cryptoassets.co.za

15 May 2026
info@cryptoassets.co.za
https://cryptoassets.co.za

Comments on the Draft Capital Flow Management Regulations (Government Gazette, April 2026)

For the attention of

Dr. Duncan Pieterse
The Director-General, National Treasury

and

Lesetja Kganyago
Governor of the South African Reserve Bank (SARB)

Thank you for the opportunity to provide comments on the Draft Capital Flow Management Regulations.

This submission focuses on the technical and operational characteristics of crypto asset systems and their implications for the enforceability of the proposed regulations.

The CryptoAssets Association represents the interests of South African users and businesses innovating with crypto assets, who share a need for clarity and certainty in legislation, balanced against a desire for efficiency and waste avoidance in terms of unnecessary spending.

We are an unincorporated association of persons, with 19 members, formed in 2019 to provide a collective response to the Crypto Assets Regulatory Working Group position paper on crypto assets.

Our membership consists of persons who run Bitcoin and Lightning nodes, offer liquidity services over the Lightning Network, perform self-custody, stake Ethereum, own NFTs, and interact with smart contracts.

We also trade crypto assets on a peer to peer basis, and on exchanges.

The organisation stores its funding in a multisignature wallet.

We made submissions in earlier processes, specifically a response to the CAR WG proposed crypto assets regulations[1], and a response to the FSCA Draft Declaration of Crypto Assets as a Financial Product[2].

We are concerned that the Draft Capital Flow Management Regulations will negatively impact the interests of members, which they have been practising for more than 12 years in some cases, such as self-custody, or running nodes.

For the purposes of this response, we will confine ourselves to the crypto assets provisions as they relate to Bitcoin and the Lightning Network, along with Ethereum.

Sincerely,
Bretton Vine
General Manager

(continued on next page)

1 http://cryptoassets.co.za/wp-content/uploads/2019/02/Cryptoassets.co_.za-response-CAR-WG-proposed-crypto-regs_20190215-redacted-version.pdf

2 https://cryptoassets.co.za/wp-content/uploads/2021/01/cryptoassets.co_.za_Response_FSCA_Draft_Declaration_of_crypto_assets.pdf

15 May 2026
info@cryptoassets.co.za
https://cryptoassets.co.za

Executive Summary

This submission sets out technical, legal, and practical concerns regarding the application of the Draft Capital Flow Management Regulations to crypto assets, specifically Bitcoin, the Lightning Network, and Ethereum.

The central issue is that the regulatory framework assumes the existence of visibility, control, and enforceability mechanisms that do not exist in decentralised crypto asset systems.

Key Findings

1. Structural Mismatch Between Regulation and Technology
   The regulations are based on a custodial, intermediary-driven financial model, whereas crypto asset systems are decentralised and peer-to-peer. As a result, many provisions cannot be consistently applied to non-custodial activity.
2. Limited Enforceability in Practice
   Several requirements, such as prior approval before transacting, forced transfer of assets, and full disclosure of holdings, lack practical enforcement mechanisms. In many cases, compliance cannot be reliably detected, prevented, or verified.
3. Jurisdictional and Classification Challenges
   Concepts such as "export", "import", and geographic location do not align with the non-territorial nature of distributed ledger systems. In addition, crypto assets are defined as not being currency, yet are treated as such in the application of capital controls, creating internal inconsistency.
4. Constraints on Search, Seizure, and Compelled Disclosure
   Crypto assets are controlled by private keys, not physical possession. As a result, search and seizure powers do not guarantee access or control, and compelled disclosure of credentials cannot be reliably verified for completeness.

5. Limitations of Threshold-Based Controls
   Transaction fragmentation, address multiplicity, and routing techniques (including Lightning Network multi-path payments) allow users to structure activity in ways that circumvent threshold-based restrictions.
6. Incompatibility with Decentralised and Off-Chain Systems
   Smart contracts on Ethereum and off-chain protocols such as the Lightning Network operate without identifiable counterparties or central control points, limiting the applicability of transaction-level regulatory controls.
7. Selective and Uneven Enforcement Risk
   The framework is more readily enforceable against users operating within regulated custodial environments, while non-custodial and decentralised activity remains largely outside practical reach. This may result in uneven application and reduced overall effectiveness.
8. Potential Unintended Economic Consequences
   The combination of limited enforceability and increased compliance burden may incentivise migration toward non-custodial, decentralised, or offshore alternatives, reducing visibility rather than enhancing it.

Conclusion

Taken together, these factors indicate that the draft regulations rely on assumptions about visibility, attribution, and control that are not consistent with the operational characteristics of crypto asset systems. This creates a risk that the framework will be only partially enforceable and may not achieve its intended policy objectives.

(continued on next page)

Recommended Approach

A more effective regulatory strategy would:

- Focus on custodial intermediaries and fiat on/off-ramps where enforceable control points exist.
- Avoid reliance on prior approval mechanisms for decentralised transactions.
- Reconsider the application of territorial concepts to non-geographic systems.
- Limit obligations to those that can be reasonably verified in practice.
- Align definitions and classifications to ensure internal consistency.

Such an approach would better align regulatory objectives with technical realities, while supporting effective oversight and minimising unintended consequences.

The following pages outline the key issues we wish to address.

Core Technical Analysis

Treating crypto assets like custodial financial infrastructure

> 3. (1) “No person, other than an authorised crypto asset service provider, may buy, sell, borrow, or lend any crypto assets from, in an amount or with a value in excess of a determined threshold, to any person other than an authorised crypto asset service provider, subject to the provisions of subregulation (3) and regulation 23(6)”

The draft regulations appear to assume that crypto asset transactions can be intermediated in a manner analogous to traditional banking systems, via "authorised crypto asset service providers", as reflected in the restriction that no person may buy, sell, borrow, or lend crypto assets except through such providers.

This assumption is not consistent with system design. Bitcoin and Ethereum are fundamentally peer-to-peer protocols, where transactions are broadcast directly to a distributed network, included in blocks by miners or validators, and validated by nodes.

No intermediary is required or necessarily involved.

This creates a fundamental distinction between custodial and non-custodial systems.

While transactions conducted through custodial service providers (such as exchanges) may be observable and subject to regulatory control, non-custodial usage, including self-custody wallets, Lightning Network payments, and smart contract interactions, operates independently of any intermediary.

As a result, the restriction in Regulation 3.(1) cannot be effectively applied to a substantial portion of crypto asset activity.

It cannot reliably detect, prevent, or verify compliance in relation to direct peer-to-peer transfers, off-chain Lightning transactions, or interactions with decentralised protocols.

Furthermore, crypto assets may be acquired through mechanisms that do not involve any service provider at all.

These include mining (in the case of Bitcoin), staking (in the case of Ethereum), and direct receipt of funds via wallet addresses or Lightning invoices.

The regulatory model therefore assumes a hub-and-spoke financial architecture, whereas crypto asset systems operate as decentralised mesh networks.

This mismatch creates a structural limitation, where the regulations can only apply to a subset of activity (primarily custodial intermediaries), while leaving non-custodial activity outside the scope of effective enforcement.

This risks creating a regulatory framework that is both under-inclusive (failing to capture large portions of activity) and over-restrictive (imposing obligations that cannot realistically be complied with).

(continued on next page)

Self-Custody Withdrawals: Ambiguity in Application of Regulation 3(1)

> 3. (1) "No person, other than an authorised crypto asset service provider, may buy, sell, borrow, or lend any crypto assets from, in an amount or with a value in excess of a determined threshold, to any person other than an authorised crypto asset service provider, subject to the provisions of subregulation (3) and regulation 23(6)"

Regulation 3(1) restricts the buying, selling, borrowing, or lending of crypto assets above a determined threshold to transactions conducted through authorised crypto asset service providers.

However, the application of this provision to routine custody transitions is unclear, particularly in the context of withdrawals from custodial platforms to self-custody wallets.

A common and fundamental activity in crypto asset systems is the withdrawal of assets from an exchange or other custodial service provider to a wallet controlled directly by the user (for example, a hardware wallet). This represents a transfer from an authorised crypto asset service provider to a non-authorised person.

It is not clear how such a transaction is intended to be classified under Regulation 3(1):

- It does not constitute a sale, as there is no exchange of value at the point of withdrawal;
- It does not constitute lending, as no obligation to return the asset arises;
- It is not clearly a transfer between two authorised parties, as the recipient is a private individual operating in a non-custodial capacity.

If interpreted strictly, the provision may prohibit or restrict withdrawals above the determined threshold from authorised service providers to self-custody wallets, as the recipient is not an authorised crypto asset service provider.

This creates a significant ambiguity, as self-custody is a fundamental feature of crypto asset systems and is widely regarded as a core user right and security practice.

From a practical perspective, the inability to withdraw assets to self-custody would:

- materially alter the nature of ownership, effectively requiring users to retain assets within custodial environments;
- increase counterparty risk by limiting users' ability to control their own assets; and
- diverge from the operational design of crypto asset systems, which are built to enable direct ownership and control via private keys.

It is therefore unclear whether the intention of Regulation 3(1) is to restrict such withdrawals, or whether this is an unintended consequence of drafting that assumes all transfers occur between intermediated parties.

A clarification of the treatment of withdrawals to self-custody wallets may be necessary to ensure that the regulation does not inadvertently prohibit or constrain ordinary and essential user behaviour within crypto asset systems.

(continued on next page)

No Practical Enforcement: “Apply to a Provider Before Transacting”

> 3. (4) Every person other than an authorised crypto asset service provider intending to buy, sell, borrow, or lend crypto assets must apply to an authorised crypto asset service provider, and must furnish the information and submit those documents that the authorised crypto asset service provider may require for the purpose of ensuring compliance with any conditions determined under subregulation (2).

This provision assumes the existence of a practical control point through which such transactions must pass.

In decentralised crypto asset systems, no such control point exists.

Wallet software (including Bitcoin Core, LND, and Ethereum-compatible wallets such as Metamask) operates without identity verification, permissioning, or communication with any central authority.

Transaction creation is a local cryptographic operation requiring only possession of a private key.

Once signed, transactions may be broadcast through a variety of channels, including public nodes, anonymisation networks such as Tor, virtual private networks, or even indirect methods such as QR codes or airgapped transfers.

In addition, crypto assets may be acquired without interacting with any service provider at all, including through mining, staking, or direct receipt from another party.

As a result, there is no identifiable stage at which a user can be required, in practice, to seek prior approval before transacting.

The provision therefore lacks a practical enforcement mechanism: it cannot reliably detect when a user intends to transact, cannot prevent the transaction from occurring, and cannot verify whether prior approval was obtained.

This creates a structural asymmetry in enforcement, where only users who voluntarily engage with custodial service providers are subject to the requirement, while non-custodial users remain outside its effective scope.

The likely outcome is not universal compliance, but selective applicability, where compliant users are burdened while non-compliant users are not meaningfully constrained.

This risks undermining both the effectiveness and fairness of the regulatory framework.

(continued on next page)

Misunderstanding Custody: "Offer crypto assets for sale to Treasury"

> "3. (6)
> (a) If a person has, as a result of an application made in terms of subregulation (4), obtained from an authorised crypto asset service provider any crypto assets and no longer requires all or any part of that crypto assets for the purpose stated in their application, that person must immediately offer for sale to the National Treasury or an authorised crypto asset service provider those crypto assets; and
> (b) the crypto assets referred to in paragraph (a) may be repurchased in South African Rand at the price at which it was sold to that person or at another price that the National Treasury or the authorised crypto service provider may determine."

This provision assumes that crypto assets can be controlled, transferred, or taken into possession in a manner analogous to funds held within a custodial financial institution. This assumption does not reflect the technical reality of crypto asset systems.

Crypto assets are controlled through possession of private keys. Ownership, in practical terms, is the ability to authorise a transaction by signing it with the relevant key. There is no central authority or intermediary capable of transferring assets without such authorisation.

As a result, there is no mechanism by which the National Treasury or any other party can compel the transfer of crypto assets without voluntary cooperation, or disclosure of private keys.

Similarly, transactions cannot be reversed without undertaking a prohibitively expensive, and practically infeasible, attack on the underlying network.

Even where crypto assets are declared, control may be constrained by technical factors, including multisignature arrangements requiring multiple independent parties, time-locked contracts, staking conditions, or funds committed to Lightning Network channels or smart contracts.

These constraints may place assets beyond immediate transferability, irrespective of legal requirements.

This creates a fundamental limitation in enforceability: the regulation cannot reliably compel transfer, cannot verify that all relevant assets have been disclosed, and cannot ensure compliance in cases where control is distributed or partially externalised.

The provision therefore treats crypto assets as if they were custodial balances or centrally controlled instruments, when in fact they function as bearer cryptographic assets.

This mismatch introduces significant practical limitations, and may raise concerns where individuals are required to relinquish control of assets that cannot be accessed or transferred without their cooperation.

This may also raise broader legal considerations where individuals are required to dispose of or transfer assets over which control cannot be externally exercised, including potential implications for property rights.

(continued on next page)

Category Error: “Export” and “Import” of Crypto Assets

> "4. (1) Subject to regulation 23(7), a person may not, except with the permission of the National Treasury or an authorised person, and in accordance with those conditions that the National Treasury or authorised person may impose–
>
> (a) take, send out or remove currency, crypto assets, gold or securities from the Republic;
>
> (b) transfer any securities to a person outside of the Republic;
>
> (c) send, consign, give or deliver currency, crypto assets, gold or securities to any person for the purpose of removing the currency, crypto assets, gold or securities from the Republic;
>
> (d) make payment to, or in favour of, or on behalf of a person resident outside of the Republic, or place any amount, either in currency, crypto assets, gold or securities, to the credit of a person outside of the Republic;
>
> ..."

This provision applies a territorial concept of movement to a system that is not geographically bounded.

Crypto assets do not exist in a specific physical location. They exist as entries on a globally distributed ledger, replicated across nodes in multiple jurisdictions simultaneously.

A transaction involving crypto assets is not the movement of an object from one place to another, but rather a state transition within a distributed system.

As such, the concepts of "export" and "import" do not map cleanly onto the underlying technology.

This creates a jurisdictional ambiguity: it is not possible, at the protocol level, to determine whether a crypto asset is located within the Republic prior to a transaction, nor whether it has been "sent out" of the Republic thereafter.

The challenge is further compounded in systems such as the Lightning Network, where payments are routed across multiple intermediary nodes using onion routing.

Each participant in the routing process only has visibility into the immediately adjacent nodes, and no participant has full knowledge of the origin, destination, or complete path of a payment.

As a result, there is no reliable mechanism to identify, track, or enforce cross-border movement of crypto assets in the manner contemplated by traditional capital flow controls.

The application of export and import concepts to crypto assets therefore introduces a category mismatch, where a framework designed for physically or jurisdictionally located assets is applied to a non-territorial, decentralised system.

This limits the practical enforceability of such provisions and may result in inconsistent or arbitrary application.

Physical Search Powers vs Cryptographic Reality

> 4. (3) An enforcement officer may search any person or any article in that person's possession or under their control for the purpose of ascertaining whether the person possesses or has control of any currency, crypto assets, gold and securities -
>
> (a) if that person has denied the possession or control of any foreign currency, crypto assets, gold or security; and
>
> (b) if the enforcement officer suspects, on reasonable grounds, that the person is in possession or control of any currency, crypto assets, gold or securities; and
>
> (4) A person may not be searched by a person of a different gender; and if there is no enforcement officer of the same gender available, the enforcement officer may authorise any person of the same gender as the person to be searched, to perform the search.
>
> (5) An enforcement officer may seize any currency, crypto assets, gold or securities found in the possession or under the control of any person, if the enforcement officer on reasonable grounds suspects that the currency, crypto assets, gold or securities are to be removed from the Republic in contravention of these Regulations.

These powers are premised on the assumption that crypto assets can be located, accessed, and seized in a manner analogous to physical property or traditional financial instruments. This assumption does not reflect the technical reality of crypto asset systems.

Crypto assets are not stored as physical objects, but are controlled through cryptographic credentials, typically in the form of private keys or seed phrases. These credentials may be stored on encrypted devices, distributed across multiple locations, or even memorised by an individual.

While a physical search may locate devices or written records, such a search does not necessarily provide access to the underlying crypto assets.

Access requires knowledge of the relevant cryptographic keys, which cannot be derived, reconstructed, or bypassed through physical inspection alone.

This creates a fundamental distinction between the ability to search and the ability to access or control an asset.

In the absence of voluntary disclosure, there is no reliable method for an enforcement officer to access or seize crypto assets, even where their existence is suspected.

In addition, crypto assets may be subject to technical constraints that further limit access or transferability, including multisignature requirements, time-locked contracts, staking conditions, or Lightning Network channel states that automatically penalise unauthorised access attempts by allocating the funds to the other party.

As a result, the practical effect of these provisions is limited: they cannot reliably detect the presence of crypto assets, cannot ensure access to those assets, and cannot guarantee their seizure.

The application of traditional search and seizure concepts to cryptographic assets therefore introduces a significant mismatch between legal authority and technical capability, with potential implications for the effectiveness and proportionality of enforcement measures.

These limitations may also engage broader considerations relating to the right to privacy, particularly where access depends on disclosure of personal cryptographic credentials.

Forced Disclosure of Keys

"4. (3) An enforcement officer may search any person or any article in that person's possession or under their control for the purpose of ascertaining whether the person possesses or has control of any currency, crypto assets, gold and securities–

(a) if that person has denied the possession or control of any foreign currency, crypto assets, gold or security; and

(b) if the enforcement officer suspects, on reasonable grounds, that the person is in possession or control of any currency, crypto assets, gold or securities; and

(5) An enforcement officer may seize any currency, crypto assets, gold or securities found in the possession or under the control of any person, if the enforcement officer on reasonable grounds suspects that the currency, crypto assets, gold or securities are to be removed from the Republic in contravention of these Regulations.

(6) An enforcement officer may–

(a) examine or search any goods consigned, letters or parcels sent from the Republic to a destination outside the Republic for the purpose of ascertaining whether those goods consigned, letters or parcels contain any currency, crypto assets, gold or securities; and

…

20. (1) The National Treasury, or any person authorised by the National Treasury, may order any person to furnish any information in any manner at such person's disposal which the National Treasury or such authorised person deems necessary for the purposes of these regulations."

The draft regulations require that persons furnish passwords or other information necessary to enable access to crypto assets.

This provision assumes that access credentials for crypto assets can be disclosed in a complete, verifiable, and enforceable manner.

In practice, this assumption does not hold.

Private keys, which control access to crypto assets, are not centrally stored and cannot be derived or reset. They may be stored across multiple devices, secured through encryption, or represented by seed phrases that can be memorised and not recorded in any physical form.

In addition, control of crypto assets may be distributed across multiple parties through multisignature arrangements, where several independent key holders are required to authorise a transaction. These parties may reside in different jurisdictions and may not be subject to the same legal obligations.

This creates a fundamental limitation in both compulsion and verification. Even where a person is required to disclose access credentials, there is no practical mechanism to ensure that all relevant keys have been disclosed, or that disclosure is complete. Partial disclosure cannot be distinguished from full compliance.

As a result, the provision cannot be reliably enforced: it cannot guarantee access to the assets in question, and cannot verify whether a person has complied fully with the requirement.

These limitations may also raise broader considerations where individuals are compelled to disclose cryptographic credentials that provide control over their assets, including implications relating to privacy and the extent to which such disclosure can be required and verified in practice.

This may engage constitutional considerations, including the right to privacy and protections against compelled self-incrimination, particularly where disclosure of credentials is the only means of accessing or controlling the asset.

(continued on next page)

Declaration Requirements vs Protocol Privacy

"10. (1)

(a) Every person in the Republic must, within 30 days or such period that may be prescribed, after obtaining control, or possession or becoming entitled to sell, procure the sale of, or transfer, any foreign asset or crypto asset, make a declaration in writing, in the form and manner prescribed to the National Treasury or to an authorised person; and

(b) The declaration must state–

(i) when the foreign asset or crypto asset was acquired;

(ii) how the foreign asset or crypto asset was acquired;

(iii) where the foreign asset or crypto asset is held; and

(iv) whether the foreign asset or crypto asset is held as cover for or in respect of any foreign liability.

(2) Any foreign asset or crypto asset in respect of which a declaration has been made in terms of subregulation (1) may not be sold, transferred or otherwise disposed of without the permission of the National Treasury or an authorised person and in accordance with those conditions that the National Treasury or authorised person may impose.

(3) Any foreign asset or crypto asset in respect of which a declaration has been made in terms of subregulation (1) may only be sold, transferred or otherwise disposed of in accordance with those conditions that the National Treasury or authorised person may impose."

The draft regulations require persons to declare the acquisition, location, and holding of crypto assets.

This requirement assumes that crypto asset ownership can be identified, located, and verified in a manner comparable to traditional financial accounts.

In practice, this assumption does not hold.

Crypto asset systems are designed around pseudonymous identifiers. Blockchain addresses are not inherently linked to real-world identities, and users can generate an unlimited number of new addresses without restriction.

It is therefore not possible to reliably associate all addresses controlled by a given individual with that individual.

The concept of "location" is similarly problematic. Crypto assets do not reside in a physical or jurisdictional space. A wallet is not a location, and control of assets may be distributed across devices, jurisdictions, or cryptographic arrangements that do not correspond to geographic boundaries.

In addition, users may employ privacy-enhancing techniques such as address rotation, CoinJoin transactions (in Bitcoin), mixer protocols (in Ethereum), or off-chain Lightning Network payments. These mechanisms are specifically designed to reduce traceability and obscure transaction flows.

This creates a fundamental limitation in both identification and verification. Even when a declaration is made, there is no practical mechanism to confirm that all relevant holdings have been disclosed, or that the declared information is complete.

The regulation therefore assumes an account-based model of traceability, where ownership and location can be clearly identified and verified.

Crypto asset systems, by contrast, operate on models such as UTXO[3] or account abstraction, with optional privacy layers that limit visibility and attribution.

As a result, the declaration requirement cannot be reliably enforced in a complete or verifiable manner.

This may result in inconsistent compliance outcomes, where accurate disclosure cannot be distinguished from partial or incomplete reporting.

(continued on next page)

[3] https://en.wikipedia.org/wiki/Unspent_transaction_output

Administrative Impracticality

Administrative Impracticality of Universal Declaration Requirements

10. (1)
(a) Every person in the Republic must, within 30 days or such period that may be prescribed, after obtaining control, or possession or becoming entitled to sell, procure the sale of, or transfer, any foreign asset or crypto asset, make a declaration in writing, in the form and manner prescribed to the National Treasury or to an authorised person; and
(b) The declaration must state–
(i) when the foreign asset or crypto asset was acquired;
(ii) how the foreign asset or crypto asset was acquired;
(iii) where the foreign asset or crypto asset is held; and
(iv) whether the foreign asset or crypto asset is held as cover for or in respect of any foreign liability.

Read literally, this requirement applies to every instance of acquisition, regardless of value or context.

This would include, for example:

- a retail purchase of a small amount of Bitcoin on a local exchange,
- receipt of crypto assets via a peer-to-peer transaction,
- rewards earned through staking or liquidity provision, and
- incremental balances received through Lightning Network activity or other protocol-level participation.

As a result, even low-value transactions, such as the purchase of R100 worth of Bitcoin, would trigger a mandatory declaration obligation within 30 days.

In addition, Regulation 10(2) provides that any crypto asset in respect of which a declaration has been made may not be sold, transferred, or otherwise disposed of without the permission of the National Treasury or an authorised person.

Taken together, these provisions create a requirement for continuous reporting and prior approval that would apply to a very large number of ordinary, low-value transactions.

In practice, crypto asset usage in South Africa includes a substantial number of retail participants engaging in frequent, low-value transactions. If Regulation 10 is applied as written, this would result in:

- a potentially very large volume of declarations submitted to the National Treasury,
- repeated filings by the same individuals for successive acquisitions, and
- a corresponding requirement for administrative processing, review, and potential approval of subsequent disposals.

This raises a significant question of administrative feasibility.

It is not clear how such a volume of declarations could be processed, verified, or acted upon within existing institutional capacity. Nor is it clear how compliance could be meaningfully monitored or enforced at this scale.

(continued on next page)

The likely consequences of this requirement include:

- Low levels of compliance, particularly for small-value transactions, due to the administrative burden on individuals;
- Processing bottlenecks, where declarations are submitted but not meaningfully reviewed or actioned;
- Regulatory overload, where the volume of information exceeds the capacity for effective analysis; and
- Erosion of regulatory effectiveness, as the system becomes impractical to operate in a consistent and timely manner.

In addition, the requirement for prior approval before disposal introduces further friction, which may discourage participation in regulated environments and incentivise migration toward non-custodial or less visible alternatives.

While the objective of improving visibility into crypto asset holdings is understandable, the application of a universal, transaction-level declaration requirement does not appear to be practically workable at scale.

A more targeted approach, such as limiting declaration requirements to thresholds, specific types of activity, or custodial intermediaries, may be necessary to ensure that reporting obligations are both meaningful and administratively feasible.

(continued on next page)

Threshold-Based Controls Are Trivially Bypassable

"determined threshold" means a value or amount determined by the Minister of Finance;

3. (1) No person, other than an authorised crypto asset service provider, may buy, sell, borrow, or lend any crypto assets from, in an amount or with a value in excess of a determined threshold, to any person other than an authorised crypto asset service provider, subject to the provisions of subregulation (3) and regulation 23(6).
(2) No person, other than an authorised crypto asset service provider may, except with the permission of the National Treasury or an authorised person, and in accordance with those conditions that the National Treasury or the authorised person may impose, buy, sell, borrow, or lend any crypto assets, in an amount or with a value in excess of a determined threshold, to any person other than an authorised crypto asset service provider, subject to the provisions of subregulation (3).

8. (1) Any person in the Republic who has under their control, obtains possession of, or becomes entitled to sell, procure the sale of, or transfer, any foreign currency or crypto assets in an amount or with a value in excess of the determined threshold must, within 30 days or a longer period that may be prescribed from the date of any of the afore-mentioned events, make a declaration in writing, in the form and manner prescribed by the National Treasury, of the foreign currency or crypto assets to the National Treasury or an authorised person.
(2) Every person in the Republic who obtains possession of, or becomes entitled, as a result of any credit or any balance in any account at any bank outside the Republic, to receive payment of any amount in foreign currency or crypto assets with a value or in an amount in excess of the determined threshold must within 30

days after becoming so entitled, make a declaration in writing, in the form and manner prescribed by the National Treasury, of the right to the National Treasury or an authorised person.

This approach assumes that transactions exceeding a given threshold can be identified and controlled as discrete events. In practice, crypto asset systems do not enforce such constraints.

Transactions can be readily fragmented into multiple smaller transfers, each below the applicable threshold. These transfers may originate from different source addresses and be directed to different destination addresses, with no reliable mechanism to determine that they form part of a single economic transaction.

This fragmentation is not an edge case, but a fundamental feature of crypto asset systems.

In Bitcoin, users can generate new addresses for each transaction, and there is no inherent linkage between those addresses.

In the Lightning Network, payments are routinely split into multiple smaller amounts and routed across different network paths using multi-path payment techniques, before being reassembled at the destination.

As a result, there is no reliable way to detect whether a series of transactions collectively exceeds a regulatory threshold, nor to attribute those transactions to a single user or economic activity.

This creates a structural limitation in the effectiveness of threshold-based controls.

While compliant users interacting with custodial service providers may be subject to such thresholds, non-custodial users can readily

structure transactions to fall below them, without any reduction in overall transaction value.

The result is a control mechanism that is not robust to evasion, and which may disproportionately affect compliant users while failing to achieve its intended regulatory objective.

This undermines the effectiveness of threshold-based regulation as a tool for monitoring or restricting crypto asset flows.

(continued on next page)

Incompatibility with Smart Contracts (Ethereum)

3. (1) No person, other than an authorised crypto asset service provider, may buy, sell, borrow, or lend any crypto assets from, in an amount or with a value in excess of a determined threshold, to any person other than an authorised crypto asset service provider, subject to the provisions of subregulation (3) and regulation 23(6).

(2) No person, other than an authorised crypto asset service provider may, except with the permission of the National Treasury or an authorised person, and in accordance with those conditions that the National Treasury or the authorised person may impose, buy, sell, borrow, or lend any crypto assets, in an amount or with a value in excess of a determined threshold, to any person other than an authorised crypto asset service provider, subject to the provisions of subregulation (3).

(3)

(a) An authorised crypto asset service provider may only engage in those actions in which the authorised crypto asset service provider has expressly been authorised to perform in terms of the appointment as an authorised crypto asset service provider;

(b) an authorised crypto asset service provider may not buy, sell, borrow, lend, receive or deliver any crypto asset, except for those purposes or on those conditions that the National Treasury may determine; and

(c) the National Treasury may, in its discretion, in writing prohibit all authorised crypto asset service
providers or any one or more authorised crypto asset service provider–

(i) from buying, selling, borrowing, lending, receiving or delivering, from any specified person, fund or foreign government any crypto asset; or

(ii) from buying, selling, borrowing, lending, receiving or delivering any crypto asset for any specified purpose, except for those purposes or on conditions that the National Treasury may determine.

(4) Every person other than an authorised crypto asset service provider intending to buy, sell, borrow, or lend crypto assets must apply to an authorised crypto asset service provider, and must furnish the information and submit those documents that the authorised crypto asset service provider may require for the purpose of ensuring compliance with any conditions determined under subregulation

4. (1) Subject to regulation 23(7), a person may not, except with the permission of the National Treasury or an authorised person, and in accordance with those conditions that the National Treasury or authorised person may impose—

(a) take, send out or remove currency, crypto assets, gold or securities from the Republic;
(b) transfer any securities to a person outside of the Republic;
(c) send, consign, give or deliver currency, crypto assets, gold or securities to any person for the purpose of removing the currency, crypto assets, gold or securities from the Republic;
(d) make payment to, or in favour of, or on behalf of a person resident outside of the Republic, or place any amount, either in currency, crypto assets, gold or securities, to the credit of a person outside of the Republic;
(e) draw or negotiate any bill of exchange or promissory note, transfer security, or acknowledge any debt so that a right (whether actual or contingent) on

the part of such person or any other person to receive a payment in the Republic is created or transferred as consideration-

(i) for the receiving by such person or any other person of a payment or the acquisition by such person or any other person of property, outside the Republic; or

(ii) for a right (whether actual or contingent) on the part of such person or any other person to receive a payment or acquire property outside the Republic;

or make or receive any payment as such consideration;

10. (1)

(a) Every person in the Republic must, within 30 days or such period that may be prescribed, after obtaining control, or possession or becoming entitled to sell, procure the sale of, or transfer, any foreign asset or crypto asset, make a declaration in writing, in the form and manner prescribed to the National Treasury or to an authorised person; and

(b) The declaration must state–

(i) when the foreign asset or crypto asset was acquired;

(ii) how the foreign asset or crypto asset was acquired;

(iii) where the foreign asset or crypto asset is held; and

(iv) whether the foreign asset or crypto asset is held as cover for or in respect of any foreign liability.

(2) Any foreign asset or crypto asset in respect of which a declaration has been made in terms of subregulation (1) may not be sold, transferred or otherwise disposed of without

> the permission of the National Treasury or an authorised person and in accordance with those conditions that the National Treasury or authorised person may impose.
> (3) Any foreign asset or crypto asset in respect of which a declaration has been made in terms of subregulation (1) may only be sold, transferred or otherwise disposed of in accordance with those conditions that the National Treasury or authorised person may impose.

The draft regulations assume that crypto asset transactions involve identifiable counterparties and, where applicable, intermediaries such as authorised service providers.

This assumption does not fully account for the operation of smart contract platforms such as Ethereum.

Ethereum enables the deployment of autonomous programs ("smart contracts") that execute deterministically when predefined conditions are met.

These contracts can facilitate financial activities including lending, trading, liquidity provision, and governance, without requiring a central operator or identifiable counterparty.

In many cases, interactions occur directly between a user and a deployed smart contract, rather than between two identifiable persons.

The contract itself is not a legal entity, cannot be regulated in the conventional sense, and may be deployed and accessed globally without regard to jurisdiction.

This creates a fundamental mismatch with regulatory provisions that rely on the identification of counterparties, the involvement of

authorised service providers, or the ability to impose permissions or conditions prior to execution.

Once deployed, a smart contract operates autonomously and cannot be selectively prevented from executing transactions based on external regulatory requirements.

There is no central party capable of enforcing compliance or restricting access.

As a result, the regulatory framework cannot be consistently applied to interactions with decentralised protocols, as it assumes a level of control and attribution that does not exist in such systems.

This limits the applicability of the framework to centralised intermediaries, while excluding a growing portion of decentralised financial activity.

(continued on next page)

Lightning Network Presents Structural Visibility Limits

> (Draft regulations 3, 4, 10, mentioned in previous item omitted from repetition for brevity)

The draft regulations assume that crypto asset transactions can be observed, attributed to specific parties, and subjected to regulatory controls based on that visibility.

This assumption does not hold in the context of the Lightning Network.

The Lightning Network is a second-layer protocol built on Bitcoin, enabling off-chain transactions through a network of payment channels.

Unlike on-chain transactions, there is no global ledger of Lightning payments. Transactions are not publicly recorded in a manner that allows for retrospective analysis or attribution.

Payments are routed across multiple intermediary nodes using onion routing. Each node in the path is only aware of the node from which it received a payment and the node to which it forwards the payment.

No participant has visibility into the full path, origin, or final destination of the transaction.

As a result, it is not possible to reliably identify the sender or receiver of a Lightning payment, determine the jurisdiction of the parties involved, or reconstruct the full transaction flow.

This creates a fundamental limitation in enforcement. The regulatory framework cannot observe Lightning transactions, cannot attribute them to specific users, and cannot apply or verify compliance with transaction-level controls.

The model therefore assumes a level of transactional visibility that is not present in off-chain systems such as the Lightning Network, limiting its applicability to such environments.

This effectively places a growing class of crypto asset activity outside the scope of meaningful enforcement under the proposed framework.

(continued on next page)

Definitional Concerns

Material Uncertainty: Indeterminate "determined threshold"

> "determined threshold" means a value or amount determined by the Minister of Finance;

The definition of "determined threshold" as a value set by the Minister of Finance introduces material uncertainty, as no specific value, methodology, or adjustment mechanism is provided in the draft regulations.

This creates difficulty in assessing the scope and impact of the regulations, as stakeholders cannot determine in advance whether they will fall within the regulatory threshold.

While existing capital control frameworks provide defined thresholds (such as the R2 million single discretionary allowance and R10 million foreign capital allowance[4]), no equivalent clarity is provided here.

In the context of crypto assets, this lack of specificity is particularly problematic due to their inherent price volatility.

For example, Bitcoin follows a predictable issuance schedule (commonly referred to as “the halving” approximately every four years), which has historically been associated with significant price appreciation.

As a result, a static Rand-denominated threshold will, over time, capture an expanding population of users purely as a function of market price movements, rather than any change in behaviour, or risk profile.

[4] https://www.resbank.co.za/content/dam/sarb/what-we-do/financial-surveillance/financial-surveillance-documents/2026/6-2026.pdf

This creates a form of arbitrary regulatory expansion, where individuals may become subject to reporting or compliance obligations, solely due to asset price appreciation beyond their control.

In order to maintain consistency, the threshold would require frequent adjustment to reflect market conditions.

Failing this, the regulations risk imposing an increasing administrative burden on both users and regulators, while reducing the effectiveness of any threshold-based control mechanism.

The absence of defined criteria for setting and adjusting the threshold also raises concerns regarding legal certainty and the potential for inconsistent or arbitrary application.

(continued on next page)

Definition of "Affected Person": Unintended Scope and Application to Decentralised Systems

> "affected person" means a deceased estate, or a juristic person, foundation, unincorporated association of persons, trust or partnership operating or vested in the Republic–
>
> (a) of which 75% or more of the capital, assets, or earnings may be used for payment to, or for the benefit of, any person who is not resident in the Republic; or
>
> (b) of which 75% or more of the securities, voting rights, capital, assets or earnings, are directly or indirectly vested in, or controlled by or on behalf of any person who is not resident in the Republic;

This definition may have unintended and far-reaching implications when applied to crypto asset systems and organisations operating within this ecosystem.

The CryptoAssets Association itself is an unincorporated association of persons and holds funds in a multisignature wallet. These funds include Bitcoin, which has a determinable monetary value.

Depending on the residency of the key holders or beneficiaries, the Association may fall within the definition of an "affected person", thereby becoming subject to additional regulatory obligations.

This raises a broader concern regarding the application of the definition to decentralised and globally distributed systems.

Many widely used decentralised finance (DeFi) protocols, including Uniswap, Aave, and Compound, are governed through token-based voting mechanisms. In practice, governance tokens are held by a geographically dispersed group of participants, the majority of whom are likely to be non-residents.

If the definition of "affected person" is applied strictly, such protocols could be characterised as being controlled predominantly by non-residents. This creates a potential scenario in which these systems would be treated as "affected persons" for the purposes of the regulations.

However, these protocols do not operate as traditional legal persons or identifiable associations within a single jurisdiction. They are decentralised software systems, deployed on public blockchains, and accessible globally without restriction. There is no central operator, no place of incorporation, and no mechanism to localise their operation within the Republic.

This gives rise to several practical and conceptual challenges:

- It is unclear how such systems would be determined to be "operating in the Republic", given their global and non-territorial nature.
- There is no identifiable entity against which obligations could be enforced, nor any mechanism to compel compliance.
- The classification may be triggered indirectly, simply by virtue of South African users interacting with globally deployed protocols.

The result is a potential over-extension of the definition, where the concept of an "affected person" is applied to systems that do not fit within the traditional legal or organisational structures contemplated by the regulations.

This may introduce legal uncertainty, as well as practical enforcement challenges, particularly where obligations are imposed on entities or arrangements that cannot be clearly identified, located, or regulated in a conventional manner.

A more precise delineation of the scope of "affected person" is necessary, particularly in relation to decentralised systems and unincorporated associations operating across multiple jurisdictions.

Absent such clarification, the definition may capture a broad range of decentralised systems in a manner that is not practically enforceable.

(continued on next page)

Definition of Financial Assistance: Unintended Inclusion of Protocol-Level Activity

> "financial assistance" includes—
> (a) the lending of currency or crypto assets;
> (b) the granting of credit;
> (c) the acquisition of securities;
> (d) the conclusion of an instalment sale agreement or lease;
> (e) the financing of sales or securities;
> (f) discounting;
> (g) factoring;
> (h) the guaranteeing of acceptance credits;
> (i) the guaranteeing of acceptance of any obligation;
> (j) a suretyship; and
> (k) a buy-back and a lease-back, but excluding—
> (i) the granting of credit by a seller in respect of any commercial transaction directly involving the passing of ownership of the goods from the seller to the purchaser; and
> (ii) the granting of credit solely in respect of the payment for services rendered;

The draft regulations define "financial assistance" to include, among other things, the lending of currency or crypto assets, as well as the acquisition of securities.

While this definition is consistent with traditional financial systems, its application to crypto asset systems may give rise to unintended consequences due to the differing nature of activities performed within these environments.

A substantial portion of typical crypto asset activity may fall within this definition, even where no traditional lending relationship or financial intermediation is present.

For example:

- Ethereum staking involves the locking of crypto assets in order to participate in network validation and consensus. While this may resemble capital deployment, it does not constitute lending to an identifiable counterparty in the conventional sense.
- Liquidity provision in automated market makers (AMMs), such as those used in decentralised exchanges, involves depositing assets into smart contracts to facilitate trading. These pools are algorithmically managed and do not represent lending to a discrete borrower.
- Liquidity provision over the Lightning Network involves committing funds to payment channels in order to route transactions and earn fees. This activity supports network functionality rather than constituting a bilateral lending arrangement.

If interpreted strictly, these activities may fall within the definition of "financial assistance", despite differing materially from the types of financial relationships the definition appears intended to capture.

This creates a potential over-extension of the regulatory framework, whereby protocol-level participation in decentralised systems is classified as financial assistance, with associated obligations that may not be appropriate or practically applicable.

In addition, these activities often lack identifiable counterparties, are executed through autonomous protocols, and may involve participants across multiple jurisdictions.

As a result, it may be difficult to determine:

- who is providing financial assistance,
- to whom such assistance is being provided, and
- where the activity is taking place for regulatory purposes.

This introduces both interpretive ambiguity and practical enforcement challenges, particularly where obligations depend on the identification of counterparties or the classification of specific transactions.

A more precise delineation of "financial assistance" may therefore be necessary to distinguish between:

- traditional lending or financing arrangements involving identifiable parties, and
- participation in decentralised protocols that facilitate network operation or market liquidity without constituting financial assistance in the conventional sense.

Absent such clarification, the definition may capture a broad range of ordinary crypto asset activity in a manner that is not aligned with its apparent regulatory intent.

This may result in a significant portion of ordinary, non-custodial crypto asset participation being brought within scope unintentionally.

(continued on next page)

Logical Contradiction: Crypto Assets Not Currency, Yet Regulated Like Currency

> "currency" means banknotes and coins in actual use or circulation as a medium of exchange in the country of issue thereof, and includes any bill of exchange, letter of credit, money order, postal order, promissory note, traveller's cheque or any other instrument for the payment of currency, but does not include crypto assets;

The draft regulations define "currency" in a manner that explicitly excludes crypto assets.

Notwithstanding this definition, crypto assets are treated in a manner analogous to currency throughout the regulatory framework, particularly in relation to capital flow controls, import and export restrictions, and reporting obligations.

This creates an internal inconsistency in the regulatory approach.

Crypto assets are, by definition, not issued by a central authority, are not redeemable, and are not tied to a single jurisdiction. These characteristics distinguish them fundamentally from traditional currency.

Applying currency-based regulatory concepts to assets that are explicitly defined as not being currency introduces a category mismatch.

This inconsistency may result in legal uncertainty, as it is unclear whether crypto assets are intended to be regulated as a distinct asset class with bespoke rules, or as a functional equivalent of currency despite their differing properties.

Such ambiguity may complicate interpretation and lead to inconsistent application of the regulations.

A more consistent classification framework may be required to ensure clarity and coherence in the regulatory treatment of crypto assets.

(continued on next page)

Synthesis

Unrealistic Assumption of Compliance Layer Visibility

Taken together, the provisions discussed above indicate that the draft regulations assume the existence of a compliance layer through which crypto asset ownership, transfers, and intent can be observed, attributed, and controlled.

This includes assumptions that regulators can reliably identify asset holders, monitor transactions, determine jurisdiction, and approve or deny activity prior to execution.

These assumptions do not reflect the operational characteristics of crypto asset systems.

As demonstrated, such systems are inherently decentralised, permissionless, and resistant to centralised control.

Transactions can occur without intermediaries, without prior approval, and in many cases without reliable attribution to identifiable parties.

As a result, the regulatory framework assumes capabilities, particularly in relation to visibility, attribution, and enforcement, that are not present in the underlying technology.

This creates a structural limitation in the effectiveness of the proposed approach.

The regulations can be applied to custodial intermediaries, but cannot be consistently extended to non-custodial usage, decentralised protocols, or off-chain systems such as the Lightning Network.

The likely outcome is a framework that is only partially enforceable, where compliance obligations fall primarily on those already operating within regulated environments, while a substantial portion of activity remains outside the scope of effective control.

This may reduce the overall effectiveness of the regulatory regime, while increasing complexity and compliance burden for those who do engage with regulated service providers.

A regulatory approach that more closely aligns with the technical and operational characteristics of crypto assets may be necessary to achieve the intended policy objectives.

(continued on next page)

Enforcement and Penalty Framework Limitations

The draft regulations establish a framework of restrictions and obligations relating to the acquisition, transfer, declaration, and disposal of crypto assets, supported by enforcement powers and potential penalties for non-compliance.

This framework assumes that non-compliance can be reliably detected, proven, and sanctioned. In the context of crypto asset systems, this assumption is significantly constrained by the technical characteristics described above.

As outlined in preceding sections, decentralised crypto asset systems do not provide consistent visibility into ownership, control, or transaction activity. Transactions may occur without intermediaries, without identifiable counterparties, and without a comprehensive or attributable record linking activity to specific individuals.

This creates a fundamental limitation in enforcement. Where non-compliance cannot be reliably detected, enforcement becomes selective. Similarly, where ownership or control cannot be conclusively attributed, it becomes difficult to establish certainty in relation to alleged violations.

In addition, several provisions rely on obligations—such as prior approval, complete disclosure of holdings, or furnishing of access credentials—that cannot be independently verified in practice. This introduces a further limitation: even where a legal obligation exists, there may be no reliable method to determine whether a person has complied fully or only partially.

The combined effect is that the enforcement and penalty framework may operate unevenly. Persons engaging with regulated custodial intermediaries are more likely to be visible and therefore subject to

enforcement, while persons operating in non-custodial or decentralised environments may remain outside the scope of practical detection.

This asymmetry risks creating outcomes where enforcement is applied primarily to compliant or visible participants, rather than uniformly across all activity. Such an outcome may undermine both the perceived fairness and the effectiveness of the regulatory regime.

Furthermore, where obligations cannot be objectively verified, there is a risk of uncertainty in enforcement proceedings, as it may not be possible to distinguish between full compliance, partial compliance, and non-compliance with sufficient evidentiary confidence.

A regulatory framework that relies on detection, attribution, and verification mechanisms that are not consistently available in the underlying systems may therefore face practical limitations in achieving its intended objectives, particularly where enforcement depends on those mechanisms.

(continued on next page)

Unintended Economic Consequences

The draft regulations seek to impose controls on the use and movement of crypto assets; however, the limitations in enforceability and scope described above may give rise to unintended economic consequences.

Where regulatory obligations cannot be consistently applied across all forms of crypto asset activity, there is a risk that compliant participants, particularly those using regulated custodial intermediaries, bear a disproportionate burden.

At the same time, non-custodial and decentralised activity may remain largely unaffected in practice. This may create incentives for users to migrate away from regulated environments toward less visible or offshore alternatives.

In addition, requirements that rely on prior approval, restrictive thresholds, or uncertain compliance obligations may introduce friction into legitimate use cases, including innovation, liquidity provision, and participation in global digital asset markets. This may discourage local development and reduce the competitiveness of South African participants in an increasingly borderless ecosystem.

There is also a potential for regulatory arbitrage, where individuals and businesses structure their activities to fall outside the effective scope of the regulations, including through the use of decentralised protocols, self-custody, or relocation of services and operations to other jurisdictions.

Taken together, these effects may reduce the effectiveness of the regulatory framework in achieving its stated objectives, while simultaneously increasing compliance costs and limiting participation in the formal, regulated segment of the market.

Regulatory Scope and On/Off-Ramp Focus

The preceding sections highlight structural limitations in applying regulatory controls directly to decentralised, non-custodial crypto asset activity. These limitations arise from the absence of identifiable control points, the lack of consistent transaction visibility, and the inability to reliably enforce or verify compliance at the protocol level.

In contrast, there are identifiable points within the crypto asset ecosystem where regulatory oversight can be applied more effectively.

These include interfaces between crypto assets and the traditional financial system, such as centralised exchanges, custodial service providers, payment processors, and banking institutions facilitating fiat on-ramps and off-ramps.

At these points, participants are identifiable, transactions are mediated, and compliance obligations—such as reporting, customer due diligence, and transaction monitoring—can be implemented and enforced with greater reliability. These environments provide the visibility and control mechanisms that the broader decentralised ecosystem does not.

A regulatory approach that prioritises these interfaces may therefore be more effective in achieving policy objectives related to capital flow management, financial surveillance, and risk mitigation. By focusing on custodial intermediaries and fiat conversion points, regulators can maintain oversight where it is technically feasible, while avoiding reliance on assumptions that do not hold in non-custodial or decentralised contexts.

Such an approach may also reduce unintended consequences, including the migration of users toward less visible or offshore alternatives,

by aligning regulatory measures with the practical realities of how crypto asset systems operate.

(continued on next page)

Procedural Concerns

Material Uncertainty for Stakeholders: Due Date for Submission of Comments

According to the media statement on the www.gov.za website, "National Treasury invites public comment on draft Capital Flow Management Regulations, 2026"[5], there is a due date for comments of 10 June 2026.

However, according to the media statement on the www.treasury.gov.za website, "PUBLICATION OF THE DRAFT CAPITAL FLOW MANAGEMENT REGULATIONS, 2026 (FORMERLY KNOWN AS THE EXCHANGE CONTROL REGULATIONS, 1961) FOR PUBLIC COMMENT"[6], the due date for comments is 18 May 2026.

Notwithstanding the short timeframes for public comment on a matter of significant economic and legal impact, the discrepancy between the two published deadlines (10 June 2026 and 18 May 2026) creates material uncertainty for stakeholders.

This inconsistency raises concerns regarding procedural fairness and administrative clarity, as affected parties cannot reliably determine the applicable deadline for submissions.

The risk is not merely confusion, but the potential exclusion, or disregard, of submissions based on an ambiguous or incorrectly applied deadline, which would undermine the integrity of the consultation process.

[5] https://www.gov.za/news/media-statements/national-treasury-invites-public-comment-draft-capital-flow-management

[6] https://www.treasury.gov.za/public%20comments/CapFlow/2026041701%20Media%20Statement%20-%20Draft%20Capital%20Flow%20Management%20Regulations%202026.pdf

This may be inconsistent with the requirements of lawful, reasonable and procedurally fair administrative action as contemplated in the Promotion of Administrative Justice Act (PAJA).

(continued on next page)

Material Risk for Stakeholders: Different Submission Addresses

Further compounding the procedural uncertainty, the email address for submitting comments differs between the two media statements and the gazetted notice[7].

The media statements direct submissions to Commentdraftlegislation@treasury.gov.za, while the gazetted notice directs submissions to CommentDraftRegulations@treasury.gov.za.

This inconsistency creates a material risk that submissions may be sent to an incorrect or unmonitored address, resulting in those submissions not being received or considered.

This is not merely a matter of confusion, but raises concerns regarding the integrity and fairness of the public participation process, as similarly situated stakeholders may be treated differently depending on which source they relied upon.

This creates uncertainty as to whether all submissions will be captured and considered, which may undermine the procedural fairness of the consultation process.

(continued on next page)

7 https://www.treasury.gov.za/public%20comments/CapFlow/Gazette_Publication%20of%20Capital%20Flow%20Management%20Regulations.pdf

Drafting Errors

Definitions Drafting Error: "authorised crypto asset service provider"

> "authorised crypto asset service provider" means a crypto asset service provider as defined in item 22 of schedule 1 of the Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001) and who is authorised by the National Treasury to facilitate transactions deemed as import and/or or and export of capital, directly or indirectly, utilising crypto assets as a medium of exchange.

This is clearly a drafting error and the definition should read "deemed as import and/or export of capital"

Definitions Drafting Error: "enforcement officer"

> "enforcement officer" means–
> (a) any officer, as defined in section 1 of the of Customs and Excise Act, 1964 (Act No. 91 of 1964);

This is clearly a drafting error and the definition should read "any officer, as defined in section 1 of the Customs and Excise Act, 1964 (Act No. 91 of 1964);"

(continued on next page)

Definitions Drafting Error: "foreign currency"

> "foreign currency" means any currency which is not a legal tender in the Republic and–
> (a) includes–
> (i) any bill of exchange;
> (ii) letter of credit;
> (iii) money order;
> (iv) postal order;
> (v) promissory note;
> (vi) traveller's cheque; or
> (viii) any other instrument for the payment of currency in a currency unit which is not legal tender in the Republic;

This is clearly a drafting error, and the item (viii) should be item (vii).

Definitions Drafting Error: Acquisition of foreign currency or crypto assets by National Treasury

> 8. (1) Any personin the Republic who has under their control, obtains possession of, or becomes entitled to sell, procure the sale of, or transfer, any foreign currency or crypto assets in an amount or with a value in excess of the determined threshold must, within 30 days or a longer period that may be prescribed from the date of any of the afore-mentioned events, make a declaration in writing, in the form and manner prescribed by the Nation

This is clearly a drafting error and the sentence should start "Any person in the Republic …"

(continued on next page)

Recommendations

1. The regulatory framework should distinguish explicitly between custodial and non-custodial crypto asset activities, and focus enforceable obligations on custodial intermediaries where identifiable control points exist.

   Consideration should be given to adopting a risk-based and activity-based regulatory approach, focusing on points where crypto assets interface with the traditional financial system.

2. Requirements for prior approval before transacting in crypto assets should be reconsidered, as such provisions rely on control mechanisms that are not present in decentralised, peer-to-peer systems.

   Declaration requirements should be limited to information that can be reasonably verified in practice, recognising the pseudonymous and non-custodial nature of crypto assets ownership.

3. The use of territorial concepts such as "import" and "export" should be reviewed in the context of crypto assets, as these concepts do not align with the non-geographic nature of distributed ledger systems.

4. Threshold-based controls should be designed with consideration for transaction fragmentation and address multiplicity, to avoid creating rules that are easily circumvented and difficult to enforce.

5. Provisions relating to search, seizure, and compelled access should account for the technical distinction between physical possession and cryptographic control, and the practical

limitations of accessing assets without voluntary cooperation.

6. The treatment of crypto assets within the regulations should be made internally consistent, ensuring that definitions and regulatory applications align clearly with the intended classification of crypto assets.

7. The framework should avoid reliance on assumptions of complete visibility and attribution, and instead adopt approaches that reflect the limited observability of decentralised and off-chain systems.

8. Ongoing engagement with technical stakeholders is recommended to ensure that regulatory measures remain aligned with the evolving design and use of crypto asset systems.