

Colombia

Natalia Escobar

Posse Herrera Ruiz, Bogotá
natalia.escobar@phrlegal.com

Rodrigo Pinilla

Posse Herrera Ruiz, Bogotá
rodrigo.pinilla@phrlegal.com

Óscar Tutasaura

Posse Herrera Ruiz, Bogotá
oscar.tutasaura@phrlegal.com

Santiago Bernal

Posse Herrera Ruiz, Bogotá
santiago.bernal@phrlegal.com

Juan Sebastián González

Posse Herrera Ruiz, Bogotá
sebastian.gonzalez@phrlegal.com

Paula Sarmiento

Posse Herrera Ruiz, Bogotá
paula.sarmiento@phrlegal.com

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

Colombia has not adopted a specific regulatory framework for fintech. However, there are specific regulations currently in place to foster innovation in the financial services industry, which may be classified into four groups, further developed below: (1) e-commerce, (2) personal data, (3) digitalisation of financial products, and (4) regulatory financial innovation tools.

E-commerce, digital contracting, and technological infrastructure for providing financial services

Decree 410 of 1971 (Code of Commerce)

Provides merchants with the possibility of executing agreements by any unequivocal means.

Law 527 of 1999 (E-commerce)

Defines and regulates the access and use of data messages, electronic commerce (including financial services and products), digital signatures and certification entities. Sets forth the 'functional equivalency principle' applicable to signatures, written documents and original compositions. Recognises the validity and enforceability of data messages.

Law 1273 of 2009

Amends the Criminal Code to include criminal offences against data and information systems' confidentiality, integrity and availability. These enhanced protections served as an enabling factor for the development of technological innovations, including fintech.

Law 1735 of 2014

Sociedades Especializadas en Depósitos y Pagos Electrónicos (SEDPEs) are financial institutions that may (1) receive deposits through simplified savings accounts; (2) make payments and transfers and act as acquirers; (3) take loans locally or internationally to finance their operation; (4) send and receive money transfers. SEDPEs may not provide loans. This law also enables financial institutions and financial services operators to access personal and biometrical identification data held by the national government when required to gain adequate access to financial services (ie, for know your customer (KYC) procedures).

Decree 1074 of 2015

Codifies several decrees regarding the commercial, industrial and tourism sectors, including e-commerce and electronic signatures regulations.

Decree 620 of 2020

Provides guidelines to foster the access of Colombian citizens to private and public digital services, including financial services.

Decree 338 of 2022

Strengthens the governance of digital security.

Central Bank External Resolution No 6 of 31 October 2023

Regulates interoperability in local immediate low-value payment systems.

External Circular 006 of 2025

Issued by the Financial Superintendency of Colombia (SFC for its Spanish acronym), this reissues the Basic Legal Circular (BLC), a compilation of mandatory regulations issued by the SFC to govern the products, services and institutions that comprise the Colombian financial system. Five chapters are noteworthy for this document.

- *SFC's BLC, Part I, Title I, Chapter VI:* Instructs financial institutions and other regulated entities on the minimum requirements for the use of cloud-based services.
- *SFC's BLC, Part I, Title I, Chapter IX:* Instructs financial institutions and other regulated entities on rules applicable to implement open finance.
- *SFC's BLC, Part I, Title I, Chapter X:* Instructs financial institutions and other regulated entities on rules applicable to offer such entities' technology and infrastructure to third parties.
- *SFC's BLC, Part I, Title II, Chapter I:* Instructs financial institutions and other regulated entities on digital transaction security, quality requirements, and standards for customer service through electronic channels.
- *SFC's BLC, Part I, Title IV, Chapter V.* Instructs financial institutions and other regulated entities on the minimum requirements for information and cybersecurity risk management.

Central Bank External Operational and Services Circular DSP-470, 2025, Subject 19

Regulates the Centralised Directory (DICE for its Spanish acronym) through which registry of individual keys for immediate payments that are processed through the low-value payment system (LVPS) are enabled.

Central Bank External Operational and Services Circular DSP-471, Subject 20, 2025

Regulates the Central Bank's Operating Mechanism for Settlement (MOL for its Spanish acronym) through which transactions of the LVPS are cleared.

Central Bank External Operational and Services Circular DSP-272, 2025

Regulates fees applicable to DICE and MOL.

Personal data and consumer protection

Unique Circular 001 of 2001

Issued by the Superintendency of Industry and Commerce (SIC) and also referred to as the Unique External Circular (UEC), it consolidates all mandatory regulations issued by the SIC. It is important to highlight the following two sections:

- *SIC's UEC, Title II:* Provides instructions regarding lending activities by non-regulated entities, including buy now, pay later (BNPL) business schemes; and
- *SIC's UEC, Title V:* Provides instructions on data protection and data processing activities applicable to all economic sectors in Colombia.

Statutory Law 1266 of 2008

Provides a protection scheme for the right of *habeas data* and regulates the treatment of personal financial and credit data, as well as personal data sharing within the country and on a cross-border basis.

Law 1328 of 2009

Provides the financial consumer protection scheme that applies to products and services offered by financial institutions to any type of consumer.

Law 1581 of 2012

Provides general protection for personal data.

Law 1480 of 2011

Provides a general consumer protection scheme, that includes rules on e-commerce platforms, electronic payments reversion, and online shopping withdrawal rights.

Decree 1074 of 2015

Codifies several decrees regarding the commercial, industrial and tourism sectors, including authorised financing activities developed by non-regulated entities such as private lenders and factoring. Several fintech business models are based on these activities.

External Circular 001 of 2025

Issued by the SIC to clarify data protection requirements that are applicable to semi-financial services provided by fintech companies.

Digitalisation of financial products

***Decree 661 of 2018 (compiled on Decree 2555 of 2010)*¹**

Authorises financial institutions to use technological tools to provide advisory and product recommendations using technical means (eg, robo-advisers).

Decree 1357 of 2018 (compiled on Decree 2555 of 2010)

Governs collaborative financing (crowdfunding) instruments (both equity and debt) based on electronic infrastructures, which may include interfaces, platforms, internet sites or other electronic communication means, to match contributors and recipients to finance a business initiative.

Decree 2443 of 2018 (compiled on Decree 2555 of 2010)

Enables some financial institutions to invest directly in financial technology innovation companies (FTIC), provided that the FTIC does not conduct any other core activities and refrains from holding equity in other entities. Colombian law and regulations strictly limit local financial institutions' equity investment capacity.

Decree 222 of 2020 (compiled on Decree 2555 of 2010)

Regulates simplified savings accounts, electronic savings accounts and low amount credit facilities by enabling digital opening, onboarding and disbursement processes. This decree also allows financial institutions and other regulated entities to enter into agreements with non-regulated agents (ie, correspondents) and broaden the means for providing services to their clients through the correspondent's physical and digital infrastructure.

¹ Decree 2555 of 2010 codified several decrees governing the finance sector, including financial, securities markets and insurance activities, and the financial institutions and other regulated entities that offer related products and services.

Decree 1692 of 2020 (compiled on Decree 2555 of 2010)

Governs LVPS, including acquiring and payment services providers' activities, such as processing, aggregation and access technologies.

Decree 1297 of 2022 (compiled on Decree 2555 of 2010)

Regulates payment initiation services, open banking, financial services ecosystems (embedded and third-party prompted), open financial architecture, and technology infrastructure services provided by financial entities to third parties.

Decree 1069 of 2025 (compiled on Decree 2555 of 2010)

Updates regulation on LVPS, including acquiring and payment services providers' activities, such as processing, aggregation and access technologies.

Regulatory financial innovation tools

Law 1955 of 2019, National Development Plan, Article 166

Authorises the SFC to issue temporary financial services licences (up to two years) in a controlled environment (known as a sandbox) to innovative technological developments related to activities reserved for financial institutions and other regulated entities. It also authorises all SFC-supervised institutions to develop and test creative technological activities under similar time conditions.

Decree 1234 of 2020 (compiled on Decree 2555 of 2010)

Provides the objectives, requirements and stages of operation of the SFC's controlled financial innovation environment (ie, sandbox) as a tool to promote innovation in financial services and facilitate the identification of new financial developments by government authorities.

External Circular 16 of 2021 (compiled in the SFC's BLC)

Provides further instructions regarding access to the SFC's sandbox.

Law 2294 of 2023, National Development Plan, Article 89

Introduces an obligation on public and private entities to share information that enables easier access to financial products and services.

Law 2294 of 2023, National Development Plan, Article 94

Introduces financial consumers' right to transfer their products and related information to another financial institution (financial portability right).

New and forthcoming laws or regulations

Bill 510 of 2025

Provides rules to create a registry of virtual asset services providers (VASPs) and requirements to be registered as such.

Draft Decree on Financial Portability

Sets forth specific conditions and requirements applicable to materialise the right of financial portability.

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

Colombia has yet to issue comprehensive regulations on crypto assets. Some initiatives have focused on warning the public about the risks of investing, offering or facilitating operations over digital assets, including crypto, and reminding financial institutions that they are not authorised to participate in such activities. Furthermore, specific anti-money laundering (AML) provisions have been implemented to address the higher AML risk profile of crypto assets.

In this vein, the SFC issued Circular Letters 29 of 2014, 78 of 2016, and 52 of 2017, addressed to public and financial institutions and other supervised entities. These state that Colombian financial institutions are not allowed to custody, invest, intermediate or operate with these instruments, nor can they use their platforms to conduct operations of cash-in or cash-out outside the controlled financial innovation environment. Financial institutions are not authorised to advise on or manage operations with crypto assets. No private or governmental guarantee or deposit insurance scheme is available to invest such assets.

Legal nature

The Board of Directors of the Colombian Central Bank (Banco de la República), the SFC, the Superintendency of Companies, the Financial Regulation Unit, the National Tax and Customs Authority, the Financial Information and Analysis Unit (UIAF, for its acronym in Spanish) and the Colombian Accounting Board (as an observing member) have concluded that, under Colombian law and regulation, crypto assets:

- may not be considered as legal tender. Only the currency issued by Banco de la República is legal tender in Colombia. As a result, it is not mandatory to receive crypto assets as a means of payment;

- if issued abroad, crypto assets may not be considered foreign currency because they are not recognised by any international financial authority or backed by any central bank;
- are not considered securities under Colombian securities law and regulations. Therefore, they may not be referred to or advertised as such; and
- may not be considered financial assets or investment assets in accounting terms.

Following these conclusions, in Colombia, crypto assets are treated as intangible assets that the public may acquire and sell. Their use is further limited by regulations preventing the massive solicitation of funds from the public and unauthorised cross-border offering of foreign financial services in Colombia.

Tax treatment

The local tax authority (Dirección de Impuestos y Aduanas Nacionales or DIAN) issued Unified Opinion on Crypto Assets No 100202208 – 1621 on 17 October 2023, under which virtual assets (1) are classified as intangible assets; (2) virtual assets’ ownership shall be informed in residents’ tax returns; and (3) any resident’s realised income derived from transfers of virtual assets is subject to the local income tax rate.

Additionally, under such Opinion, non-residents that economically exploit virtual assets in Colombia² are subject to the local income tax and complementary taxes.

Central bank digital currencies (CBDCs)

There is no specific local legal framework on CBDCs.

Additionally, the Central Bank has not announced a decision to issue a national CBDC; however, it has published analyses on the pertinence and risks of issuing a CBDC in Colombia.

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

Payment service providers

Colombia has regulated the payment services industry under the legal definition of LVPS. A payment system is an organised set of policies, rules, agreements, payment instruments, entities and technological components, such as equipment, software and communication systems, which allows the transfer of funds between system participants by receiving, processing, transmitting, clearing and settlement of payment orders or fund transfers.

2 A virtual asset is deemed as economically exploited in Colombia when (1) it is monetised in Colombia, that is, exchanged for legal tender or foreign currency; or (2) it is used as a means of payment (in kind) to acquire goods or services within national territory.

To operate, an LVPS requires (1) a low-value payment system managing company (LVPSMC) and (2) at least three or more SFC-supervised institutions and certain cooperatives (subject to requirements) to act as participants.

Access to the LVPS is considered part of the acquiring activity and, as such, may include:

- connecting merchants to the LVPS;
- providing merchants with access technologies that enable the use of means of payment (eg, debit and credit cards, QR, contactless instrument of payments, cash transfers, etc);
- processing payment orders or transfers of funds initiated through access technologies;
- aggregating merchants before LVPS; and
- receiving the proceeds of the sales made by a merchant through the access technologies supplied to it, as well as managing the adjustments that may arise from a process of disputes, returns, claims or chargebacks, and notifying the user of the confirmation or rejection of the payment or transfer order.

These activities may be carried out by the acquirer directly or through the acquirer's contractors, called payment service providers (PSPs). Acquiring activity may be carried out by the following types of entities (known in this capacity as 'acquirers'): credit establishments (including banks), SEDPEs and commercial companies not supervised by the SFC, subject to specific quantitative and qualitative requirements, including inscription in the Unregulated Acquirer Registry kept by the SFC.

In this vein, PSPs in Colombia are mostly technology service providers for acquirers. Colombian regulations recognise the following types of PSP:

- *Aggregator*: Acquirer payment service provider that connects merchants to the LVPS. It provides access technologies that allow the use of payment instruments and collects on their behalf the proceeds resulting from the order payment or transfer of funds in the merchant's favour;
- *Access technology supplier*: Provider of payment services of the acquirer that supplies the merchant with access technologies that allow the use of payment instruments in in-person and digital environments;
- *Acquirer processor*: Payment service provider of the acquirer that routes orders for payment or transfer of funds to the managing entity of the LVPS; and
- *Issuer processor*: Provider of payment services of the issuing entity of a payment, that transmits the authorisation of a payment order or transfer of funds to the entity administrator of the LVPS.

Digital wallets

Colombian regulations have yet to define digital wallets. However, the market understands digital wallets as instruments or mechanisms that, in association with a deposit account in a financial institution, allow its holder to pay a monetary obligation, transfer funds or withdraw funds physically or virtually.

Digital wallets are structured in Colombia using 'low amount deposits', a type of digital simplified deposit account available to the public, subject to specific requirements, including a cap of around US\$2,990 on the aggregated value of transactions per month and a US\$2,990 maximum account balance threshold.

While receiving funds from the general public is restricted to financial institutions with deposit-taking licences, low amount deposits have enabled partnerships between fintech and financial institutions to offer banking as a service (BaaS) products. However, in Colombia, it is not possible to provide digital wallets in which a fintech aggregates depositors before the financial institution.

Stablecoin digital wallets

While no laws or regulations have been issued on stablecoins and associated products in Colombia, a wide array of stablecoin digital wallets are currently being offered in Colombia and to Colombian residents, mainly to (1) enable protection against inflation; and to (2) streamline remittances.

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.

Sandboxes

As mentioned in Section 1, the SFC hosts a regulatory sandbox known as the *Arenera* and a 'controlled financial innovation environment'.

The Arenera provides a regulatory framework to conduct tests of technological innovations applied to financial services, the stock market or insurance services in a controlled and supervised environment. In this space, innovative companies can test new business models, applications, processes or products that have components of innovation in technology that aim to provide a benefit for the financial consumer, facilitate financial inclusion or develop the financial services markets.

The controlled financial innovation environment is a capacity-building public innovation tool that allows the Colombian government to adjust the regulatory framework to the new market dynamics and promote safe and sustained financial innovation. In this space, innovative companies that intend to implement disruptive technological developments to carry out activities reserved for regulated entities may request a temporary operation certificate valid for up to two years. Once the temporary certificate lapses, the participant may opt to obtain a full licence or to wind down its operation under close oversight by the SFC.

Accelerator programmes

While accelerator programmes exist in Colombia, such programmes are typically (1) broader, as they are not limited to fintechs; and (2) typically carried out by private entities. The regulator does not intervene on such programmes.

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

Decree 1297 of 2022, also known as the open finance regulation, authorised financial institutions to act as data processors and to commercialise the use, storage and transmission of their clients' data subject to compliance with Colombia's data protection law and regulations. It also regulated payment initiation activities and set ground rules for LVPSMC neutrality, such as removing barriers to access by payment initiators and managing conflicts of interest, and a mandate for the SFC to develop applicable security requirements. It also regulated digital ecosystems, including offering third-party services through the financial institutions' distribution channels and offering financial institutions products and services through the technological platforms of third-party providers.

Colombia opted for a regulated standard for developing open financial architecture, and the SFC issued such standards through Chapter IX of Title I of Part I of the BLC.

6. Regulation of virtual asset service providers.

As explained in Section 2, VASPs are not specifically regulated under a uniform legal framework, and a local licence is not required to provide virtual assets services. However, certain authorities have issued specific reporting regulations and requirements, under which VASPs are defined differently.

UIAF's Resolution 314 of 15 December 2021

Although the term 'virtual asset service provider' is not expressly used, this Resolution is applicable to reporting entities, which are any natural or legal persons who carry out, for or on behalf of another natural or legal person, one or more of the following activities or operations, regardless of its amount:

- exchange between virtual assets and fiat currencies, and exchange of fiat currencies for virtual assets;
- exchange between one or more forms of virtual assets;
- transfer of virtual assets;
- custody or administration of virtual assets or instruments that enable control over virtual assets;
- participation in and provision of financial services related to an issuer's offer or the sale of a virtual asset; and
- in general, services related to virtual assets.

Failure to comply with reporting obligations to UIAF may result in sanctions against the reporting entity by the Superintendency of Companies.

DIAN Resolution 240 of 24 December 2025

Under this Resolution, the term 'reporting crypto asset service provider' is defined as any natural or legal person who, as an economic activity or business, provides a service to carry out exchange transactions for or on behalf of clients. A reporting crypto asset service provider shall be understood to mean any natural or legal person acting as a counterparty or intermediary in exchange transactions, or that makes available a platform for the trading or transfer of crypto assets.

Exchange transactions are (1) exchanges between relevant crypto assets and fiat currencies; and (2) exchanges between one or more forms of relevant crypto assets.

Finally, relevant crypto assets are any crypto assets that are not a CBDC, an e-money product or any crypto assets that may not (1) be used as a payment means; or (2) acquired as an investment. Failure to comply with reporting obligations to DIAN may result in sanctions against the VASP to be imposed by DIAN itself.

Please refer to Section 7 for further details on VASPs' current obligations.

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

Compliance

Under Chapter X of its BLC (the 'SAGRILAF Circular'), the Superintendency of Companies has set forth an obligation to implement a self-control and comprehensive risk management system for money laundering, terrorism financing, and financing of the proliferation of weapons of mass destruction (*Sistema de Autocontrol y Gestión del Riesgo Integral de Lavado de Activos, Financiación del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva*, or SAGRILAF). According to Article 4.2.6. of the SAGRILAF Circular, this is applicable to local companies that:

- carry out, for or on behalf of another natural legal person, one or more activities related to virtual assets³ in an amount equal or greater than 100 legal monthly minimum wages (SMLMV), whether individually or in the aggregate (approximately US\$47,000 for 2026); and
- as of 31 December of the immediately preceding year, had total income equal or greater than 3,000SMLMV (approximately US\$1.419m for 2026) or held assets equal to or greater than 5,000SMLMV (approximately US\$2.366m for 2026).

Such companies must also conduct the enhanced due diligence procedures set forth in Article 5.3.2. of the SAGRILAF Circular, which includes:

- obtaining the approval of the employee of higher hierarchy to engage in a contractual relationship with the counterparty;

³ Such activities or operations are (1) exchanges between virtual assets and fiat currencies; (2) exchanges between one or more forms of virtual assets; (3) transfers of virtual assets; (4) custody or administration of virtual assets or instruments that allow control over virtual assets; (5) participation in and provision of financial services related to the offering by an issuer or the sale of a virtual asset; and (6) in general, services related to virtual assets.

- identifying such companies' counterparties' beneficial owner;
- taking reasonable steps to establish the source of the counterparty's resources;
- carrying out continuous and intensified monitoring of the contractual relationship and the counterparty;
- carrying out intensified due diligence on activities related with virtual assets to identify whether the counterparties in these operations and the virtual assets themselves represent a money laundering, financing terrorism or proliferation of weapons of mass destruction (ML/FT/PF) risk, in accordance with the warning signs established by the Financial Action Task Force (FATF) in the document called AML/FT risk indicators on virtual assets; and
- carrying out enhanced due diligence on the counterparties to such operations, the virtual assets, and their intermediaries.

Regarding SAGRILAFI obligations, companies required to implement this programme must:

- appoint a local compliance officer designated by the board of directors or highest corporate body who meets the minimum independence and qualification requirements set forth in the SAGRILAFI Circular;
- adopt a formal SAGRILAFI policy and procedures manual and implement a risk-based methodology (including risk appetite/tolerance, identification, segmentation, measurement, control, monitoring and reporting) supported by a documented ML/FT/PF risk matrix that is periodically reviewed and updated;
- conduct ongoing training and internal dissemination of the SAGRILAFI programme to all company personnel;
- perform third-party/counterparty due diligence proportionate to risk and, where applicable, enhanced due diligence;
- ensure internal audit/independent review of SAGRILAFI's design and effectiveness; and
- submit the legally required reports to the Superintendency of Companies and the UIAF.

Under UIAF Resolution 314 of 2021, any natural or legal person that provides virtual asset services must report to the UIAF:

- suspicious transactions immediately;
- the absence of suspicious transactions;
- transactions with virtual assets that meet the prescribed thresholds;
- the absence of such transactions; and
- a list of active, inactive and disengaged clients that appears registered in the exchange platform.

Failure to comply may give rise to administrative liability and sanctions by the Superintendency of Companies.

Moreover, under DIAN Resolution 240 of 24 December 2025, issued by such authority as part of Colombia's compliance with the OECD Crypto Asset Reporting Framework, VASPs are required to report information on all transactions processed, under different types of categories, and to provide identification information of reportable users that use such VASPs' services to transact with virtual assets.

Under such regime, reports shall be filed annually. Under Resolution 240 of 24 December 2025, reporting starts in 2027 for information relating to taxable years 2026 onwards. The regime does not set a transactional threshold (ie, reportable transactions are not conditioned on a minimum amount).

Failure to comply with reporting obligations to DIAN may result in sanctions against the VASPs to be imposed by DIAN.

While Colombian AML rules do not expressly incorporate the FATF 'Travel Rule,' the regulatory requirements referenced above, particularly DIAN Resolution 240 of 2025, pursue the same objective by requiring VASPs to identify and report originator and beneficiary information for virtual-asset transfers.

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

Tokenised assets

Colombia does not have a standalone tokenisation framework. However, depending on their features and the rights they confer, tokenised instruments may be characterised as securities (*valores*) and trigger securities offering/registration and market infrastructure requirements. Accordingly, structuring mass fundraising mechanisms through tokens may entail high regulatory risk and, in certain structures, may also be deemed as unauthorised deposit-taking activities.

Tokens may be used contractually to represent economic or ownership rights, but for assets subject to notarisation, public registration or other legal formalities (eg, real estate), the transfer of a token is not sufficient to effect a transfer of title, as the applicable legal requirements shall still be complied with. Any distributed ledger technology (DLT)/tokenisation pilot involving regulated financial activities could potentially be tested through the SFC's controlled testing space (sandbox), subject to prior authorisation and case-by-case conditions.

In practice, digital asset-related secured transactions typically rely on (1) contractual custody/control arrangements over crypto assets (eg, escrow or multi-signature setups and control of private keys); (2) security interests over receivables or other movable assets under the pledges regime; and/or (3) fiduciary structures (trusts) holding the underlying assets.

In any case, the most common funding structure of local projects is typically carried out through trusts, which (1) hold the underlying assets; (2) issue participation units to settlers; and

(3) distribute revenue. By holding part of the trust's equity, investors may rely on the underlying asset as collateral or additional pledges may be created over movable assets and registered before the National Registry of Pledges. Under an insolvency scenario, execution of such registered guarantees is prioritised after fulfilment of pending labour and tax obligations.

Collateral enforcement

The enforceability of a foreign governing law clause depends on the agreement's execution, as jurisdiction is determined by the place where the purpose of the contract will be fulfilled.

In accordance with Article 869 of the Colombian Code of Commerce (Código de Comercio), the choice of a foreign law as the governing law of an agreement is effective under Colombian law when the obligations to be performed by the parties thereunder are performed outside of Colombia. If, pursuant to the agreement that is governed by a foreign law, a party to any such foreign-law governed agreement was to initiate judicial actions in Colombian courts, there are no Colombian court decisions with precedential value pursuant to which it is possible to conclusively determine (1) if a Colombian judge assuming jurisdiction over the case would apply Colombian law or foreign law; or (2) if a Colombian judge were to apply foreign law to the case, the manner in which a Colombian judge would apply, interpret or construe foreign law.

However, pursuant to the provisions of Law 1563 of 2012, any agreement to be performed in Colombia complying with certain international requirements defined therein (and described in Section 9), could be governed by foreign laws, provided the parties thereto submit any disputes under such agreement to the forum of international arbitration.

There is the possibility that a Colombian court recognises Colombian law as the governing law of the corresponding agreement, thereby overriding the parties' agreement to a foreign governing law. The most effective way to ensure application of foreign law is to include an international arbitration clause in the agreement, as the application of foreign law is a matter that is disputed under Colombian law and its application by a Colombian court may be unpredictable in its outcome.

Collateral structure

Local collateral structures are typically based on a pledge, which shall be registered before the National Registry of Pledges to be deemed a second priority credit upon insolvency proceedings. Per applicable law, only labour, tax and family obligations are deemed as first priority credits.

In case of default, payment through a pledge that is registered before the National Registry of Pledges may be enforced through judicial enforcement, which is the applicable procedure when the parties have not agreed on a different collateral enforcement mechanism. However, the parties may agree to the collateral enforcement mechanisms of (1) direct payment, or (2) special execution.

Through the direct payment mechanism, the secured creditor is granted ownership of the collateral asset; such mechanism may be implemented (1) when agreed upon; or (2) when the secured creditor is the holder of the collateral asset.

Through the special enforcement mechanism, the secured creditor is granted the right to sell the collateral asset; such mechanism is applicable:

- by mutual agreement between the secured creditor and the grantor, as set out in the security agreement, its amendments, or subsequent agreements;
- when the secured creditor is in possession of the asset given as collateral;
- when the creditor has a statutory right of retention over the asset;
- when the asset has a value below 20SMLMV;
- when a term expires or a resolutive condition of an obligation is fulfilled, provided that the possibility of special enforcement has been expressly foreseen; and
- when the asset is perishable.

A mutually agreed special enforcement mechanism may include a special mechanism to carry out the sale or appropriation by the creditor of the asset over which the security interest is granted.

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

Under local law, an agreement's governing law is determined by the place of performance of the obligations regulated within such contract. Therefore:

- non-exclusive submission to a foreign jurisdiction is legally binding and enforceable, provided that a local court does not assume jurisdiction due to the place of performance of the obligations regulated within the corresponding contract;
- exclusive jurisdiction clauses are not enforceable, as laws on applicable jurisdiction are categorised as public order laws and, therefore, may not be circumvented through agreements. Accordingly, Colombian courts may decide to assume jurisdiction over such disputes when the place of performance of the obligations regulated within the corresponding contract is Colombia; and
- *International arbitration*: Section 62 of the Colombian Arbitration Statute (Law 1563 of 2012) provides that parties may agree to international arbitration if their contract has an international element. An international element is defined as:
 - when parties are incorporated in different jurisdictions;
 - when the fulfilment of the obligations arising from the contract shall take place in a country different from the one where the parties are domiciled in; or
 - the agreement affects the interests of international commerce.

Section 82 of the Colombian Arbitration Statute also provides that parties that agree to international arbitration may freely establish where the arbitration will seat.

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

IP protection mechanisms for crypto assets

In Colombia, innovations and inventions are protected under the intellectual property framework established by the Andean Community regime, mainly Andean Decision 486 of 2000 (Industrial Property) and Andean Decision 351 of 1993 (Copyright).

From an intellectual property perspective, protection on crypto assets arises from the different technological, creative and commercial components that make up the ecosystem. Accordingly, protection strategies typically combine several IP mechanisms.

Blockchain protocols, smart contracts, source code and platform infrastructure supporting crypto assets are generally protected as software under copyright law pursuant to Decision 351 of 1993 and Law 23 of 1982 (and its amendments). Copyright protection arises automatically upon creation and may be reinforced through registration before the National Copyright Authority for evidentiary purposes.

On the other hand, technological developments in blockchain infrastructure, or tokenisation systems that provide a technical solution to a specific problem, may be protected through patents or utility models, if novelty, inventive step and industrial applicability requirements are met. However, abstract algorithms or mathematical methods are excluded from patentability.

Crypto assets frequently use specific names or graphic representations to identify tokens, blockchain networks, exchanges, wallets, platforms or non-fungible token (NFT) collections which may be protected as trademarks before the Superintendence of Industry and Commerce. Indeed, there are specific products and services related to crypto assets that may be identified and protected through trademarks in accordance with the Nice Classification, such as:

- *Class 9:* cryptography software; cryptocurrency hardware wallets; downloadable cryptographic keys for receiving and spending cryptocurrency; utility, security and cryptography software; downloadable software for generating cryptographic keys for receiving and spending cryptocurrency; downloadable computer software for managing cryptocurrency transactions using blockchain technology; downloadable digital music files authenticated by NFTs; downloadable computer software applications for minting NFTs; downloadable digital image files authenticated by NFTs; downloadable computer software for blockchain technology;
- *Class 36:* financial trading of cryptocurrency; electronic transfer of cryptocurrency; financial exchange of cryptocurrency; financial transactions via blockchain; electronic funds transfer provided via blockchain technology; and
- *Class 42:* mining of cryptocurrency; mining of crypto assets; electronic storage of cryptocurrency; data storage via blockchain; blockchain as a service; computer programming of smart contracts on a blockchain.

Other proprietary elements such as mechanisms, structures, architectures, or operational methodologies and processes may qualify as trade secrets under Decision 486, provided that reasonable confidentiality measures are implemented.

Particularly in the case of NFTs, intellectual property protection typically focuses on the underlying digital asset rather than the token itself. Digital artworks, audiovisual content, music, designs or other creative works linked to NFTs are protected under copyright law. Ownership of copyright is not transferred through the mere acquisition of an NFT, unless expressly agreed through licensing or assignment terms when acquiring such asset.

Ownership of intellectual property rights and enforcement

Ownership of intellectual property rights in Colombia follows different rules depending on the category of rights involved. With respect to industrial property, rights are generally acquired through registration before the competent authority. In the case of trademarks, exclusive rights arise upon registration pursuant to Article 154 of Andean Community Decision 486 of 2000, and ownership is attributed to the registered holder. In patent matters, the right to the patent belongs to the inventor under Article 22 of Decision 486, and exclusive rights are consolidated through the granting and registration of the patent. Trade secrets, governed by Articles 260–266 of Decision 486, do not require registration because protection is granted to the person or entity that lawfully controls the confidential information and has adopted reasonable measures to maintain its secrecy.

In contrast, copyright protection does not depend on registration. Under Article 4 of Law 23 of 1982, the author is the original holder of rights, and protection arises upon creation in accordance with Article 9 of the same law. While moral rights remain with the author, economic rights may be transferred by written assignment. Colombian law also establishes presumptions regarding the transfer of economic rights in certain contexts, such as works created within employment or services agreements, subject to Article 20 of Law 23 of 1982.

This distinction is particularly relevant for crypto assets, where ownership over software, NFTs, patents and distinctive signs must be properly structured through registration (for industrial property rights) and written assignments (for copyright) to prevent ownership disputes.

IP rights are enforced through both administrative and judicial mechanisms, depending on the category of rights involved. With respect to industrial property, enforcement may be pursued through judicial actions arising from the infringement of exclusive rights or from acts deemed to constitute unfair competition. From an administrative perspective, decisions issued by the Superintendence of Industry and Commerce may be challenged through nullity actions filed against its resolutions.

Copyright disputes, in turn, may be brought before the civil courts seeking compensation for the damage caused by the infringement. Infringements of both industrial property rights and copyright may also give rise to criminal liability, including imprisonment and monetary fines.

Local and international protection

When determining the appropriate jurisdiction in which to seek intellectual property protection, the territorial nature of such rights must be the primary consideration. Industrial property rights, such as trademarks, patents and industrial designs, are governed by the principle of territoriality, meaning that their protection and enforceability are limited to the country or region in which they are granted.

Accordingly, protection should be sought in those jurisdictions that present a genuine commercial relation with the product or service, particularly where they are manufactured, marketed, distributed, commercialised or actively advertised. Equally relevant are the jurisdictions in which key suppliers, developers, contractors or strategic partners are located, as well as those where there is a tangible risk of infringement. A proper choice of these territorial and commercial factors is essential to define a coherent, cost-efficient and enforceable international protection strategy aligned with the business's current operations and projected expansion.

This analysis is especially important in the case of trademarks, given that many jurisdictions provide for cancellation actions based on non-use. Registering a mark in territories where it is not genuinely intended to be used within the statutory period may expose the registration to vulnerability and eventual cancellation, resulting in unnecessary costs and administrative burdens. Therefore, good filing strategy should align territorial protection with actual or planned commercial use, ensuring both enforceability and long-term validity of the rights.

IP over crypto assets monetisation strategies

In most cases, the economic value lies in the protected intangible assets that are part of the crypto assets, including trademarks (such as the name of the token, protocol or platform), proprietary software and smart contracts, graphical user interfaces, digital artwork linked to NFTs, and potentially patentable technological solutions. These assets may be monetised through licensing structures (exclusive or non-exclusive), royalty schemes, white-label arrangements, technology integration agreements, software as a service (SaaS) models, brand partnerships and merchandising strategies.

A robust monetisation strategy therefore requires a coordinated approach combining trademark protection, copyright structuring, technological protection mechanisms, and carefully drafted licensing and commercial agreements.

Colombian law does not impose intellectual property restrictions specifically applicable to crypto assets. However, the scope of monetisation is inherently defined by the nature and extent of the rights held. For instance, only the holder of the economic rights in copyrighted works may license them. Likewise, trademark-based monetisation strategies, such as licensing, merchandising or brand partnerships, are limited to the products and services for which the mark is registered and to the territories in which protection has been secured.

Therefore, the feasibility and structure of any monetisation strategy depends on the effective ownership, scope, duration and territorial coverage of the relevant intellectual property rights.



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