

2nd
Edition



Corporate Governance code for
Gibraltar Crypto Funds

Addendum to the GFIA Corporate Governance Code for
Gibraltar Collective Investment Schemes

Corporate Governance Code for Gibraltar Crypto Funds

(An addendum to GFIA's Corporate Governance Code for Gibraltar Collective Investment Schemes)

1st Edition – 23rd October 2018

Editors: James Lasry & Aaron Payas

Authors: Adrian Hogg, Benjy Cuby & Johann Olivera

2nd Edition – 30th March 2022

Editors: Aaron Payas, Benjy Cuby, Derek Baglietto, Kristian Diani, Faith Howe, Federico Corbari,
James Lasry, Jay Gomez, Johann Olivero, Jonathan Garcia, Luke Walsh & Patricia Linares

Produced by: Gibraltar Funds & Investments Association

Email: info@gfia.gi

Website: www.gfia.gi

Address: PO Box 1289, Gibraltar GX11 1AA

Date of current edition: 30th March 2022

The Gibraltar Funds & Investments Association, 2022 all rights reserved. No part of this publication may be reproduced in any material form (including photography or storing it in any medium by electronic means and whether or not transiently or incidentally to some other use of this publication) without written permission by the copyright holder. Application for permission for use of copyright materials shall be made to the Gibraltar Funds & Investments Association. Full acknowledgements to authors, publishers and source must be given.

Foreword

In 2018 Her Majesty's Government of Gibraltar enacted legislation to regulate DLT businesses in Gibraltar and in doing so, Gibraltar laid the foundations for growth as a hub for blockchain and DLT businesses. This led to the territory being considered "crypto-friendly" by the sector, investors and managers alike.

Shortly after the implementation of the DLT regime, GFIA had the foresight of publishing its first edition of this Corporate Governance Code for Gibraltar Crypto Funds. The Code supplemented the Corporate Governance Code for Gibraltar Funds.

Whilst others across the globe were grappling with the emergence of this new industry, by 2018 Gibraltar already had a regulatory framework, a regulator (the Gibraltar Financial Services Commission) which understood the sector and in the case of funds, a Corporate Governance Code for Crypto Funds. All these elements clearly helped in cementing Gibraltar as a leading jurisdiction for crypto funds.

There is little doubt that the industry has benefitted from the guidance on best practices provided by the previous edition of this Code. As with the first edition, it is intended to be read in conjunction with the Corporate Governance Code for Gibraltar Funds and takes account of the last 4 years of the industry's experience and thereby builds on the first edition. This Code continues to highlight certain challenges that may appear in Crypto Funds that will not necessarily appear in funds that invest in other asset classes. As with the previous Code, the principle is "comply or explain". In other words, the Code is not there to say how something must be done. The Code is there to encourage Crypto Funds to consider certain issues and, where the licensee feels that those issues are better dealt with in a different fashion, to document their thought process.

Since the publication of the first code, we soon realised that it was, in fact, the world's first such code. A number of entities including compliance consultancies in London such as Laven Partners and other professional associations, such as the Gibraltar Association of Compliance Officers, have since endorsed the code. It is not surprising to us that work done on the Code and on the DLT legislation back in 2018 have enabled ¹Gibraltar to become the top destination in Europe for crypto funds.

We are extremely grateful for the hard work undertaken by both the Editors and Authors of the 1st Edition of this Code and the Editors who worked on this 2nd Edition. GFIA is an extremely pro-active and vibrant association with a unique ability to bring together competitors with the objective of achieving the best possible outcome for our industry and the jurisdiction as a whole. The publication of this Code is a perfect example, and it would not have been possible without them and their individual contributions and experiences.

Yours sincerely,

Jay J. Gomez
Chairman
Gibraltar Funds and Investments Association

James Lasry
Deputy Chairman
Gibraltar Funds and Investments Association

¹ pwc-elwood-annual crypto-hedge-fund-report-may-2020

1. DEFINITIONS AND INTERPRETATION

Definitions

In this code, the following words and expressions shall have the following meaning:

‘Crypto Code of Conduct’ “Code”	means this code of conduct.
‘Crypto Fund’	means a Gibraltar collective investment scheme which invests in Digital Assets or is holding Digital Assets in its investment portfolio.
‘Digital Assets’	means a digital representation of value or contractual rights that can be transferred, stored or traded electronically, and which may (though does not necessarily) utilise cryptography, distributed ledger technology or similar technology. For the purpose of Crypto Code of Conduct, the term ‘Digital Assets’ shall be deemed to include any contractual right for future delivery of Digital Assets.
‘distributed ledger technology’ or “DLT”	means a database system in which – (a) information is recorded and consensually shared and synchronised across a network of multiple nodes; and (b) all copies of the database are regarded as equally authentic.
“value”	includes assets, holdings and other forms of ownership, rights or interests, with or without related information, such as agreements or transactions for the transfer of value or its payment, clearing or settlement.

Interpretation

In this Crypto Code of Conduct:

- A. capitalised terms which are not defined above shall be given the meaning ascribed to them in GFIA’s Corporate Governance Code for Gibraltar Collective Investment Schemes, as amended from time to time;
- B. words importing the singular shall be deemed to include the plural and vice-versa, words importing the masculine gender shall include all genders; and

- C. references to ‘persons’ includes natural persons, firms, partnerships, companies, corporations, associations, organisations, foundations and trusts (in each case whether or not incorporated or having separate legal personality and irrespective of the jurisdiction in or under the law of which it was incorporated or exists).

2. INTRODUCTION TO THIS CRYPTO CODE OF CONDUCT

- 2.1 This Crypto Code of Conduct and the general guidance issued herein in respect of corporate governance and the role of a Director of any Crypto Fund is strongly recommended by GFIA. This Crypto Code of Conduct is not designed or intended to supersede applicable laws and regulations. It is a voluntary code that GFIA recommends to ensure that Crypto Funds operate with a high standard of ethics and corporate governance.
- 2.2 This Code addresses particular nuances of funds investing in Digital Assets and should be read in conjunction with the more general Corporate Governance Code for Gibraltar Collective Investment Schemes, published by GFIA in May 2013, which is available on the GFIA website and as may be amended from time to time. In line with GFIA’s recommendation regarding the general code, in addition to adopting the general code, funds investing in Digital Assets should formally adopt the Crypto Funds Code at the fund’s board level. Adoption of the both codes shall be done on a “comply or explain” basis such that boards must document any deviations from the codes, including the reasons therefore and the alternative means, if any, of achieving the goals of the codes.
- 2.3 The Government of Gibraltar and the Gibraltar Financial Services Commission have been the drivers behind the emergence of Gibraltar as a leading jurisdiction for Digital Asset businesses, including Crypto Funds. GFIA has recognised that although Digital Assets are an evolving asset class, they come with distinct risks which can be managed and mitigated through the implementation of specific processes and other good corporate governance measures.
- 2.4 Through the creation of this Crypto Code of Conduct, GFIA intends to help keep Gibraltar strongly at the forefront of standard setters globally within the Digital Assets space.
- 2.5 In complying with this Crypto Code of Conduct, funds investing in Digital Assets should adopt a proportionate approach which takes account of the level of risk to which it is exposed. For example, a fund with an arbitrage strategy, would pay more attention to the various trading platforms it is using and its price valuation policy, while a strategy which passively invests a small portion of its portfolio in Digital Assets, would pay more attention to its holding policy.
- 2.6 Whilst navigating through this Crypto Code of Conduct, the Board of a Crypto Fund should consider whether any additional disclosures should be included in the prospectus or offering memoranda in light of the Fund’s governance over critical aspect of its strategy and compliance.
- 2.7 GFIA recognises that each Crypto Fund is unique and that the world of Digital Assets is continuously evolving. The Board of a Crypto Fund should monitor developments in the Market, particularly in relation to risks and best practice, and periodically consider whether it should modify the manner in which it complies with this Code.
- 2.8 Traditional fund governance practices ordinarily extend to Crypto Funds. However, Crypto Funds also present a novel array of nuances and challenges for which distinct governance practices are needed. Crypto Funds are characteristically differentiated in various ways, including by the managers’ experience and expertise, as well as by the differentiated risks

associated with custody, technology, valuation, regulation, asset safekeeping and money laundering. This Crypto Code of Conduct seeks to present approaches to fund governance which are sensitive to these nuances and challenges.

- 2.9 This Crypto Code of Conduct also aims to support asset managers in the Digital Asset industry, enabling them to better assess market practices and standards. This we hope will enrich their funds and clients and position their funds at a higher level of governance and a better quality of product.

3. STRUCTURE OF CRYPTO FUNDS

- 3.1 A Crypto Fund should be set up as an Experienced Investor Fund under the Financial Services (Experienced Investor Funds) Regulations 2020 except for in certain limited circumstances (see paragraph 3.3 below). Given the risks inherent in a Crypto Fund, it is preferable for them to be regulated by the Gibraltar Financial Services Commission in order to add a level of regulatory oversight in addition to the good practices recommended in this Crypto Code of Conduct.
- 3.2 An Experienced Investor Fund structured as a protected cell company has the ability to deploy different cells for the purpose of segregating and protecting cellular assets in the manner provided for in the Protected Cell Companies Act 2001.
- 3.3 Crypto Funds should only be set up as private schemes within the meaning of the Financial Services Act 2019 if the private scheme is created for a small group of persons who are previously known to each other and where there will be no promotion of the private scheme.
- 3.4 A Crypto Fund set up as a private scheme within the meaning of the Financial Services Act 2019 should appoint a Gibraltar administrator with a permission from the Gibraltar Financial Services Commission under the Financial Services Act 2019 to act as the administrator for the private scheme.

4 CORPORATE GOVERNANCE

- 4.1 A Crypto Fund must have effective corporate governance arrangements, including an appropriate structure, processes, culture and strategies given the nature and risk associated with investing in and storing Digital Assets.
- 4.2 The Board of a Crypto Fund should collectively possess the appropriate balance of skills, experience, independence and knowledge of Digital Assets, the addressable markets, investment approach, trading and hedging strategies and risk management systems in place, to enable them to discharge their respective duties and responsibilities effectively. The Board of a Crypto Fund should possess the skillset necessary to decide, formulate and implement strategic policies.
- 4.3 The Board of a Crypto Fund should be familiar with the Crypto Fund's cyber security risks and vulnerabilities, including the nature of risks associated with the technologies and systems in place.

- 4.4 A Crypto Fund's control environment should consist of the appropriate governance and management functions, as well as the attitudes, awareness and actions of the Board with respect to the internal controls. The Directors must have sufficient collective experience and knowledge of the business and the necessary authority to detect and deal with any imprudence, dishonesty and/or other irregularities in a Crypto Fund.
- 4.5 A Crypto Fund may use cloud services to host its business and trading platforms, and this may be outsourced to reputable and secure cloud service providers in or outside Gibraltar, so long as the Crypto Fund can demonstrate it has adequate oversight and control over the cloud access, storage and processing.
- 4.6 The Board of a Crypto Fund is responsible for any outsourced function and should ensure it collectively has sufficient knowledge and experience to be able to challenge the performance and results of the service provider. If relying on the use of cloud services, a Crypto Fund should identify means of backup for such functions and contingencies should the cloud service have any downtime, become vulnerable or corrupted.
- 4.7 A Crypto Fund's records need to adequately reflect the value of Digital Assets held, taking into consideration the valuation recommendations detailed in this Crypto Code of Conduct. A Crypto Fund should adopt a policy whereby the Board periodically (frequency to be set by the Board of each Crypto Fund) undertakes a reconciliation of Digital Assets.

5 RISK MANAGEMENT

- 5.1 A Crypto Fund will be expected to apply appropriate risk management practices ensuring that the Crypto Fund's core processes and systems are effectively controlled, fit for purpose and that risk is managed effectively. Such practices should be designed specifically for the risks inherent with Digital Assets, including the risk associated with high volatility Digital Assets with unique custody and valuation related exposures. The risk management practices should be appropriate for the size and complexity of the Crypto Fund.
- 5.2 The Board of a Crypto Fund is responsible for ensuring the effectiveness of its risk management framework, setting the risk appetite and overall risk tolerance limits as well as approving the key risk management strategies and policies. In particular, the Board of a Crypto Fund should be aware of, quantify (where possible) and monitor the risks associated with investing in and holding Digital Assets.
- 5.3 A Crypto Fund is expected to develop risk management strategies into a cohesive management framework with appropriate policies and procedures that are relevant to the size and complexity of the Crypto Fund. To this end, a Crypto Fund should identify and assess its key current and potential risks, including, amongst others, risks to the Crypto Fund's investors and the reputation of Gibraltar. At a minimum, it is expected that a Crypto Fund should address the risks over the custody of Digital Assets, misappropriation/theft of Digital Assets, liquidity, counterparty risk and anti-money laundering. The Crypto Fund should formalise and document these risks and other

identified applicable risks prior to launch and should monitor these risks on a periodic basis to ensure it continues to reflect the Crypto Fund's business model and any significant changes in the evolving legal, regulatory and economic environment, as well as the technological landscape (e.g. security and anti-theft practices, etc).

5.4 A Crypto Fund's risk management framework should be aimed at creating a robust, sustainable framework that delivers an effective and efficient approach to risk management and which contributes positively to effective risk-based decision-making. The framework should define clear accountability for risk management, aligning risk management to performance management as well as the Crypto Fund's strategy and objectives.

5.5 A Crypto Fund's risk management framework should assess each specific risk facing the Crypto Fund, identifying the reasons why the risk is relevant to the Crypto Fund, and accordingly, implement appropriate controls and procedures in order to monitor, manage and mitigate these risks. These controls and procedures should distinguish between preventative and detective controls. The risk management function of a Crypto Fund should ensure that these controls and procedures are reviewed, tested and challenged frequently to determine whether these are designed, implemented, and operating as expected. Where any deficiencies are identified, these should be logged, reported to the Board and remediated in a timely manner, with a follow-up review performed to validate that they have been appropriately remediated.

5.6 A Crypto Fund should have appropriate management information systems and key performance and risk indicators to allow it to monitor its risks, contributing positively to effective decision making. Crypto Funds should consider whether developing a risk register would be appropriate as a tool to document the identification, assessment and monitoring of the inherent and residual risks.

6 VALUATION

Introduction

6.1 This Code covers the much wider concept of Digital Assets, this section will focus on the valuation of crypto assets, specifically the subset of Cryptocurrencies (as defined in section 6.2 of this Code). This section aims to provide guidance on the accounting under International Financial Reporting Standards (IFRS) by the general holders of crypto assets, but it does not address the accounting for crypto assets held by the original issuer. Moreover, the specific issues related to miners, crypto-exchanges and those resulting from token sales are not addressed here.

6.2 In the following accounting analysis, 'Cryptocurrency' specifically means those Crypto Assets that constitute a peer-to-peer general-purpose medium of exchange independent of any central bank. The IFRS Interpretations Committee defined a cryptocurrency as a crypto asset with all of the following characteristics: (a) a digital or virtual currency recorded on a distributed ledger that uses cryptography for security, (b) not issued by a jurisdictional authority or other party, and (c) does not give rise to a contract between the holder and another party. Bitcoin for example would meet

this definition, it was, launched in 2009 as the first and currently the largest (by market capitalization) of the Cryptocurrencies.

Lack of Formal Pronouncements by Accounting Bodies

- 6.3 Despite the market's request for accounting guidance, the International Accounting Standards Board ('IASB') decided not to add crypto assets to its standard-setting agenda but noted that it would continue to monitor the development of crypto assets. In November 2018, the IASB requested the International Financial Reporting Standards Interpretation Committee ('IFRS IC') to consider publishing an agenda decision on how entities apply existing IFRS standards to holdings of cryptocurrencies.
- 6.4 The IFRS IC issued an agenda decision in June 2019 on how an IFRS reporter should apply existing IFRS standards to its holdings of cryptocurrencies, a subset of crypto assets. The Committee observed that a holding of cryptocurrency meets the definition of an intangible asset under IAS 38 (Intangible Assets) as it is capable of being separated from the holder and sold or transferred individually, and is not a monetary asset (i.e., does not give the holder a right to receive a fixed or determinable number of units of currency). The IFRS IC concluded that holdings of cryptocurrencies should be accounted for under IAS 38 (Intangible Assets) unless they are held for sale in the ordinary course of business, in which case, IAS 2 (Inventories) would apply. A commodity broker trader of cryptocurrencies for example would be able to measure its cryptocurrency inventories at fair value less costs to sell.
- 6.5 In March 2021, the IASB released its Third Agenda Consultation. Prior to the release of the document, the IASB performed an outreach, in which stakeholders raised further concerns that the accounting required by IAS 38 (Intangible Assets) for cryptocurrencies may not provide useful information, because the economic characteristics of cryptocurrencies are similar to cash or other financial instruments, rather than to intangible assets and, therefore, cryptocurrencies should be measured at fair value. Cryptocurrencies and related transactions have been included in the consultation document as one of the financial reporting issues that could be addressed in a potential project.
- 6.6 As the development of Digital Assets is evolving at a fast pace and there is still no formally issued accounting standards specifically for Digital Assets, consideration is required by a Board of a Crypto Fund as to an appropriate valuation policy for an investment portfolio of a Crypto Fund to ensure they are correctly accounting for the crypto assets held under IFRS.

Classification of Crypto assets

- 6.7 In the absence of a specific accounting standard on crypto assets, the following table illustrates the various classification options under existing accounting standards. The conclusion reached is that in most cases crypto assets meet the intangible asset criteria or inventory (especially where the crypto asset is held by a commodity broker/trader for sale in the ordinary course of business).

Classification		Rationale
Intangible asset	✓	<p>Crypto assets generally meet the definition of an intangible asset under IAS 38 hence this is expected to be the most common type of classification. An intangible asset is an asset without physical substance (as it exists only within the distributed ledger), it is identifiable (as units sub-divisible to an atomic level are capable of being separated and sold), it is controlled by the holder and give rise to future economic benefits for the holder.</p>
Inventory	?	<p>Crypto assets that are held for sale in the ordinary course of business could meet the definition of inventory under IAS 2.</p> <p>IAS 2 general requirements are to measure inventory at the lower of cost and net realisable value, except in the case of commodity broker-traders who measure inventory at fair value less costs to sell.</p> <p>IAS 2 states that a broker-trader is an entity that actively trades such assets, with a view to their resale in the near future and generating a profit from fluctuations in the price or broker-traders' margin. However, there is no definition of a commodity in IFRS and therefore a judgement would need to be made, but generally the crypto asset would need to be fungible and traded in an active market.</p>
Financial asset	?	<p>A financial instrument is any contract that gives rise to a financial asset of one entity and a financial liability or equity instrument of another entity. Careful consideration is required to assess the terms and conditions of the crypto assets to determine whether it gives rise to a contract. In the absence of a contract, a crypto asset is not a financial instrument. Crypto assets that are not contractual themselves could still be the subject of a contract (for example agreements entered into 'off the chain' to buy or sell crypto assets could be contracts).</p> <p>Certain stable coins, depending on the specific rights and obligations associated with the holding, especially any potential redemption rights held, may meet the definition of a financial asset.</p>

		Classification and measurement rules for financial assets are governed by IFRS 9.
Cash	✘	Due to the lack of widespread use as a medium of exchange in everyday transactions.
Cash equivalent	✘	Due to the failure of the ' <i>insignificant risk of changes in value</i> ' test imposed by IAS 7 and generally not being convertible to known amounts of cash.

Measurement of Crypto assets

- 6.8 The following sections focus on the measurement rules under IFRS for the most common type of classification for crypto assets, in particular cryptocurrencies (i.e. as an intangible asset).
- 6.9 Under IAS 38, an intangible asset is initially recognised and measured at cost. Cost includes the purchase price and the related transaction costs (such as blockchain processing fees). Where an intangible asset is acquired in exchange for another non-monetary asset, the cost is measured at fair value, unless the transaction lacks commercial substance or if the fair value cannot be measured reliably in which case the cost is the carrying amount of the asset given up.
- 6.10 IAS 38 allows two accounting policy choices for measurement of intangible assets subsequent to initial recognition. These are (a) the cost model and (b) the revaluation model. The revaluation model arguably provides more relevant information than the cost model. However, the revaluation model can only be applied if the fair value can be determined by reference to an active market, which is defined by IFRS 13 as "a market in which transactions for the asset and liability take place with sufficient frequency and volume to provide pricing information on an ongoing basis". There are no provisions in IAS 38 that allow for the fair value of an intangible asset to be determined indirectly (for example, by means of a valuation technique which uses inputs that are less observable in the market). Consequently, if there is no observable price in an active market for an identical asset, the holder will need to apply the cost model to crypto assets held.
- 6.11 The IAS 38 revaluation model calls for fair value changes through other comprehensive income to the extent there is a surplus and through profit or loss to the extent there is a deficit revaluation balance. There is no recycling of revaluation surplus through the profit and loss.
- 6.12 Given the current speculative nature of crypto assets, this treatment of gains and losses may provide less relevant information about performance than that of a debt financial asset at fair value through other comprehensive income or any financial asset at fair value through profit or loss.

- 6.13 In conclusion, while IAS 38 would appear to be the default accounting treatment for crypto assets, it is questionable whether it provides for the most meaningful presentation of performance for this type of asset.
- 6.14 If crypto assets are determined to be inventory, they need to be measured in accordance with IAS 2. If the commodity broker-trader exemption could be applied, the crypto assets could be held at fair value less costs to sell, otherwise, crypto assets would need to be held at cost less net realisable value. A broker-trader holder of a crypto asset will need to estimate costs to sell taking into consideration the transaction cost on the relevant blockchain and other fees required in order to convert the crypto assets into fiat. These fees could fluctuate significantly from period to period, depending on the current demand for processing on the blockchain.
- 6.15 Whilst determining the appropriate accounting classification, Boards need to carefully assess the business model of the entity to determine whether crypto assets are held for sale in the ordinary course of business, that is, whether the fund is engaging in active trading with a view to resale in the near future as opposed to holding for capital appreciation.

Fair Value Measurement

- 6.16 Fair value measurement assumes an orderly transaction between market participants at the measurement date under current market conditions (IFRS 13:15).
- 6.17 Fair value measurement assumes a transaction taking place in the principal market for the asset or liability, or in the absence of a principal market, the most advantageous market for the asset or liability (IFRS 13:24).
- 6.18 A fair value measurement for a non-financial asset takes into account its highest and best case use (IFRS 13:27).
- 6.19 Taking a Crypto Fund invested in Bitcoin as an example, fair value is an exit price (what you could realise for the asset at the reporting date). The first step is to determine what the principal market is. Is there a principal market for Bitcoin? Principal market is defined as the one with the *'greatest volume and level of activity for the asset or liability'*. One view is that Bitcoin's principal market is the exchange with the highest volume and level activity that has adequate security and is legally compliant/regulated. Where the Board concludes that Bitcoin has no principal market because there is no clear exchange with consistent volume and activity advantages, then in the absence of a principal market, the exit price in the most advantageous market could be used. The most advantageous market is the *'the market that maximizes the amount that would be received to sell the asset or minimizes the amount that would be paid to transfer the liability, after taking into account transaction costs and transportation costs'*. There are two views/options as follows:
- (i) Most advantageous market is the exchange with the highest net exit price (net of transaction costs) quoted in the entity's functional currency, or

(ii) Most advantageous market is the exchange with the highest net exit price (net of transaction costs) quoted in any currency (based on spot exchange rates for the foreign currency to the functional currency).

- 6.20 Boards should consider the number of challenges when measuring crypto assets at fair value. Crypto assets trade on many crypto-exchanges including platforms that are not regulated exchanges. The quality of information on the transaction volume and price varies widely across markets. Another challenge is that some crypto-exchanges focus on exchanging different types of crypto-assets for one another, rather than the sale or purchase of crypto-assets with cash consideration as these cash transactions are illiquid. It is not always clear to what extent such transactions have commercial substance. Therefore, it may be more difficult for an entity to determine the principal (or most advantageous) market and assess whether transactions are orderly. Another issue is that prices for crypto assets are volatile and may fluctuate considerably. It is important for entities to understand how an exchange determines the quoted price, which may omit transactions that are considered anomalous or otherwise irregular, in order to appropriately assess whether or not such a quoted price is consistent with the concept of fair value under IFRS 13.
- 6.21 Boards should document clearly which accounting policies have been selected and how they have established their fair valuation process. Boards should also ensure that the valuation process is applied consistently at reporting dates unless facts/circumstances dictate that a different approach is appropriate.

Conflict of interests

- 6.22 The Board of a Crypto Fund should note that, given the uncertainties surrounding the valuation of crypto assets (as discussed in this section 6), there may be instances where charging fees on a percentage basis results in a conflict of interest if the receiver of such fee can influence the valuation of the Crypto Fund's crypto assets in any way. If any such conflicts exist, these should be set out in the relevant Crypto Fund's prospectus under the '*Risk Factors*' and '*Conflicts of Interest*' sections.

Prospectus Disclosure

- 6.231 Investors in a Crypto Fund should be made aware that there are currently no accounting standards as to how crypto assets should be valued and that crypto assets are neither financial instruments nor fiat currencies. Investors of a Crypto Fund should further be informed that crypto assets are not supported by any central Governmental organisations nor are there any Governmental databases that value crypto assets.
- 6.24 Disclosure should be clearly stated within a Crypto Fund's prospectus as to the valuation policy adopted in respect of crypto assets. The Board of a Crypto Fund should ensure any change in the valuation policy, and the related impact, is adequately notified to investors.

- 6.25 It should be noted that there is a possibility that the net asset value (“NAV”) prepared under the requirements of the prospectus or offer document, could be different to the NAV prepared in accordance with IFRS. An example of this is where the prospectus or offer document intends to value crypto assets classified as intangible assets which are not traded in an active market at fair value, but under IFRS this measurement will not be compliant with IFRS. As a result, the Crypto Fund should disclose the difference between the operating NAV (that is prepared in accordance with the prospectus or offer document) and the IFRS NAV.

Consultation with the Crypto Fund Auditor

- 6.26 Given the lack of accounting standards as to the accounting treatment of crypto assets it is important that the Board of a Crypto Fund consult with its auditor in order to ensure that the auditor agrees with the valuation policy adopted by the Crypto Fund.
- 6.27 Consultation with the auditor should be done prior to the establishment of the Crypto Fund in order to avoid a ‘*problem in waiting*’ in the event that the auditor does not agree with the valuation policy adopted by the Crypto Fund.

7. SAFEKEEPING AND SECURITY

General

- 7.1. A Crypto Fund will need to ensure that adequate arrangements are in place for the safekeeping of its Digital Assets. Safekeeping in the context of Digital Assets can be undertaken via:
- (i) third parties that offer specific Digital Asset custody solutions such as independent custodians, exchanges and wallet providers - whereby the third party controls the private keys (“**Third Party Custody**”); or
 - (ii) self-hosted wallets - whereby the Crypto Fund retains sole custody of its private keys (“**Self-Hosted Custody**”).
- 7.2. Within Third Party Custody and Self-Hosted Custody options, private keys may be stored using either:
- i. cold storage – which refers to custody where the private keys are stored offline and completely disconnected from the internet and any public network (out of the reach of potential hackers); or
 - ii. hot storage – which refers to custody where the private keys are connected to the internet.
- 7.3. Custodian banks are generally unable to hold Digital Assets on behalf of the Crypto Fund in any type of storage described in paragraph 7.1 above. A Crypto Fund will therefore need to

seek alternative methods to store its Digital Assets whilst still applying the principles of safety and security.

- 7.4. The Board of a Crypto Fund should adopt a written policy which sets out the safekeeping arrangements for the Digital Assets. This policy should contain information on which wallets the Crypto Fund will use, who will have access to the private keys, the multi-party authorisation arrangements (if applicable), what physical safes will be used and what proportion of the Digital Assets will be kept in hot or cold storage (as applicable). The policy should be proportionate to the type and amount of Digital Assets held by the Crypto Fund and should consider the risks of theft and also unrecoverable loss of access along with all other identified risks.

Multiparty Authorisation

- 7.5. A Crypto Fund should ensure that every wallet in which it keeps its Digital Assets is either a multi signature wallet or uses some other appropriate multiparty authorisation whenever possible. Where multiparty authorisation is used, if practical, the second authorisation should be by a person who is independent of the Crypto Fund's investment function and, ideally, be someone based in Gibraltar. If multiparty authorisation is not used by a Crypto Fund as part of its Digital Asset safety and security policy, the Directors should document in its policy why multiparty authorisation has not been used and state the alternative policies adopted by the Crypto Fund in order to keep the Digital Assets safe and secure.
- 7.6. For the avoidance of doubt, the placing of orders on a crypto trading account may be executed by a single person. It is in respect of the transfer of Digital Assets, in and out of wallets, where the Board of a Crypto Fund must require multiparty authorisation as described in paragraph 7.5 above.

Security

- 7.7. The Board of a Crypto Fund should remain alert to the threat of hackers and cyber theft. Only the required amount of Digital Assets should be kept in hot storage at any point in time. All Digital Assets which are passively held, or which will not be used for trading, should be kept in cold storage or when converted into fiat should be held in traditional bank accounts. In each case, the safekeeping of the private keys is of paramount importance. The Board of a Crypto Fund should implement adequate processes to keep private keys secure under multiparty arrangements.
- 7.8. The Board of a Crypto Fund should make adequate arrangements to keep the Crypto Fund's cold storage device in a secure physical safe location. The Board should consider using more than one cold storage device and more than one physical safe if necessary. Access to the physical safe should also follow a multiparty arrangement. Where appropriate the Board should store cold storage devices in physical vaults with extensive security controls that are able to sustain heat, water and other natural disasters whereby only pre-approved persons are authorized to access. Procedures should be designed to consider temporary

unavailability of authorised persons, long term unavailability of authorised persons, recovery and reporting scenarios and where possible disaster recovery procedures should be tested. Emergency protocols should be considered in regards to handling a breach or loss of assets.

- 7.9. The Board of a Crypto Fund should routinely and securely backup its digital wallets so that wallets may be restored where a physical device is lost, stolen, or malfunctions, thereby preventing potential loss of assets. Wallets should be encrypted and stored under password protected files. Crypto Funds should be aware that multi-signature wallets may have security flaws and take appropriate risk mitigating precautions where multi-signature wallets are employed. Where appropriate, Crypto Funds may wish to consider generating a new wallet address for each new outward payment. The Board of a Crypto Fund should implement adequate processes to keep any back-up keys, words or phrases secure under multiparty arrangements.
- 7.10. The Board of a Crypto Fund should carry out adequate checks on the way that API keys set up with Digital Asset exchanges are managed and controlled. The Board may consider restricting the permissions under such API keys and revoking and creating new keys on a periodic basis.
- 7.11. A Crypto Fund may use third party custody providers like outsourced custodian wallet providers, however as third party custody providers hold sizeable balances of Digital Assets they are very attractive targets for hackers. As a result, the most significant risk that third party custody providers face is the loss of private keys resulting from hacks and/or security vulnerabilities. In order to safeguard their Digital Assets, Crypto Funds should only enter into business arrangements with third party custody providers that employ the highest standards of security protocols and that have robust IT security controls. In order to achieve this, prior to entering into a business arrangement with a third party custody provider, the Board of a Crypto Fund should undertake, where possible, a comprehensive review of the custody and security policies together with all other relevant security terms and measures of each third party custody provider.
- 7.12. Crypto Funds should avoid keeping all fiat or Digital Assets on an exchange, making the fund fully susceptible to that entity's counterparty risk. Where assets are kept on an exchange, the Board should be aware of the exchange's underlying infrastructure, governance, security systems and processes in order to make a reasonable assessment as to the protection of the Crypto Fund's assets. The Board should consider the jurisdictional risk associated with the exchange, as regulation in this sector continues to develop.
- 7.13. Crypto Funds should carry out stress tests to ensure its Digital Assets are protected in extreme conditions. For example, the Board of a Crypto Fund could consider, among other possible scenarios, what would happen in the event that something unforeseen happens to one of the signatories, if a private key is lost, if a hardware storage device is compromised or if access to a vault is lost. The Crypto Fund may also wish to engage a third party cyber security firm to assist with its stress tests.
- 7.14. The Board of a Crypto Fund should closely monitor advances and best practice developments

(including legal and technological developments) within the Digital Asset industry as this sector continues to develop, in particular, in respect of Digital Asset custody and safekeeping and should ensure that their safekeeping arrangements are up to date with the most advanced developments.

8. TRADING DIGITAL ASSETS

- 8.1. Where possible, Crypto Funds should trade and transact on regulated exchanges and markets or bilaterally with known counterparties. Crypto Funds should not trade through unknown counterparties or platforms.
- 8.2. Where trading is performed via a decentralized exchange, Crypto Funds should consider assessing the risk of the legality of the counterparties they are trading with. When using centralized exchanges, whether regulated or not, Crypto Funds should ensure appropriate safeguards are in place against potential account compromise and practice safe storage.
- 8.3. The Board of a Crypto Fund should monitor protocol developments, where relevant, of any particular Crypto Asset held by the Crypto Fund and consider what actions to take in the event of a hard fork of a Digital Asset or an 'air drop' where further Digital Assets are deposited in a Digital Asset's wallet address without the consent or request of the private key holder of that wallet.
- 8.4. The Board of a Crypto Fund should consider and document what actions shall be taken in the event where any Digital Asset is capable of exercising voting rights or other decision-making action on any protocol.
- 8.5. The Board of a Crypto Fund should be aware of and monitor Digital Assets which entitle the holder to claim and collect benefits, whether as a masternode or otherwise. The Board of the Crypto Fund should ensure that such benefits are identified, claimed and accounted for in a timely manner.
- 8.6. Considerations should be made prior to trading on a platform around the security of the exchange, to include the proportion of exchange holdings held in cold storage or any insurance cover, as well as the overall liquidity of holdings. This may include whether the exchange has an up to date SOC 1 or SOC 2 report issued with a third party.
- 8.7. When trading and storing Digital Assets with an online service or online exchange market, Crypto Funds should employ two factor authentication with a second device; making use of U2F (universal second factor) or TOTP (time-based one-time password) to secure its account. Two factor authentication may include fingerprint verification, biometrics verification, text messages with a code, or services such as Google Authenticator.

9. LIQUIDITY MANAGEMENT

9.1. The Board of a Crypto Fund should note that there may be instances where a Crypto Fund has a diverse Digital Asset portfolio with varying degrees of liquidity (and respective price certainty). For example, a Crypto Fund may hold Bitcoin that is highly liquid and other Digital Assets which may be illiquid. If a Crypto Fund is open-ended, the Directors should be careful to ensure that redemption requests are not satisfied via the selling of the Crypto Fund's liquid investments leaving behind its illiquid investments (which may unfairly benefit and prejudice the redeeming investors over the remaining investors).

10. ANTI-MONEY LAUNDERING

- 10.1. A Crypto Fund must have systems in place to prevent, detect and disclose financial crime risks such as money laundering and terrorist financing and proliferation financing. In particular, Crypto Funds should address the risks relating to holding and dealing with Digital Assets.
- 10.2. Crypto Funds may receive *in specie* subscriptions in the form of Digital Assets. The Directors of such Crypto Funds will need to determine the provenance of such Digital Assets by implementing appropriate measures to trace the history of the Digital Assets. Such function may be carried out internally or be outsourced to a specialist service provider.
- 10.3. Redemptions paid *in specie* in the form of Digital Assets should be processed with caution in order to address the risks relating to any such transaction facilitating money laundering and/or terrorist financing.
- 10.4. A Crypto Fund should identify each of its investors and not process transactions where the fund does not know the investor's identity. A Crypto Fund must keep records of investor details and transactions including those on a distributed ledger so that holdings and transactions can be traced to each investor.
- 10.5. A Crypto Fund's standard systems and controls to combat money laundering, terror and proliferation financing continue to apply for investors intending to undertake transactions involving Digital Assets. However, where a crypto transaction is contemplated, including subscriptions, redemptions and investments, the Crypto Fund is required to consider the inherent nature of the Digital Assets and the potential for anonymity and illicit or immoral activities in relation to money laundering and terrorist financing.
- 10.6. Given the unique set of risks relating to Digital Assets, a Crypto Fund should implement systems of control appropriate for dealing with Digital Assets. Measures should include a process of verification of ownership of the investor's Digital Assets, and a compliance check and risk analysis of the digital asset wallet.
- 10.7. A Crypto Fund should verify the beneficial ownership of the Digital Assets it receives and redeems, including undertaking checks of the digital wallets and exchange accounts of counterparties.

- 10.8 As part of the assessment of the investor's background, a Crypto Fund should undertake screening of investor wallets which will help indicate whether the wallet contains any tainted cryptocurrencies obtained, directly or indirectly, from illicit activities such as darknet transactions, theft of assets or ransomware payments, or coins coming from a wallet that is sanctioned or blacklisted. A Crypto Fund should adopt an assessment criterion for the evaluation of investor wallet, as part of its assessment of investor background and suitability for the Crypto Fund.

11. INSURANCE

- 11.1 The Board of a Crypto Fund should actively seek to obtain directors and officers insurance and cover to protect the Crypto Fund against cyber theft. At the time of writing, such insurance is not available for some Crypto Funds or too expensive to obtain but insurance underwriters are getting more comfortable with providing insurance cover in this space. The Board of a Crypto Fund should monitor and keep abreast of developments with regards to obtaining such insurance cover. If appropriate insurance policies become available, the Board of a Crypto Fund should look to purchase such cover.
- 11.2 In cases where it is not reasonably possible to obtain such insurance cover, the Board of a Crypto Fund may consider setting aside some of the assets of the Crypto Fund to meet specific claims. In such cases, the Board should develop an internal self-cover policy setting out in which circumstances the set-aside pool of assets will be utilised.

12. AMENDMENTS TO THIS CRYPTO CODE OF CONDUCT

- 12.1. This Crypto Code of Conduct may be updated and amended from time to time as may be decided by GFIA acting through its technical committee, subject to the approval of the GFIA executive committee.
- 12.2. The Crypto Code of Conduct was first published on the 23rd October 2018 and an updated version was published on the 30th March 2022.