



**South African Institute of Race Relations NPC,
Submission to the South African Reserve Bank
regarding the
DRAFT CRYPTO-ASSET MANUAL FOR CROSS-BORDER ACTIVITIES
30 September 2026**

<u>Table of contents</u>	<u>Page</u>
1. Introduction	2
2. inadequate public participation	2
3. No legal authority for the Manual	3
4. The unconstitutionality of the Regulations	4
5. The content of the Manual	5
5.1 “Deemed” cross-border transfers	5
5.2 Prohibitions on imports/exports by resident entities	8
5.3 Constraints on individuals	8
5.4 Three categories of CASPs	10
5.5 Onerous licensing, operational, compliance and reporting rules	10
5.6 Powers to search for CASPs as well	12
5.7 Suspension and other penalties under the Manual	12
6. Ramifications of the Manual	13
6.1 Intrusive and excessive powers	13
6.2 Valid concerns about kidnapping, extortion and physical attack	13
6.3 Damaging constraints on individuals and resident entities	16
6.4 No distinction between stablecoins and other crypto assets	16
6.5 High compliance costs and penalties	17
6.6 Squandering new economic opportunities in digital assets	17
6.7 Excessive constraints on a vital new sector	19
6.8 The importance of increased foreign direct investment	19
6.9 The deterrent effect of the Manual	20
7. The way forward	22

1 Introduction

On 3 August 2026 the South African Reserve Bank (“the SARB” or “the Reserve Bank”) published a draft Crypto-Asset Manual for Cross-Border Activities (“the Manual”)¹ and invited interested persons to submit written comments on it to the SARB by 30 September 2026.

This submission on the Manual is made by the South African Institute of Race Relations NPC (“the IRR”), a non-profit organisation formed in 1929 to oppose racial discrimination and promote racial goodwill. Its current objects are to promote democracy, human rights, development, and reconciliation among the peoples of South Africa.

2 Inadequate public participation

The SARB has failed to comply with the Socio-Economic Impact Assessment (SEIA) Guidelines adopted by the government in 2015. Under these guidelines, the Reserve Bank should have provided “a detailed evaluation of the likely effects of [the Manual] in terms of implementation and compliance costs as well as the anticipated outcome.”² Moreover, this assessment should have accompanied the Manual when it was gazetted for public comment.

The SARB has also failed to comply with the National Policy Development Framework of 2020.³ This Framework states that policy makers must “inform and engage stakeholders” on “the nature and magnitude of a policy issue,” as well as on its likely “impacts and risks”. These assessments of proposed policies must also be “informed by the best available evidence, data, and knowledge,” the Framework adds.⁴

Instead of complying with these obligations, the SARB has embraced a “tick-box” approach to public consultation. This is inconsistent not only with the Framework but also with Chapter Ten of the Constitution. This chapter states, in Section 195(1)(e), that “people’s needs must be responded to and the public must be encouraged to participate in policy-making.” This section underscores the fact (as the Framework points out) that “the involvement of the public in policy making is a constitutional obligation that government institutions must respect and institutionalise.”⁵

Instead of complying with these obligations, the SARB has provided little or no information as to the likely costs and consequences of the Manual. It has also attempted to limit public participation by stating that comments must be submitted by completing a table with specified headings. This table denies the public the opportunity to evaluate the proposed clauses in the Manual. Instead, it seeks to confine commentators to proposing amendments to specific clauses, accompanied by brief explanations of why the alternative wording would be better.

This approach is inconsistent with the Framework, which lists some of the key requirements for proper public participation and says. “Consultation with stakeholders should commence as

¹ South African Reserve Bank, “Crypto Asset Manual for Cross-Border Activities,” (“the Manual”), <https://www.resbank.co.za/en/home/publications/publication-detail-pages/media-releases/2026/crypto-assets>.

² Department of Planning, Monitoring and Evaluation, “Socio-Economic Impact Assessment System (SEIAS), Revised Impact Assessment: National Health Insurance Bill,” 26 June 2019 (2019 SEIAS Assessment); *SEIAS Guidelines*, May 2015, pp. 3, 7, 11.

³ National Policy Development Framework, 2020, p. 3.

⁴ *Ibid*, p. 20.

⁵ *Ibid*, p. 19.

early as possible.” All relevant stakeholders should be identified, including “those who will benefit when problems are addressed” and “those who will bear the cost of implementation of the proposed intervention.” Policy makers must also identify and counter all “barriers to active participation” and ensure that “consultation is infused in all aspects of the policy making cycle.”⁶

The SARB’s attempt to confine commentators to filling in a brief and prescribed form further assumes that the Manual is lawful, constitutional and economically advisable when none of these presumptions is true. In addition, attempting to restrict public comment in this way – and so avoid all the issues which should have been dealt with in a comprehensive socio-economic assessment – is contrary to the SEIA Guidelines, the Framework and Section 195(1)(e) of the Constitution. It underscores the fact that the Reserve Bank has omitted to provide the public with the information it needs to “*know about the issues*” raised by the Manual and then to have an “*adequate say*” on them. Yet this is what the Constitution requires in terms of public participation, as the Constitutional Court has repeatedly reaffirmed.⁷ This makes the Manual just as procedurally unconstitutional as the various other laws the Constitutional Court has struck down on these grounds.

3 No legal authority for the Manual

The SARS has failed to explain the legal authority under which it has drawn up the Manual. Instead, the wording in the Manual fudges this issue, saying: “The National Treasury is responsible for authorising, regulating and where necessary, prohibiting the import and/or export of crypto assets to/from South Africa, including granting permissions, imposing conditions and enforcing compliance with the capital flow management measures applicable to cross-border crypto asset transactions. The permissions, conditions or exemptions insofar as they relate to crypto assets are outlined in the Crypto Asset Manual for cross-border activities (Crypto Asset Manual) and *while they have no statutory force, they have the effect of law.*”⁸ (Emphasis supplied.)

The Manual adds: “The Minister of Finance has, in terms of the Exchange Control Regulations, delegated to the Governor, a Deputy Governor, the Head of the Financial Surveillance Department [“FinSurv”] as well as other officials in [FinSurv], the powers, functions and duties assigned to and imposed on the National Treasury under the Exchange Control Regulations. [FinSurv] is therefore responsible for the *day-to-day administration* of capital flow management in South Africa.”⁹ (Emphasis supplied.)

Where, then, is the legal authority for the drawing up of the Manual to be found? Neither the Treasury nor the SARB has the power to make new rules, as this is the province of Parliament under the separation-of-powers doctrine. In addition, the Treasury has no powers, under the 65-year old Exchange Control Regulations of 1961, to deal with digital crypto assets – which constitute an entirely different asset class from gold, foreign currencies and securities. Since the Treasury has no relevant powers, it cannot lawfully assign any such powers to the Reserve

⁶ Ibid, pp. 19 – 20.

⁷ Section 59(1), Constitution of the Republic of South Africa, 1996; *Minister for Health and another v New Clicks South Africa (Pty) Ltd and others*, [2005] ZACC 14, at para. 630, emphasis supplied by the IRR; *Doctors for Life*, at para. 145; *Land Access* judgment, at para. 59; *Mogale* judgment, at para. 34

⁸ Ibid, p. 4.

⁹ Ibid.

Bank. In addition, the fact that FinSurv has been made responsible for “day-to-day administration” cannot give the SARB the law-making authority it lacks.

Overall, it is difficult to understand how, in a constitutional democracy founded on “the supremacy of the rule of law,”¹⁰ the provisions of the Manual can “have no statutory force” and yet also “have the effect of law”.

The Reserve Bank may also have assumed that its Manual will in time be authorised by Treasury’s intended Capital Flow Management Regulations, once these enter into force. However, this assumption is flawed too. First, though the Manual is undoubtedly intended to supplement the draft Regulations (“the Regulations”) the Treasury gazetted on 17 April 2026 for comment by an amended deadline of 30 June 2026,¹¹ this intention is not enough to give the SARB a law-making capacity it lacks. Second, the Regulations are themselves unconstitutional – and thus cannot provide a lawful foundation for the adoption of the Manual.

4 The unconstitutionality of the Regulations

As the IRR stated in its 30 June 2026 submission to the Treasury on the Regulations: “The Currency and Exchanges Act of 1933, under which the Regulations are to be adopted, was enacted 93 years ago and more than six decades before the 1996 Constitution came into effect. The 1933 Act purports to authorise searches, attachments and forfeitures of the kind set out in the Regulations, but this is not nearly enough. All branches of government, including the National Treasury, must now comply with the Constitution at all times. [Hence,] where regulations limit guaranteed rights – including the rights to privacy, property, and freedom of trade – such limitations must be ‘reasonable and justifiable,’ as required by Section 36 of the Constitution.”¹²

The Regulations are clearly inconsistent with the constitutionally guaranteed freedom to trade, as well as the rights to privacy and property. In addition, the limits the Regulations impose on these rights cannot be justified under Section 36 of the Constitution, as “less restrictive means” to “combat money laundering, terrorist financing and the proliferation of illicit financial flows” (which is the main purpose of the Regulations) can readily be devised.

Some of the proposed rules in the Regulations are also inconsistent with constitutional provisions that fall outside the Bill of Rights and cannot be “saved” from invalidity by Section 36. For example, some of the proposed rules in the Regulations are so vague that different officials are sure to interpret them in different ways at different times. This puts these rules in breach of the doctrine against vagueness of laws. It also makes them inconsistent with the rule of law, the “supremacy” of which is a founding value of South Africa’s democracy under Section 1(c) of the Constitution.

Other proposed clauses in the Regulations are *ultra vires* the 1933 Act, with its short and relatively simple provisions. This is particularly true of the clauses dealing with crypto assets, which seek to extend a 93-year-old statute to a novel and entirely different asset class.

¹⁰ Section 1(c), Constitution of the Republic of South Africa, 1996.

¹¹ National Treasury, “Draft Capital Flow Management Regulations,” Government Notice No. 54520, Government Gazette No. 7375, 17 April 2026 (“the Regulations”).

¹² South African Institute of Race Relations NPC, “Submission to the National Treasury regarding the Draft Capital Flow Management Regulations,” 30 June 2026.

Regulations that are *ultra vires* the statute under which they are adopted are unconstitutional for this reason too. In addition, the executive (including the Treasury) has no law-making capacity under the separation-of-powers doctrine, which makes the Regulations unconstitutional for this reason as well.¹³

In summary, thus, since the Regulations are themselves unconstitutional, they cannot purport to give the Reserve Bank the legislative authority to introduce the rules contained in the Manual. These rules need to be enacted by Parliament, if they are to be adopted at all.

5 The content of the Manual

5.1 “Deemed” cross-border transfers

5.1.1 Relevant “deeming” provisions

According to the Manual, one of its key purposes is to identify the circumstances in which “crypto asset transactions would be deemed as import or export of capital in terms of the draft Regulations.”¹⁴ In keeping with this objective, the Manual includes various deeming provisions regarding cross-border transfers.

In its Introduction, the Manual says that it “sets out the permissions and conditions applicable to transactions in crypto assets *deemed* as cross-border.”¹⁵ (Emphasis supplied.)

In Section A.1, the Manual defines a “Cross-border crypto asset transaction” as “a crypto asset transaction *deemed* as cross-border by the Financial Surveillance Department.”¹⁶ (Emphasis supplied.)

In Section B.1, dealing with the Business activities of Authorised Crypto Asset Service Providers or CASPs, the Manual says: “Crypto asset transactions would be *deemed* as import or export of capital in terms of the draft Regulations at the point where crypto assets are transferred between a domestic Authorised CASP and an offshore CASP or from a domestic Authorised CASP to a non-custodial wallet, resulting in a cross-border inflow or outflow.”¹⁷ (Emphasis supplied.) (The terms used in this clause are further explained below.)

An implicit deeming provision is also found in the Manual’s new rules for “Cross-border crypto asset transaction reporting categories.” Here, the Manual (twice) lays down that: “Transactional data must be reported to the Financial Surveillance Department at the point where crypto assets are transferred between a domestic Authorised CASP and an offshore CASP or from a domestic Authorised CASP to a non-custodial wallet, *resulting in* a cross-border inflow or outflow.”¹⁸ (Emphasis supplied.)

(A similar deeming provision is contained in the Regulations too. This describes CASPs as those entities that have been “authorised by the National Treasury to facilitate transactions *deemed*

¹³ Ibid.

¹⁴ The Manual, pp. 5, 24, 28.

¹⁵ The Manual, p. 5.

¹⁶ Ibid, p. 9.

¹⁷ Ibid, p. 24.

¹⁸ Ibid, pp. 33, 35.

as import and/or or and (sic) export of capital, directly or indirectly, utilising crypto assets as a medium of exchange.” Emphasis again supplied.)¹⁹

The Manual thus has several explicit or implicit deeming provisions. However, neither the 1933 Act nor the flawed Regulations give the Reserve Bank the legislative authority to introduce binding rules on when the exporting of capital is “deemed” to have occurred. There is also a question as to whether a deeming provision of this kind is consistent with the right to due process guaranteed by Section 35 of the Bill of Rights – or with “the supremacy” of the rule of law, as proclaimed by Section 1(c) of the Constitution.²⁰

5.1.2 *Relevant definitions*

In order to assess the intended legal consequences of these deeming provisions, relevant definitions in the Manual need to be set out.²¹

A *crypto asset* is defined as “a digital representation of value that (a) is not issued by a central bank, but is capable of being traded, transferred or stored electronically by natural and legal persons for the purpose of payment, investment and other forms of utility; (b) applies cryptographic techniques; and (c) uses distributed ledger or similar technology.”

An “*Authorised CASP*” is defined as “a South African Crypto Asset Service Provider...who is authorised by the National Treasury to facilitate transactions deemed as import and/or export of capital, directly or indirectly, utilising crypto assets as a medium of exchange.”

A “*Custodial wallet*” means “a crypto asset wallet where the private keys are managed by a CASP on behalf of a client. The client interacts with the CASP, rather than the blockchain, to manage its crypto assets.”

A *Foreign custodial wallet* means “a crypto asset wallet allocated to a specific individual or legal entity, held with an offshore CASP.”

An “*offshore CASP*” means “a legal entity authorised by the central bank or relevant regulatory authority in the country of domicile to provide crypto asset services in a foreign jurisdiction.”

A “*non-custodial wallet*” means “a private crypto asset wallet where an individual or entity has complete control of their private keys and the associated value.”

A “*South African custodial wallet*” means a crypto asset wallet allocated to a specific individual or legal entity, hosted by an Authorised CASP.

5.1.3 *The impact of the deeming provisions*

Under the Manual, as law firm Baker McKenzie points out, “a transaction would be treated as cross-border when crypto assets move between an Authorised CASP in South Africa and either a foreign CASP or a non-custodial wallet, including so-called 'self-hosted' wallets controlled directly by an individual. The South African Authorised CASP facilitating the transaction would be responsible for identifying and reporting the resulting inflow into, or outflow from, South Africa to FinSurv [the Financial Surveillance Department of the South African Reserve Bank]. Notably, this means that a transfer from a domestic Authorised CASP to a client’s own self-

¹⁹ Regulations, Clause 1, Definitions.

²⁰ Sections 35, 1(c), Constitution.

²¹ Manual, Section A.1, Definitions, pp 7 – 10.

hosted wallet would be classified as an export of capital, even though no jurisdictional border is crossed and beneficial ownership of the crypto assets does not change. This is likely to be one of the most contested aspects of the proposed framework.”²²

The Reserve Bank has no legal capacity to introduce rules treating such transactions as the punishable “exporting” of capital. Yet, once such transactions have been tagged as “exports” under the Manual, the draconian rules set out in the Regulations will be triggered, with several unconstitutional consequences.

5.1.4 The legal consequences of deemed exports under the Regulations

As set out in the IRR’s 30 June 2026 submission to the National Treasury, the Regulations not only prohibit the “exporting” of crypto assets, such as bitcoin, but also allow enforcement officers to search for and “seize” any crypto assets they “reasonably suspect” are being exported.²³

The Regulation’s badly drafted clauses go on to say that such crypto assets “shall be forfeited to the state for the benefit of the National Revenue Fund,” unless “the Treasury...in its discretion, directs [that they] be refunded or returned.”²⁴

The Regulations further provide that the owner of the forfeited crypto assets must “upon written demand made by National Treasury...furnish full particulars in writing of all and any passwords, personal identification numbers or codes which are necessary to enable National Treasury to obtain access to and control over the crypto assets and their disposal.”²⁵

These rules are extraordinary. They begin by making the absurd assumption that crypto assets – digital assets that are recorded on distributed ledgers, identical copies of which are stored on thousands of computers spread across the world – are located in a single country and can be “exported” to another.

The rules also infringe the right to privacy in Section 14 of the Bill of Rights. This gives everyone the right “not to have their person, home...[or] property searched, their possessions seized, or the privacy of their communications infringed.”²⁶

In addition, by allowing forfeiture prior to adequate proof of a prior offence, the Regulations conflict with Section 25 of the Constitution. Since forfeiture in these circumstances would result in the “compulsory acquisition” or effective expropriation of the crypto assets in issue, the onus lies on the Treasury to prove that the “nil” compensation envisaged has either been agreed with the owner or has been “decided or approved by a court.”²⁷ Until one or other of these steps has been established, ownership cannot lawfully pass to the state.

As earlier noted, these clauses in the Regulations are inconsistent with the constitutionally guaranteed freedom to trade, as well as the constitutional rights to privacy and property.

²² Ashlin Perumall and Fatima Ismail, “South Africa: Proposed Framework for Cross-Border Crypto Asset Transactions”, Baker McKenzie, 24 August 2026, <https://www.bakermckenzie.com/en/insight/publications/2026/08/south-africa-proposed-framework-for-cross-border-crypto-asset-transactions#>.

²³ Regulation 4(3), Regulations.

²⁴ Regulation 4(7), *ibid*.

²⁵ Regulation 25(5), *ibid*.

²⁶ Section 14,(a) – (d), Constitution.

²⁷ Section 25(2)(b), Constitution.

Moreover, the limits on these rights cannot be justified under Section 36 of the Constitution as “less restrictive means” of “combating money laundering, terrorist financing and the proliferation of illicit financial flows” – the stated purpose of the Regulations – can readily be devised.²⁸

The deeming provisions in the Manual, read together with the Regulations, will also allow the imposition of draconian penalties without adequate proof of a prior offence. As Werksmans attorneys have pointed out, the Regulations “impose criminal penalties of up to R1,000,000 or five years’ imprisonment” – or fines “equal to the asset value where this exceeds R1,000,000.”²⁹ These are extraordinarily harsh penalties in these circumstances.

5.2 Prohibitions on imports/exports by resident entities

According to the Manual, “Resident entities may not enter into crypto asset transactions deemed as import or export of capital in terms of the draft Regulations.”³⁰

Resident “entities” would include South African companies, trusts and partnerships. As the Moonstone Information Refinery comments, these entities are to be “treated differently” from natural persons or individuals – who will be “allowed to externalise crypto assets through Authorised CASPs” within existing exchange control allowances (see below). By contrast, adds Lindsey Schutters in CryptoCorner in the *Daily Maverick*, “South African businesses will be barred from utilising crypto assets for capital imports or exports, even when the underlying commercial activity is completely lawful.”³¹

The Manual’s proposed new rule is inconsistent with Section 22 of the Constitution, which says that “every citizen has the right to choose their trade, occupation or profession freely.” Though the “practice” of a trade may be “regulated by law,”³² a complete prohibition of certain trades goes far beyond instructions as to how trades are to be carried out. In addition, it is doubtful if the Manual constitutes “law” within the meaning of Section 22.

Moreover, crypto assets have no physical location in any country and cannot be “imported” into or “exported” from South Africa. The content of the Regulations is also relevant here, as any business deemed to be “exporting” crypto assets would be vulnerable to the unconstitutional searches, seizures and forfeitures earlier outlined, as well as to draconian fines and prison terms.

5.3 Constraints on individuals

5.3.1 Deemed exports and imports

As earlier noted, “Crypto asset transactions would be deemed as import or export of capital in terms of the draft Regulations at the point where crypto assets are transferred between a domestic Authorised CASP and an offshore CASP or from a domestic Authorised CASP to a non-

²⁸ Section 36(1)(e), Constitution; IRR, Submission to the National Treasury regarding the Draft Capital Flow Management Regulations,” op. cit.

²⁹ Natalie Scott, “South Africa’s crypto crackdown: Draft Manual brings cross-border crypto asset transactions under exchange control,” Werksmans Attorneys, 4 August 2026. <https://werksmans.com/south-africas-crypto-crackdown-draft-manual-brings-cross-border-crypto-asset-transactions-under-exchange-control/>.

³⁰ Manual, B.1 (b), Resident entities, p. 31.

³¹ Lindsey Schutters, CryptoCorner, Daily Maverick, 10 September 2026.

³² Section 22, Constitution.

custodial wallet, resulting in a cross-border inflow or outflow.”³³ The ramifications of this proposed new rule are considerable and have already been outlined. It is particularly absurd that “a transfer from a domestic Authorised CASP to a client's own self-hosted wallet” (to cite Baker McKenzie again) “would be classified as an export of capital, even though no jurisdictional border is crossed and beneficial ownership of the crypto assets does not change.”³⁴

The Manual further provides that, if “a resident individual requests the transfer of crypto assets from a non-custodial wallet to a custodial wallet hosted by a domestic Authorised CASP,” this will be seen as “a non-permissible transaction.”³⁵ Again, it is absurd that such a transfer should be strictly prohibited when no jurisdictional border has been crossed and the ownership of the crypto assets remains unchanged.

Comments Mr Schutters: “Restricting transfers from self-custody back into regulated exchanges will not stop South Africans from using crypto; it will simply force them to keep wealth offshore or trade via unverified peer-to-peer grey markets. By building a one-way exit out of the local system, regulators risk inadvertently pushing financial activity into the shadows, defeating the very purpose of financial oversight.”³⁶

5.3.2 *Permitted transfers within exchange control limits*

Some transfers by individuals will be permitted. According to the Manual, “resident individuals who are 18 years and older may transfer crypto assets to a foreign custodial wallet or a non-custodial wallet, as part of the single discretionary allowance limit of R2 million per individual per calendar year” and without having to obtain a tax clearance certificate from the SARB. Transfers of up to R10m a year are also permitted under the Foreign Capital Allowance, provided the necessary tax clearance certificate is obtained. All such transfers are regarded as an “export of capital” and must be reported.³⁷

The Manual adds that “crypto assets transferred abroad in terms of the single discretionary allowance may be repatriated to the resident individual’s South African custodial wallet, hosted by an Authorised CASP, at any point in time.”³⁸ Moreover, “crypto assets purchased abroad in terms of the single discretionary allowance externalised via an Authorised Dealer, may be repatriated to the resident individual’s South African custodial wallet, hosted by an Authorised CASP, at any point in time.” Both repatriations are regarded as an “import of capital” and must be reported.³⁹

5.3.3 *Authorised remittances*

Authorised CASPS may “facilitate specific remittance transactions between individuals using crypto assets as a settlement medium.”⁴⁰ However, such transactions – generally by resident individuals and foreign labourers – are subject to “a limit of R5 000 per transaction per day and

³³ Manual, B.1, A(ii), p. 24.

³⁴ Perumall and Ismail, “South Africa: Proposed Framework for Cross-Border Crypto Asset Transactions”, op. cit.

³⁵ Manual, p. 81, check which section, add.

³⁶ Schutters, CryptoCorner, op. cit.

³⁷ Manual, B.1, (iii), (a), (hh), p. 28; see also p. 79; see also Moonstone Information Refinery, “Draft manual sets out proposed cross-border crypto regime,” 6 August 2026, <https://www.moonstone.co.za/draft-manual-sets-out-proposed-cross-border-crypto-regime/#>.

³⁸ Manual, B.1, (5), p. 29.

³⁹ Manual, B.1, (6), p. 29, see also pp. 80 – 81.

⁴⁰ Manual, B.1, (B), (i), (a), (aa), p. 24.

an overall limit of R25 000 per applicant per calendar month.”⁴¹ Here, “the client never owns or takes possession of the crypto assets,” while “settlement between the South African client and the Authorised CASP takes place in fiat currency (Rand).”⁴² All relevant details must also be reported to FinSurv.

5.4 Three categories of CASPs

Werksmans Attorneys sum up the three categories of CASP for which the Manual provides. “These are –

- Category One: Remittance transactions capped at R5,000 per transaction per day and R25,000 per month.
- Category Two: Broader cross-border crypto asset transactions via South African custodial wallets.
- Category Three: Combined Category One and Category Two operations.”⁴³

According to Masthead, a consultancy service for independent financial advisors, “this tiered approach allows regulators to tailor oversight according to the complexity and risk profile of each business model.”⁴⁴

5.5 Onerous licensing, operational, compliance and reporting rules

CASPs seeking authorisation must comply with many regulatory requirements. Moonstone Information Refinery sums up the relevant licensing rules, saying: “Applicants would have to demonstrate that they are licensed by the Financial Sector Conduct Authority (FSCA), which regulates how financial institutions treat customers and conduct business. They must also be registered with the Financial Intelligence Centre (FIC), which collects and analyses financial data to combat financial crimes.” In addition, they must “apply to FinSurv for appointment under powers delegated by National Treasury. Until formally appointed, a CASP would not be permitted to facilitate transactions regarded as cross-border.”⁴⁵

To obtain the necessary FinSurv approval, Masthead notes, “CASPs will be required to demonstrate regulatory compliance, maintain appropriate governance structures,... implement effective risk management systems...[and] meet capital requirements.”⁴⁶ These last rules require a CASP to “maintain during the lifetime of its operations a minimum unimpaired capital amount in a Rand denominated savings and/or investment type banking account segregated from [its] business account or clients’ funds.” The minimum “unimpaired capital amount” is

⁴¹ Ibid, B.1, (B), (ii), (a), (aa), p. 24.

⁴² Ibid, B.1, (B), (ii), (a), (bb), (cc), pp. 24 – 25.

⁴³ Scott, “South Africa’s crypto crackdown,” op. cit; Manual, “Business activities of Authorised Crypto Asset Service Providers,” pp. 24 – 35.

⁴⁴ Masthead, South Africa Unveils Draft Framework for Cross-Border Crypto Asset Transactions, 26 August 2026, <https://www.masthead.co.za/newsletter/south-africa-unveils-draft-framework-for-cross-border-crypto-asset-transactions/#>.

⁴⁵ Moonstone Information Refinery, “Draft manual sets out proposed cross-border crypto regime,” 6 August 2026, <https://www.moonstone.co.za/draft-manual-sets-out-proposed-cross-border-crypto-regime/#>.

⁴⁶ Masthead, South Africa Unveils Draft Framework for Cross-Border Crypto Asset Transactions,” op. cit.

“R5 million or 15% of average positive gross income over the preceding three years, whichever is higher.”⁴⁷

Under the Manual, many other compliance obligations will apply. As Masthead explains, authorised CASPs must “conduct customer due diligence, verify clients’ identities and sources of funds, retain transaction records for at least five years, maintain segregated client funds, and monitor transactions for potential breaches of exchange control rules.”⁴⁸ In addition, comments the Moonstone Information Refinery, they “must be registered with the Companies and Intellectual Property Commission, maintain a physical presence in South Africa, and ring-fence their crypto asset operations from other business activities.”⁴⁹

Reporting requirements are also onerous, as Baker McKenzie points out: “Authorised CASPs will be required to comply with FinSurv reporting rules, as well as existing Financial Intelligence Centre (FIC) Travel Rule obligations and the Crypto-Asset Reporting Framework (CARF)... Three overlapping data pipelines built on substantially the same underlying transaction set represent a material operational and systems challenge, particularly for smaller CASPs.”⁵⁰

The Manual’s obligations will come on top of existing reporting obligations are already burdensome. Under the FIC Travel Rules (which came into effect on 30 April 2025), CASPs and financial institutions, as law firm ENS notes, must “collect and transmit detailed information about both the originator and the beneficiary with every crypto asset transfer. This information must be shared, either before or simultaneously with the transfer, and retained securely for regulatory review. For natural persons, data such as full name, identity number, address, date and place of birth, and wallet addresses must be collected and verified. For legal entities, the registered name, registration number under which it is incorporated, and the registered address must be obtained and verified.” In addition, for transfers to or from self-hosted wallets, CASPs must conduct a risk assessment and may need to implement additional due diligence measures. Non-compliance with any of these obligations, notes ENS, can lead to administrative sanctions under the Financial Intelligence Centre Act of 2001. Such sanctions may “include warnings, reprimands, or financial penalties up to ZAR50 million for juristic persons and ZAR10 million for natural persons.”⁵¹

Relevant too is the Crypto-Asset Reporting Framework (CARF), developed by the Organization for Economic Co-operation and Development (OECD) and G20 countries. This enables the automatic exchange of information regarding crypto-asset transactions among some 80 tax authorities across the world. Under CARF rules, as the South African Revenue Service has explained, relevant CASPs must report on “exchanges between crypto assets, crypto asset purchases...and disposals [fiat to crypto and vice versa], crypto asset wallet transfers and reportable retail payment transactions exceeding EUR or USD 50,000.” The CARF system took effect in South Africa on 1 March 2026, with the first reporting period running from then until 28

⁴⁷ Manual, [B.2, (B), (i), (iii), p.37; Moonstone Information Refinery, “Draft manual sets out proposed cross-border crypto regime,” op. cit.

⁴⁸ Masthead, South Africa Unveils Draft Framework for Cross-Border Crypto Asset Transactions,” op. cit.

⁴⁹ Moonstone Information Refinery, “Draft manual sets out proposed cross-border crypto regime,” op. cit.

⁵⁰ Perumall and Ismail, “South Africa: Proposed Framework for Cross-Border Crypto Asset Transactions”, op. cit.

⁵¹ Angela Itzikowitz and Era Gunning, “It is better to travel well than to arrive – The FICA Travel Rule,” 30 May 2025, <https://www.ensafrica.com/news/detail/10205/it-is-better-to-travel-well-than-to-arrive-th>; see also Masthead Information Refinery, “The Travel Rule – What CASPs Need to Know About Directive 9,” 9 May 2025, <https://www.masthead.co.za/newsletter/the-travel-rule-what-casps-need-to-know-about-directive-9/>.

February 2027. The first exchange of CARF information among participating countries is due to take place in September 2027.)⁵²

5.6 Powers to search for CASPs as well

According to the Manual, CASPs must “closely monitor...all transactions passing through clients’ South African custodial wallets,” so as to find “information useful to the Financial Surveillance Department.” In doing so, adds the Manual, CASPs should remember “the powers conferred on them under the draft Regulations, which entitle them to call for any information and to search any premises to inspect any books or documents (sic) as may be necessary to ensure compliance with the draft Regulations.” These powers, it states, “should be fully availed of by Authorised CASPs” in carrying out their functions and duties.⁵³

Here, the Manual disregards Section 14 of the Bill of Rights, under which “everyone has the right to privacy, which includes the right not to have their...their property searched.” It provides no justification for this limitation of a guaranteed right. Nor does it include any safeguards – the need for consent or a prior search warrant, for example – to prevent its possible abuse.

5.7 Suspension and other penalties under the Manual

The Manual has various clauses dealing with “compliance and remedial action.” These lay down penalties for any failures by CASPs to comply with “the provisions of the draft Regulations, the requirements outlined in the Crypto Asset Manual as well as any directive issued by the Financial Surveillance Department.”⁵⁴

According to the Manual, “any deviation or non-compliance” with any of these requirements “may result in measures being taken by the Financial Surveillance Department as administrator of the capital flow management system.” Such measures may include:

- “(a) an official warning by Finsurv [though this is not obligatory];
- (b) the temporary suspension of specific business activities of an Authorised CASP;
- (c) the temporary suspension of an Authorised CASP’s authority to conduct the business of an Authorised CASP...;
- (d) a call for a complete audit of the Authorised CASP’s administration by external auditors, at the Authorised CASP’s expense...;
- (e) the invoking of the provisions [presumably, the penalty clauses] under the draft Regulations; and
- (f) the permanent withdrawal of an Authorised CASP’s approval to conduct the business of an Authorised CASP.”⁵⁵

Authorised CASPs may thus be penalised through the suspension of particular business activities; the imposition of substantial fines and prison terms (as set out in the Regulations); and the temporary or permanent withdrawal of the authorisations on which their businesses depend. In many instances, moreover, CASPs could be punished in these ways for the

⁵² South African Revenue Service, “Crypto-Asset Reporting Framework (CARF),” 20 March 2026.

<https://www.sars.gov.za/businesses-and-employers/third-party-data/crypto-asset-reporting-framework-carf/>

⁵³ Manual, A4, (A), (xii), p. 23.

⁵⁴ Manual, B.2, (K), (i), p. 46

⁵⁵ Ibid, (ii), (a) – (f), p. 47.

“deemed” exporting of capital even where no jurisdictional boundary has been crossed and the ownership of crypto assets remains unchanged.

6 Ramifications of the Manual

6.1 *Intrusive and excessive powers*

Given the extent of the crypto asset regulation already in place in South Africa under the FIC Travel Rules, the CARF system, the Financial Advisory and Intermediary Services Act of 2002, the Financial Markets Act of 2012, the (non-travel) requirements in the Financial Intelligence Centre Act of 2001, the Prevention of Organised Crime Act of 1998, the Consumer Protection Act of 2008, the Electronic Communications and Transactions Act of 2002, the Income Tax Act of 1962, the Value-Added Tax Act of 1991, and other tax legislation, there is little need for the further onerous obligations set out in the Manual.

This indicates that the real purpose of the Manual is simply to specify the circumstances in which the supposed exporting of crypto assets will be “deemed” to have occurred. These deemed “exports” will then trigger the draconian clauses in the Regulations regarding searches, seizures, the forced surrender of passwords and codes – and the compulsory “forfeiture” of crypto assets to the state. Under the penalty clauses in the Regulations, moreover, any failure to comply with these clearly unconstitutional provisions could result in severe penalties, including fines of up to R1 million (or the value of the crypto assets), as well as prison terms of up to five years for executives.

Proponents of the Regulations and the Manual argue that individuals are not entitled to full financial privacy, which must yield to national security and tax compliance concerns. However, demanding access to private keys and tracing self-hosted wallets goes well beyond traditional banking surveillance and infringes on individual digital privacy. Moreover, with data leaks proliferating – and data hacks increasing under the impact of Artificial Intelligence (AI) – demands for information of this kind could also expose the holders of crypto assets to kidnappings and violent attacks.

Holders of crypto assets not only have important rights to privacy but also legitimate concerns about their physical safety. Criminals have become aware that crypto assets can be transferred within minutes and that these transfers cannot easily be reversed. This realisation has prompted a worrying increase in so-called “wrench attacks” in many different countries.

6.2 *Valid concerns about kidnapping, extortion and physical attack*

The blockchain security firm CertiK verified 72 wrench attacks worldwide in 2025, 75% more than in 2024, with France recording 19 and overtaking the United States (US), which recorded eight.⁵⁶ In France the trend has since accelerated. The French interior minister, Laurent Nuñez, reported 77 crypto-related kidnappings, extortions and attempted extortions in the first half of 2026, against 45 in the whole of 2025.⁵⁷ The victims include David Balland, a co-founder of the

⁵⁶Decrypt, “\$41M in Losses as Crypto Wrench Attacks Hit Record High in 2025,” February 2026, <https://www.yahoo.com/news/articles/41m-losses-crypto-wrench-attacks-140102565.html>.

⁵⁷Cointelegraph, “France to strengthen response as crypto wrench attacks hit 77,” July 2026, <https://ct.com/news/french-wrench-attacks-rise-to-77-as-government-promises-more-support> (citing BFM Business).

hardware wallet maker Ledger, who was kidnapped with his partner in January 2025 and whose captors severed one of his fingers while demanding €10 million in crypto assets.⁵⁸

Commentators have linked the French wave in part to leaks of personal data that told criminals whom to target and where to find them. These leaks have come from several directions. In 2020 criminals stole the names, postal addresses and telephone numbers of some 272,000 customers of Ledger, and later published them online. Ledger subsequently reported that rogue members of the support team at its e-commerce provider, Shopify, had also exported customer records.⁵⁹ In January 2026 hackers stole the email addresses and data on the 2024 capital gains and losses of some 50,000 users of Waltio, a French crypto tax-reporting service, and tried to extort the company.⁶⁰

A 32-year-old official at the Bobigny tax office, since suspended, has been charged with complicity in violence and criminal association. Investigators allege that she searched the tax authority's "Mira" database for the new address of a prison officer – whom three armed men then assaulted at his home – and that her work computer also showed searches conducted on crypto investors. She has been in custody since 30 June 2025. She admits passing on information about the prison officer but says she did not know what it would be used for. Her lawyer disputes that she ran the search herself, and the allegations have yet to be tested at trial.⁶¹

Most recently, on 13 August 2026, the French finance ministry confirmed that an intruder had consulted and extracted tax data on individuals and businesses in late June. The ministry put the number of people affected at 678,000.⁶²

Artificial intelligence (AI) is making such leaks cheaper to cause and easier to exploit. IBM's 2025 study of data breaches found that attackers used AI in 16% of the breaches examined, mostly for phishing and deepfakes.⁶³ In August 2025 the AI developer Anthropic reported that a single criminal had used its coding tool against at least 17 organisations to automate reconnaissance, steal credentials, write malicious software and analyse stolen data so as to work out which victims could pay the most.⁶⁴

⁵⁸Decrypt, "\$41M in Losses," op. cit.

⁵⁹Ledger, "Message by Ledger's CEO – Update on the July data breach. Despite the leak, your crypto assets are safe," 21 December 2020, <https://www.ledger.com/message-ledgers-ceo-data-leak>; see also Ledger, "Update: Efforts to Protect Your Data and Prosecute The Scammers," January 2021, <https://www.ledger.com/blog/update-efforts-to-protect-your-data-and-prosecute-the-scammers>.

⁶⁰DL News, "Hackers extort French crypto company Waltio after pinching data from 50,000 users," January 2026, <https://www.dlnews.com/articles/regulation/hackers-extort-french-crypto-firm-waltio/>.

⁶¹Le Parisien, "L'agente du fisc ciblait gardiens de prison et investisseurs en cryptomonnaie pour un mystérieux commanditaire," 6 January 2026, <https://www.leparisien.fr/faits-divers/lagente-du-fisc-ciblait-gardiens-de-prison-et-investisseurs-en-cryptomonnaie-pour-un-mysterieux-commanditaire-06-01-2026-WYVSPSJXYFCUFND23GKKJR3D6Y.php>.

⁶²Leto, "Piratage du fisc : Bercy confirme la fuite des données de 678 000 contribuables," 14 August 2026, <https://www.letto.legal/news/dgfiip-bercy-confirme-fuite-donnees-fiscales-2026>; see also Aladom, "Piratage des impôts : 678 000 Français concernés par le vol de données à la DGFiP, ce qu'il faut savoir," August 2026, <https://www.aladom.fr/actualites/secteur-service/11265/piratage-des-impots-678-000-francais-concernees-par-le-vol-de-donnees-a-la-dgfiip-ce-quil-faut-savoir/>.

⁶³IBM and Ponemon Institute, Cost of a Data Breach Report 2025: The AI Oversight Gap, July 2025, <https://www.ibm.com/reports/data-breach>.

⁶⁴Anthropic, Threat Intelligence Report: August 2025, pp. 4–10, <https://www-cdn.anthropic.com/b2a76c6f6992465c09a6f2fce282f6c0cea8c200.pdf>.

The same techniques could be turned on a leaked list of crypto holders to rank them by wealth and find their homes. In addition, a leak does not require an outside attacker. The US exchange Coinbase disclosed in 2025 that a breach it classified as “insider wrongdoing” had affected 69,461 people. (This occurred after overseas support staff were allegedly bribed to hand over customer data, including images of passports and driver’s licences.)⁶⁵

The Regulations and the Manual would create the very records that criminals seek. Regulation 10(1) would require every person in the Republic to declare any crypto asset within 30 days of acquiring it, stating when and how it was acquired and where it is held. Unlike Regulation 8, it sets no minimum value.⁶⁶

The Manual requires each Authorised CASP to record every cross-border client’s residential address, identity number, the amount of crypto assets transferred and the wallet identifiers involved. The CASP must keep these records for at least five years and report every transfer to a client’s own non-custodial wallet to FinSurv, whatever the amount.⁶⁷ The CASP must also be able to supply any such data to FinSurv within 48 hours as a spreadsheet file.⁶⁸

In effect, the state would be compiling a register of people who keep valuables in a safe at home, showing where each of them lives and roughly what each safe contains. Such a register is only as secure as the least trustworthy person with access to it and the weakest system on which it is stored.

Neither the Manual nor the Regulations explain how FinSurv or National Treasury will protect this information, who may consult it, how long it may be kept, or what is to happen if it leaks. The Manual’s only data-security requirements apply to offshore and cloud storage. On the Protection of Personal Information Act (POPIA), it asks CASPs only to “acquaint” themselves with the statute.⁶⁹

South Africa’s record offers little comfort. In 2020 a fraudster obtained a dataset from the credit bureau Experian that exposed as many as 24 million South Africans.⁷⁰ In March 2024 the ransomware group LockBit released data it had taken from the Government Pensions Administration Agency.⁷¹

South Africa also has an established kidnapping industry, with recorded kidnappings having risen from 4,692 in 2014/15 to 17,061 in 2023/24. Many of these are “express kidnappings”, in which victims are held for hours or days while criminals drain funds usually held at banks.⁷² In addition, police recorded 4,638 kidnappings between April and June 2026, 172 more than in the

⁶⁵The Hacker News, “Coinbase Agents Bribed, Data of ~1% Users Leaked; \$20M Extortion Attempt Fails,” May 2025, <https://thehackernews.com/2025/05/coinbase-agents-bribed-data-of-1-users.html>.

⁶⁶Regulations, Regulation 10(1)(a)–(b); compare Regulation 8(1).

⁶⁷Manual, B.2, (G), (i), (a), (cc), (dd), (hh), (ll) and (mm), p. 43; B.2, (G), (vi), p. 44; B.1, (iii), (a), (dd), p. 28; C.1, (A), (i), p. 48; see also Table 2, p. 79.

⁶⁸Manual, C.1, (D), (v), (e), (aa), p. 53; C.1, (D), (v), (h), (gg), p. 54.

⁶⁹Manual, C.1, (D), (v), (h), p. 54; C.1, (D), (v), (i), (bb), p. 55.

⁷⁰MyBroadband, “South Africa’s privacy watchdog investigating data breaches at credit bureaus,” 2023, <https://mybroadband.co.za/news/security/507116-south-africas-privacy-watchdog-investigating-data-breaches-at-credit-bureaus-in-south-africa.html>.

⁷¹Government Employees Pension Fund, “Government Pensions Administration Agency (GPAA) data breach,” media release, 12 March 2024, <https://www.gepf.co.za/government-pensions-administration-agency-gpaa-data-breach/>.

⁷²Institute for Security Studies, “South Africa’s armed robbery problem drives kidnapping,” ISS Today, December 2024, <https://issafrica.org/iss-today/south-africa-s-armed-robbery-problem-drives-kidnapping>.

same period a year earlier.⁷³ A bank can limit daily transfers and stop a suspicious one. A self-custody wallet offers neither safeguard, so its owner becomes an attractive target once his or her identity and address are known.

The state has a legitimate interest in detecting illicit financial flows. That interest must be weighed against the right to privacy in Section 14 of the Constitution. It must also be weighed against the right in Section 12(1)(c) “to be free from all forms of violence from either public or private sources”, which Section 7(2) obliges the state to protect. Measures that gather the names, addresses and holdings of crypto owners into databases with no stated safeguards increase the risk of violence against them.

In addition, Section 36(1)(e) of the Constitution requires that any limitation of guaranteed rights must be “reasonable and justifiable,” taking into account all relevant factors. Such factors include the availability of “less restrictive means to achieve the [government’s] purpose”. The Manual states that the purpose of FinSurv reporting is to compile balance-of-payments and related statistics.⁷⁴ Aggregated returns and reporting thresholds would serve that purpose. The Regulations and the Manual make no attempt to show otherwise.

6.3 *Damaging constraints on individuals and resident entities*

Farzam Ehsani, founder and chief executive of VALR, a major South African cryptocurrency exchange platform, has warned that treating the transfer of crypto assets from a non-custodial wallet to a custodial wallet hosted by a domestic Authorised CASP as a “non-permissible” transaction is “neither practical nor sensible”. It could push South Africans using self-custodial wallets into transacting through offshore exchanges rather than regulated local CASPs, he states.⁷⁵

Mr Ehsani also objects to the way in which resident “entities”, such as companies and firms, are to be constrained. Under the Manual, resident companies, firms and partnerships are permitted to open South African custodial wallets and to engage in domestic crypto asset transactions. However, they are strictly prohibited from “entering into crypto asset transactions deemed imports or exports of capital under the proposed Regulations.”

Queries Mr Ehsani: “On what principled basis should corporations and institutions be prohibited from using this technology to move value legitimately between South Africa and the rest of the world?” Barring legitimate corporate activity through regulated providers could also “drive transactions underground or offshore,” he cautions.⁷⁶

6.4 *No distinction between stablecoins and other crypto assets*

As the Moonstone Information Refinery reports, the Treasury and the SARB have made it clear that their proposed regulatory framework “does not distinguish between different types of crypto assets and does not recognise crypto assets as an official currency in South Africa.”⁷⁷

⁷³African News Agency, “Kidnapping rise to over 4,600 as Gauteng records highest total,” August 2026, <https://africannewsagency.com/kidnapping-rise-to-over-4600-as-gauteng-records-highest-total/> (citing SAPS quarterly crime statistics).

⁷⁴Manual, C.1, (A), (i), p. 48.

⁷⁵ Moonstone Information Refinery, “Draft manual sets out proposed cross-border crypto regime,” op. cit.

⁷⁶ Moonstone, *ibid.*

⁷⁷ Moonstone, *ibid.*

According to Marius Reitz, general manager for Africa and Europe for Luno (one of the earliest and largest cryptocurrency investment platforms operating across Africa, Europe, and Asia), this failure to distinguish between stablecoins and other crypto assets will “restrict South African companies from using stablecoins for cross-border commercial transactions, supply-chain payments, and international trade.” Yet stablecoins “enable instant, low-cost cross-border business-to-business payments” and are one of the cryptocurrencies most often used. “Failing to accommodate corporate cross-border stablecoin payments would leave South African businesses out of step with an international ecosystem that is adopting next-generation payment rails,” he states.⁷⁸

6.5 High compliance costs and penalties

Shiven Moodley, chief executive of fintech firm Novaque (an advisory firm working with financial services firms and digital asset companies on stablecoin integration, regulatory compliance and other issues) notes the considerable costs of complying with the authorisation, monitoring, and reporting obligations introduced by the Manual. These obligations are likely to generate “high fixed costs before a business has achieved scale,” he cautions. This could “favour large, well-capitalised providers and make it harder for smaller South African firms to compete in the digital asset market.”⁷⁹

In addition, many authorised CASPs could find themselves confined to facilitating domestic crypto asset transactions, or dealing primarily with crypto asset remittances that are subject to low ceilings (R5,000 a transaction and R25,000 a month). These constraints will also make it difficult for CASPs to grow.

Mr Moodley warns that firms engaged in market-making, treasury, technology and other digital asset activities will come under pressure to look for more favourable jurisdictions. The effect could be to stifle investment in South African digital asset companies and drive them offshore.⁸⁰ This would also push legitimate business beyond the reach of the very surveillance the authorities are trying to strengthen. It could also result in job losses at a time when unemployment in South Africa is already at crisis levels.

6.6 Squandering new economic opportunities in digital assets

South Africa already has a substantial digital asset sector. By 31 March 2026 the Financial Sector Conduct Authority (FSCA) had received 533 licence applications from crypto asset service providers and approved 310 of them.⁸¹ Luno, the largest local platform, reports more than 6.3 million South African customers⁸² and says it holds more than R30 billion in crypto assets on their behalf.⁸³ Its figures also show that South Africans are using digital assets for

⁷⁸ Moonstone, *ibid.*

⁷⁹ Moonstone, *ibid.*

⁸⁰ Ciaran Ryan, “New cross-border crypto rules could drive business, jobs offshore,” Moneyweb, 5 August 2026, <https://www.moneyweb.co.za/news/south-africa/new-cross-border-crypto-rules-could-drive-business-jobs-offshore/>.

⁸¹ Financial Sector Conduct Authority, “Update on licensing and supervision of crypto asset service providers,” media release, 15 April 2026, as published by FA News, <https://www.fanews.co.za/article/compliance-regulatory/2/financial-sector-conduct-authority-fsca-was-fsb/1059/update-on-licensing-and-supervision-of-crypto-asset-service-providers/43764>.

⁸² TechFinancials, “Luno Hits 6.3M Users In SA As Crypto Goes Mainstream,” 20 October 2025, <https://techfinancials.co.za/2025/10/20/luno-hits-6-3m-users-in-sa-as-crypto-goes-mainstream/>.

⁸³ TechAfrica News, “Luno Hits 50,000 xStocks Users as South Africans Embrace Tokenised Investing,” 2 June 2026, <https://techafricanews.com/2026/06/02/luno-hits-50000-xstocks-users-as-south-africans-embrace-tokenised-investing/>.

more than savings (or speculation). According to Luno, its payment service processed more than 53,000 payments at some 1,900 merchants in its first year,⁸⁴ while 50,000 of its South African customers have bought tokenised shares, which are digital versions of shares and exchange-traded funds listed in the United States.⁸⁵ VALR, another major local exchange, reports that more than \$15 billion of stablecoins passed through its wallets in a single year.⁸⁶

These activities matter in stimulating economic growth in South Africa. New technologies, including artificial intelligence, are reducing the cost of starting a business. Digital assets can reduce the cost of paying suppliers and receiving income across borders, while tokenisation can make it cheaper to issue and trade shares and other securities. Such cost savings are more important in South Africa than in most countries. As shown in *Section 6.8*, the country's annual savings rate, of about 16% of GDP, is far too low to fund the investment it needs. Hence, any technology that makes capital cheaper to raise and to move deserves to be encouraged. The same holds for the next stage of the digital economy, in which software will increasingly buy and sell services on behalf of people and firms – and will need forms of money it can use at any hour.

In addition, digital assets give households a choice as to how to hold their savings. For South Africans without the means to open offshore accounts, dollar-linked stablecoins held through a local exchange offer the simplest way to protect part of their savings against a weakening rand. Rules that restrict how such assets may be moved or held narrow their choices.

A useful test for assessing the impact of any rule in this sphere is to ask what individuals and firms will still be able to do with digital assets once the rule takes effect. Measured against this criterion, the Manual fares poorly. Resident companies and other entities will not be able to enter into any crypto asset transaction deemed to be an import or export of capital.⁸⁷ Remittances through Category One CASPs will be limited to R5,000 a transaction and R25,000 a month.⁸⁸

Crypto assets that a resident moves from a local exchange to his or her own non-custodial wallet may never return to a local exchange, as inward transfers from such wallets are “non-permissible.”⁸⁹ Moneyweb aptly describes this rule as creating “a one-way door.”⁹⁰ The rule creates a further cost that is easy to overlook. The freedom to move assets between providers gives customers bargaining power, since providers must then compete on price and service to retain their business. By locking assets into the custodial wallets of existing CASPs, the Manual weakens that competition and favours the largest incumbents, reinforcing the concern raised by Mr Moodley in *Section 6.5*.

The Manual also requires CASPs to report cross-border crypto asset transactions “irrespective of the amount.”⁹¹ The US offers a cautionary comparison. There, financial institutions must

⁸⁴MyBroadband, “Cryptocurrency is becoming money in South Africa,” December 2025, <https://mybroadband.co.za/news/cryptocurrency/620513-cryptocurrency-is-becoming-money-in-south-africa.html>.

⁸⁵TechAfrica News, “Luno Hits 50,000 xStocks Users,” op. cit.

⁸⁶MyBroadband, “Cryptocurrency is becoming money in South Africa,” op. cit.

⁸⁷Manual, B.1, (iii), (b), (dd), p. 31.

⁸⁸Manual, B.1, (iii), (a), (aa), p. 25.

⁸⁹Manual, Table 1, pp. 72–73.

⁹⁰Ciaran Ryan, “New cross-border crypto rules could drive business, jobs offshore,” Moneyweb, 5 August 2026, <https://www.moneyweb.co.za/news/south-africa/new-cross-border-crypto-rules-could-drive-business-jobs-offshore/>.

⁹¹Manual, C.1, (A), (i), p. 48.

report cash transactions above \$10,000, a threshold set in 1972 and never adjusted for inflation. In December 2024 the US Government Accountability Office found that an inflation-adjusted threshold would have stood at about \$72,880 in 2023 – and that using this figure would have cut the number of reports filed by at least 90% a year since 2014. It also found that law enforcement agencies accessed only a small share of the reports filed.⁹²

A regime with no threshold at all will generate far more unused reports. Yet each report adds to the compliance costs of CASPs. Each also adds more sensitive personal information to records that, as shown in *Section 6.2*, have no specified safeguards. A meaningful threshold, adjusted each year for inflation, would reduce both burdens while leaving the authorities free to investigate suspicious transactions.

6.7 Excessive constraints on a vital new sector

Mr Ehsani of VALR adds that the draft Manual, in its current form, is “prejudicial to crypto assets and licensed CASPs”. This is particularly concerning because “stablecoins and other crypto assets can facilitate cross-border payments more quickly, cheaply, and transparently than traditional channels while remaining subject to reporting and oversight,” he adds.⁹³

Mr Ehsani also fears that the government’s heavy hand will damage South Africa’s crypto industry. David Ansara, CEO of the Free Market Foundation, shares this concern, saying there is a significant risk that the Manual, together with the Regulations, could hobble – if not destroy – South Africa’s “vibrant ecosystem of fintech entrepreneurs and start-ups,” as well as its “growing retail adoption of Bitcoin.”⁹⁴

As Mr Ansara points out: “Customers of Pick n Pay can now buy their groceries using bitcoin instead of rand. [In addition,] circular bitcoin economies have emerged in towns across the Western Cape, such as Witsand, Plettenberg Bay, and the informal areas of Mossel Bay.” In recent years, bitcoin entrepreneurs in these areas have made rapid progress in building up a fledgling industry that could become increasingly important to the South African economy.

Under the Regulations and the Manual, however, these entrepreneurs will no longer be able to keep focusing on expanding their businesses, with the wider benefits that this could bring. Instead, notes Mr Ansara, they will have to “turn their attention to defending their vital economic interests against government overreach. If the National Treasury has its way, these innovative and productive people might be forced to shut down or take their businesses, their skills and their capital to more favourable jurisdictions.”⁹⁵

6.8 The importance of increased foreign direct investment

South Africa urgently needs to increase its low growth rates and reduce its extraordinarily high unemployment levels. It cannot achieve these gains, however, unless it starts to attract much higher rates of fixed investment. As IRR CEO Dr John Endres explains:

⁹²US Government Accountability Office, *Currency Transaction Reports: Improvements Could Reduce Filer Burden While Still Providing Useful Information to Law Enforcement*, GAO-25-106500, 11 December 2024, <https://www.gao.gov/products/gao-25-106500>.

⁹³ Moonstone, *ibid*.

⁹⁴ Ansara, D., “The State Is Coming For Your Bitcoin,” *The Common Sense*, 6 May 2026. <https://www.thecommonsense.co.za/editorials/state-coming-your-bitcoin>.

⁹⁵ Ansara, *ibid*.

“The technical name for fixed investment is gross fixed capital formation, or GFCF for short. It refers to the share of national income that goes into building productive capacity: the factories, the machines, the ports, the roads, the energy infrastructure that make it possible to produce goods and services, to employ people to produce them, and to move products to customers.

South Africa’s gross fixed capital formation stood at 14.9% of GDP in 2023. In 2024 it fell to 14.5%. In 2025 it dropped further, to 13.7%. The government’s own National Development Plan sets a target of 30%. But the last time it managed to break above 20% was in 2008,...when it was 21.6%. Fixed investment in South Africa is falling woefully short of where it needs to be, and has done so for a long time.

Investment drives everything else. An economy can tick over without it, running down existing equipment, trading goods, and managing operations set up years ago. But without new investment there is no expansion. There is no growth in productive capacity, no growth in jobs, and no growth in the tax base that funds schools, hospitals, and grants.”⁹⁶

So long as investment and growth remain at their current low levels, South Africa cannot reduce its high unemployment rates, which are among the worst in the world. In the second quarter of 2026, as Statistics South Africa reports, the national unemployment rate stood at 33.6%. Among young South Africans aged 15-24, the unemployment crisis was even worse, with the joblessness rate standing at a staggering 62.8.⁹⁷

To counter the unemployment crisis, South Africa urgently needs to raise its annual rate of fixed investment from 13.7% of GDP to 25% of GDP or more.⁹⁸ It cannot rely on its own domestic savings to achieve this, as its annual savings rate is about 16% of GDP and thus too low. This means that the country cannot raise its fixed investment rate to the levels needed without attracting capital from elsewhere in the world. That in turn requires that policies should help attract foreign direct investment (FDI), rather than deter it.

6.9 *The deterrent effect of the Manual*

Far from helping to attract more FDI, the Manual (together with the Regulations) will deter potential investors from bringing their capital into the country. As IRR policy fellow Ivo Vegter has pointed out, “capital goes where capital is treated best.”⁹⁹ Not surprisingly, it is averse to going to countries where laws are damaging to business and exchange controls could prevent it from repatriating the returns it has made. He adds:

“In a globally interconnected world, investment tends to go towards countries that protect private property rights, where local laws are rational, transparent, and enforceable, and where the returns on capital can be realised and expatriated.

⁹⁶ John Endres, “Bitcoin: The freedom money that wants to change the world,” Daily Friend, 5 March 2026.

<https://dailyfriend.co.za/2026/03/05/bitcoin-the-freedom-money-that-wants-to-change-the-world/>.

⁹⁷ “Youth joblessness is SA’s biggest political risk”; Statistics South Africa, “Quarterly Labour Force Survey: Q2, 2026,” Statistical Release P0211, 11 August 2026.

<https://www.statssa.gov.za/publications/P0211/P02111stQuarter2026.pdf>.

⁹⁸ Endres, “Bitcoin: The freedom money that wants to change the world,” op. cit.

⁹⁹ Vegter, I, “The National Treasury is coming for your Bitcoins,” Daily Friend, 1 May 2026.

<https://dailyfriend.co.za/2026/05/01/treasury-is-coming-for-your-bitcoins/>.

It's a counterintuitive point. Countries that make it easier to take money out are more likely to convince investors to put it in. Panama, Singapore, Mauritius, and the United Arab Emirates are global trade and financial hubs for this exact reason.

As economist Chris Hart [posted on X.com](#): 'There is only one purpose for capital controls – that is to shield bad policies. Countries with good policies have no need for capital controls.' Hart is right...

Government's efforts to weaken, rather than strengthen, private property rights, its willingness to impose extractive policies such as Black Economic Empowerment (BEE), and its punitive tax regime make it a hard sell for investors. Its latest attack on cryptocurrency further weakens the investment case."¹⁰⁰

Against this background, South Africa needs to jettison its exchange control regulations, not seek to tighten them up. Its existing exchange control regulations were introduced by the National Party government in 1961 to curb capital flight during the apartheid era. When it came to power in 1994, the African National Congress (ANC) government could have dispensed with these apartheid era rules. Instead, it retained them, saying this was needed to maintain macroeconomic stability. More than 30 years after the political transition, these “anachronistic controls” remain in place, notes Mr Ansara.¹⁰¹

Western democracies do not apply comprehensive exchange controls of the kind introduced in South Africa in 1961 and now to be significantly extended under the Manual and the Regulations. There are no equivalent controls in the US, the United Kingdom (UK) or member states within the European Union (EU). Instead, these countries have carefully targeted financial controls aimed at countering money-laundering, inhibiting the funding of terrorism or enforcing financial sanctions against specified countries and individuals. Significant cash transactions must thus be declared, but the thresholds for reporting are relatively high: £10,000 in the UK, \$10,000 in the US and €10,000 in the EU. (These sums, in rand values, range from about R160,000 to R200,000.) Moreover, these rules have been adopted for criminal justice and national security reasons. They are not macroeconomic tools intended to keep capital corralled within these countries.¹⁰²

By contrast, countries with extensive exchange controls include Cuba, China, Iran, Russia, South Africa, Venezuela and Zimbabwe. South Africa ought to be seeking to distance itself from these countries by abandoning its current exchange controls, not extending them.

Since 1994, however, South Africa has kept its apartheid era exchange controls firmly in place. All it has done, from time to time, is to loosen some limits on capital outflows. In 2010, for example, the limit on how much South Africans could send abroad was raised to R1 million a year. In March 2026, that limit was finally raised to R2 million a year. However, this increase barely compensates for consumer inflation and the declining value of the rand over the intervening 16 years. An additional R10 million can also be taken out, but only with the permission of the South African Reserve Bank.¹⁰³

¹⁰⁰ Ibid.

¹⁰¹ Ansara, “The State Is Coming For Your Bitcoin,” op. cit.

¹⁰² Vegter, “The National Treasury is coming for your Bitcoins,” op. cit.

¹⁰³ Ibid; Camay, A. and Ahmed, A, “Extending boundaries: Adjustments to South African exchange control limits and powers,” ENSight, 13 March 2026. <https://www.ensafrica.com/news/detail/11456/extending-boundaries-adjustments-to-south-afr>.

The fact remains, however, that capital is most easily attracted to countries – such as Singapore, Switzerland, and Mauritius – that do not try to lock capital in via extensive exchange controls and coercive regulation. Hence, by further extending its existing restrictions – rather than jettisoning its exchange controls – South Africa risks isolating its domestic fintech ecosystem and deterring essential FDI, especially in the crucial tech sector.

7 The way forward

The SARB has no legislative authority to introduce the Manual. Both it and the National Treasury lack the capacity to make new rules regarding crypto assets. Instead, these rules – if they are to be adopted at all – must be enacted by Parliament under the separation-of-powers doctrine. As earlier noted, it is also difficult to understand how, in a constitutional democracy founded on “the supremacy of the rule of law,”¹⁰⁴ the provisions of the Manual can “have no statutory force” and yet also “have the effect of law”, as the SARB claims.

The SARB’s tick-box approach to public consultation has resulted in further procedural unconstitutionality. By failing to provide a comprehensive socio-economic impact assessment of the Manual and its likely costs and consequences, the SARB has failed to provide the public with the information it needs to “know about the issues” and then to have an “adequate say.” The Manual is thus as procedurally unconstitutional, under Section 195(1)(e) of the Constitution, as other laws the Constitutional Court has struck down for similar failures.

The Manual is substantively unconstitutional as well. Its key purpose is to introduce new rules on when crypto assets will be “deemed” to have been “exported.” These deeming clauses will trigger the implementation of provisions in the Regulations regarding searches, seizures, forced disclosures of private passwords and unwarranted forfeitures of crypto assets. Yet these provisions are clearly unconstitutional. A Manual whose main purpose is to unleash unconstitutional interventions by state entities is itself unconstitutional too.

In addition, the Manual’s rules will incorporate the names, addresses and holdings of crypto owners into records that have no specified safeguards. This exposing those owners to the risk of the violent crimes, described in *Section 6.1*, and is likely to put the SARB in breach of Section 12 of the Constitution, which includes the right “to be free from violence from either public or private sources.”¹⁰⁵

In addition, the Manual is clearly economically unwise. It will cripple, if not destroy, South Africa’s fledgling crypto industry, which should instead be encouraged to prosper and grow. It will further alienate prospective foreign direct investors, particularly in tech sectors. This will make it even harder to raise the rate of fixed investment from a dismal 13.7% of GDP in 2025 to the 30% rate recommended by the NDP. Yet, without a doubling in fixed investment, the growth rate will stay at its current low levels, the unemployment rate will not come down, and some 8.5 million jobless South Africans will remain mired in destitution and despair.

The Manual, like the Regulations it is intended to accompany, should simply be withdrawn. South Africa’s antiquated exchange controls should then also be repealed. Instead of adding further to an already crippling burden of regulation, the Government of National Unity should focus on fulfilling the promises it has made to increase growth, reduce debilitating joblessness, counter poverty and put the country on the proven path to prosperity.

¹⁰⁴ Section 1(c), Constitution of the Republic of South Africa, 1996.

¹⁰⁵ Section 12(1)(c), Constitution.

Should the Manual and the Regulations nonetheless proceed in some form, far more must be done to protect the privacy and the physical safety of crypto holders. As shown in *Section 6.1*, the declarations and reports these instruments require would gather the names, addresses and holdings of crypto owners into records that have no specified safeguards. They would do so in a country where kidnapping for money is already a burgeoning criminal industry. At a minimum:

1. Regulation 10 should be deleted, or confined to holdings above a substantial threshold, and no person should be required to disclose where a crypto asset is held.
2. Transfers by individuals to their own non-custodial wallets should be reportable only above a substantial threshold. Since the Manual states that FinSurv reporting serves a statistical purpose, FinSurv should receive aggregated data wherever possible.
3. The Regulations should contain binding provisions on the confidentiality and security of all declared and reported information. These should include logging of every access, a maximum retention period, and notification of affected persons within a fixed period after any breach, and should be no weaker than Sections 19 and 22 of the Protection of Personal Information Act.
4. Unauthorised access to, or disclosure of, this information by officials, CASP staff or their contractors should be a specific offence attracting a heavy penalty.
5. Neither the National Treasury nor the SARB should compile a central register of the wallet addresses of self-custody holders.

These safeguards would reduce the risk but would not removing it. The surest protection is not to require the compilation of such records at all, when experience shows that they cannot be kept safe.