

India

Sajai Singh
JSA, Bengaluru
sajai@jsalaw.com

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

Some of the notifications and regulations that relate to financial technology offerings in India are listed below.

Payment aggregators and payment gateways

Intermediaries that facilitate online payments, such as payment aggregators, are regulated primarily under the Master Direction on Regulation of Payment Aggregators, 2025 (the 'PA Directions') issued by the Reserve Bank of India (the 'Reserve Bank') on 15 September 2025. Payment aggregators are entities that facilitate e-commerce sites and merchants to accept various payment instruments from customers, pool the same and transfer to the merchants after a specific time period.

Payment gateways do not handle any funds on behalf of merchants and provide technology infrastructure to route and facilitate processing of an online payment transaction. The PA Directions are applicable to payment aggregators. Payment gateways may choose to adhere to the baseline technology-related recommendations contained in the PA Directions. Non-bank payment aggregators are required to obtain authorisation from the Reserve Bank and are required to be incorporated in India. Payment aggregators must also adhere to the due diligence and escrow account norms set out in the PA Directions.

Digital lending

On 2 September 2022, the Reserve Bank issued the Guidelines on Digital Lending (the '2022 Guidelines'), which were repealed and replaced on 8 May 2025 by the recently issued Digital Lending Directions, 2025 (the 'DL Directions'). Per the DL Directions, digital lending has been defined as a 'remote and automated lending process, largely by use of seamless digital technologies for customer acquisition, credit assessment, loan approval, disbursement, recovery and associated customer service'. It applies to digital lending applications and platforms operated by banks and non-banking financial companies, as well as to those operated by lending service providers engaged by banks and non-banking financial companies. The provisions of the 2022 Guidelines, which bring clarity and permissibility to loss-sharing arrangements in digital lending, have also been incorporated into the DL Directions. The DL Directions recognise and permit regulated entities (REs) to enter into arrangements with lending service providers or other REs, under which the latter guarantees to compensate the RE's loss due to default (up to a certain percentage) of the loans provided by the RE.

The most crucial aspect of these regulations is the imposition of a five per cent cap on the maximum loan coverage a third party can offer for the entire loan portfolio. This effectively means that most credit risk will still be borne by the lending institution (or RE). Additionally, the default loss guarantee (DLG) amount cannot be used to offset losses on specific individual loans; REs also must activate the DLG within a maximum of 120 days of a loan becoming overdue, unless the borrower pays off the loan before this period elapses.

One of the key additions in the DL Directions is the introduction of specific provisions for lending service providers partnering with multiple REs, mandating transparent disclosure of all potential

lenders and unbiased presentation of loan offers, which was absent in the 2022 Guidelines. Further, the DL Directions have also reduced the minimum cooling-off period from three days for loans with a tenor of seven days or more to just one day for all loans, regardless of the tenor. The DL Directions are being implemented in a phased manner, with most provisions coming into force with immediate effect; extended timelines for multi-lender arrangements and reporting requirements, that is, the DL Directions will be in force in entirety by 1 November 2025.

National Payments Corporation of India (NPCI)

The NPCI was set up as a joint initiative of the Reserve Bank and the Indian Banks Association under the Payment and Settlement Systems Act 2007 to operate retail payments and settlement systems in India. The NPCI has launched many payment systems in India, such as the Unified Payments Interface (UPI), RuPay (domestic card network) and so on. NPCI is not a statutory body and has been set up as a not-for-profit. The payment systems operated by NPCI have many third-party participants, which are regulated by various notifications issued from time to time by the NPCI. The UPI is a system that enables multiple bank accounts (of participating banks) to be accessed using a single mobile application, quick routing of funds and merchant payments.

Data localisation

Pursuant to its notification dated 6 April 2018, the Reserve Bank requires all system providers to store data (including end-to-end transaction details) in India relating to payment systems operated by them. For the foreign part of a transaction, the data may also be stored in the respective foreign country if required. Additionally, with respect to digital lending, the DL Directions mandate that REs must ensure that all the borrower and lending-related data is stored only in servers located within India, while ensuring compliance with statutory obligations/regulatory instructions. The DL Directions also state that in case the data is processed outside India, the same shall be deleted from servers outside India and brought back to India within 24 hours of processing.

Outsourcing

The Reserve Bank issued Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks on 3 November 2006. These restrict banks from outsourcing any 'core management functions' such as decision-making functions, including determining compliance with know your customer (KYC) norms. Similar guidelines have also been enabled for non-banking financial companies and payment system operators.

The Reserve Bank issued the Master Direction on Outsourcing of Information Technology Services on 10 April 2023 (the 'Master Directions on IT Outsourcing'), which came into effect on 1 October 2023. The Master Directions on IT Outsourcing were issued to ensure that the responsibility of REs (such as banks, credit information companies and non-banking financial companies) towards their customers does not diminish on account of engaging third-party service providers for information technology services, nor does it hinder effective supervision by the Reserve Bank. In pursuance of that, the Master Directions on IT Outsourcing impose extensive requirements on REs, including the necessity for a board-approved policy (including an exit strategy), the establishment of a risk management framework, a mechanism for handling complaints and legally binding agreements.

Credit information

The Credit Information Companies (Regulation) Act 2005 provides for regulation of credit information companies and defines the term 'credit information' to include, among other things, information relating to the amount and the nature of loans, amounts outstanding under credit cards and other credit facilities granted by a credit institution, and the creditworthiness of any borrower.

It further provides that only a duly registered 'credit information company' may, among other things, collect, process and disseminate information on trade, credit and financial standing of bank customers, and provide a credit score in respect thereof.

The Reserve Bank issued the Master Direction on Credit Information Reporting, 2025 on 6 January 2025. This consolidates existing guidelines under section 11 of the Credit Information Companies (Regulation) Act, 2005 and is designed to create a standardised system for reporting and sharing credit information, ensure the protection and confidentiality of sensitive credit data, and offer consumers ways to access their credit information and address grievances related to credit reporting by REs, including banks, financial institutions and non-banking financial companies (NBFCs).

Recurring mandates

The Reserve Bank issued a framework on the processing of e-mandates on cards for recurring transactions made through card transactions, prepaid instruments and UPI. A customer is required to register and process the first transaction using additional factor authentication. Thereafter, for recurring transactions above INR 15,000, card issuers are required to authenticate the transaction through additional factor authentication. On 12 December 2023, the Reserve Bank revised the threshold for which additional factor authentication is required, increasing the limit from INR 15,000 to INR 1,00,000 per transaction for certain categories of recurring payments such as mutual fund subscriptions, insurance premiums and credit card bill payments.

Storage of card data

The Reserve Bank required all entities in a payment chain, other than card networks and card issuers, to cease storage of card data and purge any previously stored data before 1 October 2022. Entities may store the last four digits of a card number and the card issuer's name for the limited purposes of transaction tracking and reconciliation.

The Reserve Bank has been encouraging cardholders to tokenise their cards to reduce incidents of fraudulent use and misuse of card data, and released a framework for card on file tokenisation services. The framework envisages the creation of unique codes, or 'tokens', which will replace card details. These tokens may be stored by merchants for future processing. The token creation process involves a one-time registration for each card, at each merchant's website, through additional factor authentication.

Anti-money laundering

The Prevention of Money Laundering Act, 2002 (PMLA) and the Prevention of Money-Laundering (Maintenance of Records) Rules 2005 require every banking company, financial institution (which includes the operator of a payment system) and intermediary to keep certain records and report certain questionable/suspicious transactions.

Notably, the High Court of Delhi in *PayPal Payments Pvt Ltd (PayPal) v Financial Intelligence Unit India & Anr* (WP (C) 138/2021]) has held that an online payment gateway service provider such as PayPal would be classified as a payment system operator under the PMLA. Therefore, PayPal would be mandated to adhere to the obligations falling upon a reporting entity under PMLA.

In March 2023, the Ministry of Finance notified and expanded the scope of the PMLA to include specific activities related to virtual digital assets (VDAs) under its purview. The definition of VDA is the same as in the Income-tax Act 1961. This definition is broad in nature and includes any information, code, number or token generated in digital form through cryptographic means, providing a digital representation of value exchanged with or without consideration that can be transferred, stored or traded electronically. This definition also includes non-fungible tokens (NFTs) in its ambit. The Ministry of Finance has notified that the following activities will be subject to the provisions of the PMLA:

- exchange between VDAs and fiat currencies;
- exchange between one or more forms of VDAs;
- transfer of VDAs;
- safekeeping or administration of VDAs or instruments enabling control over VDAs; and
- participation in and provision of financial services related to an issuer's offer and sale of a VDA.

Know your customer directions

The Master Direction – Know Your Customer Direction 2016 (the 'KYC Master Directions') issued by the Reserve Bank of India, imposes customer due diligence and KYC obligations on entities such as NBFCs, payment system providers and issuers of prepaid payment instruments. These include the obligation to frame KYC policies, types of data to be collected, retention periods and so on. Please see responses below for regulations governing payment systems, prepaid instruments (including wallets), open banking and crypto assets. The Reserve Bank amends the KYC Master Directions from time to time to review the extant instructions and implement necessary changes.

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

In 2018, the Reserve Bank had cautioned against dealing in virtual currencies due to the risks involved and the lack of regulation, and had restricted REs from dealing in or providing services in respect of virtual currencies.

In 2020, this notification was struck down by the Supreme Court of India in *Internet and Mobile Association of India v Reserve Bank of India* (2020) on the grounds of unreasonableness of restrictions imposed upon the exercise of freedom guaranteed under Article 19 (i)(g) of the Constitution of India. Subsequently, the Reserve Bank acknowledged that banks may process cryptocurrency-related transactions, subject to their customer due diligence procedures.

Since then, India has witnessed the introduction of some regulations that regulate cryptocurrencies and other crypto assets to a certain extent:

- amendments to taxation laws have been introduced, which, *inter alia*, tax any income from the transfer of VDAs at 30 per cent and which mandate a withholding tax of one per cent at the time of payment of consideration for the transfer of a VDA;
- the Advertising Standards Council of India, which is a voluntary, non-statutory council in advertising, has published guidelines on the advertisement of VDAs and linked services;
- the Ministry of Corporate Affairs has mandated all companies to include disclosures in their financial statements on virtual currency and cryptocurrency transactions undertaken by them in a financial year; and
- pursuant to a notification by the Ministry of Electronics and Information Technology, the Indian Computer Emergency Response Team specifically requires virtual asset service providers, virtual asset exchange providers and custodian wallet providers to keep all the information obtained as part of KYC and certain records of financial transactions for a period of five years.

In 2021, the Government of India announced the introduction of the Cryptocurrency and Regulation of Official Digital Currency Bill. The draft of this bill was not made publicly available and has not been tabled before the Parliament of India as yet. The Government of India announced that the bill would seek to prohibit all private cryptocurrencies, while creating a facilitative framework for the introduction of an official digital currency issued by the Reserve Bank and still allowing certain exemptions to promote the underlying technology and its uses.

The Government of India has also announced that the Reserve Bank would launch its own digital currency based on blockchain – the Central Bank Digital Currency – which would be exchangeable one-to-one with fiat currency (as described below).

Central Bank Digital Currency (CBDC)

The Reserve Bank proposes to introduce CBDC or the ‘digital rupee’ as a legal tender that coexists with and complements existing forms of money in a digital format. It envisages two

categories of CBDC: retail CBDC (CBDC-R) and wholesale CBDC (CBDC-W). CBDC-R is intended to be a general-purpose digital currency which would be available for use by private sector, non-financial consumers and businesses, while CBDC-W is intended to be made available only to financial institutions and intermediaries specifically for the purpose of inter-bank transfers and settlement of transactions. The Reserve Bank has launched pilots for both categories with selective banking entities.

Usage of CBDC is currently being pilot tested in the form of some studies in India. The pilot is being tried in the retail (public) and wholesale (bank and other institutions) segments. Per the FAQs issued by the Reserve Bank of India, the digital rupee can be held and transacted through digital rupee wallets offered by banks and non-banks for person-to-person payments or person-to-merchant transactions.

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

In India, payment services are primarily regulated by the Reserve Bank of India, pursuant to the Payment and Settlement Systems Act 2007 (the 'Act') and the regulations thereunder. Under the Act, a 'payment system' is defined as a 'system that enables payment to be effected between a payer and a beneficiary, involving clearing, payment or settlement service or all of them, but does not include a stock exchange'. All systems (except for stock exchanges and clearing corporations set up under stock exchanges) carrying out either clearing, settlement or payment operations (or all of them) are regarded as payment systems. Payment systems include systems enabling credit card operations, debit card operations, smart card operations, money transfer operations or similar operations. Any entity operating a payment system is a 'system provider'. An entity that wishes to begin to operate a payment system is required to be authorised to do so by the Reserve Bank.

In India, digital wallets are regulated as prepaid payment instruments (PPIs) by the Reserve Bank, pursuant to the Master Directions on Prepaid Payment Instruments 2021 (the 'PPI Directions'). PPIs are broadly categorised as follows.

- Closed system PPIs: These PPIs facilitate the purchase of goods and services from the entity issuing the PPI only. No cash withdrawals are allowed. These are not currently regulated or supervised by the Reserve Bank of India.
- Small PPIs: These PPIs require minimal details of the PPI holders to be set up and may only be used for the purchase of goods and services. Fund transfers and cash withdrawals for such PPIs are not allowed. Issuance of small PPIs requires authorisation from the Reserve Bank.
- Full KYC PPIs: These PPIs are issued after full KYC processes are conducted for the holder of the PPI and may be used for purchase of goods and services, fund transfers and cash withdrawals. Issuance of full KYC PPIs requires authorisation from the Reserve Bank.

In its Payments Vision 2025 statement, the Reserve Bank has stated that it proposes to revisit the framework on PPIs, including closed system PPIs. Additionally, on 27 December 2024, the Reserve Bank amended the PPI Directions to allow PPIs to be linked with UPI handles via third-party UPI applications, enabling PPI holders to make and receive UPI transactions via those applications.

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.

There have been several initiatives to facilitate and support the fintech ecosystem and startups in India, including regulatory sandboxes and innovation hubs. Regulatory sandboxes have been set up in financial, securities and insurance sectors by each of the respective regulators.

The Reserve Bank launched regulatory sandboxes in four cohorts:

- retail payments: tested products that engage feature phones and offline payments);
- cross-border payments: tested platforms facilitating purchase of assets listed on foreign exchanges, blockchain-based cross-border payment systems and so on;
- micro, small and medium-sized enterprises (MSME) lending; and
- the prevention and mitigation of financial fraud.

In 2025, the Reserve Bank announced that five entities were selected for the test phase of the regulatory sandbox's theme-neutral fifth cohort. The aforesaid entities offer services such as categorisation of risks in loan portfolios, digital opening of accounts for Non-Resident Indians (NRIs) through video KYC, MSME financing, unassisted video KYC and other services.

The Reserve Bank has also launched the Reserve Bank Innovation Hub to create an ecosystem that focuses on promoting access to financial services by identifying and mentoring startups. The hub has been set up through a wholly owned subsidiary of the Reserve Bank and its board comprises independent industry and academic experts. The Reserve Bank also set up a dedicated department to oversee and supervise the financial technology sector.

Furthermore, the Ministry of Electronics and Information Technology has announced the Digital India Startup Hub (DISH) initiative. This aims to enable startups around the country by facilitating fact time engagements between startups and government on a regular basis.

The government has launched a regulatory framework to establish international financial services centres (IFSCs) in India, under the purview of the International Financial Services Centres Authority (IFSCA). The IFSCA is a single regulator for the centre and is aimed at the development and regulation of financial products, financial services and financial institutions in the international financial centres in India. Currently, the Gujarat International Finance Tec-City (GIFT) is the only IFSC in India.

The IFSCA has launched a Framework for FinTech Entities in the IFSCs, which provides for a regulatory sandbox – ie, the IFSCA Fintech Regulatory Sandbox for fintech products and solutions (which would enable such players to avail grants under the IFSCA Fintech Incentive Scheme 2022) and the Interoperable Regulatory Sandbox, which tests fintech products and solutions that would typically fall within the regulatory purview of multiple financial sector regulators.

In September 2025, the IFSCA proposed to introduce an IFSCA FinTech Sandbox Framework. This framework will aim to facilitate the continued growth of fintech innovations at IFSCs in India and foreign jurisdictions by providing measures to facilitate innovation, such as regulatory/innovation sandboxes, spanning banking, capital markets, insurance, funds and so on, and technology-enabled fintech/techfin use cases pertaining to the financial products, financial services and financial institutions that are regulated or likely to be regulated in the IFSCs.

The Government of India has also approved an incentive scheme of INR 2,600 crore (approximately US\$360m) for promoting RuPay debit cards (a domestic card scheme developed by the NPCI) and low-value UPI transactions. It is expected to facilitate the construction of a robust digital payment ecosystem in India.

The Reserve Bank has launched the pilot project for Public Tech Platform for Frictionless Credit (ie, the Unified Lending Interface (ULI)), which would enable the delivery of frictionless credit by facilitating a seamless flow of required digital information to lenders and optimising the lending process, cutting operational costs, expediting disbursements and enabling scalability. The initial phase of the project prioritises products such as Kisan credit card loans, dairy loans, collateral-free loans for MSMEs, personal loans and home loans. The Reserve Bank has indicated that it intends to launch the ULI at the national level shortly.

In May 2024, the Reserve Bank issued the Framework for Self-Regulatory Organisation(s) in the FinTech Sector (the 'SRO Framework') to foster responsible innovation and enhance consumer protection amid the rapidly evolving fintech landscape. The SRO Framework empowers industry-led self-regulatory organisations (SROs) to establish and enforce regulatory standards, promote ethical conduct, ensure market integrity, resolve disputes, and foster transparency and accountability among their members. Pursuant to the issuance of the SRO Framework, the Reserve Bank has recognised the Fintech Association for Consumer Empowerment (FACE) as the first SRO in the fintech sector.

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

The primary regulation in India's open banking regime is the Master Direction – Non-Banking Financial Company – Account Aggregator (Reserve Bank) Directions 2016 (the 'Master Directions'), which were issued to regulate NBFCs undertaking the business of an account aggregator for a fee or otherwise.

Further, the Reserve Bank has also issued the technical specifications for all participants of the account aggregator ecosystem, which spells out the technical infrastructure requirements applicable to the actors in the Indian open banking regime and provides guidance on operational risk management and operational resilience.

The open banking framework in India is in its first stage and facilitates limited use cases. Under the Master Directions, account aggregators are allowed to only carry on the business of account aggregation. A registration process has been set out for an account aggregator. The Master Directions define the business of an account aggregator as the business of providing under a contract, retrieval or collection services in respect of such financial information pertaining to

its customers, as may be specified by the Reserve Bank from time to time; and consolidating, organising and presenting such information to the customer or any other user of financial information as may be specified by the Reserve Bank. Other than this, an account aggregator is not allowed to undertake any other business activity, including but not limited to supporting transactions by customers and storing financial information.

Account aggregators are envisaged to be data blind. Their limited role is to manage the consent artefact and act as a conduit for information sharing between financial information providers (FIPs) and financial information users (FIUs). Notably, the Securities and Exchange Board of India (SEBI) has joined the account aggregator framework in India for customers to share information about their mutual fund and stock holdings with financial service providers or FIUs. SEBI also requires FIPs engaged in the securities market to enter into a contractual framework with the account aggregators.

To date, only regulated FIPs and FIUs that are registered with financial sector regulators may have access to the account aggregator ecosystem. Account aggregators are required to collect the explicit consent of customers to retrieve, share and transfer their financial information. The consent is required to be collected in a standardised consent artefact.

The account aggregator framework in India was enabled on 2 September 2021. Based on information available in the public domain, there are around 16 licensed account aggregators that are currently operational.

Several banks and financial technology companies have also appeared on the network as FIPs and FIUs. A voluntary, self-organised and self-regulating body has been set up for the account aggregator ecosystem (the DigiSahamati Foundation).

6. Regulation of virtual asset service providers.

As discussed above, the Indian government has framed certain regulations to regulate virtual asset service providers (VASPs) or virtual digital asset service providers (VDASPs). The Central Government, in a notification dated 7 March 2023, brought VDAs and VDASPs within the PMLA regime (ie as 'reporting entities') so they must comply with PMLA record-keeping, KYC and suspicious transaction reporting obligations.

The government has notified the following VDA-related activities that require reporting for the purposes of PMLA:

- exchange between VDAs and fiat currencies;
- exchange between one or more forms of VDAs;
- transfer of VDAs;
- safekeeping or administration of VDAs or instruments enabling control over virtual digital assets; and
- participation in and provision of financial services related to an issuer's offer and sale of a VDA.

Further, the Financial Intelligence Unit of India (FIU-IND) under the Ministry of Finance has issued detailed AML/CFT Guidelines for reporting entities providing services related to VDAs (FIU-IND Guidelines). These guidelines set out the steps and measures that VDASPs are expected to follow to identify and curb money laundering, terrorist financing or proliferation financial activities.

VDASPs are required to register with FIU-IND and comply with PMLA obligations regardless of physical presence if they serve Indian customers. As of October 2025, 50 VDASPs have registered with FIU-IND. The registration process includes in-person verification and specified documentary requirements; non-registration has already led to penalties, site takedowns and notices to offshore exchanges. Under Indian law, there are no distinct categories of VASPs at present, nor is there a standalone dedicated enforcement authority pertaining to VDAs; however, FIU-IND regularly takes enforcement actions against VDASPs for non-compliance with the provisions of PMLA and FIU-IND Guidelines. Recently, in 2025, the FIU-IND imposed a monetary penalty exceeding INR 9,00,00,000 on a VDASP for violations of its obligations under the PMLA.

The FIU-IND also issued a circular regarding mandatory registration requirements for VDASPs on 4 July 2023 (the 'FIU-IND Circular'). Per the FIU-IND Circular, VASPs are required to submit specified documents with FIU-IND, such as:

- incorporation documents;
- director details;
- residential address proof;
- audited financial statements;
- details of technical infrastructure and system architecture; and
- internal policies and procedures for anti-money laundering (AML), counter-financing of terrorism (CFT) and KYC compliance.

Additionally, in-person verification of directors and officers of the VASP with the FIU-IND officials has been mandated, along with a requirement of live demonstration of AML/CFT systems.

Furthermore, on 15 September 2025, FIU-IND made cybersecurity audits from CERT-In empanelled auditors compulsory for all VDASPs to continue or register as reporting entities under PMLA.

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

India has adopted the Financial Action Task Force's Travel Rule by way of implementation of the FIU-IND Guidelines and by bringing business activities associated with VDAs under the PMLA. The FIU-IND guidelines require registration of VDASPs with FIU-IND as a reporting entity to ensure compliance with PMLA obligations such as customer due diligence, KYC, enhanced due diligence and suspicious transactions reporting. The FIU-IND Guidelines are binding on all VDASPs providing services or having operations in India, irrespective of whether it is an offshore or onshore entity.

Per the FIU-IND Guidelines, VDASPs must include required and accurate originator information, and required beneficiary information, on wire transfers and related messages. They must also monitor

wire transfers to detect those that lack the required originator and/or beneficiary information, and screen the transactions. Originating VDASPs must obtain and hold on to the accurate originator information and required beneficiary information on VDA transfers; submit this information to the beneficiary VDASP or financial institution immediately; and securely make such information available on request to the authorities. Beneficiary VDASPs are also required to obtain and hold the required information and make such information available upon request by the authorities.

FIU-IND has been granted powers under PMLA to issue enforcement actions against non-compliant VDASPs. As per the recent data shared by the Ministry of Finance, FIU-IND has issued notices for non-compliance to 25 VDASPs under section 13 of the PMLA. Additionally, the Director of FIU-IND exercising powers under section 79(3)(b) of the Information Technology Act, 2000, has also issued notices to certain VDASPs with respect to takedown of the application/URLs for public access that have been found to be operating illegally without complying with the relevant provisions of the PMLA in India.

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

In India, tokenised assets such as digital bonds, fractionalised real estate and DeFi instruments are generally structured through traditional legal vehicles such as special purpose vehicles (SPVs), trusts or regulated investment funds with the token serving as a digital representation of the underlying rights. This approach ensures compliance with securities and property laws (in the case of real estate assets tokenisation), which still require registration, stamp duty and other statutory formalities. Collateral in such transactions may typically include immovable property, receivables, SPV shares and contractual rights.

Moreover, lenders may also rely on conventional mechanisms like mortgages, pledges, charges and assignments backed by filings with the Registrar of Companies (RoC) and registrations with the Central Registry of Securitisation, Asset Reconstruction and Security Interests (CERSAI), alongside stamping and registration of mortgage deeds under state-specific laws.

A traditional security interest (like a mortgage or pledge) is effectively secured when the lender has a legal claim that is enforceable against third parties, usually by registering the charge, stamping documents or taking possession of collateral. However, for crypto or tokenised assets, the situation is different because these assets exist only digitally on a blockchain, and they do not have a physical form that can be physically handed over. Therefore, securing crypto or tokenised assets may also require custody or transfer of private keys, usually to a custodian or escrow agent.

Indian courts generally uphold foreign governing law clauses in contracts provided they do not contravene Indian public policy or other statutes. However, enforcement of such clauses within India requires compliance with local procedural and registration requirements. In the event of a default, secured lenders can enforce their security interests under the Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest (SARFAESI) Act, 2002. This Act empowers banks and financial institutions to recover non-performing assets without court intervention, allowing them to seize and auction properties pledged as security, with the exception of agricultural land. The enforcement process includes issuing a sale notice, taking possession of the secured asset and conducting a public auction.

While the SARFAESI Act facilitates the enforcement of security interests, it does not permit lenders to directly appropriate collateral without following the prescribed legal procedures. However, the SARFAESI Act cannot be directly enforced against digital tokenised assets due to the lack of a statutory framework to recognise control of private keys or on-chain ownership as possession. The SARFAESI Act's enforcement procedures, which include demand notice, taking possession and public auction, are designed for assets with a legal identity under Indian law (such as registered immovable property, shares and receivables). Therefore, lenders can still take collateral of tokenised assets, but enforcement would have to rely on contractual remedies under the loan/security agreement (eg, transfer of private keys from borrower to lender or escrow) and civil court remedies to enforce the contractual rights, rather than SARFAESI Act's procedures.

As an aside, the IFSCA released a consultation paper titled *Regulatory Approach Towards Tokenisation of Real-World Assets* on 26 February 2025 (the 'Consultation Paper'). The primary objective of the Consultation Paper is to highlight the approach and suitable measures to be adopted for the regulation of tokenisation of certain real-world assets, including but not limited to stocks, funds, commodities and commercial real estate. Via the Consultation Paper, the IFSCA intends to put forth the regulatory hurdles and challenges identified by it to identify proportional, reasoned and acceptable means of tackling these challenges.

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

Under Indian law, parties are generally free to choose a foreign governing law and jurisdiction for their contractual arrangements, including those relating to crypto assets. Indian courts will ordinarily uphold such clauses, provided the choice is bona fide, legal and not contrary to public policy. Exclusive jurisdiction clauses are enforceable so long as at least one Indian court would otherwise have jurisdiction under the Code of Civil Procedure, 1908 (CPC), and the contract clearly excludes all other forums. Indian courts have also upheld a view that enables the parties to a contract in international trade to mutually agree to confer jurisdiction upon a forum for the resolution of their disputes, which may be in the country of either party to the agreement or a 'neutral' jurisdiction not connected to any of the parties or the transaction.

Enforcement of foreign judgments and arbitral awards in crypto-related disputes may be subject to additional scrutiny since it remains a sensitive and partially regulated industry in India. While judgments from reciprocating territories under the Civil Procedure Code or arbitral awards under the New York Convention are generally enforceable, they may be denied recognition if, in the view of a court of law, they are contrary to India's public policy. Given that crypto assets are not recognised as legal tender in India, and are regulated as VDAs under tax and AML frameworks, Indian courts may refuse to enforce foreign rulings that conflict with domestic law or regulatory restrictions.

Thus, while foreign jurisdiction clauses are respected in principle, their effectiveness in crypto disputes is yet to be tested against India's evolving legal and policy stance on digital assets.

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

In India, innovations and inventions, including those linked to crypto assets, are protected under the existing IP framework, which includes patents for technical inventions, copyright for software and creative works, trademarks for branding and design protection for user interfaces. Ownership generally vests with the creator, unless assigned by contract, and enforcement is achieved through civil remedies such as injunctions and damages and criminal penalties for infringement. However, protecting IP in the context of cryptocurrencies is challenging due to the uncertain ownership of these assets. For example, trademark law is designed to allow the trademark holder exclusive use of their mark for their products and to prevent its unauthorised use. However, applying this to cryptocurrencies is not straightforward, as the identities of blockchain creators are often unknown, and the technology relies on anonymous, interference-free transactions. Additionally, transfer of a crypto token, such as an NFT, does not by itself transfer underlying IP rights, unless expressly provided for in the agreement.

Given the territorial nature of IP rights, protection in foreign jurisdictions must be sought separately, typically guided by the relevance of the market, risk of infringement, and availability of streamlined filing systems like the Patent Cooperation Treaty for patents and Madrid Protocol for trademarks. In India, IP rights over crypto-linked assets may be monetised through licensing, assignments, royalties or NFTs, with no direct legal prohibition. However, monetisation remains subject to tax and other applicable laws, such as the PMLA, since crypto assets are not recognised as legal tender. Thus, creators and businesses who intend to commercially exploit their innovations must do so while navigating compliance with India's broader financial regulations, including those set out above.



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