

Bahrain

Fatima Alali

Hassan Radhi & Associates, Bahrain

fatima.alali@hassanradhi.com

Saifuddin Mahmood

Hassan Radhi & Associates, Bahrain

saifuddin.mahmood@hassanradhi.com

Amna Aljanahi

Hassan Radhi & Associates, Bahrain

amna.aljanahi@hassanradhi.com

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

Financial technology (fintech) activities in the Kingdom of Bahrain can be traced back to an early stage predating its rising widespread popularity in the region, which positions Bahrain as a pioneer in this field. This sophisticated landscape is rooted in a proactive regulatory framework implemented by the Central Bank of Bahrain (CBB) under Decree No (64) of 2006 promulgating the Central Bank of Bahrain and Financial Institutions Law (the 'CBB Law'), together with the CBB rulebooks that are divided into volumes and then into modules categorised by sector and activity. Such framework facilitates creating a solid infrastructure for innovation, financial stability, and security.

The CBB established its Regulatory Sandbox in June 2017, based on finalised consultations that were issued as a final document on 28 May 2017. It forms a cornerstone of Bahrain's fintech landscape, offering a dynamic environment for innovative financial activities while ensuring robust security standards and consumer protection. While not contained in a standalone module, the Regulatory Sandbox operates under the CBB's supervisory mandate and is administered by the Fintech and Innovation Unit, aiming to provide fintech firms – and especially startups – with the necessary foundation to kickstart their business. The Regulatory Sandbox allows such firms and startups to test-drive their innovative solutions and services under a controlled and regulated setting for a period of nine months, with possible extension on a case-by-case basis. This Sandbox provides a balance between the risk-based nature of fintech activities, that span from digital banking operations to digital financial advice, and the appropriate regulatory oversight that ensures overall viability and success in this sector.

Participation in the Sandbox is subject to specific eligibility criteria set out by the Fintech and Innovation Unit of the CBB, which are as follows:

- *Innovation*: The service must be truly innovative, address a market gap or be sufficiently different from existing offerings, or offer a new use for existing technologies within financial services (as evidenced by market research and a comparison of the key features of the Applicant's technology or operating methodology against competitors);
- *Customer benefit*: The service must offer identifiable direct or indirect benefits to customers (eg, based on customer research showing improved security, customer experience, efficiency, quality of product, lower prices, or a combination of any of the above). These must be supported by quantifiable estimations or demonstrations, where possible;
- *Identification of major risks*: The applicant must identify the major risks associated with the solution or service, as well as the measures to mitigate these, including business continuity and disaster recovery;
- *Compliance with CDD and AML/CFT requirements*: The applicant must be able to comply with the customer due diligence (CDD) and anti-money laundering/counter-financing of terrorism (AML/CFT) requirements set out in the CBB Rulebook; and
- *Confidentiality requirements*: The applicant must be able to maintain the confidentiality of customer information in accordance with the CBB Law and other applicable laws.

Through these requirements, the CBB ensures that innovation is encouraged while maintaining financial stability, regulatory integrity, and consumer protection.

In that same year, the CBB launched crowdfunding regulations under the Crowdfunding Platform Operators (CFP) module, which can be found under CBB Rulebook – Volume 5: Type 7 – Ancillary Service Providers, that aim mainly to provide financing to startups and small and medium-sized enterprises (SMEs), encompassing both equity and debt crowdfunding platforms.

A year later, in 2018, the CBB laid down the standards for robo-advisory services by issuing guidelines for digital financial advice and robo-advisory, mainly governed under CBB Rulebook Volume 4 – Investment Business, specifically the Digital Financial Advice (DA) module which includes operational, technical and regulatory requirements.

In 2019, the CBB issued two more modules covering the most important and evolving types of fintech activities, which are open banking and crypto assets.

Open banking regulations have facilitated innovation and competition within this evolving sector, by way of mandating CBB licensees to enable third-party providers to have access to customers' financial data. Additionally, crypto asset regulations were introduced within Volume 6 (Capital Markets), where it details its regulatory framework encompassing all aspects of such evolving fintech service including licensing, prudential standards, business conduct rules, and AML/CTF measures in crypto-related services and activities.

The most recent module, issued in July 2025, was that of Stablecoin Issuance and Offering issued under Volume 6 (Capital Markets). This module aims to regulate the issuance and offering of stablecoins both in and from Bahrain, and to ensure compliance with the types of stablecoins that can be issued, and the requirements pertaining to the issuer's eligibility and obligations.

With the fast-paced development of fintech activities in general, the CBB have considered this dynamism and have regulated different types of fintech businesses in its rulebook. It continues to launch and update regulations that offer a stable and secure infrastructure while keeping up with international trends – ultimately serving as a breeding ground for promoting investment in the fintech sector.

To the best of our knowledge, the CBB has not formally announced specific upcoming reforms or consultation papers. However, given its established practice of incremental regulatory development and periodic updates to its rulebooks, further refinements to the fintech framework remain likely. The CBB's policy trajectory reflects an ongoing commitment to maintaining an innovation-supportive financial ecosystem.

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

The regulatory framework for crypto assets in the Kingdom of Bahrain is primarily established under the CBB Rulebook, Volume 6 – Capital Markets, specifically the Crypto-Asset (CRA) module, recently updated in July 2025. The CRA module is also supplemented by directives and supervisory guidance issued by the CBB, including the Guidance Paper on Virtual Assets, issued in November 2020 (VA Guidance Paper). Together, these instruments create a comprehensive regime governing the licensing, conduct, risk management and oversight of crypto asset

activities undertaken within or from Bahrain, while focusing on minimising any risks of financial crime and illegal use of crypto assets.

The CRA module defines crypto assets as: ‘a cryptographically secured digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology but does not include central bank issued digital currencies’. Thus, crypto assets are treated as regulated financial instruments for the purposes of capital markets regulation, and it also distinguishes between crypto assets which are regulated under provisions CRA-1 to CRA-14, and digital tokens, which, when issued in accordance with provision CRA-15, are expressly classified as securities.

The CRA module explicitly applies to activities such as trading, custody, portfolio management, advisory services, and operating crypto asset exchanges in or from Bahrain. It also expressly excluded a set of activities that do not constitute regulated crypto asset services such as the creation of crypto assets, the development, dissemination or use of software for the purpose of creating or mining a crypto asset (which are subject to copyright law as will be explored in Section 10), loyalty programmes, and any other activity deemed by the CBB to not constitute a regulated crypto asset service.

The CBB offers four categories of licences, depending on the type of regulated crypto asset service, and subjects each licensee of the four categories to specific obligations based on the category of licence they have obtained. These categories are as follows:

- *Category 1:* Licensees under this category may undertake either reception and transmission of orders, or provision of investment advice in relation to crypto assets, or both services;
- *Category 2:* Licensees may undertake trading in crypto assets as agents, portfolio management, crypto asset custody, and investment advice;
- *Category 3:* Licensees may undertake all activities denominated for Category 2 as well as trading in crypto assets as principal and act as a digital token advisor; and
- *Category 4:* Licensees may operate a licensed crypto asset exchange, custody service, and may act as a digital token advisor. Additionally, Category 4 licensees may hold or control client assets and money.

As for the legal status of each licensee, the CRA module specifies that holders of Category 1, Category 2 and Category 3 licenses must be incorporated as either a Bahraini With Limited Liability company (WLL), or as a Bahraini Joint Stock Company (BSC). Holders of a Category 4 license must be incorporated as a BSC.

The CRA module also covers other licensing conditions, such as: (1) the requirement of having the place of business and the residence of persons occupying oversight and governance functions, such as board members and persons in executive positions, to be designated in Bahrain; and (2) other requirements pertaining to the general conduct, auditing, system and adequate capital maintenance within the business, as well as technology governance and cybersecurity.

Additionally, investor protection relating to crypto asset services and transactions is one of the core pillars of the CRA module. For example, pursuant to the Governance Requirements provided for in

the CRA module, paragraph CRA-15.2.5 sets forth the board's responsibilities that include treating investors fairly. The CRA module also places several obligations on licensees that aim to provide the utmost safe and practical environment for investors.

Under the CRA module, licensees are obliged to separate client money and assets in designated bank accounts under an escrow agreement. It also requires them to conduct comprehensive suitability assessments before offering advisory services, portfolio management or complex crypto products, as well as complying with mandatory risk disclosure obligations in both Arabic and English, covering a wide range of items from unauthorised transaction liability, to stop payments rights, and cybersecurity, especially with regards to the volatile nature of crypto assets in general. Other obligations are also placed on licensees pertaining to transaction confirmations, and withdrawal rights for clients and investors.

Therefore, we can deduct from the above that under the CBB's regulatory framework, crypto assets are not regulated in and of themselves; rather, the CRA module applies to such assets when they are dealt with through regulated activities. This agile regulatory approach allows for flexibility that coincides with the nature of and the evolving pace of crypto assets under a controlled environment.

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

Bahrain has undergone major developments in the fintech sector due to the adoption and implementation of payment services that enables payment of bills and contactless payments without the need for payments in cash. This led people and establishments alike to conduct completely cashless transactions, which are one tap away from people's smart devices.

These secure and rapid cashless transactions are primarily backed by solid and innovative payment service providers (PSPs) that include both bank and non-bank entities and are regulated under the CBB's relevant regulations and resolutions, namely, Volume 5 of the CBB rulebook, specifically governed by Type 7 of the Specific Modules, which pertains to ancillary service providers (ASPs) and provides for distinct standalone categories based on each service such that it regulates other providers, alongside PSPs, such as third-party administrators, credit reference bureaus, Sharia advisory services, crowdfunding platform operators, account information service providers, and payment initiation service providers.

Digital wallets are also governed by the ASP module. This regulatory framework can be traced to the Electronic Transactions Law of 2002 that set the cornerstone for digital payments long before the inauguration of the ASP module by the CBB. This goes to show Bahrain's consistent efforts to pioneer the fintech industry.

PSPs are mainly governed by the ASP module that sets out the CBB's approach to licensing entities and persons providing regulated ancillary services in Bahrain, and the CBB's requirements for approving said persons undertaking key functions in those providers. ASPs are subject to eight licensing conditions that are in line with international good practice. These conditions prevent any person from providing, or seeking to provide, regulated ancillary services within or from Bahrain unless they have been licensed as an ASP by the CBB.

The ASP module defines regulated ancillary services as: 'any of the following activities, carried on by way of business:

- permitted services undertaken by third-party administrators (TPAs);
- card processing;
- services undertaken by Credit reference bureaux;
- permitted payment services provided by payment service providers (PSPs);
- Sharia advisory/ review services;
- permitted activities of a crowdfunding platform operator;
- providing account information services;
- providing payment initiation services; and
- any other ancillary services that are related to the financial services industry'.

It also provides a general definition of PSPs and states that: 'Payment service providers, may act as an intermediary for the following services:

- services enabling cash to be placed in clients' money account and all of the operations required for operating the account;
- services enabling cash withdrawals from clients' money account and all of the operations required for operating the account;
- the settlement of the direct debits of payment transactions;
- integrating customer delivery channels to enterprises to enable transactions at delivery channels (eg, ATMs, POS, Interactive Voice Response, mobile, internet); and
- interfacing with external networks/ institutions (eg, national switch, VISA, MasterCard), enabling automated exchange of transactions between enterprises and external networks.'

The ASP module goes as far as regulating PSPs that are undertaking regulated activities in accordance with Sharia and subjected such ASPs to comply with the standards issued by the Accounting and Auditing Organisation for Islamic Financial Institutions (AAOIFI) in all their transactions and contracts, thereby institutionalising Sharia compliance within the formal supervisory framework, such that Sharia standards and principles do not operate as a parallel informal system, but rather as a legally integrated component of Bahrain's regulatory landscape. This stands as a testament to the comprehensive nature of the CBB's regulatory framework governing PSPs.

Today, everyday transactions in Bahrain are made through one of the prominent and pioneering PSPs in the region: BenefitPay, which connects users' mobile numbers with their bank account details and KYC information. This led to most people going cashless in their everyday transactions: from paying for fuel to paying loan payments, BenefitPay proves how transformative the supportive legal and regulatory landscape has been for PSPs in Bahrain.

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.

Bahrain provides extensive special support for the fintech ecosystem, particularly fintech startups, through regulator-led programmes and dedicated innovation initiatives overseen by the CBB.

A cornerstone of this support is the CBB Regulatory Sandbox, launched in June 2017. The Regulatory Sandbox allows fintech startups, technology firms and licensed financial institutions to test innovative financial products, services and business models in a controlled regulatory environment for an initial period of up to nine months, with the possibility of extension. This programme is expressly designed to lower market-entry barriers, enable regulatory engagement at an early stage, and support innovation while maintaining consumer protection and financial stability.

In parallel, the CBB has established a dedicated Fintech & Innovation Unit, which plays a central role in supervising the sandbox, developing fintech-specific regulations, such as the issuance of crowdfunding regulations for both conventional and Sharia-compliant services in 2022, and facilitating collaboration between fintech firms and incumbent financial institutions. This unit reflects the CBB's policy of being receptive to fintech innovation and adopting a 'same activity, same regulation' approach.

In addition, the CBB has launched FinHub973, the region's first cross-border digital innovation platform. FinHub973 connects fintech companies with banks and financial institutions under the CBB's oversight and provides a digital environment for collaboration, prototyping, testing and proof-of-concept development. The platform is operated in partnership with private-sector innovation providers and is directly supported by the regulator as part of Bahrain's broader fintech strategy.

Beyond regulatory tools, fintech startups in Bahrain benefit from government-backed ecosystem support, including funding, grants, and incentives offered through entities such as the Bahrain Economic Development Board (EDB) and Tamkeen, which support innovation, entrepreneurship and skills development, through various programmes and incentives. The EDB works on building Bahrain's investment infrastructure and setting a supporting ecosystem, by hosting events such as Fintech Forward, in order to facilitate the expansion of fintech startups. This is further supported by Tamkeen's role in financially enabling Bahraini startups and SMEs by providing grants, in addition to offering various educational programmes and initiatives to upskill Bahraini talent.

In summary, Bahrain offers one of the most developed fintech support frameworks in the region. Regulatory sandboxes, digital innovation platforms, and active regulator engagement are all directly supported and operated by the CBB, demonstrating a clear policy commitment to fostering fintech innovation and supporting fintech startups.

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

Open banking is expressly and comprehensively regulated in Bahrain through the CBB's Rulebook Volume 5 (Ancillary Service Providers), Open Banking (OB) module. The OB module establishes a

binding regulatory framework governing the provision of open banking services and has been in force since November 2018, with subsequent amendments, most recently in May 2024.

The OB module applies to ancillary service providers that provide either or both of the following regulated services: Account Information Services (AIS) and Payment Initiation Services (PIS).

These services involve obtaining customer-permitted access to accounts held with licensed banks, financing companies and payment service providers operating electronic wallets (referred to as 'licensees maintaining customer accounts') through application programming interfaces (APIs). The framework is structured around four core pillars.

- Scope of application and licensing perimeter.
- Risk management, systems, and controls.
- Operating rules and customer protection.
- Technology and API standards.

Entities providing AIS or PIS must be authorised by the CBB as ancillary service providers under Volume 5 of the Rulebook. Thus, the OB module must be read together with other binding modules within Volume 5, including Principles of Business, General Requirements, Authorisation, Financial Crime, and Enforcement. This ensures that open banking providers are fully embedded within Bahrain's broader financial regulatory framework.

Additionally, AISPs and PISPs are subject to extensive governance and operational requirements. Their boards and senior management must ensure effective internal controls covering, among other things:

- cybersecurity and information security;
- API testing and penetration testing;
- fraud prevention;
- AML/CFT controls;
- record-keeping and audit trails; and
- business continuity and disaster recovery planning.

Independent security testing and external assessments are required on a recurring basis, including mandatory penetration testing of API security standards.

Additionally, customer consent is a cornerstone of Bahrain's open banking regime. AISPs and PISPs may only access customer accounts or initiate payments with explicit customer consent, which must be capable of being withdrawn. AISPs must allow customers to limit both the type of data accessed and the duration of consent (up to 12 months). The OB module also requires compliance with Bahrain's Personal Data Protection Law (PDPL), ensuring confidentiality, encryption and restricted use of customer data.

Therefore, in addition to the OB module itself, open banking providers are indirectly regulated through the Financial Crime module, Principles of Business module, Enforcement module, and the PDPL. Together, these instruments reinforce trust, security, and accountability in open banking activities.

In terms of operation, and to ensure customer protection within the open banking ecosystem, AISP and PISP must enter a framework contract with customers prior to the provision of any service. This contract must disclose, among other things:

- service characteristics and fees;
- consent mechanisms and withdrawal rights;
- liability allocation for unauthorised transactions;
- dispute resolution and complaints handling; and
- safeguards against fraud and cybersecurity incidents.

In conclusion, given the extensive amendment history of the OB module, open banking in Bahrain is an evolving regulatory regime that is rooted in structure, and striving towards stronger technology governance, alignment with evolving cybersecurity standards, and expansion of the overall open banking ecosystem using regulatory refinements rather than standalone laws.

6. Regulation of virtual asset service providers.

In Bahrain, crypto assets are not regulated in isolation of virtual asset service providers (VASPs), which are regulated as service providers, not as issuers or holders of crypto assets themselves as explored in Section 2. Therefore, the CBB adopts a functional, activity-based regulatory approach, whereby regulation is triggered when a person provides specified crypto asset services for or on behalf of others, rather than by the mere existence or ownership of crypto assets.

Similarly to the regulation of crypto assets, VASPs are regulated by the CRA module, as well as directives and supervisory guidance issued by the CBB, like the VA Guidance Paper, which defined VASPs as: 'any natural or legal person who is not covered elsewhere under the FATF Recommendation, and as a business, conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

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

Under the CRA module, VASPs must obtain a licence under one of the four categories explained in Section 2 above. During the application process, VASPs are encouraged to engage in meetings with the CBB's licensing directorate prior to filing their application to establish the type of licensing needed for the service provided. During this period, the CBB retains total discretion as to grant licences or refuse them to safeguard clients' interests.

Because of the distinct features of virtual and crypto assets that allow for rapid and easy cross-border transactions, crypto assets often foster and create opportunities for money launderers and terrorist financiers to finance their illicit activities. Thus, when applying for a licence, VASPs must provide detailed information about their business plans and must comply with extensive ongoing requirements that mainly include risk management, AML compliance, cybersecurity, technology governance, and reporting audits. Otherwise, all details mentioned in Section 2 apply to VASPs, since CBB guidance equates VASPs and crypto asset licensees.

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

Anti-money laundering in crypto assets is extensively regulated in Bahrain under Volume 6 of the CBB Rulebook, the Anti-Money Laundering and Combating of Financial Crime module (the AML module).

Provisions of the AML module serve as an enforceable regulatory framework imposing on VASPs' AML obligations and measures including requirements that function as a Travel Rule regime for accepted crypto asset transfers. Alongside the AML module, VASPs are also expected to follow the guidance illustrated in the CBB's guidance papers, such as the VA Guidance Paper that reinforced the same preventive measures provided for in the AML module when making transfers, specifically noting confidential transmission when sending a payment to another VASP.

The AML module expressly treats transfers and transactions of accepted crypto assets as functionally analogous to wire transfers, such that it requires capital market licensees, including crypto asset licensees, to comply with the provisions applicable to traditional wire transfers, including the implementation of adequate CDD measures as outlined in AML-1, and the implementation of policies to identify suspicious wallet addresses, non-transacting with such wallets, and the filing of a suspicious transaction report (STR) once it becomes aware of a suspicious wallet address.

Under the AML module, a capital market licensee's responsibility does not stop upon filing a STR. The entity must continue to monitor transactions and customer relationships, comply with the tipping-off prohibition, and cooperate with relevant authorities (including facilitating the stopping of the suspicious transaction).

Additionally, the AML module requires licensees to apply risk-based monitoring systems proportionate to the complexity of the business and the types of transactions; such systems must notably include limits for cash and non-cash transactions, including transactions in accepted crypto assets. The AML module obligates capital market licensees, including crypto asset licensees, to comply with the transfer rules set forth in AML-2A when a transaction involves an accepted crypto asset transfer.

Rule AML-2A requires capital market licensees, including crypto asset licensees, to comply with the transfer requirements whenever a transaction involves an accepted crypto asset transfer, which is

treated as functionally equivalent to a cross-border wire transfer. Accordingly, licensees acting as ordering, intermediary or beneficiary financial institutions must ensure that: required and accurate originator and beneficiary information accompanies the transfer; that such information is transmitted immediately and securely in the case of accepted crypto asset transfers; and that appropriate record-keeping, verification and risk-based controls are in place. Transfers lacking required information must be subject to scrutiny and may not be executed where the applicable requirements are not met.

As for the Travel Rule, the AML module did not expressly create such a rule directly. Rather, it introduced several provisions that implemented the core aspects of the Travel Rule, namely the rules that licensees must implement in outward transfers of accepted crypto assets that are made on behalf of customers where licensees are obliged to include the required originator and beneficiary information. Additionally, the information that must accompany all accepted crypto asset transfers includes, at minimum:

- originator name;
- originator account number (including crypto asset wallet where used);
- originator address or national ID number/customer ID/date and place of birth;
- beneficiary name; and
- beneficiary account number (including crypto asset wallet where used).

The CBB also permits operational flexibility, such that the required information does not need to be attached 'directly' to the crypto asset transfer itself and may be submitted 'directly or indirectly'. When undertaking an accepted crypto asset transfer, licensees must ensure the ordering financial institution transmits the required originator/beneficiary information immediately and securely, protecting the information from unauthorised disclosure and ensuring integrity and availability for recordkeeping and use by financial institutions.

The AML module requires licensees to treat all transfers of accepted crypto assets as cross-border transfers rather than domestic transfers. This means the Travel Rule-type information obligations are designed to apply irrespective of whether the parties are in Bahrain, and are framed to capture the cross-border risk profile of crypto transfers.

As for inward transfers, licensees must keep records for originator information received and scrutinise transfers that lack originator information. Should transfers lack such information, they must be deemed suspicious and escalated to the MLRO for possible STR filing.

In terms of responsibilities across the transfer chain, the AML module allocates different responsibilities to each player involved in the transfer, as follows:

- *Ordering financial institution*: must ensure required/accurate originator and beneficiary information, retain the information, and must not execute the transfer if it does not comply;
- *Intermediary financial institutions*: must ensure the originator/beneficiary information is retained with cross-border wire transfers and accepted crypto asset transfers and keep records, for at least five years, where technical limitations prevent information remaining with a related transfer; and

- *Beneficiary financial institution*: must identify transfers lacking required information and verify beneficiary identity if not previously verified.

Overall, the AML module ensures that all licensees adhere to and honour their obligations provided for in the module. Oversight and supervision of such applications sit with the CBB as the regulatory and supervisory authority under the AML legal framework.

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

The Bahrain tokenised assets market has been in rapid growth due to the increasing adoption of blockchain technology, growing interest in digital assets among investors, and regulatory support from the CBB.

Under CRA-15 of the CRA module, the classification of digital tokens as securities is subject to the CBB's discretion, whereby the CBB may qualify a token as a security after assessing its underlying economic purpose, structure, and characteristics. Digital tokens may either be considered as equity securities where they confer or represent ownership interest in the issuer or gives entitlement to share in the issuer's profit, or as bond or debt securities where they evidence the indebtedness of the digital token's issuer in respect of any money lent to the issuer by the digital token holder.

Thus, this characterisation by the CRA module supports the treatment of tokenholder rights as rights applied in familiar securities concepts while the relevant token is regulated through licensed crypto asset service providers. Additionally, CRA module regulates such service providers whether they operate within or from Bahrain, which is an express recognition of the cross-border operation of relevant digital tokens and crypto assets.

This regulatory framework for digital assets in general has attracted investors and startups in the region. Bahrain has introduced a licensing regime which provides a secure landscape for secured transactions. Recently in 2024, the first digital assets exchange was launched in Bahrain called ATME, which is built on a private blockchain network to facilitate the conversion of real-world assets, such as private equity and real estate, into digitally tradeable tokens, allowing smaller businesses to access capital-raising opportunities in a safe and regulated environment.

This evolving regulatory framework allows for the smooth operation of digital asset transactions, and the utmost safeguarding framework for investors alike. The CRA module requires that subscription money shall be received into a segregated client money account held in a fiduciary capacity and not commingled. It also states that funds must not be given as collateral to any third party or be subject to restrictions.

To the best of our knowledge, the CRA module is primarily a regulatory rulebook governing licensing, conduct and operational safeguards for digital tokens and crypto asset service providers. It does not set out a comprehensive regime for the creation and perfection of security interests over tokenised assets (eg, requirements for registration, notarisation, stamp duty and priority rules). Accordingly, secured transactions involving tokenised assets and crypto assets would typically be structured and enforced by reference to Bahrain's general civil/commercial and execution framework, depending on the legal character of the collateral and the enforcement pathway available.

With that said, Bahrain recently issued Law No (3) Promulgating the Secured Transactions Law (STL), which will come into force on the first day of the month following 12 months from the date of its publication in the official gazette on 29 January 2026.

The STL creates a system in which security rights are established upon movable assets in a dedicated electronic registry analogous to the procedure followed in immovable assets, and in alignment with good faith and commercial reasonableness. Additionally, the STL provides for a broad definition of such assets and collateral, defined as: ‘Movable property, whether tangible or intangible, present or future, over which a security right arises, including inventories and accounts receivable.’

Thus, we are of the view that secured transactions involving crypto assets may be structured upon the provisions provided for in the STL and detailed in the upcoming executive implementing regulations (which have not yet been issued). Until then, digital tokens transactions shall be governed by the general rules contained in the relevant civil, commercial and execution laws, including the CRA module, and courts shall apply such laws in cases of default and other disputes related to secured lenders and the recovery of their claims.

As for cross-border recognition, Bahrain’s conflict-of-laws framework permits parties to choose the governing law of their contractual relationship, provided that the chosen law does not violate public order in Bahrain. In default situations, enforcement generally proceeds through the execution framework, where compulsory execution against a debtor’s property is carried out by seizure and sale by public auction under the applicable execution procedures.

Overall, Bahrain has established an increasingly robust regulatory infrastructure for tokenised assets and crypto asset activities through the CRA module, with contractual party autonomy, subject to public order, and a defined execution process providing a basis for enforcement and cross-border structuring of digital asset transactions.

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

According to Legislative Decree No (12) of 1971 promulgating Civil and Commercial Procedures Law (CCPL), and the principles adopted by the Bahraini Court of Cassation, Bahrain’s approach regarding jurisdiction is driven by the principle that jurisdiction is connected to state sovereignty and is ultimately governed by Article (14) of the CCPL.

Under Bahraini law, submission to a foreign jurisdiction, including by way of an exclusive jurisdiction clause, is not prohibited, but it is not absolute in the sense that it automatically deprives Bahraini courts of jurisdiction if proceedings are nevertheless brought in Bahrain. Thus, Bahraini courts may still have jurisdiction to hear the dispute even where the contract contains an exclusive jurisdiction clause in favour of a different forum.

Particularly, Article (14) of CCPL provides that Bahraini courts have jurisdiction over claims against a non-Bahraini who has domicile or residence in Bahrain (with a narrow exception for foreign real estate disputes). Further, Article (15) extends jurisdiction in additional cases even where the defendant is not domiciled/resident in Bahrain, where the dispute relates to an asset in Bahrain, or an obligation arising, performed, or ought to be performed in Bahrain.

Therefore, it is our view that in crypto asset disputes – which frequently involve obligations performed in Bahrain, services provided from Bahrain, or assets/operations linked to Bahrain – a Bahrain court can still be a competent forum and claim jurisdiction notwithstanding an exclusive foreign jurisdiction clause. With that said, we are unable to report whether such disputes have arisen in the past because there are no reported disputes related to crypto assets.

Furthermore, jurisdiction of Bahraini courts is a matter of public policy: even where the parties agree to litigate abroad, Bahrain may still assert jurisdiction where one of the parties initiates an action before a different court, and the dispute has strong Bahraini connections, and/or local precautionary measures are sought.

In conclusion, submission to foreign jurisdictions and exclusive jurisdiction clauses are generally respected in Bahrain as a contractual matter and can support a jurisdictional plea. However, Bahraini courts are vested with jurisdiction if one of the parties submits the dispute before a competent Bahraini court and such dispute satisfies the conditions set forth in CCPL, regardless of the foreign jurisdiction clause agreed between the parties.

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

In Bahrain, IP rights relevant to digital/virtual assets (including crypto-adjacent software, token content, branding and underlying technical inventions) are protected through general IP laws rather than a crypto asset-specific IP regime. In other words, while Bahraini laws do not expressly regulate ‘virtual assets’ as an IP category, the IP embodied in or used by digital assets is protected under existing copyright, trademark and patent frameworks.

That said, we are of the view that, in practice, protection for software crypto projects and works is often primarily governed under copyright, trade secrets and branding rather than patents that are generally reserved for inventions that qualify as patentable technical solutions. Therefore, we will focus our response on showcasing the relevant protection under the copyright and trademark laws.

Legislative Decree No (22) of 2006 with respect to the Protection of Authors’ Rights and Attendants Rights Law (Copyright Law) protects any work of a literary, artistic or scientific nature so long as such work is innovative and is produced in a distinctive expression, including computer software and works fixed in a digital form, which encompass virtual assets. The Copyright Law provides protection upon creation without any formality or registration requirement, thus, vesting both intangible and financial rights onto the author without any requirements of formalities. Specifically, the financial rights of the author are exclusively provided for in Article (6) of the Copyright Law in respect of:

- reproduction of his work;
- translation of his work into another language, its adaptation, musical arrangement or reproducing it in another form;
- distribution to the general public of an original or copies of the work whether by sale or by any other disposal that transfers ownership;

- rental for commercial purposes of an original or copies of his work embodied in a phonorecord, cinematographic work or his work that is in the form of computer software;
- public performance of his work;
- presentation of the original or copies of his work to the public in any manner;
- broadcasting his work; and
- transmission of his work to the public.

As for works created under a contract, the author's financial rights will generally belong to the person – whether natural or juristic – for whose benefit the work was created, provided that there is no agreement to the contrary.

As for trademarks, Law No (6) of 2014 regarding the approval of the Trademarks Regulation of the Cooperation Council of the Arab States of the Gulf (GCC Trademarks Law) defined trademarks as:

'Anything with a distinctive form such as names, words, signatures, letters, symbols, figures, titles, seals, drawings, images, engravings, packaging, pictorial elements, shapes, colours or groups of colours or a mixture of them, any mark or group of marks if used or intended to be used either to distinguish goods, services of a facility or other facilities or to indicate the rendering of a service or the control of inspection of goods or services.

The sign of sound or smell could be considered a trademark.'

Therefore, brands for exchanges, token projects and fintech products are protected through the GCC Trademarks Law if they are registered in the relevant registry: protection and ownership thereof are dependent on registration, as opposed to protection and ownership under the Copyright Law (which is inferred upon mere creation). Upon registration of the trademark, protection shall be bestowed for ten years with the possibility of renewal in accordance with Article (20) of the GCC Trademarks Law; the owner of the trademark may transfer or mortgage the registered trademark. The owner may also license others to use the trademark. Additionally, rights are generally protected against third-party claims through precautionary measures against any infringement on either copyright or trademark.

Consequently, there is no pressing need to seek foreign protection of copyright-heavy assets, such as virtual assets, since Bahrain offers automatic copyright protection upon creation. However, foreign trademark filings are expected to be pursued to align with business expansion objectives.

In assessing whether protection should be sought in foreign jurisdictions, the primary consideration is the extent to which existing international frameworks already provide protection. Bahrain is a party to several key international conventions, including the Agreement on Trade-Related Intellectual Property Rights of 1994, the Berne Convention for the Protection of Literary and Artistic Works of 1886, and the WIPO Copyright Treaty of 1996. Accordingly, copyright protection for works originating in Bahrain will generally extend to other member states without the need for separate registration.

However, protection may still be sought in foreign jurisdictions where the state is not a member of the relevant international conventions, where stronger enforcement mechanisms are desirable, or where the rights holder has commercial operations, or expansion plans. In practice, this analysis most commonly affects trademark protection, as protection thereof is contingent on registration rather than automatic protection upon mere creation as explained above.

Overall, even though Bahraini IP laws do not provide for crypto-specific provisions and limits on monetisation and protection against third-party claims, the same shall be governed by the general rules contained in the relevant IP laws as shown above, subject to public order limitations and in compliance with any relevant provision under the CBB rulebook.



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