

South Africa

Bright Tibane

Bowmans, Johannesburg

bright.tibane@bowmanslaw.com

Kelle Gagne

Bowmans, Cape Town

kelle.gagne@bowmanslaw.com

Kirsten Paulo

Bowmans, Cape Town

kirsten.paulo@bowmanslaw.com

Kate Baretta

Bowmans, Cape Town

kate.beretta@bowmanslaw.com

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

There is currently no specific regulatory framework regulating fintech or financial innovation in South Africa. Notwithstanding, certain fintech products and services may fall within the scope and ambit of the traditional financial sector regulatory frameworks, as the frameworks are generally activities-based.

The most relevant laws applied to fintech products or service offerings (ie, the legislation that fintech products and services are tested against prior to their rollout) are as follows:

- the Financial Advisory and Intermediary Services Act, 2002 (FAIS), which regulates the provision of financial services (ie, investment advice and intermediary services) in relation to financial products such as crypto assets, including 'robo-advice' or automated investment advice;
- the Financial Markets Act, 2012 (FMA), which regulates capital/financial markets, particularly securities trading infrastructures and their participants;
- the National Credit Act, 2005, which regulates the provision of credit and lending activities, including peer-to-peer lending, crowd funding and buy now pay later platforms;
- the Banks Act, 1990 (the 'Banks Act'), which regulates banking business and deposit-taking related activities; the issuance of e-money/electronic money is considered to be regulated under the Banks Act;
- the National Payment Systems Act, 1998 (NPSA), which regulates the domestic payment system and role-players in the South African payment system, both banks and non-banks (such as payment aggregators and payment service providers/payment gateway providers); and
- The Exchange Control Regulations, 1961 (the 'Exchange Control Regulations') issued under the Currency and Exchanges Act, 1933, which regulate the cross-border flow of capital (including money) and institutions that facilitate the cross-border flow of capital.

In terms of new law foreseen in the near future on fintech and financial innovation, the enactment of the Conduct of Financial Institutions (CoFI) Bill is anticipated in 2026.

Once in effect, CoFI will materially change the regulatory regime currently applicable to financial institutions and parties seeking to carry out regulated financial services activities in or in relation to South Africa.

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

Legal nature of cryptocurrencies

On 19 October 2022, the Financial Sector Conduct Authority (FSCA) declared crypto assets as a 'financial product' under FAIS. Such declaration was made in terms of the 'Declaration of a Crypto Asset as a Financial Product under the Financial Advisory and Intermediary Services Act', published under General Notice 1350 of 2022 (the 'Crypto Asset Declaration').

The effect of the Crypto Asset Declaration is that any person seeking to provide 'financial services' (defined under FAIS as encompassing 'advice' and 'intermediary services') in respect of crypto assets needs to be licensed as a financial services provider (FSP) by the FSCA in terms of section 7(1)(a) of FAIS, or to be registered as a representative of an existing FSP, unless otherwise exempted from the licensing provisions of FAIS.

Exchange control considerations in terms of crypto assets

South Africa's exchange control framework, in terms of the Exchange Control Regulations and exchange control manuals and rules issued by the South African Reserve Bank (SARB) such as the Currency and Exchanges Manual for Authorised Dealers (the 'Authorised Dealers' Manual'), requires that cross-border transmissions of funds from South Africa be processed by an authorised dealer in foreign exchange (ie, a local commercial bank), or, in limited cases, by authorised dealers with limited authority (ADLAs) (ie, certain licensed non-bank entities).

The Authorised Dealers' Manual prescribes the categories of foreign exchange transactions that authorised dealers may approve on behalf of their clients without reference to the Financial Surveillance Department of the SARB ('FinSurv'). Any transaction that falls outside the permissions set out in the Authorised Dealers' Manual requires special approval from FinSurv.

In this regard, FinSurv has issued guidance that neither the Authorised Dealers' Manual nor the Currency and Exchanges Manual for ADLAs permits cross-border foreign exchange transfers for the explicit purpose of purchasing crypto assets, and that FinSurv is not empowered to approve transactions of this nature.

South African-resident corporates are not permitted to remit funds offshore to acquire crypto assets, and authorised dealers will not process such payments. By contrast, natural persons may make offshore transfers for crypto purchases within their personal offshore allowances (ie, the ZAR 1m single discretionary allowance and the ZAR 10m foreign capital allowance), although card-based crypto purchases are typically blocked and are subject to transaction limits.

Corporates do not have pre-approved foreign allowances and must support any cross-border payment with appropriate documentation; however, offshore transfers by corporates for crypto purchases remain prohibited. Corporates may hold crypto assets acquired domestically.

The High Court (Gauteng Division) recently delivered judgment in *The Standard Bank of South Africa v SARB and Others*, which considered whether cryptocurrencies constitute 'capital' for

purposes of Regulation 10(1)(c) of the Exchange Control Regulations. Regulation 10(1)(c) prohibits the export of capital or rights to capital without SARB's approval, and SARB has historically taken the view that this prohibition applies to crypto assets. The Court held that cryptocurrencies do not constitute 'capital' for these purposes. SARB has appealed the decision, meaning the judgment is suspended and SARB's current position remains in force. Should the High Court finding ultimately be upheld, cryptocurrencies may not be subject to exchange control restrictions and could be freely transferable out of South Africa.

Compliance with anti-money laundering requirements

The Financial Intelligence Centre Act, 2002 (FICA) is South Africa's chief anti-money laundering (AML) legislation, imposing the majority of its obligations on so-called 'accountable institutions', which have been designated as such in Schedule 1 to FICA.

As of 19 December 2022, FICA was amended to extend the list of accountable institutions to include crypto asset service providers.

Among other obligations, FICA requires an accountable institution to formally register with the Financial Intelligence Centre (FIC), a statutory body established under FICA for the purpose of overseeing compliance with FICA and establish a risk management and compliance programme (RMCP) compliant with section 42 of FICA and approved by the accountable institution's board of directors.

The regulatory dynamics of CBDCs

SARB is actively exploring the feasibility of a retail central bank digital currency (CBDC), often referred to as the 'digital rand' through a feasibility study ('CBDC Feasibility Study') announced on 25 May 2021. At the time of announcement, the study was expected to conclude in 2022; however, SARB has continued to conduct industry engagement and technical research beyond this period as part of its broader digital payments and innovation agenda. The objective of the CBDC Feasibility Study is to investigate if it would be feasible, appropriate and desirable for SARB to issue a CBDC to be used for retail purposes, complementary to cash in South Africa. The study is intended to highlight the different CBDC design options, and the potential policy and/or regulatory implications associated with these options. SARB has made it clear that the CBDC Feasibility Study, regardless of its outcomes, does not imply that SARB will issue a rand-based CBDC.

As part of the CBDC Feasibility Study, SARB has also identified broader risks and unintended consequences that would need to be managed, including:

- lack of adoption, buy-in and trust from consumers and businesses;
- operational risks associated with the creation, issuance, distribution, transactional usage and management of a CBDC;
- reputational risk of an unsuccessful CBDC implementation for SARB, the payment system and South Africa;

- potential unintended displacement of financial system stakeholders from their roles as intermediaries in the ecosystem, which could impact financial system stability; and
- the risk of attacks from hackers and criminals.

In South Africa, crypto assets are privately issued and enable direct peer-to-peer transfers without reliance on the banking system. A retail CBDC, by contrast, would be issued by the SARB, be linked to the rand and therefore address the price volatility associated with privately issued crypto assets. A CBDC would carry sovereign backing and minimal counterparty risk, making it closer in nature to cash in digital form.

The SARB has indicated that a CBDC is not intended to replace or compete with existing payment instruments, including privately issued crypto assets. Rather, a CBDC would operate alongside them and could offer an alternative digital payment option with different characteristics.

Investor protection in relation to crypto asset transactions

Since South Africa has extended the FAIS licensing framework to crypto asset service providers (CASPs), these entities are required to comply with fit and proper requirements, disclosure obligations, complaints-handling standards and ongoing conduct supervision by the FSCA. This places crypto-related financial services within the established retail conduct regulatory regime and subjects CASPs to governance, competence and 'treating customers fairly' principles aligned with the broader financial services sector. Investors now have statutory protection and recourse to the FAIS Ombud against CASPs.

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

Payment service providers

In South Africa, payment service providers are regulated by NPSA. Non-bank payment service providers are specifically regulated by Directive 1 of 2007 (which regulates payment aggregators/non-bank acquirers) and Directive 2 of 2007 (which regulates system operators) issued by the SARB. Payment service providers are required to be authorised by the Payments Association of South Africa, as the body mandated by SARB to organise, manage and regulate the participation of its members in the national payment system.

The South African regulated payment system encompasses the entire payment process from payer to beneficiary and 'includes all the tools, systems, mechanisms, institutions, agreements, procedures, rules or laws applied or utilised to effect payment'.

Digital wallets

Digital wallets usually have the potential to be regulated either under the Banks Act or FAIS.

Some digital wallet services have the potential to qualify as '*the business of a bank*', as regulated by the Banks Act. The Banks Act defines 'the business of a bank' as:

- '(a) the acceptance of deposits from the general public (including persons in the employ of the person so accepting deposits) as a regular feature of the business in question;
- (b) the soliciting of or advertising for deposits;
- (c) the utilisation of money, or of the interest or other income earned on money, accepted by way of deposit as contemplated in paragraph (a)-
 - (i) for the granting by any person, acting as lender in such person's own name or through the medium of a trust or a nominee, of loans to other persons;
 - (ii) for investment by any person, acting as investor in such person's own name or through the medium of a trust or a nominee; or
 - (iii) for the financing, wholly or to any material extent, by any person of any other business activity conducted by such person in his or her own name or through the medium of a trust or a nominee;
- (d) the obtaining, as a regular feature of the business in question, of money through the sale of an asset, to any person other than a bank, subject to an agreement in terms of which the seller undertakes to purchase from the buyer at a future date the asset so sold or any other asset.'

The Banks Act defines a 'deposit' to mean an amount of money paid by one person to another person, subject to an agreement in terms of which:

- '(a) an equal amount or any part thereof will be conditionally or unconditionally repaid, either by the person to whom the money has been so paid or by any other person, with or without a premium, on demand or at specified or unspecified dates or in circumstances agreed to by or on behalf of the person making the payment and the person receiving it; and
- (b) no interest will be payable on the amount so paid or interest will be payable thereon at specified intervals or otherwise, notwithstanding that such payment is limited to a fixed amount or that a transferable or non-transferable certificate or other instrument providing for the repayment of such amount *mutatis mutandis* as contemplated in sub-paragraph a) or for the payment of interest on such amount *mutatis mutandis* as contemplated in this sub-paragraph b) is issued in respect of such amount.'

Some digital wallets have the potential to qualify as electronic money/e-money, which is provided for under a Position Paper published by SARB in November 2009, titled the *Position Paper on Electronic Money* (the 'E-Money Position Paper'). Only a registered South African bank is permitted to issue e-money. This requirement often means that fintech companies will need to partner with a bank in order to provide certain services within South Africa.

The E-Money Position Paper defines e-money as:

‘... monetary value represented by a claim on the issuer. This money is stored electronically and issued on receipt of funds, is generally accepted as a means of payment by persons other than the issuer and is redeemable for physical cash or a deposit into a bank account on demand.’

In order for any business activity or representation of value to qualify as e-money for purposes of the E-Money Position Paper, *all* aspects/elements of the definition of e-money must be present or apply. As such, depending on their structure, digital wallets may meet the definition of e-money.

There is currently no e-money licensing framework in South Africa. According to the E-Money Position Paper, SARB currently allows only South African registered banks to issue e-money. The E-Money Position Paper does, however, refer to section 52 of the Banks Act, which allows for non-banks to enter into arrangements with banks, which arrangements may permit them to offer banking-related services in conjunction with registered banks. As such, if a digital wallet constitutes e-money, the issuer is able to rely on section 52 of the Banks Act and have a formal alliance with a licensed bank for purposes of issuing e-money.

Digital wallet services could also constitute financial services regulated by FAIS.

On 3 March 2025, SARB published a draft directive titled ‘Directive in respect of specific payment activities within the national payment system’. The draft Directive prescribes, inter alia, authorisation requirements for, inter alia, payment activities that are currently unregulated (including provision of payment account or store of value, as well as wallet services). The Draft Directive was driven by SARB’s support for innovation and financial inclusion warranting the need to allow non-banks to fully participate in South Africa’s national payment system by introducing an activity-based regulatory framework. In light of this, the Draft Directive was accompanied by a draft exemption notice exempting certain payment activities that qualify as the business of a bank from the Banks Act. The draft Directive was available for public comment until 16 April 2025.

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.

In 2016, the Intergovernmental FinTech Working Group (IFWG) was established (comprising members from SARB, National Treasury, FSCA, FIC and the South African Revenue Services), with the purpose of developing a common understanding among regulators and policymakers of financial technology developments, and policy and regulatory implications for the financial sector and economy.

In August 2017, SARB established a dedicated fintech unit (SARB FinTech Unit) to assess and manage the impact of fintech innovations on the financial system. The unit focuses on:

- crypto assets;
- CBDCs;
- open finance initiatives;

- financial-market tokenisation; and
- artificial intelligence in financial services.

In 2018, the Crypto Assets Regulatory Working Group (CARWG) was formed under the IFWG to consider the regulatory treatment of crypto assets.

In April 2020, the IFWG established the Innovation Hub, including:

- the IFWG Regulatory Sandbox, allowing testing of innovative fintech solutions in a controlled environment; and
- the IFWG Innovation Accelerator, providing a collaborative space for regulators to explore emerging technologies with industry participants.

In April 2020, the IFWG issued a Policy Position Paper on crypto assets ('Crypto Asset Policy Position Paper') that aimed to provide recommendations for the development of a regulatory framework for crypto assets. The Crypto Asset Policy Position Paper recommended that Schedule 1 of FICA be amended to include CASPs to the list of accountable institutions (which took place and was effective as of 19 December 2022).

In November 2020, the FSCA published a draft Declaration proposing that crypto assets be included as a 'financial product' under section 1 of the FAIS Act. In June 2021, the IFWG, through the CARWG, published a Position Paper on crypto assets. Essentially, the Position Paper provides a roadmap for putting in place a phased and structured framework for regulating crypto assets. This approach was subsequently finalised on 19 October 2022, when the FSCA declared crypto assets a 'financial product' under FAIS in terms of the Crypto Asset Declaration.

In its 2025–2028 Regulatory Strategy (the 'Regulatory Strategy'), the FSCA set out what its fintech department is set to focus on in the upcoming period, which includes:

- providing regulatory guidance for market participants and generating data and insights for policy development through the IFWG's Regulatory Guidance Unit;
- providing a live and 'safe' regulatory testing environment for new market participants and innovative solutions through the IFWG's Regulatory Sandbox;
- driving both internally orientated and market-facing innovation with the potential to deliver benefits across the regulatory and broader financial services through the IFWG Innovation Accelerator; and
- researching, monitoring and assessing technological trends and innovations to understand their external impact on financial sector business models, products, and solution design and customer outcomes, in order to inform agile and appropriate regulatory and supervisory response to technological innovations.

In its Regulatory Strategy, the FSCA has said that priority fintech focus areas include open finance, artificial intelligence, digital assets (especially stable coins and tokenisation) and blockchain.

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

The sharing of consumer financial data, including any personal information by any service provider and participating bank, is currently subject to the Protection of Personal Information Act, 2013, which regulates the processing of personal information, provides for the rights of data subjects, and prescribes the obligations of data controllers and data processors.

In November 2020, SARB issued a consultation paper on open banking activities in the national payment system, which makes various policy proposals regarding open banking, including:

- a new class of third-party providers being introduced, and access to customers' financial information being promoted so as to improve product and service offerings for customers;
- such third-party providers being regulated by SARB and FSCA;
- banks providing access to customers' financial information, subject to customer consent, to such third-party providers;
- technical standards for open banking being developed and implemented; and
- consumer education or awareness being conducted.

In 2023, FSCA issued the Draft Position Paper on Open Finance and in March 2024, the FSCA published the *Open Finance – FSCA Policy Recommendations 2024 report* (the 'Open Finance Policy') that outlined FSCA's policy approach regarding open finance. FSCA is in support of mandating open finance in the future. FSCA recommended the following in the Open Finance Policy:

- Participants in open finance should be regulated, and a mandatory approach implemented.
- Participants in open finance should be licensed and regulated.
- A suitable data protection and consent framework must be put in place.
- Appropriate risk management and disclosure frameworks must be developed.
- Data protection and sharing standards must be developed.
- Consumers must have access to information and recourse mechanisms.
- An Advisory Group for open finance, comprising industry participants and other experts, should be established.

In addition to these open finance policy developments, certain regulatory measures have already been introduced that touch on open banking-type activity. In particular, Directive 2 of 2024 ('Directive 2'), issued under the NPSA and applying with effect from 15 February 2025, regulates third-party providers issuing payment instructions on behalf of payers using screen-scraping or similar tools in the South African national payment system. Although not, in itself, an open banking framework, Directive 2 represents a step in formalising and regulating third-party access models.

Under Directive 2, no person may issue exchange-traded fund (ETF) credit payment instructions on behalf of a payer unless they:

- are registered with SARB in the prescribed manner and form; and
- have obtained the informed consent of the payer before issuing or initiating the payment; or
- have been exempted from the registration requirement by SARB.

While Directive 2 does not constitute a comprehensive open banking regime, it demonstrates regulatory movement toward safe, regulated third-party access and data-sharing.

6. Regulation of virtual asset service providers.

As noted above in the section on the legal nature of crypto assets, crypto assets have been declared a financial product under FAIS pursuant to the Crypto Asset Declaration. As a result, persons who furnish advice or render intermediary services in relation to crypto assets are required to be authorised as FSPs under FAIS or operate as a representative of an authorised FSP, unless exempt. This captures a range of crypto asset activities, including trading platforms, exchanges, brokers and other intermediaries that facilitate crypto asset transactions on behalf of clients.

In addition, and as referenced earlier, CASPs have been included as accountable institutions under Schedule 1 of FICA. CASPs are therefore subject to the anti-money laundering, counter-terrorist financing and counter-proliferation financing (AML/CTF/CPF) framework applicable to accountable institutions, including obligations relating to customer due diligence (CDD), record-keeping, reporting and RMCPs.

South Africa has not adopted separate CASP licence classes or activity-based categories beyond the FAIS and FICA frameworks. Instead, CASPs are regulated through the existing financial sector licensing and supervisory structure, with conduct and market-intermediary functions supervised by the FSCA and AML/CTF/CPF compliance overseen by the FIC.

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

As noted above in the sections on the legal nature of crypto assets and regulation of CASPs, CASPs have been incorporated into the FICA framework as accountable institutions and are therefore required to comply with the full suite of FICA obligations.

In addition to those baseline obligations, South Africa has formally implemented the Travel Rule for crypto asset transfers. On 15 November 2025, the FIC issued Directive 9, which requires CASPs to comply with the Travel Rule with effect from 30 April 2025. In line with Financial Action Task Force (FATF) Recommendation 16, CASPs must obtain, retain and securely transmit prescribed originator and beneficiary information for crypto asset transfers, including full names, identification details (or wallet/account numbers), and distributed-ledger addresses where applicable. These requirements apply to both domestic and cross-border transfers and extend to ordering, intermediary and recipient CASPs.

Directive 9 also requires CASPs to:

- verify required information as part of CDD and integrate Travel Rule controls into their RMCPs;
- refuse to execute transfers where prescribed information cannot be collected or transmitted;
- take reasonable measures to detect missing information and determine appropriate follow-up actions;
- treat transfers involving unhosted wallets using a documented risk-based approach; and
- ensure secure, immediate (or simultaneous) transmission of data, with no *post facto* transmission permitted.

CASPs must therefore ensure that appropriate systems and controls are in place to collect, verify and securely transmit originator and beneficiary information in connection with crypto asset transfers, in addition to their existing obligations under FICA and their RMCPs.

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

Although South Africa regulates the provision of financial services in relation to crypto assets, there are no prescribed legal formalities for structuring or collateralisation involving crypto assets. If the collateral for such financial instruments is cash or securities, usual South African principles would apply. There are, on the other hand, no prescribed legal formalities for digital asset collateral. Therefore, only a South African common law cession in *securitatem debiti* (security cession) in the rights to the crypto assets would be available.

A security cession is concluded by agreement between the parties. It would be up to the parties to determine how the security giver is prevented from transferring or dealing in the collateral, as well as procedures for enforcement. Security granted by way of a security cession can be enforced without a prior judgment: that is, self-help is permitted and should be agreed to in the security cession.

South African courts will generally recognise and enforce a foreign governing law clause in a contract, including a crypto asset-related contract. However, in relation to security over property, South African law provides that the *lex situs* of an asset governs the proprietary law aspects pertaining to the asset. Therefore, a South African court would consider the location of the collateral in determining which law should govern security in the collateral. If the location of the collateral is a foreign jurisdiction, then the foreign governing law clause in relation to the security would be enforceable. There is no requirement for a public auction of collateral and, outside of insolvency, a secured lender can appropriate the collateral directly.

Under South African common law, however, a cedent of collateral would always be entitled to approach a court for relief if the cessionary acts in a manner that is unduly prejudicial to the cedent.

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

South African courts will generally seek to give effect to parties' expressly stated intention to submit to the jurisdiction of a foreign court. However, there is never a guarantee that a South African court will not assume jurisdiction over a dispute, even if the parties have agreed to a clearly worded exclusive foreign jurisdiction clause. South African courts have held that parties to a contract cannot 'oust' (ie, remove) the jurisdiction of South African courts by private agreement. Although an exclusive foreign jurisdiction clause will be treated as an important factor weighing in favour of a South African court refusing to exercise jurisdiction, the court retains discretion to assume jurisdiction if there are jurisdictional links connecting a South African court to the dispute.

By way of example, a court may decide to exercise jurisdiction in circumstances where a party to a contractual dispute: (1) is domiciled in South Africa; (2) agreed to the contract in South Africa (ie, the contract was partly concluded in South Africa); and/or (3) performed the contract partly or wholly in South Africa. If a breach of the contract occurs in South Africa, that could also be considered a jurisdictional link. There is no meaningful way of mitigating against the above possibility via the wording used in an exclusive jurisdiction clause. This is because the exercise of the court's discretion does not depend on the wording of the clause but rather on the underlying jurisdictional factors that might connect a South African court to the dispute.

If a South African court were to assume jurisdiction over a dispute concerning a contract containing an exclusive jurisdiction clause, it is worth noting that the court would generally seek to give effect to the governing law clause – that is, it would be unlikely to apply South African substantive law to the dispute if the contract clearly states that a foreign legal system should be applied. South African courts generally seek to honour the parties' choice of governing law, subject to limited exceptions, such as where the choice of a foreign law was aimed at avoiding a mandatory provision of applicable national law, or where there are other public policy reasons for not applying the foreign law.

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

Legal protection

South Africa offers a robust legal framework for protecting innovations, including those in the digital and crypto asset realm. There is no separate IP regime for crypto or virtual assets; instead, existing categories of IP law apply. Key forms of IP protection include the following.

Patents

The Patents Act 57 of 1978 protects inventions that are new, involve an inventive step and are capable of being used or applied in trade, industry or agriculture. While pure software and business methods are excluded from patentability as such, computer-implemented inventions that produce a technical effect beyond the software itself may qualify. This could, for example, include a

blockchain-based process. A granted patent gives the owner the exclusive right for the duration of the patent, to exclude all other persons in South Africa from making, using, exercising, disposing of or offering to dispose of, or importing the patented invention.

Copyright

The Copyright Act 98 of 1978 provides automatic protection for original works once they are reduced to material form. Copyright covers the expression of ideas (eg, software code, digital artwork or NFT imagery) rather than the underlying concepts. It grants owners exclusive rights to prohibit certain acts, particularly the unauthorised copying of the work by another.

Trademarks

The Trade Marks Act 194 of 1993 protects brand names, logos and other identifiers distinguishing the goods or services of one undertaking from those of another. Innovators in the crypto space often develop distinctive names for coins, tokens or platforms (eg, the name or logo of a crypto exchange) that can be registered as trademarks. Registration confers exclusive rights to use the mark in respect of the goods or services for which it is registered. Trademarks (whether registered or unregistered) are also protected under South African common law through the delict of passing off, which safeguards the goodwill and reputation associated with a mark that has acquired distinctiveness through use.

Designs

The Designs Act 195 of 1993 provides protection for the registration of aesthetic designs (features judged solely by the eye) and functional designs (features dictated by function). To be registrable, an aesthetic design must be new and original; a functional design must be new and not commonplace in the art. This could apply to, for example, the physical casing of a cold wallet device. A design registration gives the owner exclusive rights for the duration of the registration, to make, import, use or dispose of articles embodying that design.

Confidential information

South African law protects confidential information through the law of contract and the common-law delict of unlawful competition. Information qualifies as confidential if:

- it is secret and not generally known or readily accessible to persons who ordinarily deal with such information;
- it possesses commercial value; and
- the owner has taken reasonable steps to maintain its secrecy.

Such information may include trade secrets and know-how, for example, proprietary algorithms, financial models, business strategies, datasets or other fintech-specific operational information. Although the legal framework for protection is well established, enforcement can be challenging in practice, as claimants must prove both the existence of a duty of confidence and the unlawful use or disclosure of the information.

Ownership

Ownership of IP in South Africa generally follows the principle that the creator or inventor is the first owner unless otherwise agreed or prescribed by statute. Key ownership rules are as follows.

Employee creations

When an employee creates copyright, designs and, to some extent, inventions during the course and scope of employment (eg, software code developed by a company's engineers) the employer is the owner of such rights. Other forms of IP (such as trade secrets, know-how and, to some extent, inventions) must be assigned in writing to the employer in order for the employer to own such IP.

Independent contractors

Absent a written assignment, independent contractors retain ownership of the IP they create. Accordingly, contractual assignment is essential where companies commission software development or digital content. An exception to be noted in relation to copyright ownership of computer programs (ie, software) is that the author, and therefore the first owner, of a computer program is the person who exercised control over the making of the program. Statutory exceptions also exist for certain commissioned works (including photographs, portraits, gravures, sound recordings or where a design is created under an agreement); in such instances, ownership vests in the commissioning party unless otherwise agreed.

Assignments and transfers

IP rights are transferable assets, and ownership can therefore be assigned from one party to another. Assignments of registered rights should be in writing and recorded with the Companies and Intellectual Property Commission (CIPC) to ensure enforceability against third parties. To be effective, an assignment of copyright must be in writing and signed by the assignor in wet ink or by an 'advanced electronic signature' (as defined in the Electronic Communications and Transactions Act, No 25 of 2002).

Joint ownership

IP may be co-owned, for example, where multiple developers or contributors collaborate on a single innovation. In the absence of a written agreement, each co-owner's ability to exploit, license or assign the IP is restricted and generally requires the consent of the other co-owners.

Publicly funded IP

Where IP arises from publicly funded research and development, the Intellectual Property from Publicly Financed Research and Development Act 51 of 2008 (the 'IPR Act') applies. The IPR Act regulates ownership of such IP, mandates disclosure and protection by recipient institutions, and restricts assignments or exclusive licences without prior approval from the National Intellectual Property Management Office (NIPMO). This is particularly relevant in the context of emerging technologies and fintech innovations originating from academic or research collaborations.

Enforcement of IP rights

South Africa provides a comprehensive framework for enforcing and defending IP rights. Enforcement typically occurs through civil proceedings in the High Court, where rights holders may seek interdicts, damages or delivery-up of infringing materials. Interim interdicts are available in urgent cases to prevent ongoing infringement, and Anton Piller orders may be obtained to preserve evidence.

While traditional enforcement mechanisms were developed with tangible works in mind, they apply equally to digital and software-based creations. Copyright infringement provisions under the Copyright Act 98 of 1978 extend to computer programs, artistic works and other digital content. Accordingly, the unauthorised reproduction, distribution or commercial exploitation of software code, digital artwork or other protected material underlying a crypto asset may constitute an infringement enforceable through civil proceedings and, in defined cases, criminal prosecution.

Administrative procedures also exist: IP applications may be opposed or revoked before the CIPC or the relevant tribunal. Domain-name disputes can be resolved through alternative dispute resolution under the Electronic Communications and Transactions Act 25 of 2002.

Defences to third-party infringement or ownership claims are recognised under statute and common law. Examples include fair dealing for copyright works, prior or honest concurrent use for trademarks, and invalidity or lack of novelty for patents or designs. Parties may also rely on contractual or common law defences, such as consent or the existence of a valid licence.

Overall, the South African IP regime affords both rightsholders and third parties with effective judicial and administrative mechanisms to assert, protect and defend their IP rights.

Seeking protection in foreign jurisdictions

IP rights are territorial in nature, meaning that protection under South African law extends only within its borders. Innovators in the digital and crypto asset space must therefore consider both where to seek protection and how infringement may be addressed across jurisdictions.

Key considerations include:

- *Treaty membership*: South Africa is a member of the major international IP treaties, which facilitates foreign filings by allowing applicants to claim priority from local filings and pursue international protection through streamlined procedures.

- *Choice of jurisdictions:* Protection is usually sought in countries of intended commercialisation, manufacturing, or investment.
- *Cost-benefit analysis:* Filing and maintenance costs are substantial, so applicants typically prioritise key jurisdictions rather than seeking blanket coverage.
- *Cross-border infringement:* The Berne Convention for the Protection of Literary and Artistic Works applies to literary and artistic works, which includes computer programs, as they are classified as 'literary works' under its framework. The Berne Convention establishes the principles of national treatment, requiring each Member State to accord foreign works the same protection as local works, and automatic protection, meaning no formalities are needed to secure copyright. The protection of software and digital works under the Berne Convention has been further reinforced by the Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement and the World Intellectual Property Organization (WIPO) Copyright Treaty, both of which affirm that copyright subsists in computer programs. Together, these instruments create a uniform international framework that enables South African creators to rely on copyright protection and to enforce their rights against infringers in other member countries, with each infringement adjudicated under the law of the country where protection is claimed.

Monetisation of IP and related restrictions

IP related to digital and crypto assets can be monetised in South Africa in the same manner as any other IP right.

Common approaches include:

- *Licensing:* IP owners may license their IP for royalties or licence fees.
- *Assignments/sale of IP:* IP assets can be sold outright to another party.
- *Granting of security interests over IP:* IP can serve as security for financing, and is recognised as a form of property capable of being pledged or assigned.

Legal restrictions

While no IP-specific barriers exist, cross-border monetisation must comply with South Africa's Exchange Control Regulations, which treat IP as a capital asset. Assignments or licensing of South African-owned IP to foreign entities may require approval by the SARB or its authorised dealers.

South Africa's IP legal regime readily accommodates innovations in the fintech, crypto and digital asset sectors within its existing statutory framework. While traditional IP categories continue to govern protection and enforcement, regulators are increasingly attuned to the commercial realities of digital technologies. By securing and strategically leveraging their IP rights (while adhering to applicable legal and regulatory processes) South African innovators in the virtual asset space can protect their creations, enforce their rights, and commercialise their IP both locally and internationally, thereby maximising the value of their IP in this sector.



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