

Mexico

Miguel Gallardo Guerra*

BGBG, Mexico City

mgallardo@bgbg.mx

Jonathan Rangel Lora†

BGBG, Mexico City

jrangel@bgbg.mx

Introduction

This report provides a Mexico-focused overview of the principal legal and regulatory considerations shaping financial innovation, digital finance and crypto asset activity in the jurisdiction. The responses below address, in an integrated manner, the core pillars of Mexico's approach to fintech regulation (including the regulated perimeter for key business models), the treatment of crypto assets and associated risk drivers, the regulatory positioning of payment service providers and wallet-type structures, mechanisms intended to support innovation (including controlled testing models), the emerging architecture for data portability and open banking, and the compliance expectations applicable to virtual asset activities, particularly in the context of anti-money laundering (AML) and prospective Travel Rule developments. The analysis also highlights practical legal implications for tokenisation and secured structuring, as well as dispute and intellectual property considerations that are increasingly relevant as digital asset use cases evolve within Mexico's financial system.

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

Mexico's fintech regulatory framework is primarily anchored in the Law to Regulate Financial Technology Institutions, published on 9 March 2018 (the 'Fintech Law'), which established a comprehensive legal perimeter for financial innovation and the operation of regulated financial technology institutions under the authorisation and supervisory competence led by the National Banking and Securities Commission (CNBV), with the participation of the Bank of Mexico ('Banxico') and the Ministry of Finance (SHCP) within their respective statutory competences.

The statute recognises two main regulated categories and a separate track for innovative models. First, collective financing platforms (crowdfunding), which may intermediate financing through debt, equity, co-ownership or royalty-type structures via digital channels. Second, electronic payment fund institutions, which issue, administer, redeem and transfer electronically registered payment funds (wallet-type models). Third, there is a special track for innovative models authorised for limited testing under the regulatory sandbox regime, allowing eligible fintech solutions to operate in a controlled environment on a temporary basis, subject to specific conditions and oversight by the financial authorities.

In addition to identifying these regulated pathways, the Fintech Law is designed to bring digital finance within a formal authorisation and supervisory perimeter, requiring regulated operators to be formally authorised and to maintain an organisational and operational setup consistent with prudential expectations for regulated financial services in Mexico. In practice, this means that regulated fintech entities are expected to operate with defined governance structures, internal controls, and operational policies that allow them to demonstrate ongoing compliance throughout their lifecycle, not only at the licensing stage.

* Miguel Gallardo Guerra is a partner at the leading Mexican law firm bgbg (www.bgbg.mx), where he leads the Financial, Banking, Fintech, Crypto and Regulatory Compliance practice. With extensive experience advising national and international clients, he specialises in navigating complex regulatory frameworks and designing legal strategies for innovative financial technologies. His practice combines deep knowledge of Mexican financial law with a forward-looking approach to digital assets and compliance.

† Jonathan Rangel Lora is a partner at the leading Mexican law firm bgbg, where he leads the Intellectual Property practice. He advises clients across the full IP lifecycle, with particular strength in trademarks and copyright matters, as well as IP enforcement and anti-counterfeiting strategies.

A central feature of the framework is that it treats technology as an inherent regulatory risk factor. The statutory concepts and implementing rules are built around the idea that a fintech's technological infrastructure is part of the regulated operating model and must be managed accordingly through documented processes, controls and oversight. This has practical consequences for topics such as system resilience, information security events and the controls expected of regulated entities that provide services through digital channels.

The Fintech Law also sits within a broader regulatory ecosystem that includes central bank oversight for sensitive payment and digital asset interfaces. For example, in the crypto-adjacent perimeter, Banxico has issued binding rules applicable to regulated financial entities, under which banks and regulated fintech entities may only conduct virtual asset activity within the narrow concept of internal operations, and only to the extent authorised by the central bank, reinforcing a policy objective of limiting customer-facing exposure to the risks of virtual assets within regulated finance.

As to the sandbox (innovative models), the framework does not treat it as a third 'institution type' equivalent to crowdfunding or electronic payment funds institutions. Rather, it is a separate authorisation track for innovative models that require regulatory flexibility to be tested under controlled conditions. In practical terms, this track is aimed at permitting eligible innovation to operate temporarily within defined limits and under heightened oversight, precisely to assess risks and outcomes before a definitive, scalable authorisation model is pursued.

Finally, the Fintech Law's architecture is closely tied to Mexico's open finance vision through standardised connectivity obligations, which are operationalised through application programming interface (API) rules issued by the financial authorities, although implementation has progressed gradually. This is relevant because it frames fintech not only as a licensing perimeter, but as an ecosystem approach in which regulated entities and other financial participants are expected to evolve toward more standardised interoperability and data portability, subject to the specific layers and conditions established in the implementing rules.

This framework is complemented by implementing and related circulars referenced in the applicable regulatory architecture, including provisions applicable to electronic payment fund institutions, collective financing institutions, 'new model' testing, and certain changes to interbank electronic payment infrastructure rules.

As of the latest official figure publicly reported by the CNBV, 76 fintech institutions had been authorised under the Fintech Law in Mexico as of 29 February 2024, comprising 52 electronic payment funds institutions (IFPEs) and 24 crowdfunding institutions (IFCs). Since that date, additional authorisations have continued to be granted, so the current number may be higher; in practice, the most defensible way to confirm the real-time total for due diligence purposes is to verify the entity's authorisation status directly in the CNBV's public registry of authorised entities.

In 2025, Mexico advanced significant reforms to its anti-money laundering (AML) framework affecting virtual asset activity, which are addressed in greater detail in the sections below, including Travel Rule-type concepts and broader compliance requirements for relevant service providers. These measures were first discussed in reform proposals circulated during 2025 and were subsequently enacted through amendments published in the *Official Gazette* in July 2025, with implementation details to be further developed through secondary rules.

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

Crypto assets are addressed in Mexico through the concept of 'virtual assets', defined as electronically registered representations of value used as a means of payment and transferable exclusively by electronic means, while excluding sovereign currency and legal tender concepts as provided under the Fintech Law.

Building on an existing AML framework, since 2025 Mexico's AML perimeter has been strengthened and made more explicit for virtual asset activity carried out on a habitual or professional basis outside the traditional financial institution perimeter. This includes the express treatment of certain virtual asset operations as a vulnerable activity, the use of the Tax Administration Service (SAT) platform for registration and notices, and the operational relevance of published thresholds and compliance parameters for obligated parties.

At the same time, the legal classification of cryptocurrencies under Mexico's general private law remains unsettled, which creates uncertainty for issues that are decisive in practice, including ownership and possession, inheritance and estate division, seizure and attachment, enforceability of rights, and the structuring of cryptocurrencies as collateral (including pledge-type arrangements).

From a regulatory policy standpoint, the approach reflected in supervisory and regulatory dynamics described emphasises risk containment, including risks arising from information asymmetries due to the technical complexity of cryptography and the formation of crypto prices, as well as AML and counter-terrorist financing (CTF) considerations, and includes the expectation that risks inherent to virtual assets should not be transferred to customers.

Banxico has issued its opinion regarding virtual assets, in addition to issuing regulations and limiting them in various ways. Banxico established that virtual assets have several problems as a substitute for the Mexican currency, derived from the fact that they do not feature money characteristics as we know them: deposit in value, means of exchange, or unit of account. In Mexico, Banxico is an autonomous constitutional entity responsible for issuing currency, generating economic policies to protect the purchasing power of our currency, working to ensure that Mexicans have a healthy financial system and, consequently, ensuring that payment systems function properly.

Banxico published in March 2019, in the *Official Federal Gazette*, Ruling 4/2019 regarding virtual assets. Such ruling provides that in connection with virtual assets, there is a problem of information asymmetry produced by two causes:

- the complexity of the mathematical and cryptographic processes that support virtual assets and the difficulty for users in knowing such processes; and
- the complexity of the factors that determine the price of virtual assets, the unawareness of the elements that determine supply and demand, and the lack of any reference with which an estimate of their price can be obtained.

Another position of Banxico is that virtual assets represent a significant risk in terms of AML/CTF due to the ease of transferring virtual assets to different destinations, as well as the absence of controls and protection measures at a global level.

Accordingly, Banxico established that a separation must be given between virtual assets and the financial system; however, it is also true that Banxico establishes that it also seeks to promote and take advantage of the use of technologies that could have a benefit, as long as they are used in the context of the internal operation of financial technology institutions and banking institutions. The above does not imply an increase in operational and financial risks, so we must understand that it is intended to protect the final consumer. That is why, in the second paragraph of Provision Three of Ruling 4/2019, it is clearly stated that the institutions authorised to operate virtual assets must prevent the transfer, directly or indirectly, of the risk of such transactions to the institution's customers.

From a tax perspective, Mexico continues to apply general tax principles rather than a bespoke crypto tax statute, so characterisation remains fact-driven and may vary depending on the nature of the activity (for example, intermediation, habitual exchange services, or other business models), which reinforces the importance of a careful legal and transactional analysis for each use case.

Central bank digital currency discussions continue to be framed in Mexico as an exploratory policy and design process; public sources describe the project as remaining in an exploratory phase and without a definitive public issuance timeline, which is relevant when contrasting the regulatory posture applicable to sovereign digital money concepts versus private virtual assets.

The SAT has established virtual assets, in accordance with Article 17, section XVI of the Federal Law on the Prevention and Identification of Transactions with Illegally Obtained Funds (LFPIORPI), as a vulnerable activity:

'The usual and professional offering of exchange of virtual assets by subjects other than financial institutions that are carried out through electronic platforms, who manage and operate by facilitating or conducting operations to buy or sell such assets owned by their customers, or providing means to keep, store, or transfer virtual assets other than those recognised by the Bank of Mexico in terms of the Fintech Law.'

As of February 2020, it is mandatory to carry out the registration procedure related to virtual assets as a vulnerable activity for the purposes of LFPIORPI with the SAT through the Anti-Money Laundering Website (SPPLD). Therefore, notices must be submitted by the 17th day of the following month in which the act or transaction was made to the Financial Intelligence Unit (UIF) through the SAT. However, if no transaction has been carried out during the corresponding month, a report shall be submitted stating that no acts or transactions were carried out in the corresponding month that are the subject of the notice.

Furthermore, the SAT states that information and documentation that supports vulnerable activity must be kept, protected, and prevented from the destruction or concealment, as well as the one that identifies its customers or users. Therefore, those who carry out vulnerable activity with virtual assets must have a document with their guidelines for identifying customers or users, as well as the internal criteria, measures, and procedures to comply with the provisions of the LFPIORPI, its regulations, general rules, and other requirements derived from this law.

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

Payment service providers and digital wallets are regulated principally through the category of electronic payment fund institutions, which are described as entities that manage electronically registered balances used for payments and transfers, maintaining one or more accounts per client and enabling transfers among clients through digital channels.

Within the regulatory design referenced, these models may be linked to money transmission services regulated as auxiliary credit activities under Mexico's General Law of Credit Organisations and Auxiliary Credit Activities (LGOAAC) and may provide additional services described in the same context, including specified credit/overdraft functionality subject to applicable conditions and other operational services referenced.

The regulatory perimeter also includes constraints specific to wallet-type institutions, including prohibitions on paying interest or monetary benefits on accumulated balances. The applicable framework is further supported by implementing circulars issued for electronic payment fund institutions. No specific new, standalone wallet or payment service provider (PSP) statute is identified beyond the cited rulebook and related ongoing developments in connected areas such as 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.

Mexico provides a special mechanism intended to support fintech innovation through controlled testing of 'new models', commonly understood as a regulatory sandbox. Under this approach, innovative models that do not fit squarely within traditional regulatory schemes may operate under a temporary authorisation issued by the financial authorities on a discretionary basis, which operates through two distinct authorisation procedures depending on the nature of the applicant.

One authorisation track applies to commercial entities that are not financial technology institutions, regulated financial entities, or otherwise subject to supervision by a supervisory commission or Banxico. A separate authorisation track applies to entities that are already regulated and supervised. The temporary authorisation is described as being granted for a limited period aligned with the service, with a duration that depends on the applicable authorisation track, ranging from up to two years, with the possibility of a one-year extension to facilitate the transition toward a definitive authorisation where relevant, for commercial entities, or up to one year, with a single one-year extension, for regulated entities.

Any entity seeking sandbox authorisation must submit to the Commission the documentation and information required for the evaluation of the innovative model, which varies depending on whether the applicant is a commercial entity or an already regulated entity, and includes, among other elements:

- draft bylaws reflecting the innovative model;
- a description of the product or service to be offered to the public and an explanation of why it requires testing in a controlled environment;
- a description of the risk analysis policies, including the procedures to be followed with respect to technological infrastructure security and information security;
- an explanation of how the reserved activity will be carried out and why the model represents a benefit to users compared to what is currently available in the market;
- identification of the target market or, as applicable, a maximum number of clients to whom the product or service will be offered during the testing period;
- an explanation of how the entity will compensate clients for damages that may arise in connection with services provided during the testing period;
- evidence that the project is sufficiently mature to commence operations immediately, so it can be tested with a limited number of clients; and
- an exit procedure to be implemented if the financial authorities do not grant definitive authorisation, registration or concession, or if the temporary authorisation (or any extension) expires, as applicable.

Separately, both commercial entities and regulated entities that intend to continue offering the product or service on a regular basis must pursue definitive authorisation during the temporary period. At the discretion of the financial authority, the temporary authorisation may be extended for up to one additional year to allow the entity to complete the process for definitive authorisation. Once temporary authorisation is granted, the entity must also prepare and submit the reports required by the financial authorities within the applicable timeframes and in the form specified, including information regarding: (1) the number of transactions conducted during the period; (2) the number of clients; (3) any risk events or risk situations that occurred during the period; and (4) any other information requested by the financial authorities. The regulatory architecture referenced includes a circular specifically associated with the 'new model' regime.

In practical terms, Mexico's regulatory sandbox has not operated as an effective support mechanism for the fintech ecosystem: although the framework was designed to enable time-bound, supervised testing followed by a path to definitive authorisation, the mechanism has not produced a meaningful or consistent pipeline of sandbox participants reaching stable market operation within the contemplated timeframes, and the number of applications itself has remained marginal compared to the core Fintech Law authorisations, underscoring that the sandbox has not become a practical route to market for innovation in Mexico.

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

Under Mexican law, open banking is regulated under the Fintech Law, which provides that financial entities shall establish standardised computer APIs that enable connectivity and access

to other interfaces developed or managed by the same entities and by third parties specialised in information technology, for purposes of sharing open financial data, aggregated data and transactional data. Such regulations also provide that entities may only use the information for the purposes previously authorised by customers, and that open banking remains subject to further rules to be issued by the financial authorities, including Banxico. Entities and participants authorised to implement open banking functionalities may be subject to authorisation by Banxico, and any applicable fees must be approved by the financial authorities.

Currently, Mexican financial authorities have issued certain rules in connection with open banking, primarily through secondary regulations issued by CNBV focused mainly on public information, including ATM location data. In addition, Banxico has issued technical regulations governing the implementation and operation of APIs by institutions under its supervision, addressing aspects such as availability, connectivity and technical standards. The next set of regulations is expected to address the sharing of customers' transactional data.

6. Regulation of virtual asset service providers.

The regulation of activities involving virtual assets follows a dual dynamic that distinguishes between regulated financial entities and non-financial operators. For banks and regulated fintech entities, virtual asset activity is framed as limited to 'internal operations' and subject to prior authorisation by Banxico, in accordance with the provisions issued by this authority, with the expectation that institutions implement safeguards so that risks inherent to virtual assets are not transferred to customers. Internal operations are described as activities carried out internally to support customer-facing operations and services, including support for international transfers. Authorisation requests are described as being submitted through the central bank's authorisations and queries channels.

In parallel, for subjects other than financial institutions, the habitual and professional offering of exchange of virtual assets through electronic platforms, covering facilitation of buying and selling and certain means to store and transfer virtual assets as described, falls within Mexico's AML statute as a 'vulnerable activity', triggering registration and notice-filing obligations through SAT infrastructure.

Operationally, the 'vulnerable activity' classification triggers a two-track compliance workflow: (1) enrolment in the obligated parties' registry; and (2) ongoing filings through the dedicated platform administered by SAT. For virtual asset operators, the onboarding process is not purely digital: official guidance contemplates preregistration documentation that must be delivered in person at SAT offices (with different documentary packages for individuals and companies), after which the authority confirms that the applicant may proceed to complete the online in the AML portal.

Once registered, for virtual asset operations, the identification obligation applies in all cases, meaning the operator must capture and retain the identification data required for the relevant client/user and, where applicable, the beneficial owner/controlling beneficiary, consistent with the information scheme used for filings. The notice-filing duty is triggered when several thresholds are met, provided that these thresholds are operationalised in the AML portal and are reflected in the official SAT guidance for virtual asset activity. Procedurally, filings are made through the SAT system due no later than the 17th day of the month immediately following the month in which

the relevant operation occurred. The filing content must include (at minimum) general data of the obligated party, general data of the client/user (and beneficial owner when applicable), and a general description of the reported operation.

Two practical features of the regime matter for day-to-day operations. First, if the operator detects facts or indicia suggesting illicit origin or destination of resources, an accelerated filing is required within 24 hours, even if the transaction was not ultimately completed; similarly, accelerated filing applies when the client/user appears on AML lists published by the UIF. Second, if there are no reportable operations in a given month, the operator must still make a filing without specific information by the same monthly deadline. In addition, the portal guidance expressly contemplates aggregation: operations that individually may not exceed a reporting threshold can become reportable if the cumulative amount (by type of operation) reaches the notice threshold within a six-month period.

Finally, the framework treats governance as part of compliance. For legal entities (and structures acting through trusts or analogous vehicles), the operator must designate a representative in charge of compliance before SAT and keep that designation current; in practice, this becomes the anchor for portal access administration, internal accountability and regulator-facing communications.

Additionally, the 2025 strengthening of the vulnerable activity perimeter for virtual asset operations reinforces that, in the absence of a full 'virtual asset service provider (VASP) licensing regime' established through a single standalone statute, non-financial providers performing exchange or other professional services involving virtual assets are not subject to prudential authorisation requirements. Instead, such activities are primarily regulated through AML registration and notice-filing obligations administered by the SAT and linked reporting to UIF.

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

Mexico has adopted AML obligations applicable to certain virtual asset activities through the 'vulnerable activity' regime, which includes registration on the SAT portal and the filing of notices for operations that meet the statutory threshold, together with record-keeping and retention obligations.

For non-financial virtual asset operators, the regime is structured as an AML registration and reporting framework rather than a prudential licensing system. Accordingly, compliance focuses on customer identification, verification of the beneficial owner, transaction monitoring and reporting thresholds.

Mexico has strengthened AML coverage over virtual asset activity through the vulnerable activity regime and related reforms; however, a fully specified, technical 'Travel Rule' implementation should be described as still developing. The oversight mechanics referenced for these AML obligations remain linked to SAT processes and UIF reporting.

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

Tokenisation is described through a functional taxonomy that includes utility or governance tokens, security tokens and non-fungible tokens (NFTs). The legal environment is characterised by the absence of a fully adapted securities market regime for tokenised securities, with legacy infrastructure and legal formalities acting as practical barriers to the development of a domestic security-token market.

While the use of tokenised instruments is acknowledged in this conceptual framework, no detailed structuring templates for tokenised real estate, digital bonds or DeFi instruments are provided.

In relation to secured transactions involving crypto assets, the legal treatment of crypto assets under Mexico's general civil and commercial law is described as unsettled, and this uncertainty expressly affects issues such as the use of crypto assets as collateral (including pledge-type structures), with corresponding implications for enforceability and risk allocation.

No procedures are provided to create perfect security interests in tokenised or crypto collateral (including notarisation, registration, stamp duties or equivalent formalities), and no specific enforcement mechanics are described for secured lenders (including auction requirements or appropriation concepts). Existing civil and commercial law mechanisms may apply depending on the legal characterisation of the underlying asset, but there is no tailored statutory framework addressing crypto assets as a distinct category of collateral.

Similarly, no specific discussion is provided on the recognition and enforcement of foreign governing law clauses in crypto asset-related contracts. However, under general principles of Mexican private international law, foreign governing law clauses in commercial agreements are typically recognised and enforceable, subject to public policy and mandatory law limitations. The principal point established is that enforceability questions can arise in practice due to the unresolved private-law status of crypto assets.

In practical structuring, the legal analysis in Mexico tends to turn less on the token label and more on the legal characterisation of the underlying rights (for example, whether the token represents a contractual claim, a receivable-like position, or another recognisable category), and on whether the chosen collateral wrapper fits recognised secured-transaction mechanisms and perfection formalities under Mexican civil and commercial law. This point becomes particularly important given that the enforceability and perfection analysis will usually follow the nature of the underlying right and the applicable perfection route, rather than the tokenisation layer itself.

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

Mexican law does not contain specific jurisdiction or conflicts-of-law rules tailored to crypto asset disputes. Instead, the validity and enforceability of submission to a foreign jurisdiction or exclusive jurisdiction clauses are assessed under the general principles applicable to commercial agreements. The key litigation-relevant point established is that disputes involving crypto assets may be materially impacted by the absence of an express private law classification, which can affect issues

such as ownership and possession, succession and inheritance, seizure, and the enforceability of rights and obligations, thereby shaping risk assessment and dispute strategy in practice.

From a Mexican law perspective, it is also important to distinguish between negotiated commercial contracts and adhesion/consumer-style contracting. Recently, the Supreme Court in Mexico issued a relevant criterion addressing clauses of express submission to foreign jurisdiction in adhesion contracts offered in Mexico through online platforms, limiting enforceability in circumstances involving adhesion contracts and imbalances between the parties, particularly where consumer protection considerations are implicated. This jurisprudential development is not crypto-specific, but it is highly relevant for crypto asset disputes where platform terms are frequently adhesion-based and cross-border. Separately, cross-border enforcement in Mexico often becomes a matter of: (1) recognition and execution of foreign judgments under applicable procedural rules; and/or (2) the use of arbitration, where Mexico's commercial arbitration framework and treaty commitments support recognition and enforcement of arbitral awards.

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

In Mexico, innovations and inventions related to digital and virtual assets, including blockchain-based technologies and crypto assets, are protected under the general framework of intellectual property law. Patents are available for inventions that meet novelty, inventive step and industrial applicability requirements, while software and source code are protected as literary works under copyright law. Trademarks may protect names, logos, and other distinctive signs used in connection with digital or virtual goods and services.

Ownership of IP rights is generally vested in the inventor or author, or in the employer when created within the scope of employment, subject to statutory rules and contractual arrangements. Rights are acquired through registration (for patents and trademarks) or by creation (for copyright) and may be transferred or licensed. Enforcement is carried out primarily before the Mexican Patent and Trademark Office (IMPI) and federal courts through administrative actions, civil claims and, in certain cases, criminal proceedings, allowing rightsholders to stop infringing activities and claim damages.

The decision to seek protection in foreign jurisdictions is assessed on a case-by-case basis, considering factors such as target markets, commercialisation strategy, technological relevance, enforcement strength, costs and the risk of infringement. Priority is typically given to jurisdictions where the technology will be developed, exploited or licensed, or where enforcement is expected to be critical.

IP rights related to crypto assets can be monetised locally through licensing, assignment, technology transfer agreements, and commercial exploitation of protected software, platforms or brands. While Mexico does not currently recognise crypto assets as legal tender, there is no general prohibition on monetising IP associated with them. However, such activities must comply with applicable financial, AML, consumer protection and data protection regulations, particularly when involving VASPs or public offerings.



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