loans to small and medium-sized enterprises through the SME Credit Guarantee Scheme.

Regarding adequate access to knowledge, the government has committed to strengthening the business climate for highly skilled migrants by providing a specific regulatory system for entry and residence called the 'highly skilled migrant scheme'. At the same time, the government announced that it is also working on the introduction of a pilot scheme for the residence permit for essential start-up personnel. The latter is specifically designed for young innovative companies that cannot meet the minimum salary requirement of the highly skilled migrant scheme.

Lastly, the government is exploring how to make financial legislation more 'future-proof', with particular attention to proportionality and effectiveness. Citing a report by DNB that highlights the need for greater proportionality in the fintech market, the government announced plans to engage with market participants to study the issue further. It also emphasised that supervisory costs will be a key area where proportionality will receive special consideration.

In 2021, the Dutch Minister of Finance announced that a significant proportion of the announced actions had progressed and a number of actions had completed. Following the Fintech Action Plan, DNB, the AFM and the ACM established the InnovationHub. The InnovationHub is not a regulatory sandbox in which laws and regulations are (temporarily) set aside or waived. However, the InnovationHub:

- provides guidance and consultation on specific supervisory rules and policies at each stage of a company's innovation process;
- helps companies to get in touch with the appropriate regulator;
- provides information on the scope of supervision; and

- provides insight into innovative developments within the regulatory authorities that could potentially support a company's innovations, such as innovation in information exchange between the company and its regulators.

These initiatives align with the Dutch FinTech Action Plan, which as discussed aims to ease market entry while maintaining supervision. Although no dedicated government accelerator exists, the aforementioned regulatory initiatives programmes integrate with broader EU efforts to support fintech innovation.

The following private initiatives also support the Dutch fintech ecosystem:

- The Holland Fintech Association, (<https://hollandfintechassociation.org/>). The goal of this private initiative is to foster a vibrant fintech ecosystem in the Netherlands by promoting innovation, collaboration, and growth among their members. Through events, workshops, and online platforms, the association provide a space for fintech professionals to connect, learn, and grow.
- Money20/20 Europe (Amsterdam Conference), <https://europe.money2020.com/>. Money20/20 Europe is a leading global fintech conference held annually in Amsterdam. It gathers executives, innovators, and decision-makers from banking, payments, tech, startups, and policy sectors.

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

There is no specific regulation on open banking in the Netherlands in addition to the limited European regulation in this field.

The practice of banks sharing customer data with other services providers is governed by several existing regulations that affect open banking, most notably PSD2. PSD2 was an important first step into open finance, and requires banks to provide mandatory access to payment accounts to providers of payment initiation services and/or account information services. PSD2 draws a fundamental distinction between payment initiation service providers (PISPs), which are authorised to provide payment initiation services, and account information service providers (AISPs), which are authorised to provide accounting information services, as well as account servicing payment service providers which manage the underlying payment accounts.

In the EU Digital Finance Package, the European Commission identified the creation of a European financial data space as a priority. This will entail a move from 'open banking' to 'open finance'. The EU Digital Finance Package establishes the framework for such transition and identifies the hurdles to achieve this. PSD3 is also likely to positively impact open banking across EU Member States.

In 2022, the Dutch Ministry of Finance conducted a national evaluation of the Dutch implementation of PSD2, which led to the following general observations:

- PSD2 has contributed positively to competition in the payments market and to a more unified single European payments market;
- PSD2 has fostered innovation in the payments market;

- PSD2 has enhanced the security of the payments chain;
- PSD2 has strengthened consumer protection; and
- PSD2, in combination with the GDPR, offers adequate protection of privacy.

Based on the aforementioned results of the evaluation, the Dutch Ministry of Finance identified potential improvements to the existing payment data sharing provisions of the PSD2 framework and to the development of an effective general framework for open finance. These recommendations were fed back to the EU legislator with the aim of addressing these shortcomings in PSD3.

6. Regulation of virtual asset service providers

As mentioned above, CASPs in the Netherlands are now regulated under the directly applicable MiCAR, complemented by Dutch implementing legislation and supervision by the AFM and, for certain functions, DNB.

The main regime is MiCAR, which lays down licensing, conduct of business, prudential, governance and market abuse rules for issuers and CASPs across the EU, including the Netherlands. The MiCAR aims to establish a harmonised framework for crypto assets which supports innovation and fair competition. According to the recitals, the framework should enable crypto asset service providers to scale up their business on a cross-border basis.

MiCAR has applied to crypto asset service providers since 30 December 2024; Dutch-specific enforcement and supervisory powers are laid down in an implementing Act (*Uitvoeringswet verordening cryptoactiva*) and related amendments to the Wvft and decrees promulgated thereunder.

For anti-money laundering/counter-financing of terrorism (AML/CFT) purposes, the Dutch Wvft still applies in parallel. However, the previous Wvft-based registration regime for virtual asset service providers has been replaced by MiCAR licensing for CASPs, with the old registration only relevant as a historical stepping stone and for a transitional period which ended on 30 June 2025.

Any person wishing to provide crypto-asset services in the EU must either: (1) obtain a CASP licence under Article 63 MiCAR; or (2) be a 'CASP-art.60' financial institution already authorised under sectoral EU law (eg, credit institutions and investment firms) and notify the competent authority to extend its existing licence to crypto-asset services.

In the Netherlands, stand-alone CASPs must obtain a MiCAR licence from the AFM; CASPs that were previously registered with DNB under the Wvft-based regime could use a six-month transitional period until 30 June 2025, after which a MiCAR licence was required to continue serving Dutch clients.

The AFM has opened a dedicated MiCAR/CASP licensing process and maintains a public register of licensed CASPs; cross-border activity in other Member States can be conducted under MiCAR passporting once authorised.

MiCAR defines a 'crypto asset service provider' broadly as a legal person or other undertaking whose business is the provision of one or more crypto-asset services to third parties on a professional basis.

The crypto asset services that trigger CASP status (and thus licensing/notification) include, among others:

- custody and administration of crypto assets on behalf of clients (custody/wallet services);
- operation of a trading platform for crypto assets;
- exchange of crypto assets for funds (fiat) or for other crypto assets (brokerage/exchange);
- execution of orders for crypto assets on behalf of clients;
- placing of crypto assets;
- reception and transmission of orders for crypto assets;
- advice on crypto assets;
- portfolio management of crypto assets;
- transfer services for crypto assets on behalf of clients.

The MiCAR framework explicitly states that it does not aim to establish a framework that regulates the underlying technology. It therefore mainly focuses on crypto services and activities of market participants. Because of this, third-country crypto asset service providers are also regulated by MiCAR whenever they market their services in the EU, unless the European based client on one's own initiative requests the service (ie, in reliance on 'reverse solicitation').

Dutch supervisory architecture and enforcement

For CASPs authorised under MiCAR, the AFM is the primary competent authority for licensing, conduct-of-business, disclosure, and market-abuse supervision under MiCAR. It maintains the licence register for crypto-asset service providers. DNB remains relevant for prudential supervision where crypto asset services activities are provided by entities that are also credit institutions or other prudentially supervised institutions, and has a lead role in relation to certain stablecoin issuers (asset-referenced tokens/electronic money tokens) and qualified holdings assessments under the broader prudential framework.

7. AML and the Travel Rule in crypto asset transactions

The Netherlands has adopted a comprehensive legal framework to address anti-money laundering risks in the crypto sector. The current framework is based on the implementation of the Fifth Anti-Money Laundering Directive (AMLD5) through the *Wwft* and the *Sanctiewet 1977*. The regulatory landscape has evolved significantly and was further strengthened by Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto assets (TFR), which came into effect on 30 December 2024. As a directly applicable EU regulation, the TFR has binding legal force across all Member States, including the Netherlands, without requiring national transposition.

At the heart of the TFR lies the so-called 'Travel Rule', which requires that information on originators and beneficiaries accompanies transfers of crypto assets. The underlying rationale is straightforward: by ensuring traceability, authorities are better equipped to prevent, detect and investigate money laundering and terrorist financing. Beyond these information requirements, the TFR also establishes rules on internal policies, procedures and controls to ensure compliance with restrictive measures.

The scope of the Travel Rule is broad as it applies to all transfers of crypto assets – including those executed via crypto-ATMs – where the CASP, or an intermediary CASP, of either the originator or the beneficiary is established or has its registered office in the EU. Notably, unlike the regime applicable to traditional fund transfers, the TFR does not distinguish between domestic and cross-border transactions; all crypto asset transfers are subject to the same requirements.

The TFR aligns its definitions with the MiCAR as defined above. As discussed before, a CASP is defined as a legal person or undertaking that professionally engages in providing crypto asset services to clients, such as operating a trading platform, exchanging crypto assets, and providing custody of crypto assets on behalf of clients. The concept of a 'transfer of crypto assets' is defined broadly. It encompasses any transaction aimed at moving crypto assets from one distributed ledger address, crypto asset account or storage device to another, provided that at least one CASP is involved on behalf of either the originator or the beneficiary. This definition applies regardless of whether the originator and beneficiary are the same person, or whether a single CASP serves both parties.

The TFR does, however, carve out certain exemptions. Transfers where both the originator and beneficiary are CASPs acting on their own behalf fall outside its scope, as do person-to-person transfers conducted without the involvement of any CASP.

When initiating a transfer, the CASP of the originator bears responsibility for ensuring that the transfer is accompanied by key identifying information. This includes the originator's name, distributed ledger address (where applicable), crypto asset account number, and either an address with official personal document number and customer identification number, or alternatively, the originator's date and place of birth. Where available, the current legal entity identifier (LEI) or equivalent official identifier must also be included.

Similarly, information on the beneficiary must accompany the transfer. This includes the beneficiary's name, distributed ledger address (where applicable), crypto asset account number, and where provided, the current LEI or equivalent official identifier.

Importantly, this information must be submitted in advance of, or simultaneously with, the transfer itself, and through secure channels. The TFR does not require the information to be attached directly to the transfer – it may travel alongside it through separate means.

Verification obligations apply at both ends of the transaction. Before executing a transfer, the CASP of the originator must verify the accuracy of the originator's information using documents, data or information from reliable and independent sources. Such verification is deemed satisfied where the originator's identity has already been established and the relevant records have been retained. The CASP of the beneficiary, in turn, must verify the beneficiary's information before making the crypto assets available.

Transfers involving self-hosted addresses – that is, distributed ledger addresses not linked to a CASP or equivalent non-EU entity – attract additional scrutiny. In such cases, the CASP must obtain and retain the required originator and beneficiary information. For transfers exceeding €1,000, the CASP must also take adequate measures to assess whether the self-hosted address is owned or controlled by its client. This reflects the heightened money laundering and terrorist financing risks associated with non-custodial wallets.

On the receiving end, the CASP of the beneficiary must implement effective procedures to detect whether the required information accompanies the transfer. Where information is missing or incomplete, the CASP must take a risk-based approach: it may reject the transfer, return the crypto assets, or request the missing information before releasing the assets to the beneficiary.

Beyond the information requirements, CASPs must establish internal policies, procedures and controls to ensure compliance with EU and national restrictive measures when performing crypto asset transfers. The European Banking Authority published guidelines on 14 November 2024 specifying the measures CASPs should adopt in this regard.

CASPs are also required to cooperate with authorities. They must respond fully and without delay to enquiries from bodies responsible for preventing and combating money laundering or terrorist financing concerning the information required under the TFR.

Record-keeping obligations are equally important. Originator and beneficiary information must be retained for five years. Upon expiry of this period, personal data must be deleted, unless national law provides otherwise. Member States may permit further retention only where necessary for the prevention, detection or investigation of money laundering or terrorist financing, subject to a maximum additional period of five years.¹

Finally, Member States must establish rules on administrative sanctions and measures for breaches of the TFR. These sanctions must be effective, proportionate and dissuasive.² In the Netherlands, DNB is responsible for overseeing compliance with these obligations. Specific breaches attracting sanctions include repeated or systematic failure to accompany transfers with required information, failure to retain records, and failure to implement effective risk-based procedures.³

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

In the Netherlands, crypto assets are rarely used in structured financial transactions. The Dutch Civil Code lacks a comprehensive framework for tokenised transactions, and existing legal frameworks were not designed with digital assets in mind.

The legal classification of crypto assets under Dutch private law remains subject to ongoing academic and judicial debate. Dutch property law operates as a closed system (*numerus clausus*), meaning parties cannot create new types of property rights beyond those recognised by law, and can only acquire such rights in the manner prescribed by law.

1 Art 26, TFR.

2 Art 28, TFR.

3 Art 29, TFR.

Tokenisation

Tokenised financial instruments remain rare in the Netherlands, though some issuers have launched small-scale pilot digital bond issuances. In the context of these issuances, the bond is often structured as a claim in registered form (*vordering op naam*) with the token intended to evidence the holding of the bonds. These digital bonds typically still require traditional transfer mechanics (ie, assignment (*cessie*) by way of a deed of assignment) to actually transfer the bonds. Due to the closed system of Dutch property law, mere transfer of the token on the distributed ledger is insufficient to effectuate a transfer of claims with in rem effect.

Full tokenisation of real estate is not possible under Dutch law. Transfer of real property (*onroerende zaken*) requires a notarial deed (*notariële akte*) and registration in the land registry (*Kadaster*). These mandatory formalities cannot be replaced by blockchain-based transfers or smart contracts. While fractional ownership through tokens representing shares in a property-holding entity is theoretically possible, such arrangements do not constitute direct property ownership and raise additional legal, regulatory and tax considerations.

Security interests in tokenised transactions

As a matter of Dutch law, security can only be created for obligations for the payment of money. Article 3:227 of the Dutch Civil Code (*Burgerlijk Wetboek*) provides that a right of pledge (*pandrecht*) or mortgage (*hypotheek*) can only secure a monetary claim or an obligation convertible into such a claim. Consequently, a tokenised transaction can only be secured where the underlying legal relationship constitutes a payment obligation. Where a token represents a debt instrument, derivative contract or other arrangement giving rise to monetary claims, security interests may be established. However, where a token represents a utility right or other non-monetary entitlement, traditional security interests may not be available.

Security can be created over most valuable assets, including receivables, movable assets (*roerende zaken*), real property (*onroerende zaken*), shares and intermediated securities. Whether security can be created over a tokenised asset itself remains debated, given uncertainty regarding their legal qualification and difficulties applying traditional security mechanisms to digital assets.

A right of pledge (*pandrecht*) can be established over movable assets, receivables, shares and other rights, while a mortgage (*hypotheek*) is reserved for real property and certain registered assets. Perfection requirements vary by asset class. For receivables, a disclosed pledge (*openbaar pandrecht*) requires debtor notification, while an undisclosed pledge (*stil pandrecht*) requires registration with the Dutch tax authorities. For movable assets, a possessory pledge requires transfer of possession, while a non-possessory pledge requires a notarial or private deed that is registered with the Dutch tax authorities. For shares in a Dutch private limited liability company, a notarial deed and company acknowledgment are required. For real property, a notarial deed and land registry (*Kadaster*) registration is mandatory.

Outside of financial collateral arrangements within the meaning of the EU Financial Collateral Directive, title transfer by way of security is not permitted under Dutch law.

Enforcement of Dutch security rights

Upon default, a secured creditor may enforce its Dutch law security right. The security holder may generally sell the pledged assets through public auction without court intervention, or through private sale with court or security provider approval.

Outside of financial collateral arrangements within the meaning of the EU Financial Collateral Directive, a security holder may not appropriate the secured assets subject to a Dutch law security interest, but may place a bid at the sale.

9. Litigation and jurisdiction in crypto asset disputes

Disputes involving crypto assets raise complex jurisdictional questions. Given the borderless nature of blockchain technology and the global reach of crypto platforms, determining which court has jurisdiction over a particular dispute is often far from straightforward. The applicable framework depends primarily on the domicile of the parties involved, the nature of the claim, and on the nature of the (contractual) relationship – whether it qualifies as a consumer or B2B contract.

The determination of which court has jurisdiction over crypto asset disputes depends primarily on whether the Brussels I bis Regulation applies or whether recourse must be had to Dutch national jurisdictional rules under the Code of Civil Procedure (*Wetboek van Burgerlijke Rechtsvordering, Rv*).

Brussels I bis applies where the defendant is domiciled in an EU Member State. In such cases, the Regulation's uniform rules on jurisdiction, recognition and enforcement govern the dispute. For consumer contracts under Articles 17-19 Brussels I bis, both the consumer and the professional counterparty must have the requisite connection to EU Member States for the protective consumer jurisdiction rules to apply.

Where the defendant is domiciled outside the EU, or where in consumer matters the necessary EU connection is absent, Brussels I bis does not apply. Jurisdiction must then be determined under Dutch national law. This distinction is of particular practical importance in crypto asset disputes, given that many crypto platforms, exchanges and service providers are established in third countries outside the EU, such as the United States, Singapore, the Cayman Islands or other offshore jurisdictions.

The following analysis focuses primarily on the Brussels I bis framework, which provides the most relevant and harmonised regime for intra-EU crypto disputes. Where appropriate, reference is made to the corresponding provisions of Dutch national law under the Rv. In addition, it is important to note that parties to crypto asset transactions may also agree to resolve disputes through arbitration rather than litigation before national courts. However, this raises distinct questions beyond the scope of this article.

For consumer contracts, Brussels I bis provides significant protection. A natural person acquiring crypto assets outside their trade or profession qualifies as a consumer under Article 17. Under Article 17(1)(c), a consumer contract exists where the professional directs commercial activities to the consumer's Member State of domicile and the contract falls within the scope of those activities. Given that crypto platforms typically operate globally accessible websites and actively market their services across the EU, this threshold is readily satisfied in most cases. Consequently,

Dutch-domiciled consumers contracting with foreign crypto exchanges generally benefit from the protective jurisdiction rules.

In such cases, Articles 18 and 19 impose strict limitations on jurisdiction clauses: they are only enforceable if agreed after the dispute arose, or if they grant the consumer additional forum options beyond those already available under the Regulation. Article 18 Brussels I bis grants the consumer a choice of forum: proceedings may be brought either before the courts of the Member State where the professional is domiciled, or before the courts of the consumer's own domicile. Conversely, proceedings against a consumer may only be brought in the courts of the Member State where the consumer is domiciled. This asymmetry ensures that consumers cannot be compelled to litigate in distant or unfamiliar jurisdictions. This significantly curtails the effectiveness of standard terms and conditions imposed by crypto platforms on retail users.

Importantly, the consumer jurisdiction rules extend beyond purely contractual claims. Where a consumer brings a tort claim that is inextricably linked to a contract concluded with a professional counterparty – such as claims for misrepresentation or fraud in connection with crypto asset transactions – the Court of Justice has confirmed that such claims fall within the scope of Articles 17–19 Brussels I bis. In B2B disputes, the position is markedly different. Exclusive jurisdiction clauses are generally enforceable under Article 25 Brussels I bis, provided they meet the formal requirements: the clause must be in writing (or evidenced in writing), clearly formulated, and relate to a particular legal relationship. Where parties have validly agreed to submit their disputes to a specific court, that agreement will ordinarily be respected.

For contractual matters under Article 7(1) Brussels I bis (or Article 6(a) Rv), jurisdiction is conferred on the courts of the place of performance of the obligation in question. For service contracts – which would encompass many crypto asset management and trading arrangements – this is the place where the services were or should have been provided. However, where services are performed on a blockchain, determining the place of performance presents significant challenges. Whether a claim qualifies as contractual depends on whether interpretation of the contract is necessary to determine unlawfulness; if not, the claim falls under Article 7(2) as a non-contractual matter. Blockchain technology is inherently omni-territorial: transactions are validated by nodes distributed across multiple jurisdictions simultaneously. Where the contract does not specify a place of performance and the services are executed entirely on a decentralised blockchain, it may be impossible to identify a single place of performance with sufficient certainty to ground jurisdiction under Article 7(1).

A parallel can be drawn with the Dutch *Airbnb* case. In that case, the court addressed whether Dutch courts had jurisdiction over Airbnb Ireland under Article 7(1)(b) Brussels I bis for disputes concerning service fees charged to Dutch consumers. The place held that the court of service provision could not be determined from the contract itself and therefore examined where services were performed. Critically, the court found that Airbnb's characteristic obligation – operating an online platform accessible worldwide – was performed in Dublin, where Airbnb operated the platform. The court rejected the argument that services were provided in the Netherlands merely because Dutch consumers accessed the platform there, noting that passive availability does not constitute active service provision and that the platform's global accessibility made the consumer's location an insufficiently predictable connecting factor.

For non-contractual claims under Article 7(2) Brussels I bis (or Article 6(e) Rv), jurisdiction is conferred on the courts of the place where the harmful event occurred or may occur. This encompasses both the place of the causal event (*Handlungsort*) and the place where the damage materialised (*Erfolgort*). In crypto asset disputes involving pure economic loss – such as the misappropriation of crypto assets or losses arising from platform failures – localising either element presents difficulties. The causal event may occur on a blockchain that cannot be attributed to any single jurisdiction, while pure economic loss lacks the physical manifestation that would permit straightforward localisation. However, recent case law of the Court of Justice provides workable connecting factors in specific contexts, which may be applied by analogy to crypto disputes.

The Court of Justice has developed specific connecting factors for localising pure economic loss in two contexts that may be relevant to crypto disputes: prospectus liability and digital platforms. In *Kolassa v Barclays Bank* (Case C-75/13, ECLI:EU:C:2015:37) and *Vereniging van Effectenbezitters v BP plc.* (Case C-709/19, ECLI:EU:C:2021:377), the *Handlungsort* was the place where the prospectus was drawn up or decisions on its content were taken; the *Erfolgort* was where investors held accounts and made investment decisions. By analogy, where crypto issuers publish misleading white papers or offering documents, jurisdiction under Article 7(2) may lie where the documentation was prepared or where investors' wallets are maintained and investment decisions taken, provided sufficiently concrete connecting factors exist (eg, the issuer's registered office, platform operations or targeted marketing). In *Stichting Right to Consumer Justice, Stichting App Stores Claims v Apple Distribution International Ltd, Apple Inc.* (Case C-43/24, ECLI:EU:C:2025:936), the Court held that where a platform operator directed services to a Member State through a localised storefront, national language and sales to users predominantly located there, courts of that Member State had jurisdiction under Article 7(2), with the virtual storefront corresponding to the entire Member State territory. Applied to crypto platforms offering Dutch-language interfaces, euro payments and targeted Dutch marketing, Dutch courts may have jurisdiction over misconduct claims even where the operator is established elsewhere. The critical factor is whether the platform created sufficient nexus with the Netherlands through commercial activities, not whether the blockchain itself can be localised. Conversely, genuinely global platforms operating solely in English without Dutch market targeting would not support Dutch jurisdiction absent other connecting factors.

For B2B transactions involving crypto assets, careful attention to jurisdiction clauses is essential. Parties should expressly designate both the applicable law and the competent forum, specifying a court with clear jurisdiction rather than relying on the default rules. Given the difficulties in localising blockchain-based performance, reliance on Article 7(1) as an alternative ground of jurisdiction is inadvisable. Similarly, parties should be aware that where disputes arise from transactions executed on permissionless blockchains, the omni-territorial nature of the technology may preclude reliance on special jurisdiction grounds. In collective actions brought by representative entities on behalf of multiple claimants, the consumer jurisdiction rules of Articles 17–19 Brussels I bis do not apply where the representative entity itself is the claimant and individual consumers are not parties to the proceedings. In such cases, jurisdiction must be determined under the general rules of Articles 4 and 7–8 Brussels I bis. This may result in different jurisdictional outcomes compared to individual consumer claims, and parties should be aware of this distinction when considering collective redress mechanisms.

Where multiple defendants are involved in a crypto asset dispute, Article 8(1) Brussels I bis (or Article 7 Rv under Dutch national law) may provide an alternative basis for jurisdiction. This provision permits a

defendant domiciled in one Member State to be sued in the courts of another Member State where any co-defendant is domiciled, provided the claims are so closely connected that it is expedient to hear and determine them together to avoid the risk of irreconcilable judgments resulting from separate proceedings. In crypto transactions involving platforms, intermediaries, wallet providers and individual counterparties, this rule may enable a claimant to consolidate proceedings before a single court by joining a defendant domiciled in the desired forum as an 'anchor defendant'. However, the Court of Justice has emphasised that Article 8(1) must be interpreted restrictively to prevent abuse. The connection between the claims must be genuine and substantial; mere factual overlap or commercial convenience is insufficient. The risk of irreconcilable judgments must be real, not hypothetical. Courts will scrutinise whether the joinder is designed primarily to circumvent the ordinary rules on jurisdiction, particularly where the anchor defendant plays only a marginal role in the dispute. In practice, Article 8(1) may prove useful where, for example, a crypto platform operator domiciled in the Netherlands is sued alongside its parent company or affiliated service providers domiciled elsewhere, and the claims against each defendant arise from the same factual circumstances and raise overlapping legal issues. Claimants should be prepared to demonstrate the requisite connection and the risk of conflicting outcomes if separate proceedings were pursued.

The applicable regime for assessing the validity of a jurisdiction clause depends on the parties' domicile and the designated forum. Three distinct regimes may apply.

First, where both parties are domiciled in EU Member States and the jurisdiction clause designates courts of a Member State, Article 25 Brussels I bis governs. Under this regime, a jurisdiction agreement conferring jurisdiction on the courts of a Member State is valid if it is: (1) in writing or evidenced in writing; (2) in a form which accords with practices established between the parties; or (3) in international trade or commerce, in a form which accords with a usage of which the parties are or ought to have been aware. The agreement confers exclusive jurisdiction unless the parties have agreed otherwise. In crypto asset disputes between businesses, such clauses are generally enforceable provided they meet these formal requirements and relate to a particular legal relationship.

Second, for disputes involving parties domiciled in states party to the Hague Choice of Court Convention – including the UK, Singapore and Mexico – Articles 5 and 6 of that Convention apply. The Convention requires that the choice of court agreement be concluded or documented in writing or by any other means of communication which renders information accessible to be usable for subsequent reference. The chosen court has exclusive jurisdiction unless the parties have expressly provided otherwise. Importantly, the Convention applies only to exclusive choice of court agreements in international cases concerning civil or commercial matters, and excludes certain matters such as consumer contracts and employment relationships.

Third, where neither Brussels I bis nor the Hague Convention applies – for example, where the defendant is domiciled outside the EU and outside Hague Convention states, or where the designated forum is in a non-Convention state – Dutch national rules under Article 8 Rv determine enforceability. Article 8(1) Rv provides that Dutch courts have jurisdiction where parties have by agreement designated a Dutch court or the Dutch courts for disputes arising from a specific legal relationship, provided there is a reasonable interest in doing so. Conversely, Article 8(2) Rv provides that Dutch courts lack jurisdiction where parties have by agreement exclusively designated the courts of a foreign state.

Special considerations apply to asymmetric jurisdiction clauses – that is, clauses that limit one party's ability to bring proceedings to a single designated court while permitting the other party to bring proceedings before that court or any other competent court. Following the Court of Justice's judgment of 27 February 2025 in *Società Italiana Lastre* (C-537/23, ECLI:EU:C:2025:120), such clauses are valid under Article 25 Brussels I bis only if: (1) the clause designates courts in EU Member States or in States party to the Lugano Convention; (2) it identifies objective and precise factors enabling the relevant court to verify its jurisdiction; and (3) it does not conflict with other provisions of Brussels I bis.

Dutch case law specifically addressing jurisdiction in crypto disputes remains limited. Lower courts have addressed crypto-related claims without extensively analysing jurisdictional issues, and neither the AFM nor DNB has issued specific guidance on jurisdiction in this context. As the crypto sector matures and disputes become more frequent, further judicial and regulatory clarification can be expected.

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

In the Netherlands, innovative ideas and inventions can be protected in one of two ways: either by registering the invention as a patent: that is, with the European Patent Office as a European patent or with the Netherlands Patent Office as a national patent, or as a trade secret.

Protecting innovation through patents

Patent laws applicable in the Netherlands are divided between the two types of patents as described above, with the Dutch Patent Act 1995 governing national Dutch patents and the European Patent Convention governing European patents. A European patent is awarded by the European Patent Office following a comprehensive examination procedure, and will after grant provide a bundle of national designations in each of the EU Member States, Liechtenstein, Norway, Switzerland and Turkey. Across the Dutch Patent Act 1995 and the European Patent Convention, an invention which forms part of a patent application will need to possess: (1) novelty; (2) an inventive step; and (3) needs to be susceptible of industrial application. These characteristics are examined *ex tunc*, based on the state of the art as it existed on the application date of the European patent application.

In regard to digital and virtual assets and crypto-applications, the rules on 'computer-implemented inventions' apply. Inventions that solely consist of a computational or algorithmic component (eg, computer programs, software and mathematical methods) and artificial intelligence and machine learning applications (such as artificial neural networks, genetic algorithms, support vector machines, k-means, kernel regression and discriminant analysis) are excluded from patentability as they are deemed not to have a 'technical effect'. Instead, such applications will need to be combined through both a physical (eg, hardware) and virtual (eg, software, algorithms, etc) component in order to become patentable (the so-called 'any hardware approach'). If, for example, an applicant tries to obtain a patent in respect of, for example, a novel blockchain application or a new type of virtual token, the applicant will need to show that due to a combination of physical and virtual components a 'further technical effect' is established, which goes beyond

the mere combination of the 'normal' physical interactions between the program (software) and the computer (hardware) on which it is run. Whether a combination of hardware and software components has such a 'further technical effect' is highly case dependent. If you want to pursue a patent application for computer-implemented inventions, we recommend engaging a licensed patent attorney.

Elements which merely have an ornamental or aesthetic effect or other creative value cannot be protected under patent laws. These elements fall under the protection of, for example, copyright or trademark laws.

Since 2013, a number of European Member States including the Netherlands have ratified the Unified Patent Court Agreement, a multilateral legal instrument that created the Unified Patent Court, which opened its doors on 1 June 2023. With the creation of the Unified Patent Court, it became possible to apply for a European patent with unitary effect (also referred to as a 'unitary patent') which, in contradiction to a 'classic' European patent, forms a single asset with unitary effect across the ratifying jurisdictions. Currently, 18 EU Member States have ratified the Unified Patent Court Agreement: Austria, Belgium, Bulgaria, Denmark, Estonia, Finland, France, Germany, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Portugal, Romania, Slovenia, and Sweden.

Ownership is determined through the patent application process: the patent applicant will be deemed to be entitled to ownership of the patent once granted. The patent proprietor can monetise the patent as an intangible asset, for instance, by selling and assigning the patent to third parties, by licensing the patent, or by securitising the patent as collateral in financing.

Furthermore, the patent proprietor can assert its patent towards third parties that infringe upon that patent. The patent proprietor benefits from various remedies which are available including an injunction, recall, rectification, surrender of profits made by the infringing party and reimbursement of damages such as lost profits, and reimbursement of legal costs.

After grant, third parties are able to instigate opposition proceedings before the European Patent Court to nullify the patent, for example, by citing 'prior art' which precludes the validity of a European patent due to the fact that it renders that patent not novel or obvious (ie, lacking an inventive step over the state of the art).

In addition to the nullification of a patent during opposition proceedings (as described above), third parties can either on their own account or as a defence to an infringement claim file invalidity arguments regarding a patent. A national court seized in respect of a national Dutch patent or the Dutch designation of a European patent can only decide on the invalidity of that patent, whereas the Unified Patent Court can decide on invalidity across the unitary patent ratifying Member States in one sweep.

Protecting innovation through trade secrets

An alternative way of protecting innovation is through trade secrets. In the Netherlands, trade secrets are governed by the Dutch Trade Secret Protection Act, which forms the Dutch implementation of the Trade Secret Directive (Directive 2016/943/EU). A trade secret is eligible for protection under the Trade Secret Protection Act if it concerns: (1) 'information' (ie information in a broad sense, whether it is commercial information or know-how or technical

in nature); that is (2) secret; and (3) which derives independent economic value due to its secrecy. The proprietor of a trade secret will need to show that they have taken reasonable steps to keep the information secret. A trade secret proprietor is able to assert its trade secret against any third party it suspects to have infringed upon its trade secret, akin to the remedies available to patent proprietors.

As a trade secret is – by its very nature – confidential, there is no separate application procedure or register of trade secrets as is the case with patents. However, monetisation can still be obtained through, for example, the sale and assignment of the trade secret or by licensing the trade secret to third parties.

Protection in foreign jurisdictions

As described above, registering for a European patent or for a unitary patent provides uniform protection throughout the EU Member States/the ratifying states of the Unified Patent Court Agreement. Further expansion of the protection provided by a patent is possible through applying for patent protection in other jurisdictions within one year of the first filing date of the patent application, the so-called ‘priority year’, which allows patent applications in other jurisdictions to benefit from the ‘priority date’ of the initial patent application.

Trade secrets benefit from uniform protection throughout the EU under the (national implementations of) the EU Trade Secret Directive. Similar legislation exists in, for example, the 2016 United States Defend Trade Secrets Act.



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