South Africa's Crypto Assets Market Study

FSCA
Financial Sector Conduct Authority

Table of Contents

Abbreviations

AML	-	Anti Money Laundering
BA	-	Blockchain Association
CFT	-	Combating the Financial of Terrorism
CAR WG	-	Crypto Assets Regulatory Working Group
CBDC	-	Central Bank Digital Currency
COFI	-	Conduct of Financial Institutions
CRC	-	Crypto Rating Council
CASPs	-	Crypto Asset Services Providers
DLT	-	Distribution Ledger Technology
FSCA	-	Financial Sector Conduct Authority
FSR Act	-	Financial Sector Regulation Act
FSP	-	Financial Services Provider
FAIS Act	-	Financial Advisory and Intermediary Services Act
FMA	-	Financial Markets Act
FMIs	-	Financial Market Infrastructures
ICO	-	Initial Coin Offering
IFWG	-	Intergovernmental Fintech Working Group
IPO	-	Initial Public Offering
KYC	-	Know your Customer
NFT	-	Non-Fungible Token
TCF	-	Treating Customers Fairly

List of Figures

List of Tables

Executive Summary

In recent years, the market for financial products and services associated to crypto assets has expanded quickly, becoming more and more integrated into the regulated financial system. The crypto asset market has grown significantly overall and shows no sign of slowing down anytime soon. The potential for blockchain technology and crypto assets to transform numerous industries still exists, despite the industry's regulatory and other difficulties.

The term 'crypto assets' has been adopted as it encapsulates and is seen as a broader, or 'umbrella', term for different crypto asset tokens used for a variety of uses. South African consumers are increasingly engaging in financial activities involving crypto assets, including investing in derivative instruments with crypto as the underlying asset, especially given the proliferation of online trading platforms. Heightened take-up and abuse in the retail market necessitates a suitable and proportionate regulatory and supervisory response. The volatility of crypto assets, coupled with the high gearing of derivative instruments poses significant risks to customers.

In October 2022, the Financial Sector Conduct Authority (FSCA) officially declared crypto assets as a financial product in terms of the Financial Advisory and Intermediary Services Act (FAIS). This means that any individual or business that provides financial advice or intermediary services in respect of crypto assets – what is typically understood to be a "broker" or "advisor" - will have to register as an FSP. The Declaration in effect puts in place a regulatory and licensing regime for persons providing financial services in respect of crypto assets. With the declaration on place, it is not necessarily tailored around crypto assets services providers, and the specific risks posed in the crypto asset environment. Therefore, there is need to develop bespoke and/or refine further the existing framework to ensure that it is fit for purpose and addresses crypto asset specific risk, without stifling innovation in a significant manner.

To better understand the crypto asset-related activities performed by Crypto Asset Financial Service Providers (FSPs) in South Africa, the FSCA, in accordance with paragraph 3(2) of FSCA FAIS Notice 90 of 2022, requested Crypto Asset FSPs to furnish the authority with information relating to their business and business practices. The information gathered is intended to support the work of the FSCA, particularly in relation to the development of licensing, supervision, and regulatory frameworks for Crypto Asset FSPs, by highlighting consumer exposure to crypto assets; and in line with risk-based supervision, identify risks that may negatively impact consumer well-being.

The information gathered suggests that the majority of Crypto Asset FSPs in South Africa provide financial services by making use of unbacked crypto assets, followed by stablecoins and security tokens. Most unbacked crypto assets are used for speculative purposes rather than as a medium of exchange. Further, the observed crypto assets-related business models are diverse. However, in some instances, the business models mirror traditional financial activities such as operating an exchange or providing advice. These activities require consumers to trust centralised entities which is against the disintermediation function that crypto assets were designed for.

Other findings include:

- Almost all Crypto Asset FSPs claim to disclose risks relating to crypto asset activities to their customers and the public.
- Cape Town leads the way in head office location. The results bear testimony to the fact that Cape Town is considered the largest technology hub in Africa.
- The majority of Crypto Asset FSPs earn their revenue from trading fees and most of the remuneration models identified mirror traditional financial revenue models.
- The majority of crypto assets Crypto Asset FSPs have interventions in place to handle complaints. However, these interventions would need to be coordinated with the management and processing of complaints related to the Treating Customers Fairly (TCF) outcomes.
- More than half of the Crypto Asset FSPs have built their businesses around retail customers. Understanding the extent of retail participation over time will be critical in assessing the consumer protection risk and impact of this market.

The information gathered will assist the FSCA in enhancing its approach to licensing and supervision of crypto asset activities, with a view to appropriately mitigate risk in this environment, thereby ensuring better financial customer outcomes in the crypto asset environment. This is anticipated to enable the authority to make more informed decisions concerning the potential future regulation for crypto asset-related activities.

1. Introduction

Crypto assets and its associated products and services have grown rapidly in recent years, becoming increasingly interlinked with the regulated financial system. While the industry faces regulatory and other challenges, the potential for blockchain technology and crypto assets to transform the financial sector remains significant.

The crypto economy in Sub-Saharan Africa is the smallest among all regions, accounting for 2.3% of the global transaction volume from July 2022 to June 2023. In the same time frame, the region attracted an approximate total of $117.1 billion in on-chain value[1]. While Sub-Saharan Africa consistently stands as one of the smaller cryptocurrency markets, a closer analysis reveals that cryptocurrency has made significant inroads among key populations. Nigeria exemplifies this better, ranking second on the 2023 Chainalysis Global Crypto Adoption Index[2]. Other countries in the region that score high on the index include Kenya (21), Ghana (29), and South Africa (31). Further, a 2022 study by Triple A (Singapore Blockchain company) indicates that over 5.8 million people, 9.44% of South Africa's total population - currently own crypto assets, with 43% of the population expected to be using them by 2030[3].

Retail customers use crypto assets for transacting and speculation/investment but were - until now – largely unprotected, often investing in products without understanding the risks and complexities of the instruments. Moreover, crypto assets are increasingly being used as the underlying assets in derivative instruments and becoming more popular with retail customers with the proliferation of online trading platforms.

In general, governments and regulators are grappling with how to regulate the crypto asset ecosystem given its decentralised nature and global reach. Regulatory challenges often relate to jurisdiction and understanding how Crypto Asset Service Providers (CASPs) fit into the existing financial sector laws and supervisory landscape. More severe challenges include preventing money laundering and other illegal activities, protecting investors from scams and fraud, and monitoring the potential financial stability of the financial system.

The regulation of crypto assets varies depending on the country and region.

1 The 2023 Geography of Cryptocurrency Report. Available at: https://go.chainalysis.com/rs/503-FAP-074/images/The%202023%20Geography%20of%20Cryptocurrency%20Report.pdf?version=0

2 The 2023 Geography of Cryptocurrency Report. Available at: https://go.chainalysis.com/rs/503-FAP-074/images/The%202023%20Geography%20of%20Cryptocurrency%20Report.pdf?version=0

3 Cryptocurrency information about South Africa: Available at: https://triple-a.io/crypto-ownership-south-africa-2022/

When considering crypto asset regulation, there are essentially three approaches available[4]:

1. **Ban:** Some countries have completely banned the use of crypto assets, such as China, Algeria, Bolivia, and Egypt.
2. **Regulate:** Some countries have given legal recognition to crypto assets, often with licensing restrictions, such as Japan, the United States of America (US), Canada, the European Union (EU), and Australia. In these countries, crypto assets are regulated under existing laws and financial regulations, such as Anti-Money Laundering (AML), Know Your Customer (KYC), and tax laws. These may include registration and licensing. In some cases, crypto assets may be classified as securities and subject to securities regulation. Some countries have consumer protection laws that apply to crypto assets, which may include restrictions on advertising, disclosure requirements, and measures to prevent fraud and scams. Central banks in some countries regulate crypto assets to control the money supply, monitor the potential impact on financial stability, and prevent money laundering and other illicit activities.
3. **Wait and learn:** Some countries have opted to observe and monitor crypto asset innovation before intervening. Over time, as the regulators gain capacity around crypto assets innovation and the technology becomes more commonly adopted, policymakers may incrementally amend or change existing regulations. For instance, The Central Bank of Ireland does not have specific crypto assets regulation, and there is no prohibition of crypto assets activities within Ireland. Instead, the Central Bank of Ireland has taken a "do nothing" approach to the regulation of crypto assets.

In addition to government regulation, there are also self-regulatory organizations within the crypto industry, such as the Crypto Rating Council (CRC) and the Blockchain Association (BA), which are working to establish standards and best practices for the industry.

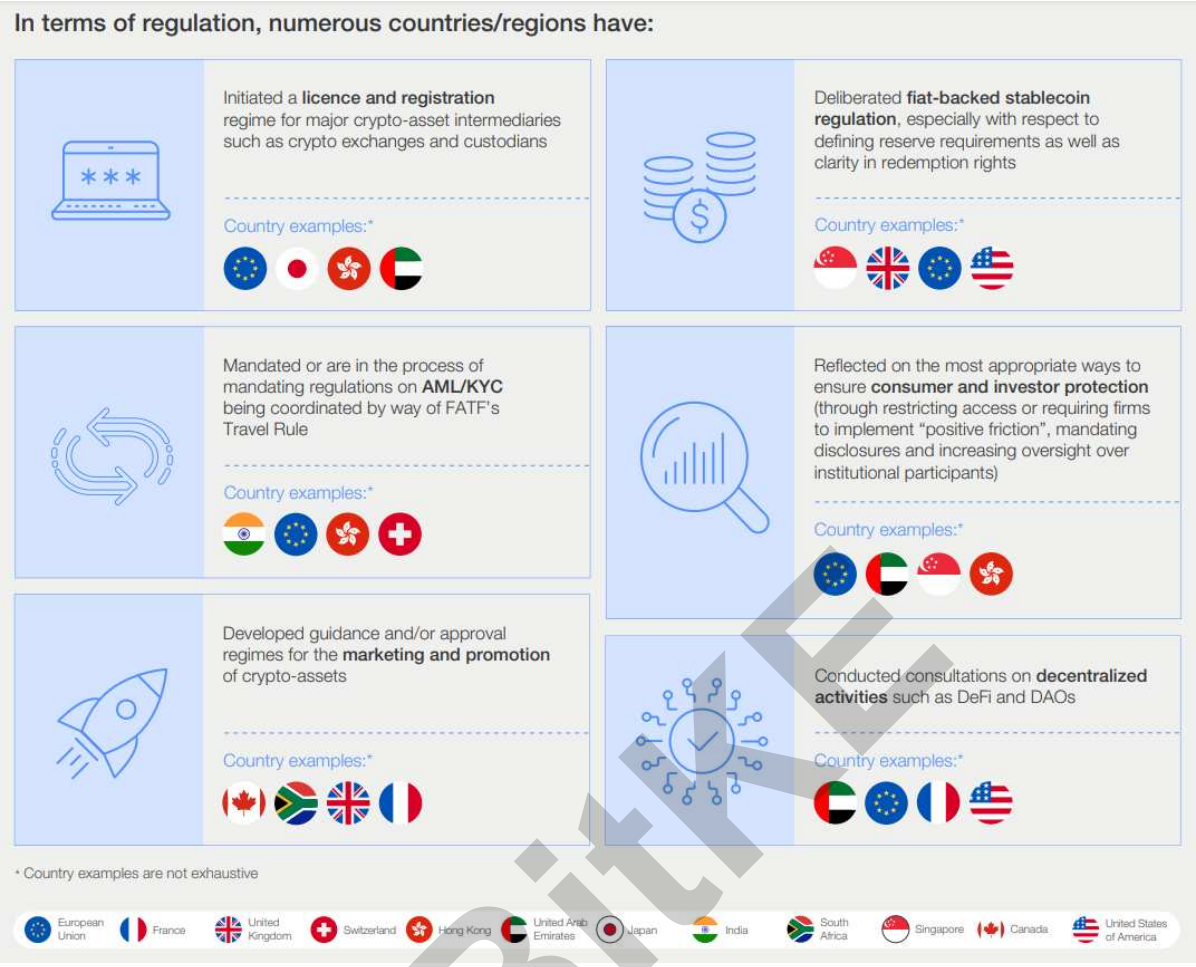
1.1 Recent regulatory developments

1.1.1 International context

Throughout the world, several jurisdictions have implemented various regulations for crypto assets, creating a fragmented regulatory environment. The degree and range of these regulations are determined by several factors, including the stage at which the cryptocurrency ecosystem is developing, perceived threats to the stability of the financial system, the capacity of the regulatory bodies in charge of regulating cryptocurrency assets, the intention to promote innovation, and other regionally specific factors[5]. These factors combine differently for every country, creating a complex regulatory environment where some countries (like China) banned the use of cryptocurrency, while other countries (like El Salvador[6] and the Central African Republic) have made certain cryptocurrency assets (like Bitcoin) officially recognised as legal money[7].

4 IFWG, Position Paper on Crypto Assets, 2021. Available at: https://www.ifwg.co.za/Reports/Position%20Paper%20on%20Crypto%20Assets.pdf
5 Pathways to the Regulation of Crypto-Assets: A Global Approach. Available at: https://www3.weforum.org/docs/WEF_Pathways_to_the_Regulation_of_Crypto_Assets_2023.pdf
6 EL Salvador and Cryptocurrency. Available at: https://freemanlaw.com/cryptocurrency/el-salvador/
7 Pathways to the Regulation of Crypto-Assets: A Global Approach. Available at: https://www3.weforum.org/docs/WEF_Pathways_to_the_Regulation_of_Crypto_Assets_2023.pdf

Figure 1: Crypto Asset Regulatory Developments



Source: Pathways to the Regulation of Crypto-Assets: A Global Approach [8]

1.1.2 Local context

In South Africa, the Crypto Assets Regulatory Working Group (CAR WG) of the Intergovernmental Fintech Working Group (IFWG)[9] published the final Position Paper (CAR Paper) on crypto assets for South Africa in June 2021[10]. The CAR Paper signalled a regulatory and policy response to crypto assets activities in South Africa.

The CAR WG Paper made 25 recommendations for crypto assets and related activities and essentially provides a roadmap for a regulatory framework for CASPs. The CAR Paper proposed the FSCA to be the regulatory authority to license, supervise and investigate Crypto Asset FSPs.

8 Pathways to the Regulation of Crypto-Assets: A Global Approach. Available at: https://www3.weforum.org/docs/WEF_Pathways_to_the_Regulation_of_Crypto_Assets_2023.pdf

9 The IFWG is a collaborative effort and resultant body of several South African financial sector regulators, including National Treasury, the Financial Intelligence Centre (FIC), the FSCA, the National Credit Regulator (NCR), the South African Reserve Bank (SARB) South African Revenue Service (SARS) and the Competition Commission

10 IFWG: CAR WG Position Paper on Crypto Asset in June 2021. Available at: https://www.ifwg.co.za/Reports/Position%20Paper%20on%20Crypto%20Assets.pdf

In line with the crypto assets developments that were happening within the IFWG CAR WG, in November 2020 the FSCA published for public consultation a draft Declaration of crypto assets as a financial product under the FAIS Act. This proposed Declaration signalled the FSCA's acute interest in CASPs and was put forward as an interim step to mitigate conduct and consumer protection risks in the crypto asset environment, pending the anticipated Conduct of Financial Institutions (COFI) Bill framework and the broader policy discussions taking place at the time through the CAR WG.

In October 2022, the FSCA officially declared crypto assets as a financial product in terms of the FAIS Act[11]. This means that any individual or business that provides financial advice or intermediary services in respect of crypto assets – what is typically understood to be a "broker" or "advisor" - will have to register as an FSP. The Declaration in effect puts in place a regulatory and licensing regime for persons providing financial services in respect of crypto assets. Crypto Asset FSPs[12] must be licensed and will be subject to the FSCA's oversight and supervision.[13]

Following the declaration, in December 2022 the FSCA published an Information Request in accordance with paragraph 3(2) of FSCA FAIS Notice 90 of 2022, requesting Crypto Asset FSPs to furnish the authority with information relating to their business and business practices.

Broader developments surrounding crypto assets will likely be given effect through the COFI Bill, which constitutes the future consolidated legal framework governing the conduct of all financial institutions. Financial services related to crypto assets will likely be included in the licensing activities under the COFI Bill, potentially expanding the scope of crypto asset activities that are currently regulated under the FAIS Act.

2. Problem Statement

After declaring crypto assets as a financial product, the FSCA remains of the view that crypto asset related activities pose significant risks to financial customers. While there is a legal framework is in place, it is not necessarily tailored around crypto assets services providers, and the specific risks posed in the crypto asset environment. Therefore, there is need to develop bespoke and/or refine further the existing framework to ensure that it is fit for purpose and addresses crypto asset specific risk, without stifling innovation in a significant manner.

Further, the regulation of crypto asset related activities is a new development and the FSCA is still unpacking the specific risks inherent in this environment. To regulate effectively, the FSCA needs to develop a deeper understanding of these risks and market dynamics to enable it to refine its approach to licensing and supervising of crypto asset activities with a view to appropriately mitigate risk in this environment, thereby ensuring better financial customer outcomes in the crypto asset environment.

11 Reference the Declaration ie what was the official title.
12 Means a person that is required to be licensed under section 8 of the Act to render a financial service in relation to crypto assets and currently renders financial services under the exemption provided in terms of FSCA FAIS Notice 90 of 2022.
13 Financial Advisory and Intermediary Services Act, 2002 (Act No. 37 Of 2002)

3. Purpose

The purpose of this research is to assist the FSCA to better understand crypto asset related activities performed by Crypto Asset FSPs[14] in South Africa, in order to:

i. Support the work of the FSCA, particularly in relation to the development of licensing, supervision, and regulatory frameworks for Crypto Asset FSPs, by highlighting consumer exposure to crypto assets; and

ii. In line with risk-based supervision, identify risks that may negatively impact consumer well-being, in support of the FSCA's regulatory and supervisory approaches.

4. Research Approach

The study employed a "mixed methods" approach. The FSCA obtained information related to crypto assets-related activities in South Africa directly from Crypto Asset FSPs, by issuing an Information Request in December 2022[15]. In terms of the Financial Sector Regulatory Authority (FSRA) 9 of 2017, the FSCA is empowered to request information from regulated persons in the fulfilment of its objectives and functions[16].

The purpose of the Information Request is to assist the authority in obtaining a better understanding of crypto asset-related activities that Crypto Asset FSPs are currently performing in the crypto asset environment, in turn, to better understand related conduct risks.

Information submitting by the Crypto Asset FSPs was augmented by desk-based research. The desk-based research drew information from different sources, including policy and academic texts, and national and international datasets from both public and private stakeholders.

14 Means a person that is required to be licensed under Section 8 of the Act to render a financial service in relation to crypto assets and currently renders financial services under the exemption provided in terms of FSCA FAIS Notice 90 of 2022.

15 FSCA Information Request 7 of 2022 (2022) FAIS.

16 Financial Sector Regulation Act 9 of 2017. Available at: https://www.gov.za/documents/financial-sector-regulation-act-9-2017-english-sepedi-22-aug-2017-0000

5. Scope of the Information Request

The scope of the Information Request included crypto assets-related activities performed and business practices of Crypto Asset FSPs in South Africa as at December 2022.

The Information Request covered:

i. Crypto Asset FSP supply-side driving factors;
ii. Crypto Asset FSP outsourcing arrangements;
iii. Crypto Asset FSP business models;
iv. Crypto Asset Market dynamics;
v. Crypto Asset FSP demand-side driving factors; and
vi. Complaints.

6. Overview of the Crypto Assets Operating Environment

This section provides an overview of the crypto asset ecosystem, taxonomy, market essential functions, and activities. The section sets the stage for the evaluation in section 7, which looks in more detail at the Crypto Asset FSP activities in South Africa.

6.1 Crypto Asset Ecosystem

For the purposes of this paper, the definition of crypto asset is adopted from the IFWG CAR WG Position Paper on Crypto Assets. The paper defines crypto asset as[17]:

i. a digital representation of value that 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;
ii. applies cryptographic techniques; and
iii. uses distributed ledger technology (DLT).

17 IFWG, Position Paper on Crypto Assets, 2021. Available at: https://www.ifwg.co.za/Reports/Position%20Paper%20on%20Crypto%20Assets.pdf

Various naming conventions have been used over the years by ecosystem participants, from 'digital tokens' and 'digital assets' to 'cryptocurrency' and 'crypto assets'. Considering naming conventions, the central banks, in particular, have been reluctant to refer to these digital representations on blockchain ledgers as 'currency' as it is not deemed to be a form of legal tender or fiat currency.

The regulatory authorities have taken a functional approach, focusing on the economic activities being performed, compared to a more generic, 'all-encompassing' classification. It is acknowledged that crypto assets may perform certain functions similar to those of 'traditional' currencies, securities, or financial products and commodities.

The term 'crypto assets' is thus preferred and has been adopted by the Intergovernmental Fintech Working Group, as it encapsulates and extends to these functions. 'Crypto assets' are seen as a broader, or 'umbrella', term for different crypto asset tokens used for a variety of uses.

Regarding the functioning and organisation of the crypto assets market, Box 1 below gives a detailed description of the various participants in and components of the crypto asset market:

Box 1: Key Crypto Asset Ecosystem Components and Actors

1. **Blockchain** is the foundation of the crypto assets' ecosystem, a type of distributed ledger where transactions are recorded, and participants transact with other participants and decentralised applications.
2. **Customers** in the crypto-assets market take part and are involved in transactions. They could be individuals, institutions, and businesses.
3. **Financial intermediaries** such as brokers provide advice or facilitate the purchase of crypto assets by investors.
4. **System administrators** such as crypto assets issuers (this includes those who issue tokens through an Initial Coin Offering - ICO[18]) and auditors (allowed to view the ledger but not allowed to make changes). They issue crypto assets, decide who can access the network, and maintain and administer dispute resolution rules.
5. **Miners/validators** and **transaction processors**, who are incentivised by remuneration to verify transactions and add them to the ledger.
6. **Trading platforms and exchanges** facilitate transactions between participants and ensure a liquid market.
7. **Payment providers** enable customers to pay for services or goods received using a crypto asset.
8. **Wallet providers** enable customers to make coin transactions and secure the storage of crypto assets.

For traditional financial institutions, avoiding crypto assets entirely may not be possible. Although banks may prohibit certain types of crypto asset transactions (e.g. blacklisting certain counterparties), it may not be feasible for them to fully unplug from the crypto assets' ecosystem if their customers or third parties remain involved in it. For instance, if customers can engage in crypto asset transactions, even outside of the perimeter of traditional financial institutions, then the flow of funds through their accounts may represent a risk related to money laundering or fraud.

18 An initial coin offering (ICO) is a type of capital-raising activity in the crypto assets and blockchain environment. The ICO can be viewed as an initial public offering (IPO) that uses crypto assets.

6.2 Crypto Assets Taxonomy

No internationally agreed taxonomy exists for crypto assets and as a result, crypto asset types have been categorised into various forms, such as[19][20]:

1. **Non-Fungible Tokens (NFT)** – A unique digital asset that represents ownership of a specific item or asset e.g. art, music, in-game items, videos, and more. They are bought and sold online, frequently with crypto assets, and they are generally encoded with the same underlying software as many crypto assets[21].
2. **Security tokens** - Although the definition of a security token varies across jurisdictions, these are tokens that provide the holder with rights like that of traditional security, for example, the right to a share in the profits of the issuer. Securities tokens are often subject to securities laws and regulations.
3. **Utility tokens** - These tokens provide the token holder with access to an existing or prospective product or service. These are usually limited to a single network (that is, the issuer) or a closed network linked to the issuer. For example, a tokenized store card or certain gaming tokens might be considered types of utility tokens.
4. **Unbacked crypto assets** - These crypto assets are transferable, primarily designed to be used as a medium of exchange, and are often decentralised. Unbacked crypto assets are the oldest and most prominent type of crypto asset. They do not rely on any backing asset for value but instead on supply and demand. Most unbacked crypto assets are currently used for speculation and not for payment purposes. Prominent examples include Bitcoin and Ether (although in some jurisdictions with broad definitions of securities, these might be considered security tokens).
5. **Stablecoins** - This type of crypto asset aims to have a stable price value. This objective is normally pursued by the crypto asset being linked to a single asset or a basket of assets, for example, fiat funds, commodities such as gold, or other crypto assets. Prominent examples include Tether, Binance USD, and USD Coin.
6. **Central Bank Digital Currency (CBDC)** - A CBDC can be defined as a form of money that is denominated in fiat currency (central bank money), in an electronic form, and which is a liability on the central bank's balance sheet similar to cash and central bank deposits[22].

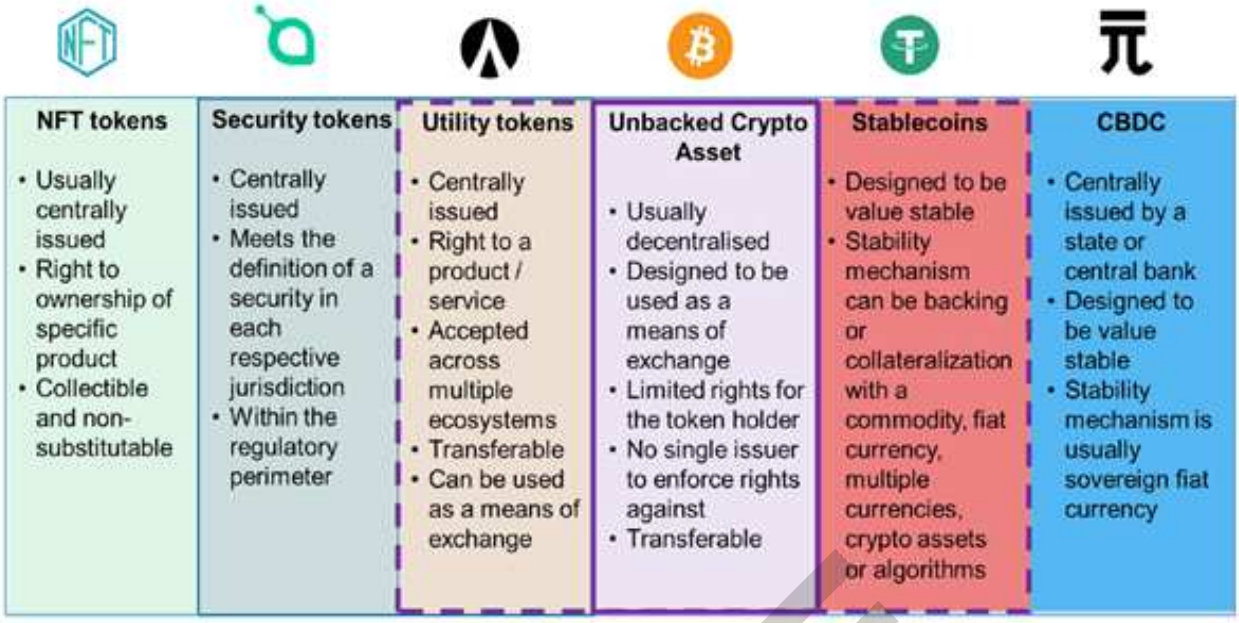
19 Regulating the Crypto Ecosystem, the Case of Unbacked Crypto Assets, IMF note 2022/007. Available at: www.imf.org/en/Publications/fintech-notes/Issues/2022/09/26/Regulating-the-Crypto-Ecosystem-The-Case-of-Unbacked-Crypto-Assets-523715

20 IFWG: CAR WG Position Paper on Crypto Asset in June 2021. Available at: https://www.ifwg.co.za/Reports/Position%20Paper%20on%20Crypto%20Assets.pdf

21 What is NFT, Forbes article. Available at: https://www.forbes.com/advisor/investing/cryptocurrency/nft-non-fungible-token/

22 Frequently asked questions on central bank digital currencies. Available at: www.resbank.co.za/content/dam/sarb/what-we-do/banknotes-and-coin/CBDC%20FAQ%27s.pdf

Figure 2 : A Taxonomy of Crypto Asset



Source: Regulating the Crypto Ecosystem the Case of Unbacked Crypto Assets, IMF note 2022/007[23]

6.3 Crypto Assets Functions and Activities

The crypto asset market features a wide range of functions and activities, many of which resemble those in the traditional financial system. Table 1 identifies essential functions around crypto assets, as well as prevalent activities associated with these functions. Annexure 1 provides a detailed list of activities, their service providers, associated vulnerabilities and risks, as well as potentially relevant international standards.

Table 1 : Essential Functions and Activities in the Crypto Asset Ecosystem

Functions	Activities
Creation, issuance, distribution, redemption and underlying infrastructure	• Creating, issuing, and redeeming crypto-assets, distribution, underwriting, placement, market-making, marketing, and sales • Operating infrastructure and validating transactions
Wallets and custody	• Provision of custodial (hosted) wallet and custody services • Provision of non-custodial (unhosted) wallets
Transfer and transactions	• Payment for/of goods, services, gifts, and remittances. • Exchange between crypto-assets or against fiat currencies, clearing and settlement
Investment, leverage and risk management	• Use as collateral to borrow/purchase other crypto assets • Trading/borrowing/lending of crypto assets • Direct/outright exposures to crypto assets • Synthetic/derivative exposures to crypto assets

Source: FSB Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets Consultive document 2022.

23 Regulating the Crypto Ecosystem, the Case of Unbacked Crypto Assets, IMF note 2022/007. Available at: www.imf.org/en/Publications/fintech-notes/Issues/2022/09/26/Regulating-the-Crypto-Ecosystem-The-Case-of-Unbacked-Crypto-Assets-523715

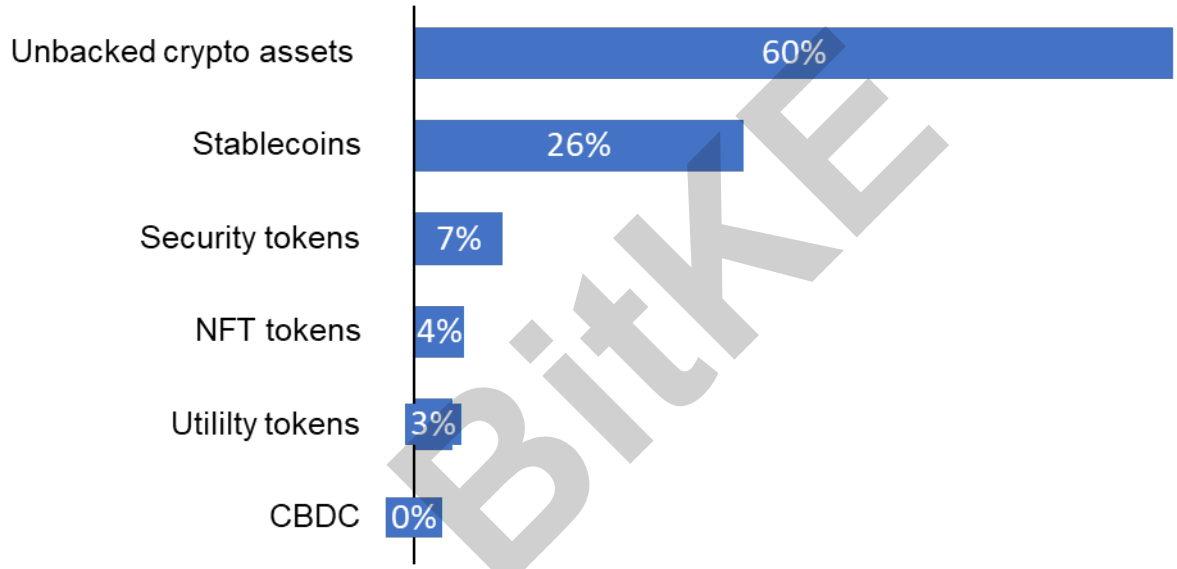
7. Key Findings from the Information Request

7.1 Supply-side

47 Crypto Asset FSPs responded substantively to the FSCA's Information Request[24].

7.1.1 Type of Crypto Assets

Figure 3: Types of Crypto Assets



The majority of Crypto Asset FSPs in South Africa provide financial services by making use of unbacked crypto assets (60%), followed by stablecoins (26%) such as USD Coin and Binance Coin. This is then followed by security tokens (7%) and NFT tokens (4%).

Unbacked crypto assets are the oldest and most widely recognized digital assets. They derive their value solely from supply and demand dynamics, without any physical or underlying asset to support them. The assets offer limited or no rights to token holders and are often issued through decentralized means. Unbacked crypto assets are primarily utilised for speculative purposes rather than serving as a means of exchange[25]. Notable examples of unbacked crypto assets include Bitcoin and Ether. Stablecoins on the other hand, aim to have stable price value by being linked to a single asset or basket of assets such as fiat currency, commodities, or other crypto assets.

24 While 56 submissions were made, some of the responses were received from licensed FSPs as a way of confirming that they do not perform any activities that constitute financial services in respect of crypto assets.

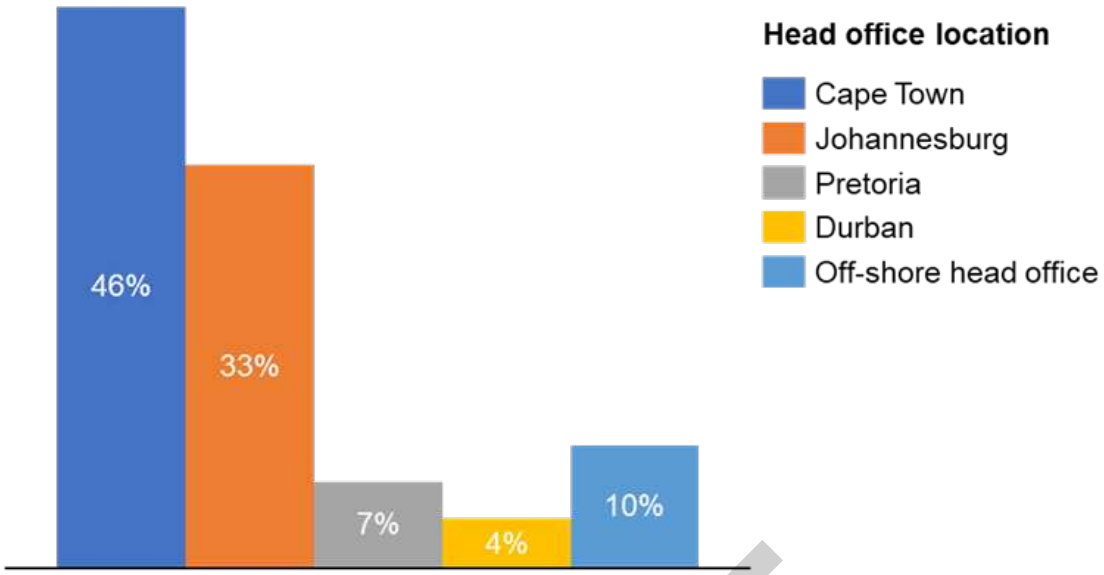
25 Regulating the Crypto Ecosystem, the Case of Unbacked Crypto Assets, IMF note 2022/007. Available at: https://www.imf.org/en/Publications/fintech-notes/Issues/2022/09/26/Regulating-the-Crypto-Ecosystem-The-Case-of-Unbacked-Crypto-Assets-523715

7.1.2 Head Office Location

Cape Town leads the way in head office location with the largest percentage of Crypto Asset FSPs having established their head offices in the city. It is followed by Johannesburg (33%) and Pretoria (7%). The results bear testimony to the fact that Cape Town is considered the largest technology hub in Africa and has been dubbed the Silicon Valley of Africa, home to more than 450 tech start-ups[26]. A small proportion of Crypto Asset FSPs operating in South Africa have their head offices in foreign countries.

26 BusinessTech. South Africa's 'silicon valley' has over 450 tech firms and employs more than 40,000 people. Available at: https://businesstech.co.za/news/technology/489253/south-africas-silicon-valley-has-over-450-tech-firms-and-employs-more-than-40000-people/

Figure 4: Head Office Location



The strong local presence bodes well for regulatory and supervisory protection. For the 10% of entities that have an off-shore head-office, consideration will need to be given to the requirements relating to having a local branch[27]. This is important because it, amongst other things, creates a physical presence that would allow the FSCA to have appropriate oversight over and ensure accountability of the institution conducting activities in South Africa.

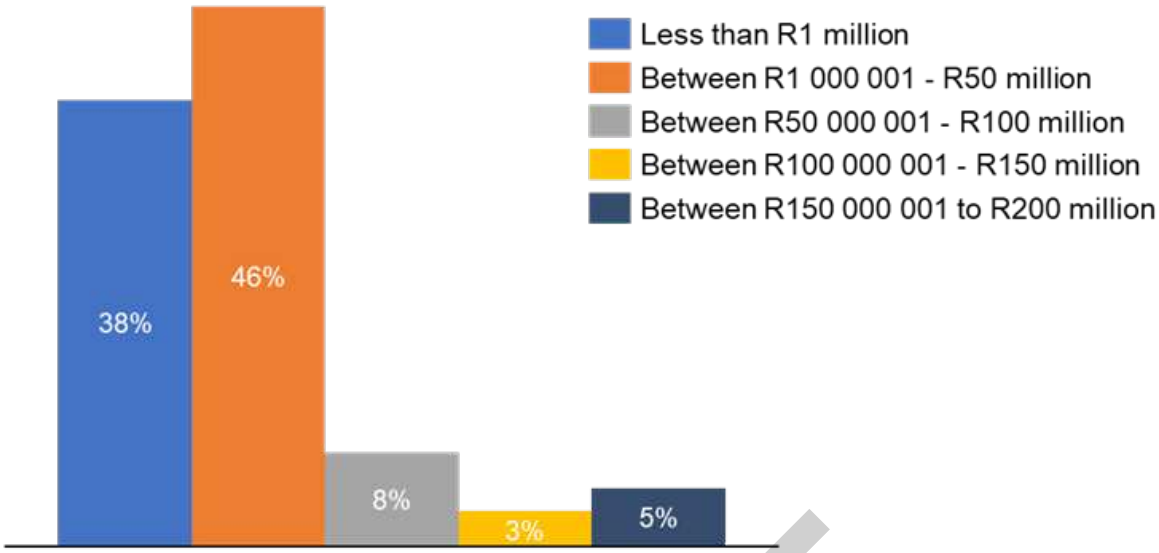
7.1.3 Summary of Annual Total Revenue (may comprise a combination of traditional and crypto asset activities)

The data received showed that 38% of the Crypto Asset FSPs received revenue less than ZAR one million, while 46% received revenue between ZAR 1 and 50 million. About 10% of Crypto Asset FSPs derive their income from both regulated[28] and unregulated financial services.

27 Even in the absence of a requirement of a local branch, they must register as an external company in terms of Section 23 of the Companies Act, as they will be engaging in a course of conduct or have engaged on a course or pattern of activities (in this case providing financial services as defined in FAIS) within the Republic over a period of at least six months, such as will lead a person to reasonably conclude that this offshore company intended to continually engage in business within the Republic.

28 "Regulated" means regulated in terms of the FAIS Act and includes all activities that constitute financial services.

Figure 5: Annual Total Revenue



7.2 Outsourcing Arrangements

7.2.1 Outsourced Services

KYC/AML, exchange platform, custody, cyber security, information technology services, and blockchain monitoring services are some of the activities that are outsourced by Crypto Asset FSPs. This means that some of the financial services in respect of crypto assets and technical activities inherent to the provision of crypto assets financial services are outsourced.

The outsourcing of the activities does not relieve Crypto Asset FSPs from their responsibilities to ensure fair treatment of customers. They, therefore, will have to comply with specific outsourcing requirements relating to the responsibilities of a Crypto Asset FSP, including requirements relating to:

- the ability, capacity, and authorisation (as required by law) of the person to whom the functions have been outsourced
- the contract that governs the outsourced arrangement
- oversight of the outsourced activities
- risk management controls and processes (including disaster recovery contingency plans)
- effective access to data related to the outsourced activities.

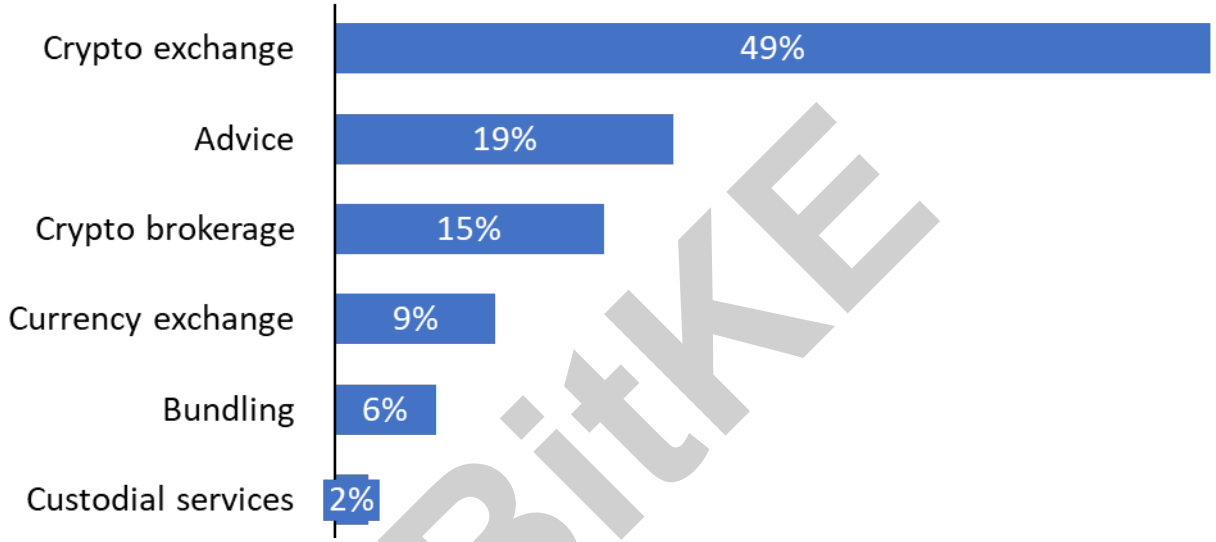
It should also be understood by market participants that outsourcing financial services activities can only be done to entities that are themselves licensed and regulated under the FAIS framework. This mitigates the risk of regulatory arbitrage.

7.3 Business Model

7.3.1 Business Model

The observed business models[29] are diverse. However, in some instances, the business models mirror traditional financial activities such as operating an exchange or providing advice. The only difference is that they use a different type of technology. These activities require consumers to trust centralised entities which is against the disintermediation function that crypto assets were designed for. The increasing significance of these alternative activities could result in them being categorised as systemic financial market infrastructures (FMIs). Going forward, it will be important to consider an equivalent regulatory and supervisory treatment for these crypto activities to their traditional counterparts, based on the "same activity, same risks, same rules" principle being embraced by certain international standard setting bodies[30] and regulators[31].

Figure 6: Summary of Business Models

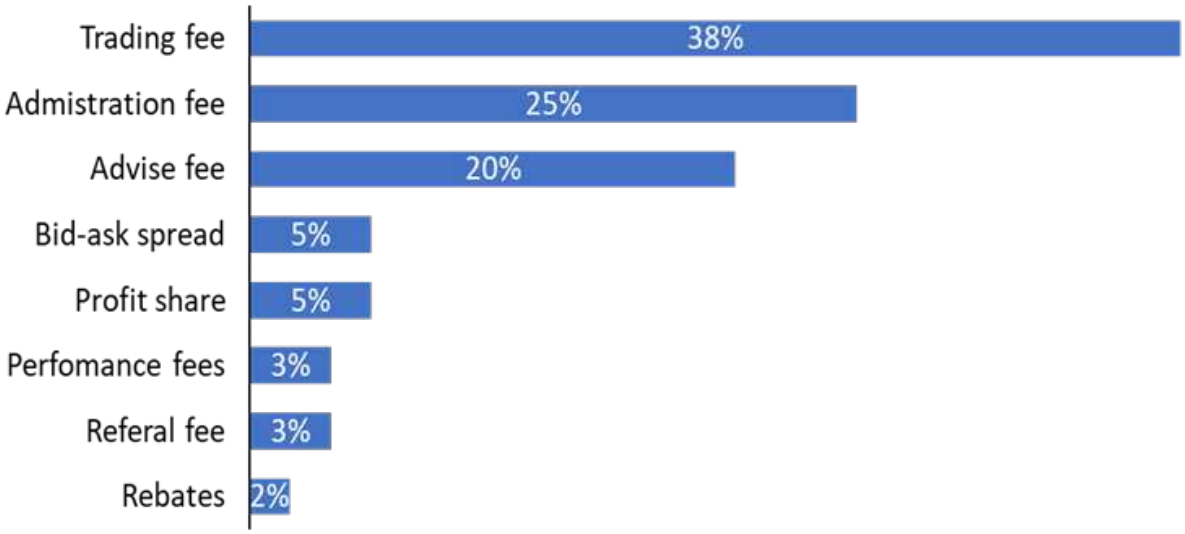


7.3.2 Remuneration Model[32]

The majority of Crypto Asset FSPs charge trading fees (38%) followed by 25% who earn their revenue from administration fees while 20% earn revenue from advice fees.

29 A business model describes how businesses create, deliver, and capture value.
30 Financial Stability Board proposes framework for the international regulation of crypto-asset activities. Available at: https://www.fsb.org/2022/10/fsb-proposes-framework-for-the-international-regulation-of-crypto-asset-activities/
31 Future financial services regulatory regime for cryptoassets. Available at: https://assets.publishing.service.gov.uk/media/63d94ea68fa8f51881c99eb4/TR_Privacy_edits_Future_financial_services_regulatory_regime_for_cryptoassets_vP.pdf
32 The remuneration model refers to the structure and formats used by Crypto Asset FSPs to compensate for the services rendered.

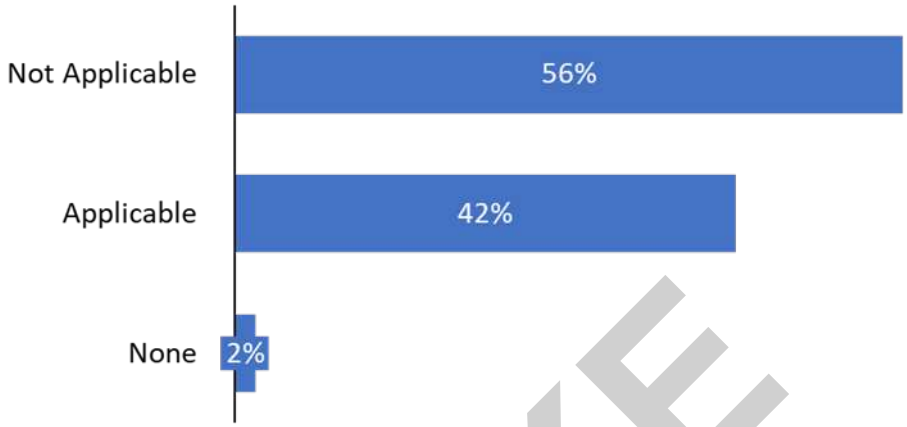
Figure 7 : Summary of Common Remuneration Model (%)



7.3.3 Cross Border Business Monitoring

56% of Respondents indicate that cross border monitoring is not applicable in their current operations, while 42% consider cross border monitoring as part of their business to promote good governance, fair treatment of customers, and regulatory compliance.

Figure 8 : Cross Border Business Monitoring Activities



Box 2: Summary of Cross-border Monitoring Activities

i. Implementation of KYC process to ensure adherence to AML and Combating the Financial of Terrorism (CFT) requirements
ii. Implementation of background checks, risk assessment (related to customers, geographic area, products and services and delivery channels) and transaction monitoring
iii. Personal and business allowance monitoring and confirmation that clients are aware of exchange control limits
iv. Implementation of key governance policies and procedures ordinarily incumbent on licensed financial services provide
v. Sign up with regulated providers
vi. Performs due diligence on all providers and exchanges
vii. Assessment of geographical risk and localised standards are measured against South African standards
viii. Obtain trust scores from various centralised sources to ascertain the legitimacy of a correspondent Crypto Asset FSPs

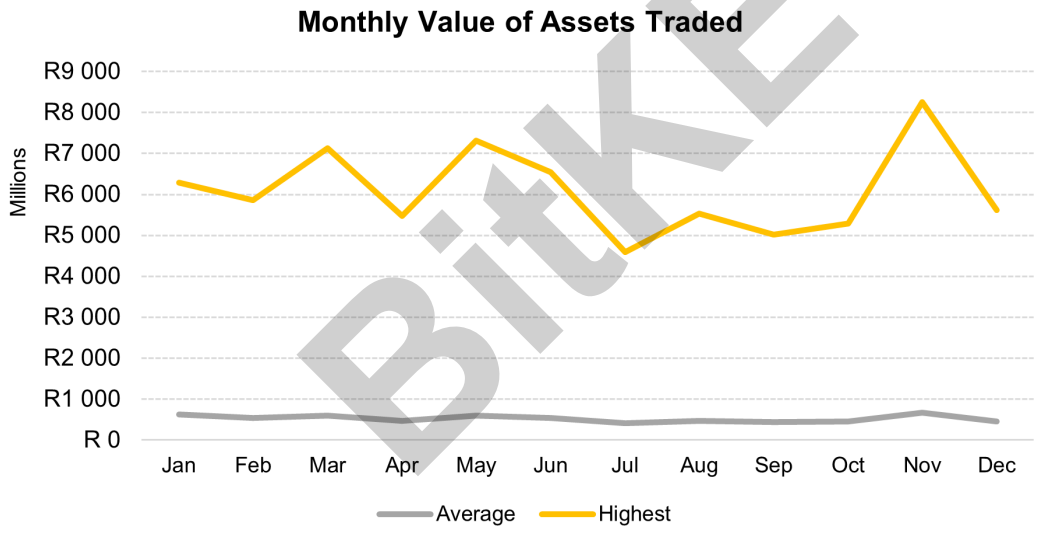
Effective cross border monitoring mitigates and reduces the risk of money laundering and the financing of terrorism activities. This is essential in protecting the integrity of markets and the global financial framework.

7.4 Market Dynamics

7.4.1 Value of Crypto Assets Traded per Month in 2022

South African Crypto Asset FSPs recorded the highest monthly transaction value which was over ZAR8 billion in November 2022. The average crypto assets traded were approximately ZAR520 million per month during the year. South Africa is one of the African countries with the highest number of crypto assets users in the region[33]. Monitoring changes in trading patterns may be an important conduct risk indicator; for example, substantial increases in trading volumes may bring additional operational risk, and unusual trading could signal market abuse.

Figure 9 : Monthly Crypto Assets Traded from January 2022 to December 2022



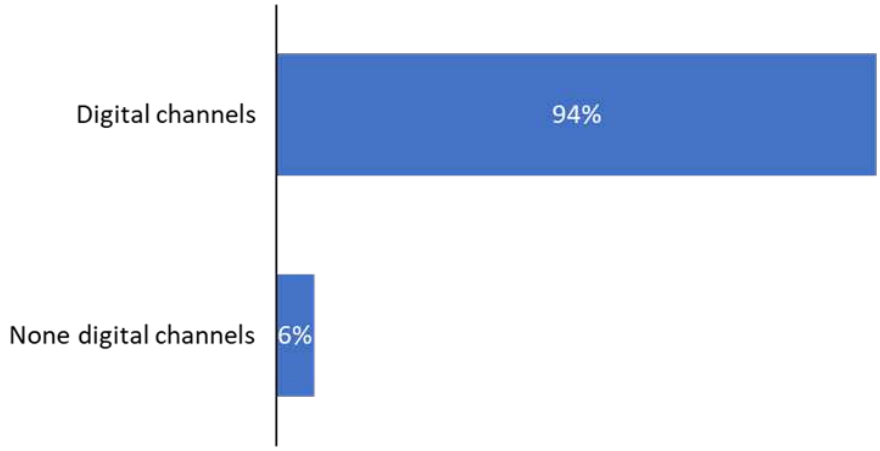
7.4.2 Distribution channels

Distribution channels are the avenues through which customers encounter a business and become part of the sales cycle. They allow the business to communicate directly, obtaining feedback from customers that in turn assists with improving its product offerings and customer experience. Crypto Asset FSPs should satisfy themselves that the channels used to distribute their financial products are appropriate to the nature and complexity of that financial product and the targeted financial customer.

Over 94% of the Crypto Asset FSPs use digital channels[34] to distribute and market their products and services while 6% utilise non-digital channels[35].

33 Africa's Growing Crypto Market Needs Better Regulations. Available at: https://www.imf.org/en/Blogs/Articles/2022/11/22/africas-growing-crypto-market-needs-better-regulations
34 Digital channels include emails, social media platforms, website, podcasts.
35 Non-digital channels include in person meetings, billboards, and direct phone calls

Figure 10: Distribution Platforms and Strategies

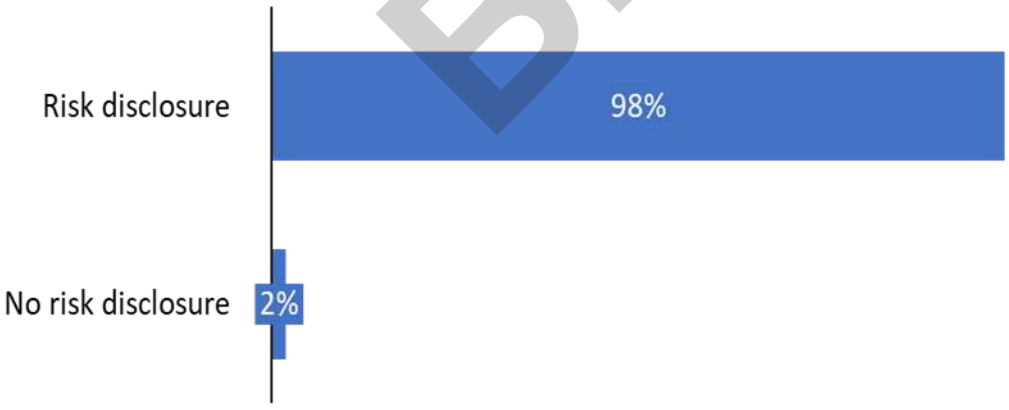


Some of the marketing strategies employed include building the client base through trading on peer-to-peer exchanges and in-person meetings with clients to discuss product and services offering.

7.4.3 Risk Disclosure

Almost all Crypto Asset FSPs claim to disclose the risks relating to crypto asset activities to their customers and the public. The accuracy of this claim and the quality of disclosure will need to be monitored over time.

Figure 11: Risk Disclosure



The risk disclosures are made to the clients is several ways which include:

Box 3: Summary of Risk Disclosure

i. Risks are disclosed when clients are signing up.
ii. Risk disclosures are made on the website, exchange platform and in all communication with the clients.
iii. Risk disclosures are made on social media platforms, webinars, events and media interviews.
iv. Clients sign a crypto assets declaration describing the risks and that they understand the implications of trading with crypto assets.

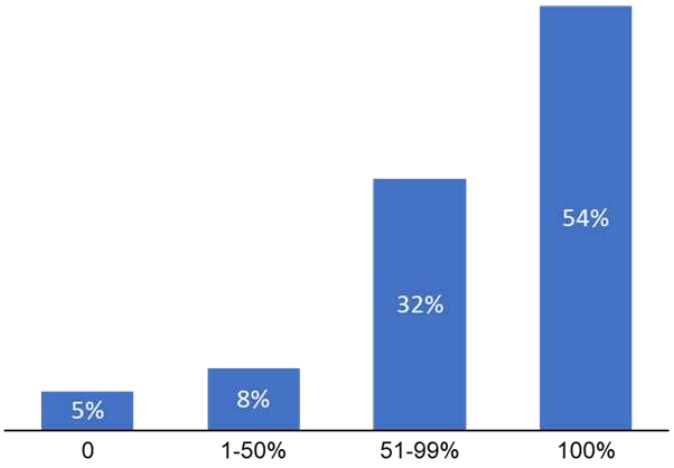
7.5 Demand Side

7.5.1 Proportion of Retail Customers

The information gathered suggests that more than half of the Crypto Asset FSPs have 100% of their businesses built around retail customers.

The activities identified span both financial markets and financial services. This will be instructive for the development of both the COFI Bill and Financial Markets Act (FMA) revisions.

Figure 12: Proportion of Retail Customers

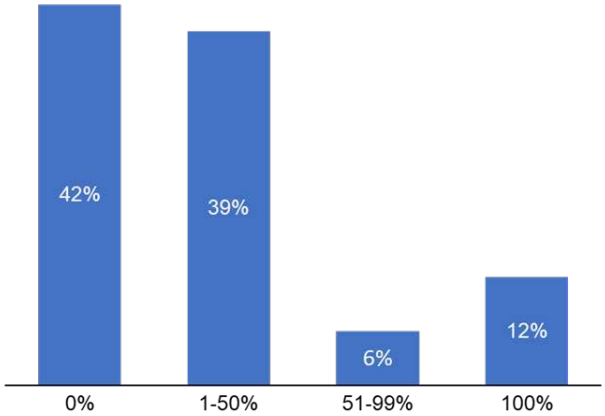


Understanding the extent of retail participation over time will be critical in assessing the consumer protection risk and impact of this market. Under the COFI Bill, provision is expected to be made for a targeted regulatory framework for retail customers. Understanding marketing and distribution strategies, as highlighted above, will be a particular focal point. Consistent with international developments, consideration may be given to prohibiting more risky products and services from being marketed to higher risk and more vulnerable customer groups[36].

7.5.2 Proportion of Financial Institutions

The information gathered suggests that approximately 12% of Crypto Asset FSPs have 100% of their businesses centered around financial institutions. The statistics also reflect that Crypto Asset FSPs have no customers which are retirement funds.

Figure 13: Proportion of Financial Institutions



36 FCA bans the sale of crypto-derivatives to retail consumers. Availalble at: https://www.fca.org.uk/news/press-releases/fca-bans-sale-crypto-derivatives-retail-consumers

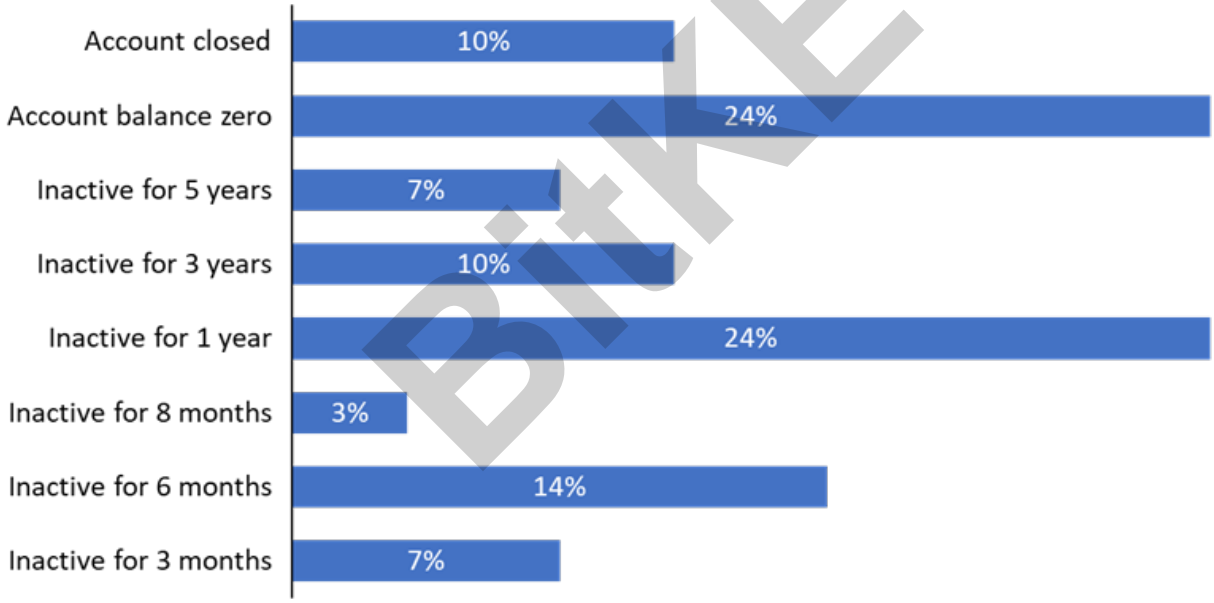
7.5.3 Definition of Dormant Account

The results suggest three main approaches to classification of dormancy, with most specifying some level of account inactivity:

- account is closed (10%)
- account has a zero balance (24%)
- level of account inactivity (65%)

Understanding the extent of dormant crypto asset accounts and unclaimed crypto assets is important to inform further development of the proposed framework for unclaimed financial assets, including dormant accounts[37], that are currently under consideration. It will also provide insights into how Crypto Asset FSPs are embedding the Treating Customers Fairly (TCF) principles into their processes and business practices and will provide supervisory insights into the suitability of the product for those customers.

Figure 14: Definition of Dormant Account



Some Crypto Asset FSPs reported that they have interventions in place to respond to dormant accounts. For instance, their consultants reach out to customers to understand why they (the clients) have stopped using their accounts; the account is suspended until the client signs a new annual mandate; or the dormant account automatically triggers an alert on AML/CFT tools.

37 See the Discussion Paper on 'A Framework for Unclaimed Financial Assets in South Africa' .

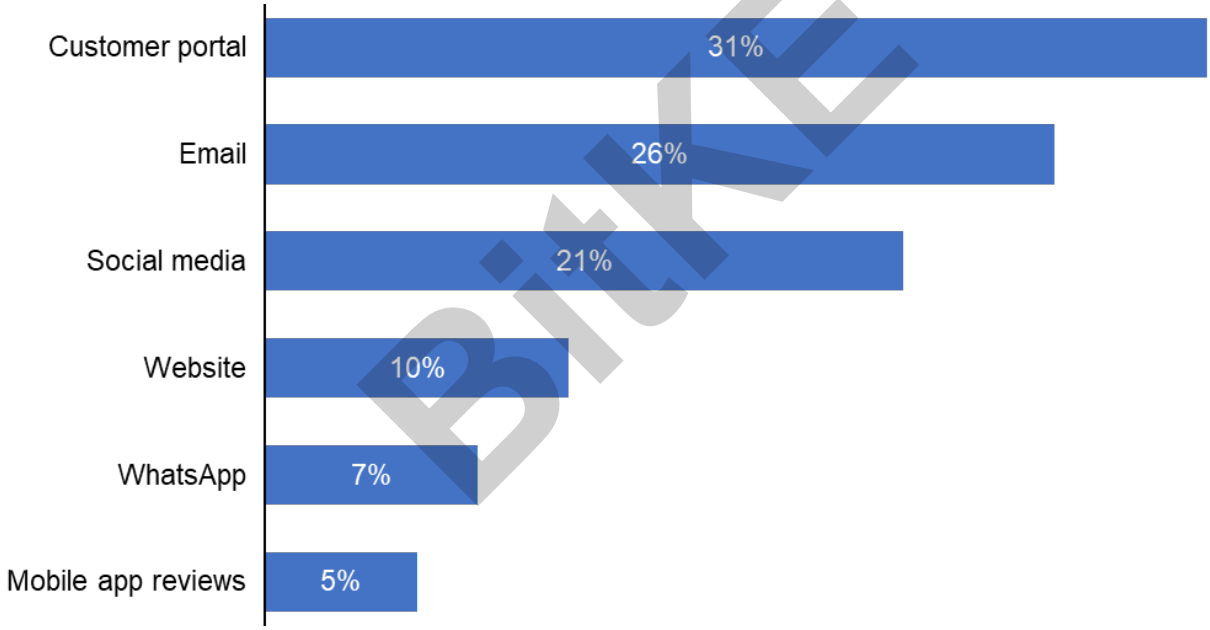
7.6 Complaints

Crypto Asset FSPs are required to establish and maintain an internal complaints management framework, as the effective management of complaints is a vital component of TCF and contributes to the protection of financial customers. Such framework, inter alia, must provide for adequate systems for record keeping, monitoring, and analysis of complaints to enable Crypto Asset FSPs to identify trends and incidence of complaints, manage conduct risks, and effect improved outcomes and processes for customers.

7.6.1 Sources of Complaints

The average number of customer complaints received between January 2022 to December 2022 was over 1 500 and were communicated via digital platforms.

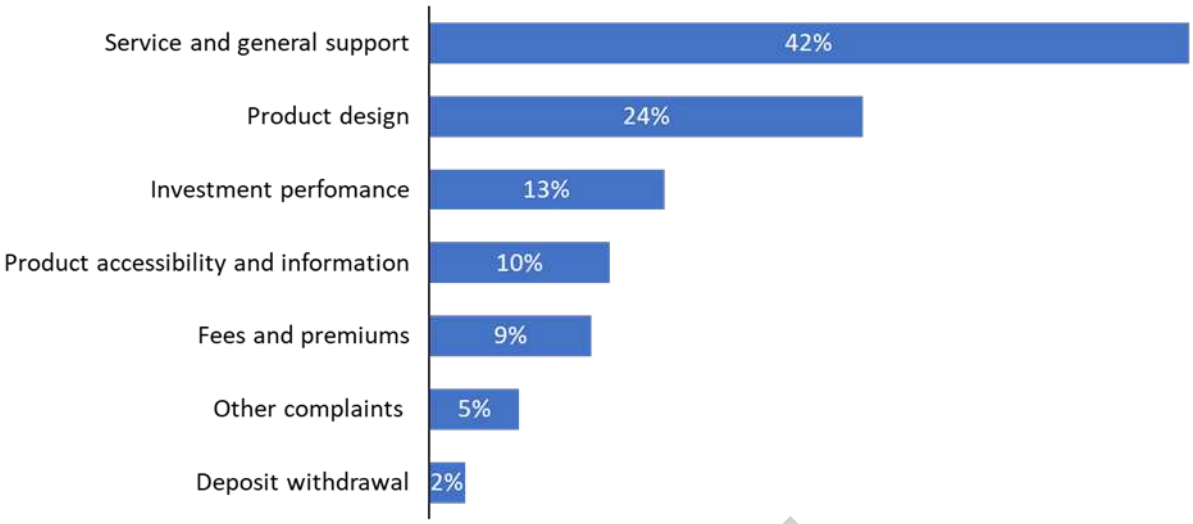
Figure 15 : Source of Complaints



7.6.2 Categorisation of Complaints

A large proportion of complaints were categorised as service and general support (42%), product design (24%) and investment performance (13%). The nature of complaints reflected suggests that the percentage of complaints relating to 'service' could be higher than reported suggesting that achieving good customer outcomes may not yet be embedded within the processes and practices of the Crypto Asset FSPs. The product and investment complaints may suggest that the crypto asset products are not suitable for the target market or may not be performing as customers were led to expect. The FSCA will need to explore whether customers are provided with key information on their products on a regular and ongoing basis and that information provided is appropriate and being understood by the target market. Complaints data is a valuable supervisory source of information that enables the FSCA to identify and more quickly and effectively respond to risks.

Figure 16 : Categorisation of Complaints



As an important pillar of TCF[38], the FSCA will also in future monitor complaints received through the ombud system to identify potential systemic conduct issues.

7.6.3 Complaints Handling Policy

The majority of crypto assets Crypto Asset FSPs have interventions in place to handle complaints. However, Crypto Asset FSPs will need to align the management and processing of complaints with the TCF outcomes. Some of these interventions are summarised in table 2 on the next page.

Table 2: Summary of Complaints Handling Interventions

Complaints Handling Interventions
• Communicate with clients, how and when they will be updated on the progress of their complaints.
• Specifies channels through which customers can submit complains either through email, telephone, website, application, or customer representative.
• Specifies timelines of complains handling process.
• Highlights the need to maintain comprehensive records of all complaints and resolution.
• A structure approach that describes how complains are addressed and resolved is in place.

38 Treating Customers Fairly (TCF) is an outcomes based regulatory and supervisory approach designed to ensure that regulated financial institutions deliver specific, clearly set out fairness outcomes for financial customers.

8. Conclusion

The FSCA aims to promote the development of an innovative, inclusive, and sustainable financial system in South Africa. Research undertaken in support of this objective allows the FSCA to better understand fintech and other related innovations currently taking place. The findings of this research contribute to the growing body of knowledge on financial sector innovations, both domestically and internationally. This allows us as the regulator, but also other affected stakeholders, the ability to better understand and explore how we can more proactively assess and respond to emerging risks and opportunities.

The information drawn will support the work of the FSCA, particularly in relation to the development of licensing, supervision, and regulatory frameworks for Crypto Asset FSPs, by highlighting consumer exposure to crypto assets. In line with risk-based supervision, the identified risks will support the FSCA's regulatory and supervisory approaches going forward. It is envisaged that this will assist the authority in making more informed decisions regarding the potential future regulation of crypto assets-related activities.

Annexure 1: Essential Functions, Risks and Relevant International Standards

Function 1: Creation, issuance, redemption, distribution, and underlying infrastructure of crypto assets

Activities	Service providers and activity/entity pair	Key Regulatory and financial stability risks and vulnerabilities	Potentially relevant international standards and policies
1. Creating, issuing and redeeming crypto assets (Developing protocols, designing a smart contract and choice of the consensus mechanism), placement, marketing and sales	1. Issuers, including those: i) -not incorporated as a legal entity. ii) -incorporated as a legal entity but not licensed or registered by regulatory authorities. iii) -incorporated as a legal entity licensed or registered by regulatory authorities. 2. Project development team 3. An underwriter or facilitator of issuance or capital formation. 4. An entity undertaking marketing and sales	**1) Credit risks:** the issuer may fail to meet redemptions in stressful situations if they have promised redemption to users. **(2) Liquidity risk:** Selling crypto assets quickly, especially during periods of high volatility or market stress can be difficult. This lack of liquidity can create significant losses for investors who need to sell their assets quickly. **(3) Misconduct risk** (insider information, price manipulation, false disclosure); Weak governance related to protocols, and consensus mechanism. **(4) Conflicts of interest** in designing the arrangement, selecting participant entities (especially in permissioned DLTs) Some issuance lack clear definition of roles and responsibilities of the governing body and lack of effective contractual and accountability mechanisms among participating entities. Absence of a clearly identifiable entity that can be held accountable for meeting rights of holders, addressing operational risk and ensuring compliance with AML/CFT standards. **Others: ML/TF risks**	1. **IOSCO** Objectives and Principles of Securities Regulation for underwriting 2. **CPMI-IOSCO** Principles for financial market infrastructures (PFMI) (only if an activity is performed by a systemically important FMI) 3. **CPMI-IOSCO** Guidance on the Application of the Principles for Financial Market Infrastructures to stablecoin arrangements

Function 1: Creation, issuance, redemption, distribution, and underlying infrastructure of crypto assets

2. Operating the infrastructure and validating transactions	1. Permissioned DLT: Entities that perform validation and settlement of transactions. They are normally selected and authorised beforehand. 2. Permissionless DLT: Validator nodes (Miners) can be set up by anyone fulfilling the technical requirements and the protocols. 3. Centralised platforms (often a trading platform that performs many other functions) that keep records off-chain, hold assets in custody, and settle transactions.	(1) Operational risks (including cyber risks): risk from the technology and operations the issuer controls. This includes smart contracts design risks, deficient cyber security resulting in unavailability or hacking of wallets that hold/mint/burn tokens, other operational risk events such as loss of keys, fraud, mismanagement of token supply or trustworthy settlement of transactions, validation and settlement patterns of cross-chain transfer. Operational risk at the issuer level could lead to, e.g., a disruption of users' ability to transfer their tokens or a loss of value of the tokens. Misconduct such as miners front-running attack in which a miner includes its own transaction in the block instead of someone else's and does not include the original transaction. (2) Settlement risk Crypto assets may have settlement risks when used for payments. (3) Climate transition risk affecting validation and scalability: changes of the consensus protocol and validation mechanisms, both voluntary or imposed by legal restrictions for a certain type of activities (ban from certain territories and/or climate restrictions. (4) Concentration risk: concentration of validators and technology service providers. (5) Third-party risks (e.g., a failure that arise in sub-contractors and other centralised entities that keep records or network services). (6) Others: AML/CFT, financial crime (e.g., direct exchange of illegal proceeds for mined coins with no transaction history).	1. BCBS Principles for Operational Resilience 2. BCBS Principles for the Sound Management of Operational Risk 3. CPMI-IOSCO Principles for financial market infrastructures (PFMI) (only if the activity is performed by a systemically important FMI) 4. CPMI-IOSCO Guidance on the Application of the Principles for Financial Market Infrastructures to stablecoin arrangements 5. CPMI-IOSCO, Guidance on Cyber Resilience for Financial Market Infrastructures (only if the activity is performed by a systemically important FMI) 6. IOSCO Objectives and Principles of Securities Regulation 7. IOSCO Principles on Outsourcing 8. FSB Regulation, Supervision, and Oversight of "Global Stablecoin" Arrangements 9. FSB Effective Practices for Cyber Incident Response and Recovery

Function 2: Wallets and custody

Activities	Service providers and activity/entity pair	Key Regulatory and financial stability risks and vulnerabilities	Potentially relevant international standards and policies
3. Provision of custodial (hosted) wallet and custody services	Custody service providers could be i) regulated financial institutions; They manage crypto assets (i.e., private keys) for retail and institutional customers, usually provided in conjunction with other services such as offline key management services and insurance services as a hedge against loss, in addition to the transfer and exchange of crypto assets. They may manage crypto-assets administratively or jointly (e.g., using multi-signature) with their customers. ii) other entities; They manage crypto assets (i.e., private keys) on behalf of their customers, but may be exempt from regulation for reasons such as the sole activity of management of crypto-assets is not within the regulatory perimeter in some jurisdictions or they manage crypto-assets jointly with their customers and have no controlling authority. In other cases, the actual situation is unclear and it is challenging for authorities to determine whether they are within the perimeter. In addition to this, there are some entities that do not comply with regulations, such as unregistered service providers. iii) DeFi protocols They manage users' crypto assets or information about their interests in crypto assets using smart contracts that pool users' crypto assets, typically as part of	(1) Operational risks: cyber security risks leading to unavailability or un-authorised outflow of customers' crypto-assets; This includes technical vulnerabilities including wallet software design and cyber security measures, and operational vulnerabilities such as loss or mismanagement of private keys. Misconduct risk from, e.g., loss of funds due to negligence, fraud/theft, poor administration, inadequate record keeping, or co-mingling of assets. (2) Concentration risks: When a small number of service providers, wallet software or software libraries account for the majority of market share, failures/vulnerabilities in them affect many customers' crypto assets (e.g., loss of crypto assets) and spill over to crypto assets ecosystem. (3) Third-party risks (e.g., a failure that arises in sub-custodians and other subcontractors) (4) Others: AML/CFT N.B. The type of custody service varies significantly with different risk features, covering operational, conduct, and market knock-on effects, depending on the contractual agreement between the provider and the user.	1. BCBS Principles for Operational Resilience 2. BCBS Principles for the Sound Management of Operational Risk 3. BCBS Principles for Sound Liquidity Risk Management and Supervision 4. CPMI-IOSCO Principles for financial market infrastructures (PFMI) (only if the activity is performed by a systemically important FMI) 5. CPMI-IOSCO, Guidance on Cyber Resilience for Financial Market Infrastructures (only if the activity is performed by a systemically important FMI) 6. IOSCO Objectives and Principles of Securities Regulation 7. IOSCO Recommendations Regarding the Protection of Client Assets 8. IOSCO Recommendations for Liquidity Risk Management for Collective Investment Schemes 9. IOSCO Principles on Outsourcing 10. FSB high-level recommendations (Specific to global stablecoin arrangements) 11. FSB Effective Practices for Cyber Incident Response and Recovery 12. FATF Standards and Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers

Function 2: Wallets and custody

4. Provision of noncustodial (unhosted) wallets	i) regulated financial institutions; To offer solutions for retail and institutional customers or for general public to manage their crypto assets (i.e., private keys) themselves. Users use unhosted wallets for considerations on cybersecurity, transaction costs, etc. and, they typically use their self-hosted wallets in combination with regulated entities' services such as an exchange of crypto assets. ii) others; They may only develop and sell the hardware/software and are typically not subject to regulations. There may be some entities who do not comply with regulations. iii) DeFi protocols They may offer solutions for users or for general public to manage their crypto assets (i.e., private keys) themselves to promote the use of DeFi protocol. Other entities might provide support services for wallets.	(1) Operational risks: including cyber security risks leading to unavailability or unauthorised outflow of users' crypto assets; This includes technical vulnerabilities including wallet software design. Operational vulnerabilities are often due to users (e.g., carelessness, lack of knowledge). (2) Concentration risks: When a small number of wallet providers, wallet software or software libraries account for the majority of market share, failures/vulnerabilities in them affect many users' crypto assets (e.g., loss of crypto assets) and spill over to crypto assets ecosystem. (3) Third-party risks (e.g., a failure of hardware/software wallet that arise in sub-contractors) (4) Others: AML/CFT (Users can use the wallet without going through KYC, CDD, STR etc.)	1. BCBS Principles for Operational Resilience 2. BCBS Principles for the Sound Management of Operational Risk 3. CPMI-IOSCO Principles for financial market infrastructures (PFMI) (only if the activity is performed by a systemically important FMI) 4. CPMI-IOSCO, Guidance on Cyber Resilience for Financial Market Infrastructures (only if the activity is performed by a systemically important FMI) 5. IOSCO Objectives and Principles of Securities Regulation 6. IOSCO Principles on Outsourcing 7. FSB high-level recommendations 8. FSB Effective Practices for Cyber Incident Response and Recovery

Function 3: Transfer and transaction

Activities	Service providers and activity/entity pair	Key Regulatory and financial stability risks and vulnerabilities	Potentially relevant international standards and policies
5. Payment for/of goods, services, gifts and remittances	Payment and settlement providers, including: i) Traditional FMIs (both payment and securities systems, e.g., Credit Card provider); ii) Financial institutions (including banks); iii) Other entities37, typically centralised trading platforms; iv) DeFi protocols.	(1) Market risks: excessive volatility, rapid price swings can hamper the use of crypto-assets in transactions, particularly in settlement operations. Sharp depreciation may generate outflows and jeopardize the use of certain crypto assets. (2) Counterparty credit risks: Depending on the mismatch of exposures of the two payment legs. (3) Operational risks, in particular for unregulated entities whose records may be less reliable including cyber security risks, and legal risks where uncertainties of the legal status of crypto-assets and their broader ecosystem could expose entities different forms of legal risks. Misconduct by any service provider of the crypto-asset ecosystem, in particular, in unregulated centralised trading platforms; (4) Reputational risks, in particular for traditional FMIs that promote or enable the use of crypto-assets in payment transactions, which could face reputational risks in the event of payment failure. (5) Exchange rate risk. Using for payments or clearing, crypto assets could substitute local currency, especially in EMDEs and non-reserve currency nations. This can generate volatility and changes in the level of exchange rate. (6) Settlement risks. Crypto assets may have settlement risks when used for payments. (7) Others: Investor protection: lack of protection discourages users from using in transactions for payment, in cases of unregulated entities. A specific case relates to the lack of legal clarity in single instruments (e.g., whether it is a financial	1. FATF Standards and Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers 2. CPMI-IOSCO, Guidance on Cyber Resilience for Financial Market Infrastructures 3. CPMI-IOSCO Principles for financial market infrastructures (PFMI) (only if the activity is performed by a systemically important FMI) 4. CPMI-IOSCO Guidance on the Application of the Principles for Financial Market Infrastructures to stablecoin arrangements 5. BCBS, Principles for Operational Resilience 6. BCBS, Revisions to the Principles for the Sound Management of Operational Risk 7. BCBS, Prudential Treatment of Crypto asset Exposures (second consultation)

Function 3: Transfer and transaction

6. Facilitate the exchange of crypto assets: either between crypto-assets or between crypto-assets and fiat-currency, or fiat currency-backed financial contracts	i) Traditional FMIs ii) Traditional financial institutions, broker-dealers, custodians iii) Unregulated entities, such as an unregulated centralised trading platform iv) DeFi protocols	(1) Market risks: excessive volatility, rapid price swings can hamper the use of crypto assets in transactions, particularly in settlement operations. Sharp depreciation may generate outflows and jeopardise the use of certain crypto assets. (2) Counterparty credit risks: Depending on the mismatch of exposures of the two payment legs. (3) Operational risks, in particular for unregulated entities whose records may be less reliable including cyber security risks, and legal risks where uncertainties of the legal status of crypto-assets and their broader ecosystem could expose entities different forms of legal risks. Misconduct by any service provider of the crypto-asset ecosystem, in particular, in unregulated centralised trading platforms; (4) Reputational risks, in particular for traditional FMIs that promote or enable the use of crypto-assets in payment transactions, which could face reputational risks in the event of payment failure. (5) Exchange rate risk. Using for payments or clearing, crypto assets could substitute local currency, especially in Emerging markets and developing economies (EMDEs) and non-reserve currency nations. This can generate volatility and changes in the level of the exchange rate. Others: Conflicts of interest associated with exchanges. The use of crypto assets may compete with fiat currency in EMDES and amplify volatility to non-reserve currencies and currencies of EMDEs. The above-mentioned risks could be amplified in the case of FIs with direct or indirect exposures due	1. FATF Standards and Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers 2. CPMI-IOSCO, Guidance on Cyber Resilience for Financial Market Infrastructures 3. CPMI-IOSCO Principles for financial market infrastructures (PFMI) (only if the activity is performed by a systemically important FMI) 4. CPMI-IOSCO Guidance on the Application of the Principles for Financial Market Infrastructures to stablecoin arrangements 5. BCBS, Principles for Operational Resilience 6. BCBS, Revisions to the Principles for the Sound Management of Operational Risk 7. BCBS, Prudential Treatment of Crypto asset Exposures (second consultation)

Function 4: Investment, lending, insurance, leverage and risk management

Activities	Service providers and activity/entity pair	Key Regulatory and financial stability risks and vulnerabilities	Potentially relevant international standards and policies
7. Use as collateral to borrow other crypto assets, including stablecoins	Institutional investors, they can be i) Centralised investor entity (e.g., hedge funds, family offices, pension funds, can be either traditional FIs or unregulated entities) ii) Centralised crypto asset trading platforms iii) DeFi protocols Other entities providing support services, such as custodian, advisor, and asset manager. They can also, be any of the three above categories.	(1) Credit risk: leverage magnifies potential losses and financial stability consequences of losses (e.g., liquidity impact of unwinding collateralized positions in response to price moves). (2) Counterparty credit risk: Collateralisation exposes the lender to the value of crypto assets. Collateral value and borrower solvency are likely to be correlated. (3) Others: Risk contagion as losses and liquidity stresses spill over to the core part of the financial system. Consumer protection when engaging retail investors Crypto assets allow for repeated rehypothecation and leverage, creating the possibility of very sharp declines and automated unwinding and liquidation. This hidden leverage may be difficult for regulators to monitor and address.	1. BCBS standards on capital and liquidity 2. CPMI-IOSCO Principles for financial market infrastructures (PFMI) (only if the activity is performed by a systemically important FMI) 3. IOSCO Objectives and Principles of Securities Regulation 4. IOSCO Recommendations for Liquidity Risk Management for Collective Investment Schemes

Function 4: Investment, lending, insurance, leverage and risk management

8. Lending in crypto assets (Including direct lending in crypto-assets or facilitator for traditional financial instruments i.e., loans, derivatives, investment vehicles, etc.)	Lenders of crypto-assets or lenders that accept crypto assets in business, they might be: i) Centralised crypto asset platforms ii) DeFi protocols iii) Traditional financial institutions including banks Other entities providing support services, such as custodian, advisor, asset manager. They can also be any of the three above categories.	(1) Liquidity risks, (2) Credit and counterparty credit risk: the risk that the counterparty will fail to meet its obligations in accordance with agreed terms. This risk is particularly relevant in lending operations between users involving crypto-assets: as such, high level of volatility of crypto-assets may amplify this source of risk (3) Market risk related to investing assets with proceeds from depositors/investors (4) Operational risks fraud, failed process or infrastructure failure. (5) Others: Market integrity related to inadequate disclosure, misconduct in sales and promotions. Consumer protection when engaging retail investors. Risks may mutually reinforce and give rise to the rapid transmission of stress due to tight interconnections. Use of crypto-assets in traditional financial activities may create new risks, such as elevated volatility, technical risks, and sudden price dislocations ("flash crashes") and increases the potential for stress in crypto-asset system to spill over to the traditional financial system.	1. IOSCO, Report on Issues, Risks and Regulatory Considerations Relating to Crypto- Asset Trading Platforms 2. BCBS, Prudential Treatment of Crypto asset Exposures (second consultation) 3. CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI) (only if the activity is performed by a systemically important FMI)
9. Insurance	Insurance of digital assets (e.g., crypto-asset wallets), holding of digital assets and underwriting of crypto-related risks. Also includes replacement of fiat currency as a form of payment (premiums and claims). Important to note that there is little to no activity in / exposure to digital assets in the insurance industry i) Traditional insurers ii) Centralised platforms iii) DeFi protocols (very rare in practice due to difficulty in pricing the risk)	(1) Credit risk, market risk, liquidity risks in relation to accepted/ invested etc. crypto assets (2) Operational risks for insurers in relation to (i) holding of own assets (custody of keys etc.), (ii) transfers of crypto assets, (iii) conversions in fiat money, and (iv) compliance with AML/KYC regulations	IAIS: No specific standards and no specific guidance on insurance based on crypto assets exist. However, general standards apply, e.g., on risk management and internal controls (ICP 8), valuation of assets and liabilities (ICP 14), and investments (ICP 15) whereby the supervisor requires the insurer to invest only in assets where it can properly assess and manage the risks.

Function 4: Investment, lending, insurance, leverage and risk management

10. Direct/outright exposures to crypto assets (including, writing of products, margining, market making, etc.)	1. Institutional investors, retail investors, banks, and insurers 2. Centralised crypto asset trading platforms 3. Brokerage firms/ investment advisers 4. Settlement provider 5. Custodian They can be: i) Traditional FMIs ii) Traditional financial institutions (Bank, insurance, funds) iii) Unregulated centralised platforms iv) DeFi protocols	(1) Market risks, including basis risks in hedging (2) Liquidity risks (3) Credit and counterparty credit risks (4) Operational risks. (5) Concentration risk (6) Others: Market integrity/investor Protection. Holding crypto assets outright gives rise to the risks outlined above but is also a necessary condition for generating the risks posed by crypto assets when used as a means of payment or as collateral.	1. IOSCO, Report on Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms (2020) 2. IOSCO, Consultative Report on Principles for the Regulation and Supervision of Commodity Derivatives Markets (2021) 3. IOSCO Recommendations Regarding the Protection of Client Assets 4. IOSCO Recommendations for Liquidity Risk Management for Collective Investment Schemes 5. IOSCO, Risk Mitigation Standards for Noncentrally Cleared OTC Derivatives (2015) 6. BCBS, Prudential Treatment of Crypto asset Exposures (second consultation) 7. CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI) (only if the activity is performed by a systemically important FMI)

Function 4: Investment, lending, insurance, leverage and risk management

11. Synthetic/ derivative exposure to crypto assets, including exposure to derivatives referenced by crypto assets	1. Institutional investors, retail investors, banks, and insurers 2. Centralised crypto asset trading platforms 3. Brokerage firms/ investment advisers 4. Settlement provider 5. Custodian They can be: i) Traditional FMIs ii) Traditional financial institutions (Bank, insurance, funds) iii) Unregulated centralised platforms iv) DeFi protocols	(1) Market risks, including basis risks in hedging. (2) Liquidity risks. (3) Credit and counterparty credit risks. (4) Operational risks. In particular misconduct in engaging retail investors and may spillover and have knock-on effects. (5) Concentration risks. Derivatives can give rise to virtually unlimited exposure, thereby amplifying losses and liquidity demands to sustain exposures In addition, given the indirect exposure to crypto assets it provides, traditional financial system participants who may have concerns with operational resilience of direct holding of crypto assets are incentivised to hold synthetic exposure to crypto assets, which would increase interconnectedness between crypto-asset markets and the traditional financial sector	1. IOSCO, Report on Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms (2020) 2. IOSCO Objectives and Principles of Securities Regulation 3. IOSCO, Consultative Report on Principles for the Regulation and Supervision of Commodity Derivatives Markets (2021) 4. IOSCO Recommendations Regarding the Protection of Client Assets 5. IOSCO Recommendations for Liquidity Risk Management for Collective Investment Schemes 6. IOSCO, Risk Mitigation Standards for Noncentrally Cleared OTC Derivatives (2015) 7. The Basel Framework (capital and liquidity standards) 8. BCBS, Prudential Treatment of Crypto asset Exposures (second consultation) 9. CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI) (only if the activity is performed by a systemically important FMI)

The nature of complaints reflected suggests that the percentage of complaints relating to 'service' could be higher than reported suggesting that achieving good customer outcomes may not yet be embedded within the processes and practices of the Crypto Asset FSPs. The product and investment complaints may suggest that the crypto asset products are not suitable for the target market or may not be performing as customers were led to expect. The FSCA will need to explore whether customers are provided with key information on their products on a regular and ongoing basis and that information provided is appropriate and being understood by the target market. Complaints data is a valuable supervisory source of information that enables the FSCA to identify and more quickly and effectively respond to risks.

Annexure 2

Some of the risks reported by the Crypto Asset FSPs are shown in Annexure 2.

Summary of common risks identified:

i. Regulatory risk: Governments around the world are still figuring out how to regulate the crypto asset industry. This uncertainty creates regulatory risk for investors, as new laws and regulations could significantly impact the value of their investments.

ii. Volatility risk: Crypto assets are highly volatile, which means their value can change rapidly and unpredictably. This volatility can lead to significant gains or losses for investors, making it a risky investment. Market risk: The crypto asset market is relatively new and has been unregulated, which makes it vulnerable to manipulation, fraud, and other market risks.

iii. Operational risk: Crypto assets are stored in digital wallets, which are vulnerable to hacking and theft. If a wallet is compromised, investors could lose their entire investment.

iv. Liquidity risk: Crypto assets can be difficult to sell quickly, especially during periods of high volatility or market stress. This lack of liquidity can create significant losses for investors who need to sell their assets quickly.

v. Cybersecurity risk: Crypto assets and the underlying blockchain technology are vulnerable to cyber-attacks and hacking attempts, which can lead to the loss of funds or personal information.

vi. Adoption risk: The widespread adoption of crypto assets by businesses and consumers is not yet assured, and failure to achieve widespread adoption could negatively impact the value of crypto assets.

vii. AML and KYC risk: Crypto assets can be used to facilitate illegal activities, such as money laundering and terrorist financing. To combat these risks, AML and KYC regulations require crypto exchanges and other virtual asset service providers (VASPs) to verify the identity of their customers and monitor their transactions for suspicious activity.

viii. Terrorist Financing risk: Crypto assets can be used by terrorist groups to finance their activities anonymously. This risk is mitigated by AML and KYC regulations, which help identify suspicious transactions and prevent the use of crypto assets for illicit purposes.

ix. Fraud risk: Crypto assets are vulnerable to fraud, such as Ponzi schemes, phishing scams, and fake ICOs. Investors can fall victim to these scams, losing their investments in the process.

Financial Sector Conduct Authority

Contact Us

For more information, or any queries regarding the contents of this paper, contact:

E-mail: fintech@fsca.co.za || info@fsca.co.za

Phone: +27 12 428 8000

Call Centre: 0800 20 37 22

Website: www.fsca.co.za

Riverwalk Office Park, Block B, 41 Matroosberg Road, Ashlea Gardens, Pretoria, 0002