

France

Jean-François Adelle*

Jeantet, Paris

jfadelle@jeantet.fr

Olivier Lyon-Lynch†

Jeantet, Paris

olyon-lynch@jeantet.fr

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

In France, there is no single set of regulations for fintechs. There is also no legal definition of fintechs. They are generally considered to be companies carrying innovative technologies in digital, artificial intelligence (AI) and data processing (big data) applied to the finance industry, where they play a role of accelerators of change, often disruptive.

These technologies are typically deployed in the field of payments, digital assets (cryptocurrencies, tokens, stablecoins), financing (crowdfunding platforms), management of insurance products (insurtech), assistance with risk management and compliance (regtech), and the management of financial contracts (smart contracts), where their application sometimes precedes the adaptations of the law and regulations to the new problems raised.

Fintechs and their activities will accordingly be potentially concerned by a diverse set of laws and regulations from French and European Union sources, and guidelines. These comprise:

- regulation on payment services (Articles L314-1 à L314-16) and intermediaries in banking and payment services regulation (Articles L519-1 à L519-17) of the Monetary and Financial Code (MFC);
- regulation of the issuance and management of electronic money (Articles L315-1 à L315-9) of the MFC;
- Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020, on European crowdfunding service providers for business;
- regulation of service providers of digital assets (Articles L54-10-1 à L54-10-5 of the MFC), Decree No 2019-1213 of 21 November 2019 relating to issuers of tokens (Articles L551-1 to L552-7 of the MFC) and Articles 721-1 *et seq.* of the General Regulation of the Financial Markets Authority (AMF);
- regulation on e-marketing, hawking and distance delivery of financial services (Articles L341-1 to L343-2 of the MFC);
- regulation on providers of data communication services (Articles L549-1 to L549-2 of the MFC);
- regulation on intermediaries in miscellaneous assets (Articles L551-1 à L551-5 of the MFC);
- Ordinance No 2017-1674 of 8 December 2017, on the use of a shared electronic recording device for the representation and transmission of financial securities;
- Delegated Regulation (EU) No 2018/389, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR);

* Former Co-Chair (2023-2024) and member of the Advisory Board (since 2005) of the IBA Banking and Financial Law Committee, contributor to the 2022 edition and the updated 2024 and 2025 editions.

† Contributor to the 2024 and 2025 updated editions.

- law on monetisable digital objects and gaming companies, adopted on 10 April 2024 within the context of a law on digital space and web user protection (SREN);
- Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (the DORA Regulation), applicable since 17 January 2025. The DORA Regulation is supplemented by delegated regulations such as the regulation (EU) No 2025/295, No 2025/420, No 2025/1190, and No 2025/532;
- Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (published in the Official Journal of the European Union on Friday 9 June 2023) (MiCAR) which came into force on 29 June 2023. Most of its provisions are applicable since 30 December 2024. MiCAR is supplemented by the implementing regulation (EU) No 2024/2984 of 29 November 2024, and by delegated regulations such as the regulations (EU) No 2025/292, No 2025/293, No 2025/294, No 2025/295, No 2025/296, No 2025/297, No 2025/298, No 2025/299 and No 2025/1140;
- Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849, applicable since 30 December 2024;
- Ordinance No 2024-936 of 15 October 2024 on crypto-asset markets and Order No 2024-937 of 15 October 2024 on strengthening anti-money laundering and counter-terrorist financing obligations in relation to crypto-asset transfers; and
- Law n° 2025-391 of 30 April 2025 and Decree No 2026-420 of 29 May 2026, concerning the transfer of ownership and the pledging of digital assets.

Further regulation is being contemplated, namely the Proposal for a Regulation of the European Parliament and of the Council on a framework for Financial Data Access, and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554.

Soft law also complements the above laws and regulations. The regulators have issued the following guidelines on this subject:

- the Prudential Control and Resolution Authority (ACPR) issued sector-specific implementing principles for digital asset service providers (DASPs), as of November 2022;
- the ACPR issued a Q&A on the DORA Regulation, updated on 8 September 2025; and
- the AMF issued a Q&A on the DASPs regime, updated on 17 June 2025.

As regards AI, EU regulation 2024/1689, which came into force on 1 August 2024, aims to establish a harmonised legal framework within the EU for the use of AI. The ACPR should be responsible for verifying the proper application of this text in the financial sector.

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

France was a pioneer in establishing a legal framework for crypto assets.

The first step was Ordinance No 2016-520 of 28 April 2016, regulating certain uses of blockchain technologies – notably, a shared electronic recording device for minibond and financial securities not admitted to the operations of a central securities depository.

The Law on the Growth and Transformation of the Companies (the Loi Pacte or Pact Law) of 22 May 2019 (codified in the MFC) then provided a comprehensive regulation of crypto assets. It purported, without waiting for European regulations, to offer a regulatory framework that both protects investors and is flexible to allow for changes. The regulation addressed digital assets, digital services and digital services providers.

The framework set by the Pact Law has now been replaced by MiCAR. It is worth noting that the Pact law also partly inspired MiCAR. This is why the French regulatory framework for crypto assets has not been disrupted by the entry into force of MiCAR.

Classification of crypto assets

Under MiCAR, the classification takes into account the nature of the risks posed by each category of crypto asset. A distinction can be made between crypto assets with a financial purpose and crypto assets without a financial purpose.

Crypto assets with a financial purpose

These are known as stablecoins. MiCAR recognises two types: asset-referenced tokens and electronic money tokens.

An asset-referenced token, referred to by its English name ART, is defined in Article 3.1 (6) of MiCAR 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’. They can be used as a means of payment.

Article 3.1 (7) of MiCAR provides the following definition of an electronic money token or e-MT: ‘a type of crypto-asset that purports to maintain a stable value by referencing the value of one official currency’. Official currency is that of a country issued by a central bank or other monetary authority.

Regarding ‘security tokens’, understood as crypto assets that qualify as financial instruments, they are excluded from the scope of MiCAR (Article 2.4). They are therefore subject to financial instruments regulations.

Utility tokens

This means any digital asset representing one or more rights that can be issued, recorded, stored or transferred by means of a distributed ledger technology enabling the owner of the asset to be identified, directly or indirectly, excluding those meeting the characteristics of a financial instruments and the savings bonds.

Therefore, the assets covered by this definition must be usable for non-financial purposes. In other words, the token must be able to be used to access goods or services.

MiCAR defines 'utility tokens' as tokens that do not refer to one or more assets. According to Article 3.1 (9) of MiCAR, they are 'intended solely to provide access to a good or service provided by its issuer'. This is a somewhat 'catch-all' category intended to accommodate, by default, assets that are neither financial instruments, asset-referenced tokens, nor electronic money tokens.

Regarding non-fungible tokens (NFT), MiCAR provides that:

'It should not apply to crypto-assets that are unique and not fungible with other crypto-assets, including digital art and collectibles. The value of such unique and non-fungible crypto-assets is attributable to each crypto-asset's unique characteristics and the utility it gives to the holder of the token. Nor should this Regulation apply to crypto-assets representing services or physical assets that are unique and non-fungible, such as product guarantees or real estate' (Recital 10).

The criteria for qualifying a crypto asset as an NFT within the meaning of MiCAR will be detailed in guidelines published by the European Securities and Market Authority (ESMA).

Initial coin offering

MiCAR provides a specific regime for initial coin offering (ICO), under which it means a 'communication to persons in any form, and by any means, presenting sufficient information on the terms of the offer and the crypto-assets to be offered so as to enable prospective holders to decide whether to purchase those crypto-assets' (Article 3 (12)). Article 1 (13) of MiCAR defines an offeror as 'a natural or legal person, or other undertaking, or the issuer, who offers crypto-assets to the public'. However, for public offerings of utility tokens, the offeror is necessarily a legal person who must meet the conditions set out in Article 4 (1), in particular to draft, notify, and publish the information document known as the 'white paper'. The condition concerning the white paper, as well as part of the condition relating to commercial communications, is, however, waived in the cases mentioned in Article 4 (2):

- the offer is made to fewer than 150 natural or legal persons per Member State of the EU when those persons are acting on their own behalf; and/or
- the offer, over a period of 12 months from the start of the offer, does not exceed €1m; and/or
- the offer is intended solely for qualified investors.

Crypto-assets services

Crypto-assets services under MiCAR are enumerated and defined by Article 3.1 (16), (17), (18), (19), (20), (21), (22), (23), (24), (25) and (26) of MiCAR. Such services include in particular:

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

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

The French regulation of payment service providers and wallets is derived from EU Directives 2007/64/EC and 2015/2366 on payment services.

Payment services are essentially:

- the execution of fund transfers and direct debits;
- the transmission of funds;
- services enabling the payment or withdrawal of cash; and
- the transmission of a payment account, the execution of transactions for which the payer uses a telecommunications, digital or computerised device.

Payment services are regulated.

Payment services are a subset of banking operations, which can still be provided by credit institutions, but which are open to a new category of regulated providers – payment institutions. Payment institutions may also provide related services, including granting of loans under certain conditions. Payment services can also be provided by electronic money providers.

Payment institutions must be licensed by the ACPR. However, only registration as an account information service provider is required if the only payment service provided is the account information service. Furthermore, a simplified payment institution licence is available for payment institutions whose payment volume is not expected to exceed a monthly average of €3m and which do not plan to provide the money transmission service.

There is an exemption from the licensing requirement for undertakings which provide 'payment services based on means of payment which are accepted for the acquisition of goods or services

only on the premises of that undertaking or, under a commercial agreement with it, in a limited network of persons accepting those means of payment or for a limited range of goods or services’.

Examples include gift cards issued by commercial networks which are only accepted for payment in the stores of that network, or other types of payment cards (eg, public transport cards). The exemption is granted by the ACPR, which verifies that the conditions are met, and the arrangements ensure the security of the means of payments and consumer protection.

The service provider may start operating before filing for an exemption until the total value of executed payment transactions or electronic money outstanding within the previous 12 months exceeds €1m.

Directives 2007/64/EC and 2015/2366 are currently being revised (a draft directive and regulation are under review). The proposal 2023/0209 (COD) would apply to electronic money, and thus merge the statuses and licensing of payment institutions and electronic money institutions. The main changes would concern strong customer authentication, fraud prevention, competition and open banking.

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.

The French fintech sector is experiencing rapid growth. It brings together approximately 1,000 companies totalling 50,000 skilled jobs in all areas of finance: banking services, payments, insurance, asset management and crypto assets. There are 14 fintech ‘unicorns’ (startups valued at over \$1bn) in France.

The French regulators are particularly aware of challenges related to the rapid evolution of the financial sector, especially regarding the fintech ecosystem. The AMF, the ACPR and the Banque de France have created special fintech development units with high-level experts to attend and support the development of fintechs and have put forward a common cell, the ‘Fintech Pole’ (*Pôle Fintech*). The ACPR runs the Fintech Forum alongside the AMF, which brings together professionals several times a year to discuss regulatory and supervisory issues related to fintech and innovation, analyses more cross-sectoral innovations and monitors the digitalisation of French financial companies. In addition, since 2020, the ACPR, the AMF and the France FinTech association (whose mission is to represent French fintech companies to public authorities and regulators) organise the ‘French Fintech Week’ every year. These events aim to promote the richness of the French fintech ecosystem by drawing on the contributions of representative public and private organisations that are working to boost digital finance by considering the conditions conducive to its growth, and helping to strengthen the assets of the Paris financial centre.

To closely monitor the efficacy of the legal framework for fintechs, French authorities have set up a ministerial delegation and a commission on finance, general economy and budgetary control.

On the regulatory side, to provide an adequate regulation facilitating the development of fintechs while protecting the fintech development, France has elected a ‘proportionality of regulation system’,

offering a panel of regulated regimes adapted to the needs of fintechs ranging from licences to registrations, and including an optional visa.

In areas of joint authority of the regulators such as licensing DASPs (the mandatory registration of DASPs is carried out by the AMF, subject to the assent of the ACPR), to ensure swift and smooth review applications, the ACPR's and the AMF's departments exchange views on all aspects of an application and appoint a team of analysts from both authorities for each application.

To facilitate the fintech licensing process, the ACPR has issued a charter targeting fintechs with startup projects. It aims to present an overview of the main authorisation procedures for fintechs under the supervision of the ACPR, and provide greater visibility regarding processing time and exchanges of information. A toolkit of useful documents providing assistance in filling in the applications is available on the ACPR's website.

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

There is no single regulation on open banking. However, the practice of banks sharing data on their customers with other service providers falls under several existing regulations that affect open banking.

The second Payment Services Directive (PSD2), replacing and superseding the first Payment Services Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market, requires banking institutions to open their information systems to third parties and creates the status of agent of payment institutions (PIs) and of electronic money institutions (EMIs). It further strengthens payment security in the era of electronic payment, and provides the framework for two new payment services related to open banking:

- account information service providers (AISPs), who can only provide the service of collecting information on one or more payment accounts (eg, aggregating payment accounts to analyse a company's cash flow or allowing consumers to view their various bank accounts on a single platform); and
- payment initiation service providers (*prestataires de services d'initiation de paiement* – PISPs), who initiate a payment order for an account held with another provider at the user's request.

In their development of application programming interfaces (APIs), platforms must comply with the regulatory technical standards (RTS) adopted in March 2018 by Delegated Regulation (EU) No 2018/389, which are directly applicable in domestic law.

Open banking is also subject to regulations on data protection (GDPR).

In a press release dated 15 March 2022, the ACPR commented that the emergence of agents licensed by authorised PIs or EMIs that market or develop new services has led to two changes in distribution: (1) the establishment of large-scale physical retail networks alongside banking agencies (offices, booksellers, lottery agencies), which are in charge of the customer relationship, while the PI or EMI performs the service; and (2) an increasing 'platform' of the sector, with innovative players

having the status of agents developing their own service offering under the supervision of the entities that mandate them.

Going further, open banking fosters specific risks (cybersecurity, consumer data protection, etc) that are not yet adequately addressed by existing regulation. In its press release, the ACPR recalls that authorised institutions remain fully responsible for their external providers, including agents, and must have systems in place that ensure ongoing supervision and oversight.

The new EU DORA Regulation addresses some of these risks, under new obligations applicable to financial entities dealing with cloud service providers and new rules regarding their supervision. DORA sets conditions related to the geographical link of cloud service providers to the territory of the EU, and a prohibition on financial entities using cloud service providers that are not established in the EU. It also strengthens the contractual obligations of cloud service providers.

Other risks will need to be considered in the forthcoming review of PSD2.

A concern has been recently expressed on the French market on the potential adverse effects of the oligopolistic structure of the cloud market, combined with the technological dependency of banks on the expertise of cloud service providers, which led to their deep interconnection with the entire financial system. Indeed, this is likely to reverse the traditional balance of power between customers and service providers.

Cloud service providers are not subject to the rules imposed on the banking sector, especially regarding the protection of sensitive information and personal data. They are a small number of companies, mainly American and Asian, to whom the regulations of the banking profession do not apply. This introduces a certain disequilibrium in the contractual relationship, but the lack of conformity of certain clauses in the outsourcing contracts exposes banks to risks of administrative sanctions and liability issues, particularly with respect to their clients.

A new legal framework is under discussion which aims at extending open banking, introduced by PSD2, to open finance.

Open banking has enabled the development of new value-added services based on payment data – such as real-time credit risk analysis, streamlining of the identification process when entering into a relationship with third party providers, payment initiation, and aggregation of payment accounts. This new set of forthcoming regulations is now planning to go further, and is raising the issue of opening up all financial data (such as savings, insurance, investments, etc) which would enable a multiplication of value-added services.

To this end, the European Commission has proposed, in June 2023, to:

- amend and modernise the current PSD2, which will become PSD3;
- establish a Payment Services Regulation (PSR); and
- adopt a new directive for a framework for financial data access.

At this stage, the timetable for the implementation of this new legal framework remains highly uncertain.

6. Regulation of virtual asset service providers.

Before the application of MiCAR, the regulatory framework governing licensing and registration of VASPs was set by the MFC. This framework is harmonised at European level since 30 December 2024.

Initially, the MFC provided for mandatory registration of VASPs and optional licensing for the provision of certain services. VASPs registered/authorised under the French regime before 30 December 2024 may continue to operate under French status until 1 July 2026. After this date, they must have obtained their MiCAR licensing in order to continue their activities. Applications for licensing made after 30 December 2024 are processed in accordance with MiCAR.

MiCAR licensing as a crypto asset service provider (CASP) involves the following services and activities:

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

Article 62 of MiCAR lists the requirements in order to be licensed as a CASP. These include:

- governance arrangements;
- knowledge, professional skills and experience of the management body;
- good reputation and absence of criminal record in respect of convictions and absence of penalties imposed under commercial law, insolvency law and financial services law, of the members of the management body and the shareholders;
- prudential conditions and minimum capital requirements depending on the services provided: between €50,000 and €150,000;
- internal control mechanisms, policies and procedures to identify, assess and manage risks, including money laundering and terrorist financing risks, and business continuity plans;
- customer protection mechanisms and complaints handling;

- procedures and policies relating to information and communication technology, commercial policies; and
- specific requirements depending on the services the applicant wishes to offer (eg, procedures and policies relating to custody and administration of crypto assets, segregation of crypto assets or funds, operating rules of the trading platform, procedure and system to detect market abuse).

The AMF is responsible for assessing licensing applications, which take place as follows:

- acknowledgement of receipt of the application file within five business days by the AMF services. The AMF services will forward the file to the ACPR for review of the section relating to compliance with anti-money laundering and counter-financing of terrorism (AML/CFT) requirements;
- assessment of the completeness of the file within 25 business days from the date of receipt of the application;
- decision on completeness or incompleteness. If the application is incomplete, the AMF services will set a deadline by which the applicant must provide all missing information. After this deadline, the AMF may refuse to re-examine an application that remains incomplete;
- assessment of the file within 40 business days from the date of the decision on completeness. During this period, the AMF services may request any additional information necessary to complete the assessment;
- decision to grant or refuse authorisation;
- notification of the decision within five business days from the date of said decision.

MiCAR licensing then allows CASPs to operate in different European Member States after providing the required information to the supervisory authorities of the states concerned.

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

France has not established an AML-specific regime for CASPs but has included them within the scope of its AML/CFT measures applicable to various financial services providers (eg, credit institutions, PIs, investment service providers, insurers and e-money institutions).

The French regulatory framework for money laundering derives from European directives and regulations. This framework is set out in the MFC under Chapter 1 of Title VI of Book V (Articles L561-1 to L564-2), and by the Order of 6 January 2021.

CASPs are notably required to:

- apply due diligence measures designed to implement obligations under Chapter 1 of Title VI of Book V of the MFC, based on an assessment of the money laundering and terrorist financing risks entailed by their activities;

- conduct customer due diligence before entering into a business relationship with their customers or assisting them in preparing or carrying out a transaction (eg, identifying customers and beneficial owners; verifying information on presentation of documentary evidence). Constant vigilance and careful examination of transactions shall also be carried out throughout the duration of the business relationship;
- report via an appointed declarant, in writing, to the French Financial Intelligence Unit ('Tracfin') the sums entered in their books or transactions involving sums which they know, suspect or have good reason to suspect originate from an offence punishable by a custodial sentence of more than one year or are linked to the financing of terrorism;
- set up an organisation and internal procedures to counter money laundering and the financing of terrorism, taking into account their risk assessment. Internal procedures shall specify in particular the process for developing the risk classification, defining and up-dating the risk profile of each business relationship, information and reporting procedures to Tracfin; and
- appoint an AML compliance officer responsible for implementing the anti-money laundering system financing of terrorism framework.

The AMF is also responsible for supervising CASPs regarding AML requirements.

In addition, the Order No 2024-937 of 15 October 2024 has introduced a 'travel rule' into French law. These provisions entered into force on 30 December 2024. This order introduces new obligations, including:

- the application of measures to mitigate the risks of money laundering and terrorist financing to correspondent relationships between a CASP established and registered in the EU and a financial institution (including a CASP) established in a jurisdiction outside the EU (Article L561-10-3 of MFC);
- the implementation of additional due diligence measures by CASPs that execute or receive a transfer of crypto assets to or from a so-called self-hosted address (Article L561-10-4 and R561-21-1 of the MFC). CASPs shall implement additional due diligence measures that include one or more of the following actions, depending on the risks identified:
 - (i) verification of the identity of the initiator or beneficiary of a transfer of crypto assets made to or from a self-hosted address, or the beneficial owner of the originator or beneficiary of such transfer, including by using third parties;
 - (ii) collection of additional information on the origin and destination of the crypto assets transferred;
 - (iii) implementation of enhanced ongoing monitoring of these transactions; and
 - (iv) any other measures aimed at mitigating and managing the risks of money laundering and terrorist financing.

Finally, CASPs fall within the scope of Regulation 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the anti-money laundering and counter-terrorist financing

authority (the AMLA), and may therefore be among the 'selected obliged entities' subject to direct supervision by the AMLA.

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

How are financial instruments structured in relation to tokenised assets (eg, tokenised real estate, digital bonds, DeFi instruments)?

Under French law digital assets (*actifs numériques*) include tokens and virtual currencies that do not have the characteristics of financial instruments (ie, financial securities (*titres financiers*) and financial contracts (*contrats financiers*)) and treasury bonds (*bons de caisse*). Financial-instrument-type tokens (security tokens) are treated under existing financial regulation, not as crypto assets. Therefore, tokenised securities (eg shares, bonds) are not a wholly new legal class, but rather standard financial instruments whose 'register' (ownership) is recorded on a blockchain (*dispositif d'enregistrement électronique partagé* or DEEP). However, tokens structured with securities (shares, bonds that do not qualify as financial instruments, or treasury bonds) are governed by MiCAR. Furthermore, France has implemented a pilot regime for market infrastructures based on distributed ledger technology (DLT) under EU rules that allows certain infrastructure players to experiment DLT based issuance/trading/settlement, while being exempt from or adapting some traditional requirements.

Tokenisation of real estate assets can be structured in two ways.

- Direct tokenisation of a real estate property right (eg, right to the ownership or usufruct of physical real estate or to access to another form income from real estate) registered on a DLT. Property transfers via blockchain are valid but require publication in the French land registry (*fichier immobilier*). Therefore, those tokens have a limited practical interest due to formalities and costs associated with ordinary property transfers.
- Tokenisation of rights to shares or bonds in a special purpose vehicle (eg, *société civile immobilière* (SCI)) or regulated investment vehicle (eg, *société civile de placement immobilier* (SCPI) or *organisme de placement immobilier* (OPCI)), or alternative investment fund (AIFs).

The offer and sale of such tokens to individual or institutional investors is subject to the legal regime applicable to the marketing of these instruments. Tokens are typically sold to investors on a decentralised platform, and can be used as a security on DeFi markets to borrow crypto or other assets. Revenues generated by the underlying property or the proceeds of the sale of the property are distributed automatically to the token owners via smart contracts.

Tokenisation of financial securities was possible in France before the transposition of MiCAR into French law, as the Pact Law provides for the use of blockchain technology for the transfer of unlisted securities and fund units. It allows the registration of an issue or transfer of financial securities in a blockchain to have the same effect as the registration of financial securities in an account, and does not create any new obligations or reduce existing guarantees relating to the representation and transfer of the securities concerned. Tokenised financial securities give to their

holder the same rights over the issuer as traditional financial securities. Both forms are fully fungible and share the same ISIN code.

Tokenised DeFi instruments include a broad range of use cases and underlying assets, including:

- tokenised lending instruments representing loans, debt positions or interest-bearing claims;
- tokenised derivative instruments representing synthetic exposure or leveraged positions; and
- governance and utility instruments representing voting power in protocols.

The implementation of tokenisation of classes of assets requires dedicated infrastructure, and a Euro counterparty for settlement and delivery.

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

Common types of collateral used in digital asset transactions, such as loans or exchanges of crypto assets, include financial securities and other financial products, cash and receivables and other crypto assets.

Please describe the procedures to create and perfect a security interest in these types of collateral, including any requirements for notarisation, registration, stamp duty, or other legal formalities. In the case of a default, what enforcement procedures are available to secured lenders to realise their security interest and recover their claims? Is a public auction required for enforcement? Can a secured lender appropriate the collateral directly in certain cases?

Under French law, crypto assets may be given as security by way of pledge or assignment by way of security within the framework of *fiducie* security, and in both cases with or without dispossession. Furthermore, under the Diverses Dispositions d'Adaptation au Droit de l'Union Européenne (DDADUE) law of 30 April 2025, crypto assets will qualify as eligible financial collateral as from 1 July 2026.

Pledge

The law DDADUE has introduced a specific regime of 'pledge' of crypto assets, detailed at article L226.5 of the MFC. Further details will be provided by an implementation decree, still awaited. It was inspired by doctrinal works of the Haut Comité Juridique de la Place Financière.¹

The general civil law regime of security interests for movable assets may apply to crypto assets. Article 2355, Paragraph 5 of the French Civil Code refers, in the absence of special provisions, to the regime governing pledges of tangible movable property, which provides that the contract must

¹ Rapport sur le règlement MiCAR du Haut Comité Juridique de la Place Financière de Paris, Annexe 5, 27 January 2024.

be in writing, and its enforceability is achieved either by dispossession or by public notification of the pledge. In the absence of dispossession, the secured creditor is in competition with the other creditors of the pledgor and, in the event of the debtor's liquidation, has a relatively low priority ranking. Self-enforcement requires evaluation by an expert, and is paralysed in the event of an insolvency proceeding. Certain types of crypto assets like money tokens or NFTs fall within the scope of security interest over money receivables.

Before the special pledge was established, Order No 2017-1674 of 8 December 2017, relating to the use of a DEEP for the representation and transmission of financial securities, took into account the specific nature of financial securities registered on the blockchain. This lay in the fact that they were not registered in an account and, provided that those securities were pledged directly without transfer to a pledged account, contrary to other financial securities.

It is unclear whether, the general civil law regime continues to be available for crypto assets as Article 2355, paragraph 5 of the French Civil Code above specifies it is available in the absence of special provisions. Furthermore, the Cour de Cassation (highest civil court) precedents have ruled that when a specific security regime is available, the common law one is no longer available.

The specific regime covers digital assets, ie, crypto assets targeted by MiCAR and cryptocurrencies. It should also apply to NFTs and collateral used in the context of DeFi.

Perfection

A pledge over crypto assets (*nantissement de crypto-actifs*) is established by a statement of pledge signed by the owner of the crypto assets. The statement of pledge must include mandatory information, to be detailed by the implementing decree. The statement of pledge may be executed using a smart contract executor. When the crypto assets are held by an authorised service provider under MiCAR, the latter stores and manages the crypto assets for the account of the grantor. The secured creditor may obtain, upon request, a pledge certificate including an inventory of the pledged crypto assets as of the certificate's issuance date. No other legal formalities are required for the perfection of the pledge. The statement of pledge renders the pledge valid between the parties and enforceable against third parties, including the service provider when it is the custodian of the pledged crypto assets.

Scope

The pledge includes:

- the crypto assets listed in the statement of pledge;
- those substituted to them or those supplementing them as security for the initial claim of the secured creditor, and, unless otherwise agreed by the parties, their fruits and proceeds (*fruits et produits*) consisting of crypto assets; or
- where applicable, sums in any currency, derived from the immobilisation of the pledged crypto assets in a DLT trading and settlement system.

An additional statement is required for additional digital assets, fruits and products supplementing the pledge, which is retroactive as of the date of signature of the initial statement of pledge. In order to secure the cash payments associated with crypto assets, the grantor must have a special account opened with a credit institution and refer to this account in its statement of pledge.

Successive pledges/ranking

When the crypto assets initially pledged are subject to several successive pledges, the ranking of creditors is determined, in relation to each digital asset, by the chronological order of their initial declaration. Each pledge is then notified to the CASP.

Right of use

The secured creditor and the grantor may define the conditions under which the latter may dispose of the crypto assets and sums included in the collateral base.

Right of retention

The secured creditor benefits from a right of retention over the pledged crypto assets and sums, enforceable against an insolvency proceedings.

Enforcement

The pledge may be self-enforced after the expiry of an eight-day or otherwise agreed notice period, by the crypto-asset service provider responsible for the custody of the pledged assets or, where applicable, the holder of the income and proceeds. The notice may be carried out by a smart contract.

Enforcement occurs up to the limit of the amount of the secured claim: (1) for sums in any currency, directly by transfer of full ownership to the secured creditor; and (2) for crypto-assets, in accordance with the terms agreed between the grantor and the secured creditor.

Where applicable, realisation takes place in accordance with the order specified by the grantor of the pledge.

In the absence of an agreement between the grantor and the pledgee, the valuation of the crypto assets is performed using an objective method that reflects normal market conditions, determined, where applicable, by the service provider responsible for the custody of the pledged digital assets.²

Transfer of title over the crypto assets by way of security

The transfer is made to a fiduciary (trustee) (essentially a credit institution, portfolio management company or attorney (*avocat*) acting for the benefit of the secured creditors). *Fiducie* security is

² Article L226-5, French MFC.

governed by Articles 2011 *et seq* of the French Civil Code, which provides that the fiduciary holds the assets in a segregated patrimony.

The transfer can be made by entry in the distributed ledger, or by transfer of a private key to the fiduciary. The *fiducie* agreement will provide for the list of the crypto assets given as security. The parties will define whether fruits and products are also to be transferred, by way of amendment to the *fiducie* agreement.

The contract may provide for a right of use and enjoyment of the crypto assets. Enforcement will give rise to the transfer of ownership of the crypto assets and, as the case may be, fruits and products to the secured creditor.

The *fiducie* contract and its amendments must be registered within one month of their date with the tax office of the fiduciary's registered office (or with the tax office for non-residents if the trustee is not domiciled in France), failing which they shall be null and void.

The *fiducie* security assets are bankruptcy immune. Enforcement is not subject to the stay unless there is retention of a right of use and enjoyment by the settler of the crypto asset. In all cases, the secured creditor may not be subject to a restructuring plan.

Financial collateral

While the question arises whether the Collateral Directive should be amended at European level to crypto assets, French law has taken the lead by broadening the scope of assets eligible as financial collateral to crypto assets listed in Article L211-36 *et seq* of the MFC, pursuant to DDADUE law, with effect from 1 July 2026. Enforceability is not subject to any formalities and results from the transfer of the assets and rights in question, the dispossession of the grantor or their control by the beneficiary or by a person acting on their behalf. The reform has specified that in the case of digital assets, this shall be effected by any computer process designating the crypto assets subject of the financial guarantee.

The definition of the transactions benefiting from the financial collateral regime has not been modified. It applies to transactions entered into between eligible parties such as credit institutions, funds and insurance companies, which can be settled in cash or by delivery of financial instruments; or among one eligible party and a non-eligible party where the secured financial obligations stem from transactions relating to financial instruments. In both cases, it insulates close-out netting of reciprocal payment and delivery obligations from relevant insolvency proceedings.

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

French law recognises the principle of free choice of law provided this is not contrary to principles of French public policy as applicable in international matters (*ordre public international*) or to French or foreign mandatory rules (*lois de police*). Mandatory French rules of private international law retain the concept of *lex situs* (or *lex rei sitae*), according to which the law applicable to proprietary issues relating to assets, including collateral assets, is the law where the assets are located. Furthermore, for the designated foreign law to be valid, there should be a cross-border element.

Crypto assets present a challenge as their location on DLT is difficult to determine under traditional legal concepts.

For transactions involving financial securities recorded on a blockchain, paragraph 4 of Article L211-7 of the MFC provides that:

‘The conditions and property effects of transactions involving financial securities recorded using distributed ledger technology under the conditions set out in Regulation (EU) 2022/858 of the European Parliament and of the Council of May 30, 2022, are determined by the law of the State where the entity authorised to operate the DLT settlement system or, where applicable, the DLT trading and settlement system is located.’

French courts have not yet addressed this jurisdictional issue regarding the *situs* of crypto assets other than financial securities. French doctrine proposes to refer to the nature of the tokenised asset: a token representing ownership of a specific asset may also justify its connection to the location of that asset, whereas for a token representing a security, the location of the issuing company could constitute a legitimate connection. The parties may also choose the applicable law or convention.

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

Is a party’s submission to a foreign jurisdiction legally binding and enforceable under the laws of your jurisdiction?

Under French law, a party’s submission to a foreign jurisdiction is legally binding and enforceable as long as it is mutually binding, subject to French public order requirements.

Any final and conclusive judgment obtained in a non-EU country will be recognised and enforced in France, after due service of process, if:

- the court of the non-EU country had indirect jurisdiction based on the connection of the dispute to the non-EU country court apprised of the case;
- the French court did not have exclusive jurisdiction over the matter;
- the foreign judgment is in conformity with the French public international order on the merits and procedure (*ordre public international de fond et de procédure*); and
- the foreign judgment is not tainted with fraud.

For EU countries, control by a French court is limited to verification that:

- such judgment is not held to be contrary to the French public policy, such being generally considered as the French public policy applicable in international matters (*ordre public international*);

- if such judgment has been given in default of appearance, the defendant has been duly served with the document which instituted the proceedings or with an equivalent document in sufficient time to enable them to arrange for their defence;
- such judgment is not contrary to any judgment given in a dispute between the same parties by any French court;
- such judgment is not contrary to an earlier judgment given in another EU Member State or in a third state involving the same cause of action and between the same parties, and which fulfils the conditions necessary for its recognition in France; and
- there is no violation of the principle of adversarial process.

Asymmetrical jurisdiction clauses designating an exclusive jurisdiction for all parties, yet allowing one or certain parties – generally the financial parties – to designate other courts, are valid provided that the competent jurisdictions can be objectively determined through factors that must be sufficiently precise to enable the court seized to ascertain whether it has jurisdiction, whether those factors are referred to in the clause or, where appropriate, can be determined by the particular circumstances of the case, on the basis of:

- Article 23 of Regulation (EC) No 44/2001 (which has been replaced from 10 January 2015 by Article 25 of Regulation (EU) No 1215/2012 of 12 December 2012 known as Brussels I Bis); or
- Article 23 of the Lugano Convention of 30 October 2007 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Lugano II).

That position should now be considered qualified by the judgment rendered on 27 February 2025 by the Court of Justice of the European Union (CJEU) (case C-537/23) on a matter referred by the Cour de Cassation. The CJEU confirmed that there is no prohibition in principle of asymmetric jurisdiction clauses, provided that such clauses meet the following conditions:

- they designate the courts of one or more states that are either EU Member States or parties to the Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters;
- they identify objective elements with sufficient precision to enable the court seized to determine whether it has jurisdiction; and
- they are not contrary to the provisions relating to the protection of weaker parties (consumers, workers, insured persons) nor do they derogate from exclusive jurisdictions under the Brussels I Bis Regulation.

Are exclusive jurisdiction clauses respected and enforceable?

Under French law, exclusive jurisdiction clauses are legally binding and enforceable, provided the parties' consent is clear and the clause itself is not contrary to French public order. French public policy as applied in domestic matters may extend to other principles of French law than those expressly stipulated by French law as being of public policy, such as in contracts:

- the principle of good faith;
- precontractual duty of information;
- lawful and certain content;
- voidness of contracts with an illusory or derisory consideration; or
- prohibition of clauses that deprive of substance the essential obligation of the debtor.

The scope and content of the French international public policy rules is generally narrower than those of French public policy. It includes the principle of respect for acquired rights and non-retroactivity of laws, the right to access to the judge, equality between creditors and stay of proceedings in insolvency proceedings.

The exclusive jurisdiction clause effect might be limited, in case of consumer or employee, where the choice of court is particularly regulated: the clause must have been concluded after the dispute arose or increase the number of courts to which the consumer may refer the matter (Brussels I-bis, Article 19).³

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

In France, digital creations related to crypto assets (software code, databases, virtual content) are protected automatically by copyright from the moment of creation without any formalities if they meet the condition of originality (intellectual contribution specific to its author). Crypto content (NFTs, virtual works) can fall under copyright and database rights, it being specified that the IP protection covers the creation, not the token as such. Authorship is presumed by the name under which the work is disclosed. Collaborative, composite and collective works have specific ownership rules.

Technical inventions related to crypto assets (protocols, hardware wallets) are protectable by patent if they are novel, involve an inventive step and capable of industrial application. The right to a patent belongs to the inventor. For employee inventions, patent ownership belongs to the employer upon payment of an additional compensation (invention of mission) or of a fair price (invention outside mission with attribution rights).

Defence against third parties combines interim measures/injunctions, seizure-counterfeiting, information measures and damages calculated on losses, the infringer's gain and/or a lump sum exceeding hypothetical royalties.

For international protection, EU priority (Paris/PCT), European patents and the Unified Patent Court are prioritised. Countries offering reciprocity/equivalent priority and presenting markets/manufacturing/distribution are targeted.

Local monetisation is possible via assignments and licences (exclusive/non-exclusive) published in the National Patent Register.

³ Cour d'appel, Toulouse, 3e chambre, 25 June 2025 – No 24/02146 (Analyse JurisData).



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