CRYPTO ASSETS SUPPLEMENTAL WHITE PAPER

Addressing Certain Operational Issues for Asset Servicers of Regulated Investment Funds in Ireland

June 2023

Irish Funds Fintech Working Group

if irish funds

CONTENTS

INTRODUCTION

In May 2022, Irish Funds published a White Paper titled '*Crypto Assets - Opportunities, Risks and Future Possibilities for Regulated Investment Funds in Ireland*'[1]. The White Paper was issued in response to increased investor appetite for crypto asset exposure in a more risk-managed way.

Its intention was to lay the groundwork for a collaborative effort exploring the feasibility of Irish authorised Crypto Asset Funds[2]. With that in mind, the White Paper set the scene on investor demand for crypto assets and identified the enormous opportunity that exists for Irish authorised Crypto Asset Funds. It discussed some of the considerations relevant to Irish authorised Crypto Asset Funds and identified some of the key risks which would need to be addressed in order to make Irish authorised Crypto Asset Funds viable operationally.

The White Paper concluded by setting out a number of recommended next steps (see Appendix 1) which, if implemented, would help to ensure that Ireland utilises its current strengths as both a leading investment funds and asset management centre and a significant technology hub to take advantage of the opportunities presented by crypto assets.

Since then, developments have continued apace in the crypto assets arena. In the same month that the White Paper was published, Terra Luna, and its associated stablecoin UST, collapsed which saw investors lose assets with no avenues for recourse. The crypto winter, which had set in by the time the White Paper was published in May 2022, persisted and cryptocurrencies continued to fall in value with crypto-related firms announced significant job losses. Most significantly, perhaps, the crypto exchange FTX collapsed in November 2022. In parallel with these issues, The European Parliament voted on 20 April 2023 to approve the EU Markets in Crypto Assets Regulation (MiCA) in the summer of 2023 and paves the way for a comprehensive regulatory framework for crypto assets markets in the EU to enter into force by 1 Jan 2025. Separately, on 4 April 2023, the Central Bank of Ireland advised that Qualifying Investor AIFs (QIAIFs) could gain indirect exposure to crypto assets of up to 20% of Net Asset Value for open-ended QIAIFs and up to 50% of Net Asset Value for closed-ended QIAIFs or QIAIFs with limited liquidity.

The path forward for crypto assets has certainly not been smooth. Notwithstanding this, regulatory regimes tailored specifically for crypto assets are imminent (e.g., MiCA) and investor demand persists. Therefore, the Irish Funds Fintech Working Group is continuing to develop its knowledge gathering and information sharing around crypto assets. In particular, we are focussed on how prospective service providers to Irish authorised Crypto Asset Funds and service providers to non-Irish domiciled Crypto Asset Funds (referred to as 'Asset Servicers' in this Supplemental White Paper) might, in practical terms, address the key operational issues identified in the White Paper.

With that intention in mind, the purpose of this Supplemental White Paper is to build upon the White Paper. This Supplemental White Paper shares information on current industry thinking and market practices around how some the key risks in AML, valuation and the technical attributes of crypto assets could be addressed in practice.

1. https://cdn.irishfunds.ie/x/64e81dd414/2022-05-6824-irish-funds-crypto-assets-whitepaper.pdf
2. Terms used in this Supplemental White Paper bear the same meaning as set out in the White Paper.

There are preparatory tasks to be undertaken by Asset Servicers intending to provide support services to Irish authorised Crypto Asset Funds.

These services will be regulated both within the existing Irish investment fund legislation (e.g., UCITS, AIFMD) and, shortly, under the MiCA framework. In this section, we will consider what actions Asset Servicers could take in the following areas to prepare for servicing Irish authorised Crypto Asset Funds and Crypto Assets:

1) AML and Crypto Asset: Practical Steps

2) Valuations of Crypto Assets

3) Technical Attributes of Crypto Assets

As an overarching observation, we believe that Asset Servicers will need to maintain operational structures which ensure independence, dual controls, segregation of duties, and adequate oversight when servicing crypto assets. Careful consideration will be necessary as key controls must be augmented to adapt to crypto asset transactions and their safekeeping whilst ensuring that innovation is not stifled, and the potential of crypto assets is realised and exploited.

AML and Crypto Assets: Practical Steps

Today, in practice, the majority of subscription and redemption activity in Irish authorised investment funds remains largely traditional bank-to-bank driven. This allows investment funds and their services providers to use existing AML controls, in terms of KYC and sanction screening procedures, to meet their AML obligations.

In relation to Crypto Asset transactions, a number of new scenarios exist that require consideration around enhanced AML controls. For example, the need may arise to accept crypto assets as a subscription into the fund pr payment of a redemption to a digital wallet or as an in-specie transfer into a Crypto Asset Fund. Asset servicers also need to consider how new providers such as VASPs and Digital Asset Analytics firms can be incorporated into their current AML processes.

The following table highlights the main themes being discussed that would need to be expanded beyond present-day KYC procedures:

Controls	Enhancements
Know Your Customer (KYC)	✓ Include the customer KYC from VASPs ✓ Independently identify counterparties to transactions ✓ Controls to monitor the IP of a client. ✓ Develop an approach to apply wallet identification criteria, including non-custodial wallet addresses
Customer Risk Profile	✓ Develop risk score and due diligence procedures upon VASPs
Know Your Transactions (KYT) Transaction Tracing & Source of Funds Destination	✓ Establish a process for tracing fund flows to/from crypto exchanges and for each digital asset supported. ✓ Expand monitoring to identify high-frequency transactions and patterns to specific crypto exchanges of high-risk jurisdictions
Suspicious Activity Monitoring & Sanctions Screening	✓ Deployment of “Crypto Asset Analytics” to supplement standard transaction monitoring. ✓ Determine how to incorporate metrics and findings from digital analytics monitoring to ensure the quality of data, alert triggers and understand potential gaps

ADDRESSING CERTAIN OPERATIONAL ISSUES

In terms of identifying and deploying solutions, there is a rapid pace of growth in this field with an array of options designed to support KYC and KYT (Know Your Transactions) programs under compliance, fraud, and operational teams. For example, targeted data and visualisation solutions provide real-time access and insights into understanding beneficial owners of each address and the money flows between wallets, detection of risky transactions from sanctioned addresses, darknet markets, scams, and Smart Contract security score assessments. Regarding Crypto Asset analytics, there is already a concentration of sophisticated players emerging even though this is a relatively new and growing area. There are two broad categories: on-chain monitoring and orderbook and market surveillance. These providers come to the market with a variety of price points and provide services to regulators, exchanges, and increasingly, banks.

VALUATION OF CRYPTO ASSETS

Crypto assets can transact 24/7 and across many, often unregulated, platforms. This introduces various issues for the Asset Servicers in performing the function of net asset value (NAV) calculation:

- The nature of the trading volumes means activity is moving instantaneously between venues, affecting liquidity and has the potential to create a material degree of difference in pricing marks between trading venues/exchanges.
- The method by which information is published may not always be transparent.
- There is a potential risk of market manipulation on platforms.
- There may be a failure to provide any pricing in certain circumstances.
- The decimal precision on pricing and current system limitations in handling up to 18dcp.
- It can be challenging to price assets where large volumes are traded off-exchange.

To assist with addressing the various issues for the Asset Servicers in performing the NAV calculations, we suggest that they consider the following:

Valuation framework

Mindful of the range of variables at play, it may be necessary to apply some discretion and develop a valuation framework with guiding principles to support the determination of value. Clearly defining the role of the valuation agent and determining the role of boards may be necessary. While there is an inherent risk with providing boards or board-delegated bodies discretion which could result in artificial volatility, this may be the optimal way to determine fair value in the absence of efficient and reliable information.

Incorporate multiple platforms and transaction volumes

Unlike traditional assets, there is no market close or no conventions around when a valuation should be established. Therefore, it is recommended to avoid limiting valuations of digital assets to only the price observed on one platform and to incorporate transaction volumes into determining value.

Unique disruptions

There can unique disruptions, such as any disruption to activity upon the platform or venue, that may affect valuation. Asset Servicers need to analyse these and incorporate them into the assessment of pricing verification procedures.

Calculation agent

The Asset Servicer performing the role of calculation agent should also be provided with a framework for verification of price and valuation. This framework could include specific criteria in terms of approved sources, over-average trading patterns and volume. Factors such as the decimal precision applied should also be clearly stated.

Transparent and consistent application

Ultimately, the valuation methodologies should be applied transparently and consistently with scenarios documented in the valuation framework to deal with any possible impacts and disruption to the platform.

Finally, we examine some concepts underpinning blockchain technology and consider new requirements facing Asset Servicers in cyber security and technology resiliency.

Most ledgers that support digital asset networks are public by design, whether operating a permissioned or permissionless blockchain (see Appendix 2 Explainer). (In a private blockchain where the authority of nodes and the operation of the blockchain are centralised, access and details of the ledger are private/restricted).

The nature of the public blockchains means there is by design no central authority, and in case of theft or inadvertent data corruption, there is likely no redress, regardless of cause. Potential events on the platform's underlying technology could alter the nature of the crypto asset and impact the ability to value the asset. An example of such an event is the potential disruption due to protocol version updates. These are known as forks (see Appendix 2 Explainer) and can take the form of an agreed/expected change or result from an attack on the platform.

For the Asset Servicer, the features of blockchains and forking scenarios pose risks and challenges, some of which are aspects of technology security which already exist (cloud storage, disaster recovery etc.) and others (key management) which will require new and non-conventional systems in the industry to monitor and protect assets.

Some considerations when thinking about software updates and interacting with blockchains for Asset Servicers include:

1. There is a high degree of digital and physical risk when considering safeguarding private keys when providing digital custody.
    a. Management of keys of multi-signature wallets both from a physical and digital perspective.
    b. Ensuring effective coordination of distributed parties required to sign transactions leading to potential time delays in trade execution and increased risk-surface.
    c. Companies are working to address these issues with solutions that enhance speed and security, using features such as multi-party computation (MPC) and hardware security modules (HSM) leveraging cryptographic methods to ensure key security.
2. Potential asset retrieval when faced with the loss of private keys via accident, including disaster recovery implications for physical cold-storage wallets or malicious intent.
3. Managing the network stability and uptime with robust solutions and testing to manage potential failures.
4. Handling the scenario where two distinct chains resulting from a controversial fork that may have a material impact on the value of the old protocol. Including both the new and old chains within the "Custody Network".
5. Impact on valuation and operational risk due to disruption events resulting in an inability to use determined valuation sources vendor, pricing provider or exchange downtime, for example.
6. Inability to transfer assets into a wallet or material impact on the settlement of transactions.
7. Assurance of ownership, insurance, bankruptcy remoteness of assets/entity, safe custody and segregation of assets when using a wallet-based system.

NEXT STEPS FOR IRISH FUNDS - WORKING GROUP ACTION PLAN

Asset Servicers are currently facing the challenge of addressing the operational matters discussed in this Supplemental White Paper. Our hope is that the information set out above will assist them in their considerations.

Moving forward, we believe that continued collaboration and information sharing amongst services providers, asset managers, professional services and other interested stakeholders in Ireland is needed to share solutions and disseminate knowledge and expertise across the industry. This will help inter-industry connections and provide the basis for a coordinated approach to dealing with the key risks and operational issues identified in the White Paper and such further issues as may arise.

With this belief in mind, we have set out a table of initiatives under the title "Irish Funds Digital Assets Action Plan for 2023". We will be undertaking these initiatives through cross-working group collaboration to ensure we can continue to provide practical support and guidance to Asset Servicers as they as they seek to address the challenges of providing services to Irish authorised Crypto Asset Funds.

APPENDIX I

White Paper: Summary of Recommended Next Steps

- **Qualifying Investor AIFs (QIAIFs):**
  - Clarification by the Central Bank of the extent of indirect exposure which is acceptable within a QIAIF and a description of the conditions which would need to be present to make greater exposure acceptable.
  - Consideration by the Central Bank of the conditions under which direct exposure by QIAIFs in crypto assets would be allowable.

  On 4 April 2023, the Central Bank of Ireland published revised investment limits for QIAIF exposure to crypto assets with the key points being:

  1. up to 20% of NAV for open-ended QIAIFs,
  2. up to 50% of NAV for closed-ended QIAIFs or QIAIFs with limited liquidity,
  3. pre-submission process for QIAIFs proposing to gain indirect exposure to crypto assets was removed.

  To avail of these limits the AIFM must (a) have an effective risk management policy addressing (at least) liquidity, credit, market, custody, operational, exchange risk, money laundering, legal, reputational and cyber risk, (b) carry out appropriate stress testing, (c) have an effective liquidity management policy, (d) have clear prospectus disclosure, and (e) where the QIAIF is open-ended, ensure the portfolio as a whole is suitable to provide that level of liquidity.

  Direct exposure by QIAIFs to crypto assets continues to be prohibited at this time pending satisfactory demonstration that the depositary obligations can be complied with.

- **Retail Investor AIFs (RIAIFs)**
  - Articulation by the Central Bank of any additional risk mitigation measures required to make indirect and direct exposure to crypto assets permissible for RIAIFs.
  - Commitment by the Central Bank to revise the RIAIF chapter of the Central Bank's AIF Rulebook to provide for exposure to crypto assets by RIAIFs as soon as the additional risk mitigation measures described in the previous point have been settled.

  On 4 April 2023, the Central Bank of Ireland advised that, taking into account the specific risks involved, "the Central Bank is highly unlikely to approve a RIAIF proposing any exposure (either direct or indirect) to digital assets".

- **UCITS**
  - Ireland, as a leading EU Funds Domicile, should be leading the discussion regarding the eligibility of crypto assets within UCITS funds at ESMA.

- **EU Convergence**
  - Engagement by the Central Bank with peer regulators, European Supervisory Authorities and the European Forum of Innovation Facilitators to ensure a convergence of approaches towards crypto assets. This might also include the registration and supervision of VASPs across the EU.

APPENDIX I

- **Government to create a specific taskforce on tokenisation within the Fintech Steering Group to ensure the policy and legislative conditions exist to support the creation and operation of tokenised platforms within Ireland.**

- **Replication of the legislative conditions which exist in other EU Member States as regards crypto assets and decentralised finance platforms.**

- **Industry should continue to support the Irish Government, the Central Bank and other industry stakeholders by producing thought leadership and information notes which will enable better understanding and higher levels of investor protection.**

- **The development of a financial literacy programme for transition year students to incorporate materials on crypto assets has been significantly progressed.**

  - Irish Funds launched a pilot modular, experiential Financial Literacy TY Programme aimed at 16–18-year-olds in January 2023. Tailored content was procured for all 15 modules, and this included a dedicated Digital Assets module as part delivery in 6 weekly sessions to 12 schools nationally. 7 schools were outside Dublin and over 400 students participated.

APENDIX II

Explainer

Permissionless Blockchain (Public, e.g., Bitcoin, Ethereum)

- Anyone can operate a node and validate a transaction, and the database has no single owner.
- Records are immutable once added.
- Anyone can contribute to the ledger, and all users have identical copies of the database.
- No individual can block a transaction being added to the ledger, meaning integrity is based on consensus.
- It is trustless, meaning the system's structure provides trust, and participants are not reliant on other parties being trustworthy/benevolent actors.

Permissioned Blockchain

- As the name suggests, participants on these blockchains need to be authorised; only entities with the correct digital certification can add nodes to the network and records to the blockchain.
- Levels of access can be defined and customised within the network and the ledger.
- The limited nature of the blockchain means each node is pre-authorized, resulting in greater integrity, easier maintenance, and reduced consensus concerns.
- It is more centralised and potentially contains the risk of having "rules" changed in an ad hoc fashion.

Private Blockchain

- A highly restricted form of blockchain which is run by an organisation.
- Fully centralised and ledger records are not available publicly.

* Nodes store a full copy of transaction history, validate transactions and provide security within the blockchain

Fork

A fork occurs when an update is made to blockchain protocol software. Soft forks occur when an update to the protocol has backward compatibility with previous versions. The ledger chain is unbroken, and nodes running on older versions of the software can still contribute to the network. When a hard fork occurs, the updated software version is no longer compatible with previous versions. Nodes that do not update their software will no longer be able to contribute to the updated version of the network. The result of a hard fork is two different blockchains with distinct native digital assets, the legacy chain, which continues to run the previous software version and the forked chain, which has the new software version (Bitcoin has undergone multiple forks, both hard and soft). In the extreme situation, a hard fork may be caused by malicious actors manipulating the platform and market to take over the majority of the network (a 51% attack).

Dublin

Ashford House, 18-22 Tara Street,
Dublin 2, D02 VX67, Ireland.

T: +353 (0) 1 675 3200
F: +353 (0)1 675 3210
E: info@irishfunds.ie

www.irishfunds.ie

Brussels

6th Floor,
Square de Meûs 37,
1000,
Brussels.

if irish funds