Sponsored by:

KPMG

AIMA

Digital Asset Trading

An AIMA Industry Guide

Disclaimer

The information contained in this Industry Guide on Digital Asset Trading (the "Guide") has been prepared by The Alternative Investment Management Association Limited ("AIMA") in conjunction with KPMG International Limited ("KPMG") and a working group comprised of AIMA members (the "Working Group") for general informational purposes for users of this guide only.

The Guide does not constitute or offer legal, tax, commercial or other advice and users of the Guide should not rely on it as such advice. Although care has been taken as to what is contained in the Guide, no attempt has been made to give definitive or exhaustive statements of law or any opinions on specific legal, tax or commercial issues and no representation is made or warranty given that the information is complete or accurate. As more legislation and regulatory guidelines are issued or updated, the accuracy of the information contained in the Guide may alter. Anyone requiring advice on any of the matters referred to herein should consult lawyers or other professionals familiar with the appropriate jurisdiction and legislation.

To the extent permitted by law, none of AIMA, KPMG, any member of the Working Group, or any of their respective partners, employees, agents, service providers or professional advisors assumes any liability or responsibility for, or owes any duty of care for any consequences of, any person accessing, using, acting or refraining to act in reliance on the information contained in the Guide. None of AIMA, KPMG, or any member of the Working Group, or any of their respective partners, employees, agents, service providers or professional advisors shall be liable to any person for any loss or damages (including, for example, damages for loss of business or loss of profits) arising in contract, tort or otherwise from the access or use of (or inability to use) the Guide.

Users of the Guide are responsible for complying with all applicable copyright laws. AIMA permits users of the Guide to make copies of the Guide as necessary and incidental to users' viewing of it; users of the Guide may take a print of so much of the guide as is reasonable for private purposes. Users of the Guide must not otherwise copy it, use it or re-publish it in whole or in part without this section nor without first obtaining consent from AIMA (which AIMA reserves the right to refuse without giving a reason). The rights in the contents of the Guide and their selection and arrangement, including copyright and database rights, belong to AIMA.

English law will govern any legal action or proceedings arising between users of the Guide and AIMA, KPMG, or any member of the Working Group in relation to the Guide and users of the Guide submit to the exclusive jurisdiction of the English courts.

Contents

Foreword

This Guide is the initiative of AIMA's Digital Assets Working Group (the "AIMA DAWG").[1] Following the publication of the AIMA Digital Asset Custody Guide, this latest Industry Guide aims to provide industry guidance on sound practices and key considerations for institutional investors engaged, or determining whether and how to engage, in the trading of digital assets.

The Guide has been written by a cross section of practitioners, as the trading of digital assets is cross-functional in nature, ranging from technologists and cyber security professionals to legal, operations and compliance teams. It is designed for those who are seeking to expand or diversify their investments into the digital assets space, i.e., the target audience are those firms who will need the capability to hold or transact in digital assets. These firms will want to work with trading counterparties and venues who have strategic plans around servicing clients and enabling them in the digital assets economy and can use the Guide as understanding the industry sound practices.

As a general resource, the Guide should not be regarded as a substitute for professional advice, which should still be obtained where appropriate. Further, institutions engaging in digital asset custody should pay close attention to applicable regulatory requirements and guidelines issued by regulatory authorities in applicable jurisdictions. The main text of this Guide is written to be as jurisdiction neutral as possible in order for it to be of the most use to institutional investors around the world. However, the Guide does not replace or override any legal and/or regulatory requirements. Although the Guide does in some instances identify examples where specific regulators have prescribed requirements, this should not be regarded as exhaustive and institutional investors should comply with the requirements specifically applicable to their businesses in all events. Where the Guide identifies practices that are not specifically required by their particular regulators, institutional investors should consider these as a matter of sound practice to the extent they do not conflict with the requirements applicable to them.

We would like to thank the contributors to this Guide (who are listed in **Appendix B**), all of whom have generously volunteered their time and expertise to produce the Guide. We intend to revise the Guide further as and when material developments occur.

Jacob Prudhomme
KPMG in the US

Kareem Sadek
KPMG in Canada

Co-Chairs of the Working Group

1 The AIMA DAWG is a cross section of senior industry experts including managers, allocators and service providers. It is tasked with driving AIMA's regulatory engagement, thought-leadership initiatives and operational guidance in the area of digital assets. For further information, please see www.aima.org.

Glossary

altcoin	a term used to refer to any cryptocurrency other than Bitcoin or Ethereum (not including stablecoins or other instruments pegged to a set value or reference point)
AML	anti-money laundering
AMM	automated market maker is a type of decentralised exchange protocol that quotes prices and matches orders between two or more assets in an automated fashion
API	application programming interface is a way for two or more computer programs to communicate with each other
Bitcoin (BTC)	a type of digital currency in which a record of transactions is maintained in a global, decentralised ledger, and new units of currency are generated by the computational solution of cryptographic problems by network participants; described as a global payment system and store of value independent of central banks or other authorities in the 2008 Bitcoin White Paper by pseudonymous author Satoshi Nakamoto.
blockchain	a distributed network of computing nodes maintaining a system of data records that are connected and secured using cryptography to protect data
CBDC	a Central Bank Digital Currency, which uses an electronic record or digital token to represent the virtual form of a fiat currency of a particular nation. A CBDC is centralised and is issued and regulated by the competent monetary authority of the country
CDD	customer due diligence
CEX	a centralised crypto exchange, which typically acts as a custodian of its users' assets and facilitates trading
cryptocurrencies	are digital tokens that serve as units of account, stores of value, or other utility on a decentralised ledger, generally not backed by other assets. These tokens can be a payment mechanism (e.g., Bitcoin), may be used to pay for units of compute to exercise activities on a blockchain protocol (e.g. Etherium "gas"), for governance voting rights (e.g. UNI), or for other purposes specific to an asset's native blockchain or associated protocol. Tokens native to a given blockchain are typically used to incentivise transaction validators, who provide the distributed security for the blockchain protocol.

cryptography	the conversion of data into private code using encryption algorithms, typically for transmission over a public network
decentralised	a system that has no single authority or administrator
DeFi	decentralised finance, which is a category of financial services, such as borrowing and lending, operating via applications powered by smart contracts hosted on decentralised, public blockchain networks
DEX	a type of crypto exchange that operates on a decentralised blockchain network, without the need for intermediaries
DLT	distributed ledger technology, which uses multiple independent computers to store information and transactions rather than a single centralised database
Ethereum	a blockchain network that is similar to Bitcoin. It has its own native cryptocurrency, called Ether or ETH, and is smart-contract-enabled, which means decentralised applications can be built and published on its network, and other types of tokens, such as governane tokens or NFTs, can be issued
fiat currency	a government-issued currency that is not backed by a commodity, like oil or gold, but rather by the issuing government itself, such as the US dollar or the Euro
hosted wallet	a wallet typically held by a third-party provider
HSM	hardware security module used to store private keys
institutional investor	for the purposes of the Guide, an institutional investor may be: (i) a family office; (ii) a manager investing on behalf of a client or a fund; or (iii) a manager investing for its own account
KYC	know your customer
liquidity	a measure of how easily an asset can be traded
liquidity pool	a digital pile of cryptocurrency locked in a smart contract, typically used to facilitate the liquid trading of digital assets on a decentralised exchange
LUNA	the native token of the Terra blockchain network

manager	the entity that performs the day-to-day portfolio and risk management functions for a product/account and/or is responsible for the day-to-day business, operation or affairs of a product. A manager for the purposes of this Guide may be: (i) a discretionary investment manager; (ii) a non-discretionary investment advisor; (iii) a registered investment adviser under the U.S. Investment Advisers Act of 1940; (iv) a commodity trading advisor under the U.S. Commodity Exchange Act; and/or (v) an alternative investment fund manager under the AIFMD. Depending on the circumstances, "portfolio manager" and "investment fund managers" (each as defined under applicable Canadian law) and any other similar entities under applicable local law may also be considered managers
MFA	multi-factor authentication is a multi-step account login process
MiCA	the European Commission's proposal for a regulation on Markets in Crypto-Assets
miners	nodes in the network responsible for processing new cryptocurrency transactions through solving computational problems that validate blocks of transactions and update the blockchain ledger
MPC	multi-party computation wallet, which shards the private key into multiple pieces
NFT	a non-fungible token that represents ownership of a unique item, such as digital-only artwork, music, or games. This means that the token cannot be interchanged with something else
OTC	over-the-counter, trading crypto assets directly between two parties in a closed trading market
prime broker	provide investors with access to a marketplace for the trading of digital assets
private key	the secret access to encrypted digital information that is paired with a public key and shared by the encoder with an authorised party to enable access to the information
proof-of-stake	a consensus mechanism used in blockchain networks where participants commit a stake of their private or collective capital to the platform in the form of the platform's native tokens, which are locked up for a given period of time
proof-of-work	a consensus mechanism used in blockchain networks that involves miners solving complex mathematical problems/algorithms in order to place a block of transactions on the chain
RFQ	request-for-quote

SEC	U.S. Securities and Exchange Commission
security token	a type of digital token that represents ownership or a financial interest in a company, asset, or investment product. Security tokens can represent various types of assets, such as equity shares, real estate, bonds and commodities. They are typically issued and traded on blockchain-based platforms that enable fractional ownership and offer greater liquidity compared to traditional markets
slippage	financial loss during trading as a result of market inefficiencies and illiquidity
smart contract	a programmatically executed transaction coded into a blockchain network based on predefined terms
SOC	Service Organization Controls
spoofing	a form of market manipulation in which a trader places one or more highly-visible orders but has no intention of keeping them
stablecoin	a type of cryptocurrency that is designed to maintain a stable value relative to a specific asset, such as a fiat currency. Different types of stablecoins exist with varying risks and dependencies, (e.g., fiat currency-backed, crypto-backed and non-collateralised)
tokenisation	the process of digitally representing an existing "off-chain" or "real world" asset onto a distributed ledger, such as blockchain
TWAP	time-weighted average price orders are a strategy of executing trades evenly over a specified time period
unhosted wallet	a wallet held by the user
Uniswap	a DEX protocol built on the Ethereum blockchain that facilitates the trading of cryptocurrencies without the need for intermediaries such as centralised exchanges. UNI is the governance token for the Uniswap protocol
USDC	USD Coin (USDC) is a stablecoin pegged to the U.S. dollar.
USDT	Tether (USDT) is a stablecoin pegged to the U.S. dollar
UST	a stablecoin that is native to the Terra blockchain network. It is designed to maintain a stable value of 1:1 with the U.S. dollar by using a combination of algorithmic and market-based incentives to adjust its supply in response to changes in demand
utility token	a type of digital token that is designed to provide access to a specific product or service within a decentralised network

VWAP	volume-weighted average price is a trading indicator that calculates the daily average price for BTC and other cryptocurrencies
wallet	an application or device for storing the private keys providing access to the digital asset
wash-trade	a form of market manipulation in which an investor simultaneously sells and buys the same financial instruments to create misleading, artificial activity in the marketplace
Web 3.0	the next evolution of the internet that provides a more decentralised method of user-content generation and allows users to interact via peer-to-peer networks

1 Introduction

Over the past several years, digital assets, such as Bitcoin and Ethereum, have emerged as an investable alternative asset class. Many investors, ranging from hedge funds, pension funds, sovereign wealth funds and global financial institutions making private equity investments to corporate entities and insurance companies making direct allocations, have disclosed investment exposure to this nascent asset class.

Despite this significant institutional adoption, the digital asset industry was marred by many tumultuous events throughout 2022 and early 2023. Many lessons of opaqueness, contagion and counterparty risk that "TradFi" relearned in the 2008 Global Financial Crisis have been learnt first-hand by digital asset industry participants. The impact of the collapse of the Terra Luna ecosystem following the UST stablecoin falling to zero in May 2022 reverberated across the entire industry. Many participants rapidly learned the importance of assessing the underlying collateral quality and liquidity. As a result, many investors saw their LUNA and UST investments marked down to zero.

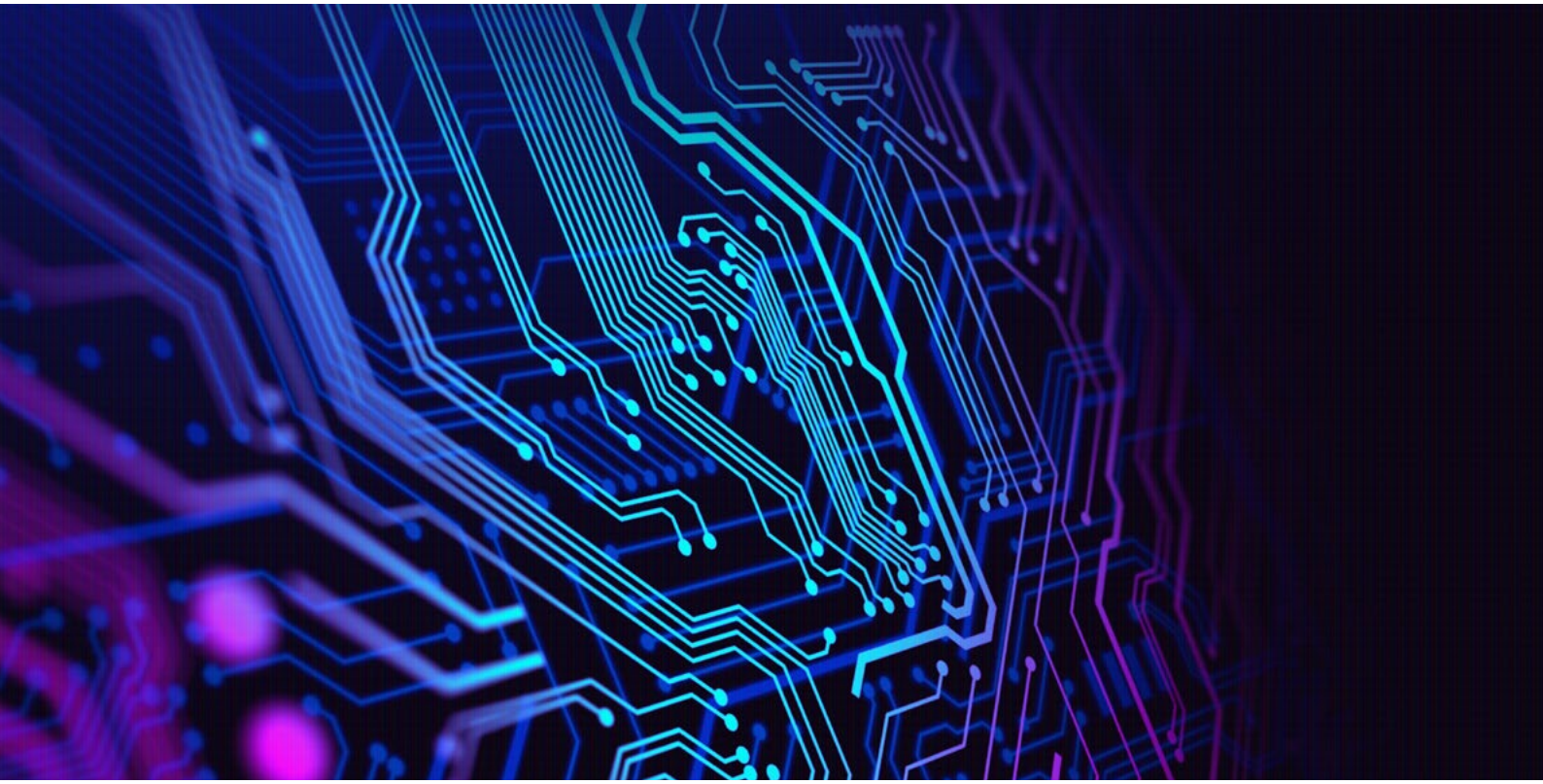
As the dust from LUNA began settling, questions of counterparty risk and hidden exposure to the Terra Luna ecosystem began to arise. This led to a digital assets industry-wide credit crunch as lenders across the globe began recalling lines of credit. Consequently, many hedge funds, liquidity providers and other borrowers returned loans, which resulted in liquidity worsening and spreads widening. These adverse market conditions led to one of the digital assets industry's largest proprietary-trading firms, Three Arrows Capital, facing significant losses and ultimately filing for bankruptcy. Further

contagion began to propagate, as many digital assets lenders had exposure to Three Arrows Capital, which in turn wiped out their equity. As a result, other digital assets lenders followed suit by filing for bankruptcy, including Celsius, Voyager and Babel Finance.

After this period of intense market stress, the industry experienced some reprieve as the Ethereum network's "Merge" update was implemented successfully in September 2022. This upgrade resulted in Ethereum's consensus mechanism shifting from proof-of-work to proof-of-stake. An important by-product was the reduction in energy required to process transactions and maintain the blockchain.

Unfortunately, the period of optimism was short-lived as more market stress emerged once the solvency of FTX and Alameda Research arose as a question. Shortly after, FTX experienced a massive run where users pulled out billions of dollars in a short period. This run revealed financial conditions at FTX and Alameda Research that were much more dire than most expected. While the exact details are far from fully resolved, early evidence indicates that FTX's leadership abused their control over clients' digital assets by secretly lending to Alameda Research. As a result, FTX and Alameda Research both entered bankruptcy and further contagion emerged, culminating in the bankruptcy of BlockFi and Genesis Trading.

These events will have profound implications for the digital asset trading ecosystem, including operational design of trading venues and regulatory oversight globally. This industry guide aims to provide an overview of the digital asset trading ecosystem and lifecycle, as well as highlight some key enterprise risks and due diligence considerations.



2 Digital Asset Trading Ecosystem

Institutional investors have increased their interest in the digital asset space over the past few years, with several notable investors announcing investment exposure. This progress has been supported by crypto-native service providers maturing to meet institutional requirements, as well as traditional service providers launching digital asset service offerings. As the digital assets space has grown, several trading approaches have emerged with their own unique characteristics and risk profiles.

2.1 Different trading approaches

The first approach is to execute trades on a centralised exchange or retail platform, where investors sign up directly and trade after depositing funds. The second is OTC desks, which are popular with institutional investors who do not need to pre-fund in order to trade. Third, decentralised exchanges where investors interact with each other or market makers and settle directly into their own wallets are increasing in popularity.

Centralised exchange (CEX)

Centralised exchanges enable a range of trading functions. Similar to traditional equity exchanges like the Nasdaq and NYSE, these exchanges operate CLOBs that allow investors to trade and access liquidity for a range of digital assets. Each CEX runs a matching engine that balances buy and sell order flow by matching buyers and sellers directly.

Additionally, CEXs charge trading commissions and sometimes provide rebates. Fees are usually tiered based on volume traded and depend on whether the investor is providing (making) or removing (taking) liquidity. The more volume an institution trades, the smaller the fee charged.

Furthermore, CEXs have historically required pre-funding, meaning assets must be transferred to the exchange before an institutional investor can execute trades for which the exchange essentially operates as a custodian, without a consistent regulatory approach or set of disclosures. Many investors push back against pre-funding requirements, however, because of concerns over counterparty risk which came to the fore after events surrounding FTX (i.e., credit risk with the exchange acting as custodian of the institution's funds). Workarounds typically involve off-exchange settlement, which can mirror traditional finance and involve a tri-party arrangement where a custodian settles trades between the exchange and the trader. Some CEXs are introducing the ability for institutional traders to keep their collateralised assets off the CEX (possibly with an affiliated custodian). For larger institutional traders, some CEXs may also offer trade credit to avoid pre-funding requirements. Other alternatives involve using prime or agency brokers to access CEXs for otherwise unavailable liquidity.

CEXs differ in terms of whether an investor can connect to them via API or an execution management system, or if they can directly execute trades on the exchange's graphical user interface. Additionally, execution parameters, monitoring and post-trade transaction cost analysis differ from exchange to exchange, and in general, pre-trade and post-trade analytics capabilities have not yet caught up to those of traditional markets. Institutions can develop their own software or select among vendors who provide a variety of market impact mitigation strategies when trading on exchanges, including randomisation, multi-exchange trading algorithms or targeting participation rates in specific markets or overall.

Over-the-counter (OTC) execution

Trading digital assets OTC is another approach that institutions can employ. OTC trading results in immediate risk transfers, where an investor can receive streaming prices and respond via API, using OTC provided user interfaces or can trade via RFQs from the individual OTC desks. With RFQs, investors are asking the OTC desk to take additional time risk and generally are required to trade the entire order at once. In the case of streaming quotes, particularly over APIs, trading strategies range from one order at a time to a variety of algorithmic strategies including those that are partitioned over time such as TWAP or VWAP.

OTC trades are peer-to-peer, so institutional investors should consider the counterparty credit risk. Once a trade is agreed upon, transfers of assets (i.e., settlement) can occur hours later, as many counterparties settle only once per day (or on a mutually agreed upon schedule). It is prudent to trade with counterparties that the institutional investor knows will be able to settle in a timely manner. Failure to settle can result in unhedged risk on either side of the trade and potentially litigation. One way to combat settlement risk is through a

tri-party agreement in which case a custodian settles the trade on behalf of the buyer and the seller and is aware of available balances before the trade occurs. Including a neutral third party to accept and deliver settlement could reduce Herstatt risk, also known as settlement risk. This separation also ensures that a dealer or institution cannot single-handedly decide who and who not to settle with - which can be beneficial in case of a bankruptcy.

Institutional investors should be aware of all fees associated with OTC trading, and account for slippage. While many OTC desks do not charge explicit trading fees, institutional investors should be aware that prices often contain markups, and OTC desks often widen their spreads significantly during periods of market volatility. As a subject of wide discussion in traditional finance, "last look" is still a common industry practice in OTC digital asset trading. Last look gives a liquidity provider the opportunity to pull out of trades at the last moment, even after the trade was accepted by a liquidity taker, thus increasing rejection rate and potentially resulting in deteriorating execution quality. As the digital assets market is highly fragmented, there is a place for every type of execution - including firm liquidity and "no last look" practices - and there is no one-size fits all execution model.

Institutional investors should be aware of all fees associated with OTC trading, and account for slippage.

While many OTC desks do not charge explicit trading fees, institutional investors should be aware that prices often contain markups, and OTC desks often widen their spreads significantly during periods of market volatility.

Interacting with OTC desks, particularly when using RFQ methodologies among several brokers simultaneously could increase the risk of orders being front run as it leaks information and as there is currently limited regulation in the space. Traders often use personal connections with OTC dealers in order to perform trades. Contact with these parties can be routed through both non-traditional communication channels like Telegram or Slack messaging as well as Bloomberg channels. In designing their trading processes, institutional investors should consider requirements around electronic communications surveillance, brought into focus recently by SEC enforcement actions related to communications on messaging platforms such as Telegram and WhatsApp and resulting in $1.8 billion in fines.

Similar to traditional finance, however, OTC execution is steadily moving to fully electronic trading with a new class of players emerging: single-dealer platforms and multi-dealer platforms. This can make it beneficial for institutions to collaborate with crypto native firms who have OTC connections either directly or via multi-dealer platforms, and experience requesting multiple quotes in order to execute superior pricing.

In addition, multiple prime brokers with digital assets experience have emerged allowing institutional investors to access multiple CEXs or OTC desks using the account credentials of the prime brokers, so the institutional investors do not need to onboard on to each exchange, with the added benefit of eliminating pre-funding risk highlighted previously. Prime brokers can often either provide or allow clients to use a smart order router to access the best liquidity, volume and price for a given digital asset. Importantly,

prime brokers may charge a fee to insulate its clients from credit risk with exchanges.

DEX and DeFi protocols

Decentralised exchanges, or DEXs, enable peer-to-peer transactions without the need for an intermediary. There are two main types of DEXs: CLOBs and liquidity pools. A DEX CLOB is similar to a CEX CLOB, except that assets are exchanged on-chain from the buyer's wallet to the seller's wallet.

The other type of DEX uses liquidity pools – a collection of tokens that are locked in a smart contract and used for trading between the tokens locked in the pool. In a liquidity pool, there are liquidity providers and takers. A liquidity provider will provide a pair of cryptocurrencies like ETH and USDC in a set proportion. In return, they will receive a liquidity pool token, which designates their contribution to the pool. When a liquidity taker comes to the pool, they may be looking to, for example, buy ETH and sell USDC. The investor will sell USDC to the pool and withdraw ETH at a price designated by the proportion of ETH and USDC in the pool. By doing so, the proportion of ETH and USDC in the pool will change and thus the liquidity provider's ownership of ETH and USDC changes as well. There are more complicated scenarios and pool setups, but this example highlights a simple trading use case.

As for fees, the liquidity provider receives a small fee (in basis points) as a percentage of the volume the liquidity taker swapped - from USDC to ETH in the example. The DeFi protocol may also take a small fee and add it to its treasury.

During the 2022 digital assets market volatility, and amid the collapse of FTX, some of the benefits of DeFi platforms were revealed. DeFi platforms utilise the trustless nature of the blockchain, eliminating counterparty and settlement risk, as the transactions settle as soon as they are signed to the blockchain, which can occur in minutes. The decentralised nature of DeFi platforms makes them more vulnerable to attacks, as hackers target specific bugs in the software suites, which are very transparent since the apps are open source. Decentralised oracle providers and code audits can be used as preventive measures against such code exploits. Lastly, using DEXs requires additional gas fees, typically paid in ETH, for interacting with the applications.

Though there has been some institutional use of DeFi protocols, institutional investors have yet to access DEX liquidity in a meaningful way, and these developments are still at very early stages. Significant regulatory issues, such as AML and KYC compliance considerations exist, presenting hurdles for regulated institutional investors to participate in DeFi platforms. Closed KYC pools - in which all members of the pool undergo CDD or KYC checks - may pave the way for more institutional investor participation in the future.

At present there is growing regulatory interest and scrutiny over DeFi platforms, particularly from U.S. regulators who it is believed do not consider any existing DeFi platforms to be decentralised enough to be outside of scope of regulation. It is, therefore, unclear the extent to which DeFi will be

able to continue in its current form, or if changes will be required to satisfy regulatory concerns.

2.2 Major trading products

Digital asset markets trade around the clock - 24 hours a day, 7 days a week.

Digital asset trading products tend to mirror those available in traditional finance. Below is an overview of the most common digital asset trading products.

Spot trading

Spot trading of digital assets predominantly occurs on exchanges (CEXs and DEXs), though it also occurs bilaterally in OTC trading. Where digital assets are traded on a CEX, the digital assets are held at the CEX and a trade between two CEX counterparties is recorded as a ledger entry (digital assets are not transferred from one counterparty's wallet to the others). OTC and DEX trading involves the parties directly exchanging the digital assets themselves.

Digital asset markets trade around the clock - 24 hours a day, 7 days a week. Digital assets listed on an exchange are priced as a trading pair (cross) with another digital asset or fiat currency. Typically, an exchange will facilitate trading in a digital asset against certain select stablecoins (e.g., USDT or USDC) or fiat currencies (e.g., USD, GBP, EUR). However, stablecoin crosses comprise the vast majority of global digital asset spot trading volumes due to their operational efficiencies relative to trading in fiat currencies, as they operate on crypto rails that provide quick and secure settlement around the clock. In some instances, altcoins, the common term for tokens other than BTC and ETH, may be priced against BTC and/or ETH. More liquid altcoins may also be priced against other liquid altcoins.

Price differences in the same digital asset are regularly observed across digital asset exchanges because of the different fees charged by exchanges, as well as the varying levels of trading volumes and perceived credit risk. These price differences have narrowed significantly over the years - differences are usually constrained to a few dollars now, as opposed to hundreds of dollars in years past. However, during periods of high volatility and market uncertainty, these price differences have been observed to widen. Most notably, during the days surrounding the FTX collapse, prices for BTC-USD differed by hundreds of dollars on FTX compared to other exchanges. Similar trends have been observed when venues or large counterparties are failing, often driven by fears of credit risk increasing. Due to a lack of widely accepted best bid and offer (BBO) in the digital asset space, institutional investors should understand price differences across exchanges before attempting to execute orders.

Arbitrage across digital asset markets tends to be more prevalent when compared to traditional markets because of the heightened price volatility and because many digital asset market capitalisations are lower than equity, bonds or precious metal markets and so it takes smaller size to move prices

up or down on any given venue. The recent banking crisis and resultant variance in the availability of banking across platforms may also create price differences across exchanges. There are, however, some risks with arbitrage trading and opportunities in this regard have decreased over time as market efficiencies improve and technological competition increases.

Derivatives: Futures, perpetual swaps, options

Derivatives are particularly attractive in the digital asset space as they offer investors an opportunity to benefit from price movements on the underlying digital asset in a more capital efficient manner without taking on the risks associated with holding digital assets (e.g., security, technology and operational risks) or with structures which give limited loss exposure. Futures and other derivative products are generally not fungible between exchanges. Having exposure to these products requires leaving collateral on exchange.

While there is not a risk of derivatives being transferred into a different wallet, security, technology, operational and counterparty risks are the same as one has when trading spot on a centralised exchange.

While traditional finance includes forwards, futures, options and swaps, there are three main types of derivatives prevalent in digital assets today, as shown in Figure 1 below.

Figure 1

Futures	Obligates the buyer to buy and the seller to sell the underlying digital asset at an agreed price at a future date;
	Standardised, trade on exchanges and can be settled physically or in cash;
	May trade at a premium to the underlying (i.e., contango) or at a discount (i.e., backwardation);
	May not always be tradeable 24/7.
Perpetual swaps (Perps)	Similar to futures, except they do not expire;
	Use a funding mechanism to tether contracts to their underlying spot price, unlike future prices which converge to the spot price as expiration nears;
	Exchanges are responsible for calculating the funding mechanism and it involves the use of an oscillating price marker to determine whether long or short traders need to pay fees or receive rebates;
	Unlike traditional futures markets, where investors are liable for losses beyond the collateral they post, in crypto exchanges, liability is limited to the collateral. This is facilitated by real time, 24/7 liquidation engines that enforce the collateral rules and safeguard the treasury of the exchange.
Options	Gives the holder the right, but not obligation, to buy (a call option) or sell (a put option) a digital asset for a specific price (the strike) on, and sometimes before, a predetermined future date.

Digital asset derivatives continue to evolve. At present, perpetual swap volumes relative to spot trading at CEXs are significantly larger worldwide in crypto, but option volumes are much smaller to what is observed in traditional markets. Additionally, perpetual swap volume is significantly higher than dated futures. While spot, futures and perps are largely exchange-traded, most options volume is done as arranged trades with OTC desks, that are often "printed" on an exchange.

ETFs, ETPs and closed-ended trusts

Regulated investment products are familiar to traditional market participants. Each vehicle corresponds to standards set by a country's regulators and are often accompanied by a prospectus. Most products are traded on traditional trading venues. Europe and Canada have ETFs/ETPs that hold digital assets directly, meanwhile, asset managers in the U.S. can only buy and sell bitcoin futures ETFs currently.

Closed-ended trusts investing in digital assets have been around for many years, with Grayscale's GBTC and ETHE products being the largest. Unlike ETFs, closed-ended trusts do not have a redemption mechanism and may trade at a premium or discount to NAV. In certain market conditions, some closed-ended trusts can trade at a discount to the underlying assets and as a result Grayscale is currently seeking to convert to an ETF format, and is in litigation with the SEC to require them to enable that conversion, which the SEC has blocked to date.

ETFs/ETPs remove the barriers to entry for investors who may be unwilling to bear the risks, costs and technology factors associated with direct cryptocurrency exposure. They are designed to be low-cost products, and some providers have now launched staked ETPs with minimal or zero fees. Large index sponsors in the traditional finance space are starting to build digital asset indicies and partner with ETP providers, which could further bolster investor appeal for products.

Structured products

Structured products are geared towards sophisticated institutional investors who require very specific risk parameters. Very common in traditional markets like currencies and commodities, structured products have not yet gone "mainstream" in digital asset markets, but a select few firms are offering them to qualified clients. Trades like the "principal-protected note", "coupon accumulator" and a "decelerator" are considered effective methods of expressing a view with very strict limits.

2.3 Core digital asset market activities

The digital assets space involves many core activities similar to those found in traditional finance.

However, there are nuances and special considerations that should be taken into account with respect to these core activities in the digital assets space. There are also new activities that are unique to this space, such as staking.

Lending

Like other traditional assets, digital assets are regularly used to collateralise loans or are themselves loaned out. Lending can take many forms and includes both collateralised and uncollateralised loans. In the collateralised context, loans may be over-collateralised, which results in a borrower only being able to borrow up to a certain percentage of deposited collateral. For this reason as well, collateralised digital lending tends to not involve extensive credit review.

By depositing digital assets on a lending platform, users earn interest on those deposits. These deposited funds are then in turn loaned out to borrowers wholesale that pay for a portion (or all) of the interest paid to the depositor. Funds can also be alternatively invested to earn additional yield.

Figure 2

While the mechanics of digital asset lending may vary by platform, it typically will involve the following steps:

1. Third-party platform connects lenders and borrowers;
2. Borrower deposits digital assets that will be used as collateral upon making a loan request (i.e., BTC or ETH);
3. Lenders will automatically fund the loan (i.e., USDT or USDC);
4. The platform will monitor the health of the loan and may liquidate the posted collateral if predefined risk thresholds are breached (i.e., loan-to-value); and
5. When the borrower pays off the loan, the collateral becomes unlocked and can be withdrawn.

A key distinguishing factor in digital asset lending is whether the lending process is decentralised and facilitated through the use of smart contracts or is instead facilitated through a central actor. On a centralised platform, interest may be paid in kind or with the native platform token. On a decentralised platform, interest is paid out in kind, and may also include bonus payments to incentivise use and help facilitate growth early on. In both centralised and decentralised uncollateralised digital asset lending, some form of credit intermediation occurs either by the central actor performing a credit review or the platform requiring a user to satisfy certain credit thresholds before being onboarded to use the decentralised platform (i.e., address whitelisting).

An additional form of lending unique to the digital asset space are flash loans. Flash loans allow for uncollateralised borrowing without a credit evaluation. Flash loans leverage smart contracts to give borrowers access to funds on an uncollateralised basis as long as the borrowed assets plus fees are returned in the same block (i.e., the transaction is atomic and automatically cancels itself unless the borrow and repayment occurs in the same block). While flash loans mitigate credit risks, they are not riskless and do introduce additional layers of smart contract risk and flash loan attacks in which hackers take out flash loans from lending protocols and use them to manipulate the market in their favour.

Although most digital asset lending takes place via lending platforms, market participants also engage in OTC lending transactions bilaterally.

Liquidity provision in DeFi

Automated market-makers ("AMMs") are a unique part of the DeFi trading ecosystem. AMMs facilitate the trading of digital assets by using liquidity pools rather than a traditional market of buyers and sellers. AMMs support liquidity pools by offering liquidity providers the incentive to supply these pools with assets often in return for earning trading fees. Instead of trading between buyers and sellers, users of AMMs trade against a pool of tokens. Users supply liquidity pools with tokens and the price of the tokens in the pool is determined by a mathematical formula.

The mathematical formula used by an AMM seeks to create a constant state of balance – i.e., the formula maintains that tokens in a liquidity pool must remain at a fixed relative value. For example, where a liquidity pool consists of only two digital assets (e.g., Uniswap), buying one digital asset brings the price of that asset up (and conversely, selling that digital asset brings it down) along the mathematical formula's curve.

AMMs are desirable in the DeFi context as they enable any project to offer liquidity for their token without relying on CEXs for listings and market-makers for providing liquidity. However, usage of AMMs can preclude trade flexibility as they are not compatible with limit orders, stop-loss orders and other order methodologies traders may be used to in traditional finance.

Although most digital asset lending takes place via lending platforms, market participants also engage in OTC lending transactions bilaterally.

Staking

One defining characteristic of a blockchain is its consensus mechanism, where a decentralised network of unknown parties agree on which transactions should go into a block and onto the blockchain. Proof-of-stake is one form of consensus mechanism whereby stakers (validators) stake or lock the protocol's native asset in order to participate in determining network consensus, typically proposing new blocks to the blockchain or voting on the validity of new blocks proposed by others. Validators receive staking rewards for performing this work accurately and in a timely fashion. However, by requiring validators to stake tokens, many proof-of-stake blockchains enforce financial penalties (i.e., slashing) on validators that perform their responsibilities poorly or behave maliciously.

Rewards, penalties and unbonding times vary by blockchain, hence staking can be highly speculative, but it does pose the opportunity to generate incremental yield on a digital asset position. Additionally, since staking renders staked assets temporarily illiquid during the staking and unbonding period, liquid staking protocols are one tool to help mitigate liquidity risk. Liquid staking is a means of delegating tokens to a platform or service that stakes tokens on the institutional investor's behalf and provides a tokenised representation of the investor's staked assets in return. This liquid token representation tracks the institutional investor's staked balance and any accrued rewards, and can be used across the DeFi space (e.g., to earn additional yield, collateralise positions, etc.).

Rewards, penalties and unbonding times vary by blockchain, hence staking can be highly speculative, but it does pose the opportunity to generate incremental yield on a digital asset position.

3 Trade Lifecycle Considerations

The intent of this section is to review key considerations regarding managing a digital asset trade from pre-execution to settlement in respect of OTC trades. This includes, for example, the pre-sale preparation, trade strategy clearing, trade execution and settlement. The processing of the trade lifecycle will clearly vary depending on the selected mechanisms. AIMA has published a Guide to Sound Practices for Operational Risk Management, which includes a section on lifecycle of traditional trade risk and may be a useful resource for understanding the operational risks involved and providing insightful and pragmatic actions.

3.1 Lifecycle flow

Similar to the traditional trade execution process, there is a comprehensive and complex process to transact in digital assets. Figure 3 provides an overview of the processes supporting digital assets trade execution lifecycle. When choosing a digital asset trading counterparty or venue, institutional investors should understand and assess the risk associated with each step of the lifecycle.

Figure 3

The digital assets trade execution trade lifecycle comprises the following steps:

ONBOARDING

Comprises due diligence on the investor including KYC and CDD protocols. In addition, the investor will configure accounts such as users, authorisation.

ORDER PROCESSING

Can be initiated through user interfaces, APIs or investors calling or emailing the trading counterparties and venues to submit trade requests, including desired order parameters.

EXECUTION

Involves sourcing liquidity from venues and liquidity providers according to the investor's order parameters until the order is completed or cancelled.

CAPTURE

The formal recording of the trade, including validation, enrichment and processing.

CONFIRMATION

The trading counterparties and venues will notify the investor's trading desk of the executed trade and should send an automated trade confirmation providing trade economics and settlement requirements. At this stage, the investor is legally bound to settle the trade.

INSTRUCTIONS

Used to communicate the movement of the asset to the custodian. The operations team transfers fiat currency balances from the investor's bank account to trading counterparties and venues. Both fiat currency and digital assets must be available to settle the trade through investor funding or credit arrangement. Prior to enabling the investor to confirm settlement, the trading partner performs a pre-settlement check to ensure both fiat currency and digital assets are available to facilitate settlement. The trading counterparties and venues work with the investor to resolve any failed checks. This step may be skipped if an investor has pre-funded the trade.

SETTLEMENT

The exchange of digital assets between buyer and seller. Once pre-settlement checks are complete, the operations team logs into trading platform, selects trades they want to settle and confirms to execute settlement.Settlement can occur t+0 given it can all be done on-chain.

POST TRADE SERVICING

Includes reconciliation, reporting services and invoicing. Post trade reports should be available to be downloaded through an API by the investor for trade and balance reconciliations, P&L and cost-basis calculations and investor reporting.

3.2 Key considerations

This section covers some of the key areas relating to the trade lifecycle for digital assets, such as custody, best execution, prime brokerage, listing process, market fragmentation, AML and KYC processes, and credit and leverage.

Custody

In traditional markets, institutional investors rely on a depositary or third-party custodian to secure their financial assets to reduce the risk of theft, loss and insolvency and satisfy regulatory requirements which limit their ability to custody their own assets. In the digital assets space, the parallel is the safekeeping of private keys for hot or cold wallets. Digital asset custody is essential for securely managing digital assets, as the private key acts as a single point of failure. To protect against potential errors, theft, loss or destruction of this vital element, a different technological setup might be used. An institutional investor will need to assess the potential of available technological solutions while adhering to authorised and supervised regulations set forth by relevant governing bodies and agencies.

At the highest level, there are three possible options:

- **Self-custody**, which includes hot (browser-based), warm (software-based) and/or cold (offline-based) wallets storage and provides for greater control of digital assets. Self-custody requires the user to assume responsibility for assets, asset servicing and associated risks (compliance and financial crimes, technology and cyber risks etc.) and requires relevant expertise. Self-custodial services are also often provided as a software solution, rather than as a custodial service. From a liability limitation perspective, this often means that the service provider would seek to limit its liability to the amount of fees paid, rather than the value of the assets held in custody.

- **An exchange hosted wallet**, which gives fast and easy access to digital assets, but comes with legal and counterparty credit risks with the exchange, especially security risks. If institutional investors trade on multiple exchanges, this setup is not capital efficient and requires proper collateral management in fast markets. There is less transparency with respect to what custodial solutions exchange use and whether or not they do indeed keep all assets custodied one-for-one or practice fractional-reserve banking. As further detailed below, the events surrounding FTX's collapse and insolvency exemplified the dangers of using an exchange hosted wallet as a custody solution.

- **Third-party custodian**, which stores digital assets on behalf of institutional investors providing certainty and security over the safekeeping of the assets and assuming responsibility for assets, asset servicing and associated risks. In some jurisdictions this activity might be overseen by the financial regulator. Generally third-party custodians

After the FTX collapse, there is extra attention being paid to how a counterparty custodies assets and any institutional investor involved in digital assets must take extra care to research and explore the options thoroughly.

will operate either by holding the complete private keys secure for clients, or via an MPC solution (where the third-party custodian "shards" the keys into sections, and implements technical solutions to enable those shards to be held by multiple parties (including the investor) to increase security). The liability cap in these arrangements should be expected to be no less than the value of the assets being custodied and the time. There is also an increasing expectation that this custody solution should be supported by viable insurance coverage.

After the FTX collapse, there is extra attention being paid to how a counterparty custodies assets and any institutional investor involved in digital assets must take extra care to research and explore the options thoroughly. Many institutional investors will maintain multiple custody relationships to spread out exposure and risk. An institutional investor should know which custodial solution a trading counterparty is relying upon. For further information on digital asset custody, see the AIMA Industry Guide on Digital Asset Custody.

Best execution

Digital asset markets offer a range of options for liquidity provision, including CEXs, DEXs and liquidity providers/OTC desks.

Smart order routing ("SOR") technology allows investors to access multiple pools of liquidity at once, increasing the chance for more optimal execution. Depending on the SOR technology, institutional investors may be able to trade across centralised, decentralised and liquidity providers for a single order. By leveraging multiple venues (and types of venues), SOR technology can facilitate more efficient execution than what could be achieved by a single venue alone.

Multilateral platforms combining different institutional OTC liquidity providers, with some that additionally incorporate both centralised and decentralised exchanges have emerged as a solution to address some of the challenges presented by fragmented liquidity sources in digital asset markets. Such platforms are capable of providing enhanced liquidity at prices superior to individual exchanges or liquidity providers. These platforms leverage multiple sources of liquidity and can combine that with algorithmic tools to fulfil larger orders and allow investors to achieve better execution than what could otherwise be achieved via single source solutions like exchanges or OTC desks. Additionally, some multilateral platforms and prime brokers reduce operational complexity associated with connecting multiple individual OTC counterparties by providing a single interface that connects users directly with multiple sources of institutional liquidity simultaneously. In some cases, this solution streamlines the legal process as the end-client does not have to pass through onboarding with every OTC desk and/or exchange, having signed one bilateral legal document with the multilateral platform.

Prime brokerage

Prime brokerage for institutional investors is a suite of services provided by a financial institution that allows them to buy and sell digital assets, as well as manage risk associated with those activities in a more efficient and cost-effective way. For example, through prime brokerage, an institutional investor can access global markets without having to establish separate accounts in various jurisdictions and receive value-added services. Such services may include structuring complex trades, access to leverage and portfolio margining services which allow institutional investors to offset gains or losses against other positions held in their portfolio. Furthermore, prime brokers provide counterparty risk protection by offering clients exposure limits and credit support facilities. However, using a prime broker does create counterparty risk with the prime broker itself. Similar to the considerations for custodians, institutional investors should consider the reputation of the prime broker, any losses incurred in the past (and if those losses were passed to clients), insurance and segregation of client accounts. Additionally, prime brokers may be restricted in the jurisdictions in which they can take clients. Institutional investors should confirm that potential prime brokers are connected to the CEXs, DEXs and OTC desks with which they want to trade.

As it stands at the time of writing, there are still many gaps between traditional financial markets and digital assets markets when it comes to prime brokerage services due largely to the global nature and complexity created by fragmentation within the digital asset infrastructure landscape.

The development of prime brokerage services, which are usually used by institutional investors in traditional financial markets, is experiencing a period of exploration in the digital assets markets. This is due to the global nature of digital assets and its infrastructure fragmentation, which has resulted in an underlying market structure that is more complex and entangled than traditional financial markets. Among the main companies looking to build prime offerings are digital asset exchanges, custodians and OTC desks, seeking the best way to leverage existing infrastructure while also staying on top of regulatory changes and avoiding conflicts of interest.

As it stands at the time of writing, there are still many gaps between traditional financial markets and digital assets markets when it comes to prime brokerage services due largely to the global nature and complexity created by fragmentation within the digital asset infrastructure landscape.

Listing process

After tokens launch, and as the project team builds up a community and improves their products or services, they may be eligible for listing on CEXs. Typically, CEXs charge a listing fee in exchange for listing the token and launching a co-marketing campaign. All CEXs have their own listing criteria and there is no listing standard across all CEXs presently. Prior to CEX listings, projects typically rely on DeFi protocols for liquidity, as their permissionless nature makes listing and offering liquidity accessible to all projects.

An option for issuing tokens directly on CEXs is the Initial Exchange Offering (IEO). IEOs are similar to Initial Coin Offerings (ICO) but typically involve more vetting from the exchange itself. This increased scrutiny can help protect investors from scams and fraudulent projects while giving projects access to more investors. Due to the frequency of scams and fraudulent behaviour in the past, investors

participating in initial offerings should exercise additional caution. Liquidity and price movement of new tokens is often unpredictable and highly volatile.

ICOs and IEOs were hugely popular in 2017 and 2018, but were marred by significant levels of fraudulent activity. As a result ICOs and IEOs are not as prevalent now as they were, but do still exist for larger, more reputable projects that are seeking fund raising. Airdrops as part of an initial token launch have become one of the most common types of tokens generating events. Large airdrops typically have significant community participation and trading activity, which leads to immediate listings across many CEXs.

Market fragmentation

High fragmentation adds complexity to the digital assets market. Digital assets are one of the most, if not the most, fragmented electronically traded asset class. First, it increases the complexity of finding counterparties and transactions which can be completed within a time frame. This makes it more difficult for institutional investors to get quick price indications on their desired assets and compromises the liquidity of markets. Additionally, market fragmentation reduces the ability to accurately gauge supply and demand since investors now have to go through multiple different on-exchange and OTC liquidity pools to find counterparties. There are often sizeable pricing discrepancies between exchanges, although, aside from periods of high volatility or perceived credit risk, such differences are smaller than the aggregate fees and capital costs one would incur to arbitrage them. It is also worth noting that there is a fair amount of variability in the data quality between exchanges, in large part due to lack of regulation. Many non-U.S. exchanges have been accused of allowing wash trades and not preventing other forms of manipulation.

Finding a way to accurately aggregate multiple market data sources is essential for digital asset trading.

In terms of settlement, market fragmentation can also lead to increased costs, operational complexity and processing delays due to the difficulty in coordinating multiple settlements. As such, settling trades becomes more expensive and slower. Custody solutions become increasingly necessary when dealing with multiple different wallets from various platforms and exchanges. As a result, these services often come with higher fees, as well as extra gas fees needed to transfer between exchanges or wallets, which add another layer of expense for investors looking to store their assets securely.

Fragmentation across different blockchains poses additional risks as, historically, cross-chain bridges have been an area with a high level of fraud and cyberattacks. While the technology of such bridges is constantly evolving, lack of control leaves users vulnerable. The custody element during a bridge transfer may also not be completely secure as separate chain interoperability depends on multiple components working together. Finally, market fragmentation also affects market data quality since there are now more sources of data that need to be monitored closely in order to understand pricing trends across all exchanges or platforms. Finding a way to accurately aggregate multiple market data sources is essential for digital asset trading.

AML and KYC processes

AML and KYC processes are essential for institutional investors to comply with the regulations set out in each applicable jurisdiction. These processes allow market participants to verify the identity of their counterparties before engaging in any transactions to ensure compliance with AML laws, as well as protecting financial institutions from being used for illicit activities. As digital assets markets become increasingly regulated in different parts of the world it is essential that investors develop strong AML/KYC policies in order to minimise risks associated with these types of activities while still allowing them access to market opportunities.

When it comes to KYC, institutions need to establish a robust CDD system that can verify and validate a customer's identity, determine the risk level associated with each customer, conduct background checks, maintain records of all transactions and monitor their activity on an ongoing basis. Institutional investors must also implement adequate measures to detect suspicious activity or attempted fraud.

AML and KYC are material challenges within DeFi. Without having a central authority overseeing user accounts and activities there may be the risk of non-compliance. Institutions willing to use DeFi projects should be aware of the risks associated with lack of information on counterparty identity. As the DeFi space matures, technology is emerging that can analyse liquidity pools using existing data points on potentially riskier wallets – helping to mitigate money-laundering and financial crime risks.

Credit and leverage

Credit and leverage are important aspects of the trading lifecycle in digital asset markets. While they can be used to increase return potential and capital efficiency, they also come witha greater risk of losses and can create potential problems if not managed appropriately.

Many digital asset exchanges offer margin trading products where users can borrow funds from lenders at varying interest rates depending on their risk profile and collateral requirements set forth by the exchange itself. Though these products may increase return potential, they also carry high levels of risk since prices are very volatile and large price swings can cause borrowers to incur significant losses if they do not manage positions properly. This is exacerbated by the unique feature of auto-liquidation in digital asset markets whereby the collateral may be liquidated during adverse market moves without warning. While this limits investor losses to the collateral posted, when there is significant price volatility, highly leveraged investors can be liquidated quickly, further exacerbating price movement. Robust collateral management requirements are crucial.

Credit and leverage are important aspects of the trading lifecycle in digital asset markets. While they can be used to increase return potential and capital efficiency, they also come with a greater risk of losses and can create potential problems if not managed appropriately.

Beyond digital asset markets, there are many examples of how excessive leverage in financial markets can lead to potential problems, starting from Long Term Capital Management in 1998 to Archegos Capital Management in 2021. Mirroring the failure of these firms, proprietary-trading firm Three Arrows Capital ultimately entered bankruptcy in 2022 after experiencing significant losses. All these trading firms heavily relied on borrowing, which led to significant losses when global financial and digital asset markets experienced periods of increased volatility, low liquidity and spreads widening.

With increased focus on counterparty risk, investors should consider whether they want to use prime brokers, exchanges, or both for access to leverage, as collateral will be stored with the selected party. Certain custodians are working towards solutions that would enable clients to utilise their collateral for exchange trading without requiring said collateral to be stored at the exchange. Unlike many traditional asset classes, there is currently no concept of a clearing house for digital assets, although, in the wake of the FTX collapse, some platforms have begun to emerge.

4 Enterprise Risk Management

Digital assets present investors with similar categories of risk as in traditional asset classes. However, because of the newness, fast growth and pace of innovation in digital assets, some of the familiar risk categories are not as easily monitored and mitigated, and the familiar risk management tools from other assets classes may not be immediately applicable. Also, many of the market participants, trading processes and market structures in digital assets are relatively new and may not have the historical data, activity and reputation required for traditional risk assessment. Furthermore, digital assets rely on new and different technologies and security protocols, which must be taken into account when monitoring and managing risks. Limited regulation and lack of process standardisation lend themselves to an increased need for investors to focus on risk management and mitigation.

For these reasons, investors in digital assets should approach risk conservatively. Participants should adopt and require risk management practices and procedures that address known risks and provide caution, consideration and resilience against categories of potential additional risk. Investors should look for thoughtful application of proven risk management techniques from other asset classes as well as controls, management tools and mitigants for risk specific to digital assets. It is important to also look for trading counterparties and venues who approach risk conservatively and provide transparency, have made risk management integral to their processes, and who pursue industry certifications, safeguards and sound practices. Compared to many traditional asset classes, an additional focus on operational risk, as opposed to market risk, is often warranted.

4.1 Cyber risk

Institutional investors can be one of the most lucrative and attractive targets for cyber criminals given the frequency in which they conduct transactions, access private keys and the multitude of exchanges and blockchains they interact with while seeking returns. Institutional investors should implement strong cyber security risk management and due diligence controls to mitigate as much cyber risk as possible.

Cyber security in the context of institutional investors involved with digital assets retains much of the same risk and control considerations of traditional asset managers, but digital assets do introduce a host of new risks that are unique in how they are monitored and mitigated. Interaction with anonymous counterparties and the irrevocability of blockchain transactions leads to new opportunities for bad actors. These new risks primarily revolve around the use of private keys and wallets to execute transactions and interact with smart contracts. Other important considerations include operational procedures for scam and fraud avoidance, assessing exchange security features, reviewing SOC reports and insurance, conducting penetration testing and bug bounties, blockchain network security and more.

Robust cyber security is a combination of physical, software, hardware and cryptographic protocols, as well as clearly documented procedures and controls.

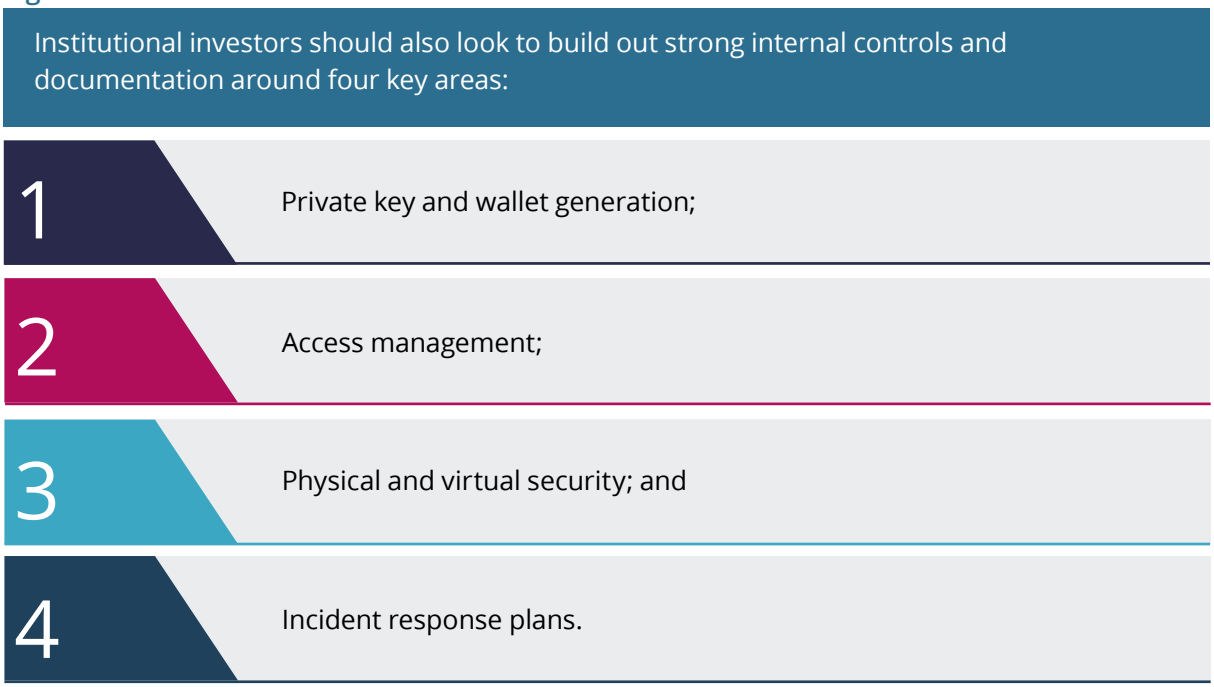
Robust cyber security is a combination of physical, software, hardware and cryptographic protocols, as well as clearly documented procedures and controls. Investors should look for trading counterparties and venues with leading edge technology security protocols and a combination of preventative and detective controls related to cyber security, as well as a governance framework for critical processes (key management, incident response, etc.). Investors should also look at how trading counterparties and venues assess their service providers in terms of cyber security risk management processes.

Leading industry practices

Appropriate safeguards and controls for interacting with digital assets is pertinent to every institutional investor that is involved in digital asset activities. There is a diverse set of leading industry practices that investors should be aware of as they engage with this technology. Some of these practices may not apply to all strategies, for instance some are specific to interacting directly with blockchain-based applications versus interacting with trading counterparties and venues.

The first area to consider is how custody of digital assets is managed by the institutional investor. Some important security controls around custody include the use of technologies such as hardware security modules (“HSMs”) to store encrypted private keys, multi-signature and MPC wallets to build in technology-level segregation of duties for signing transactions, data sharding sensitive wallet accessibility components such as seed phrases and private keys (as applicable depending on the architecture and custody tools in use), IP and wallet address whitelisting, transaction velocity limits and more.

Figure 4



This documentation should explain how the institutional investor:

- securely generates their private keys and wallets with appropriate oversight and segregation of duties;
- accesses private keys and other sensitive components to sign transactions with appropriate approvals;
- stores private keys and other sensitive components both virtually and physically; and
- has mapped out different disaster recovery scenarios related to digital asset components and vendors that could have a small to significant impact on the business.

Once the institutional investor has a solid grasp of the digital asset custody environment, understanding common operational pitfalls and how to avoid them is an important next step. Understanding the different types of operational risk and how to protect the institutional investor from these threats is essential for an investor looking to securely transact on a blockchain or through third-party exchanges, custodians and more.

Accounts with digital asset exchanges that take custody of digital assets have long been a target for cyber criminals since as long as they are able to access the account it can be easy for them to withdraw the balances directly to their own wallet they control. As such, institutional investors should employ as many security features available to them on a digital asset exchange as possible such as MFA.

Additional protections that institutional investors should employ on digital asset exchanges to mitigate cyber security risk would include the use of wallet address whitelisting, IP address whitelisting for API keys and trading velocity limits, as available. Wallet address whitelisting is the act of specifying on the exchange platform that no transfers of digital assets should occur to any wallet address other than those approved and input by the institutional investor into the digital asset exchange user interface. The process of whitelisting a wallet address requires MFA approval and to alter any whitelisted address usually requires a 24-72 hour hold period after appropriate approval. This is a vital security feature because in the event that an exchange account is breached, wallet address whitelisting can stop a cyber criminal's ability to withdraw digital assets to their own wallet. Note that if they are able to breach the account, the cyber criminal would have the MFA approve a whitelisting address change, but the hold period along with email notifications should provide sufficient time for the institutional investor to put a freeze on the institutional investor's account with the exchange and stop the attacker.

Many institutional investors also employ the use of API keys to the exchange accounts to automate trading and withdrawing. Institutional investors should use IP address whitelisting for API keys to ensure that even if an API key is breached by an attacker remotely, they would be unable to initiate any trades or withdrawals without breaching the trading systems traditional cyber environment as well.

Another type of cyber attack that has recently been reported on is referred to as a "forced API trade attack" and is a situation where a cyber criminal has gained access to an API key that only has the ability to trade funds, but cannot withdraw to external addresses that are not whitelisted, and the attacker can force a trade of a highly liquid digital asset such as BTC or ETH for a very low liquidity newer digital asset. The primary way in which an institutional investor can mitigate this type of attack is to utilise IP whitelisted API keys, ensure secure practices around API key management and refreshing and contact each relevant exchange with digital asset balances and request that they restrict the institutional investor's velocity limits to trade on highly illiquid digital asset markets. Additional cyber security controls to mitigate the risk of API key data leakage include controls around appropriate set up of permissions for API keys (read only, trade only, withdraw only, etc.) as well as ensuring that API key secrets are only ever stored in secure containers. Institutional investors should also be cautious to never expose API key secrets to public GitHubs or other collaborative code repositories. Similar to traditional finance, institutional investors should consider implementing a segregation of duties for individuals who can deposit and withdraw funds and have trading permissions.

While they most commonly interact with digital asset exchanges, many institutional investors also interact directly over a blockchain to settle trades with OTC desks or interact with applications on a blockchain. Due to a blockchain's immutable nature, institutional investors need to be cautious when signing transactions directly from their wallets as there are a variety of different risks to consider. One of the simplest controls an institutional investor can employ is to utilise test transactions whenever interacting with a new wallet address. An institutional investor should execute a test transaction with an immaterial

amount and after sending the funds, use a blockchain explorer to ensure the transaction was successfully executed to the designated address. Like test transactions, always trace the transaction after submitting the approval to a block explorer for the relevant blockchain. Institutional investors should always carefully check the destination address shown on the computer, mobile, or hardware device screen always matches the address they intend to send to. Awareness of these risks can help protect institutional investors from many operational scams and mistakes, such as fake wallet websites where transactions are submitted or accidentally sending a settlement payment to an incorrect address for an OTC settlement.

If institutional investors are interacting with more complex blockchain applications, such as smart contracts associated with DeFi like AMMs, there are several controls to consider including smart contract security audit assessments, limiting and monitoring authorised spending limits, reviewing contract source code, analysing the project's Total Value Locked (TVL), length of smart contract operation and any previous exploits, if applicable. The smart contract security code audit report should cover the latest version of the smart contract deployment and that any modifications or redeployments have been audited. If an institutional investor is considering interacting with an unaudited smart contract, a review should be completed to evaluate uninitialised variables, access controls are properly implemented and secured and access modifiers are used efficiently and correctly to control access to contract functions and state variables. To verify that a contract's access controls are secure and properly implemented, review the code to make sure it is using the right access modifiers such as private, public, internal and external. Regardless of the method used to review the smart contract code, the security or operations team of the firm responsible for smart contract interactions should review the protocol documentation and past transactions involving the smart contract(s) being evaluated to gain an understanding of the logic of the contract interactions.

Transactions interacting with DeFi smart contracts usually require a user to sign a message to the given smart contract that approves a specific spending limit for how the contract can interact with the institutional investor's address when a transaction, such as a swap, is subsequently submitted. Most decentralised applications ("dApps") use an unlimited spending limit by default, which allows the dApp to access all of the users' approved tokens or any NFT collection at any time in the future with no restrictions. Institutional investors should be cautious in their dApp contract usage, as upgrades to a contract may lead to potential bugs in the future. To help ensure their security, institutional investors should avoid using the default approval limit and instead set a custom approval limit within the software that they are comfortable with. Along with setting reasonable approval limits, institutional investors can also regularly use a token approval checker site to check which contracts have an unlimited spending approval from their addresses. If an institutional investor no longer plans to use the dApp, it should revoke the approval by reducing the allowance to zero. This requires a transaction fee, but it will help protect an institutional investor funds from a potentially malicious dApp.

Enhanced disclosures about policies and procedures

Leading industry practices around safeguarding digital assets are vital for any entity interacting with digital assets but given an evolving regulatory environment it begs the question of what types of enhanced disclosures relative to digital asset controls may be appropriate. Today the only types of digital asset disclosures evident surround exposure or material exposure to digital assets of public companies on their financials as well as certain regulatory disclosure requirements for issuers of digital assets. None of these disclosures at this moment describe different policies and procedures that are in place to mitigate various types of risk, including cybers ecurity risk.

Looking forward it may be appropriate for institutional investors as well as their vendors to provide enhanced disclosures surrounding controls related to how custody of digital assets are managed as well as exposures to different digital asset products and strategies which can correspond with different risks.

Figure 5

Disclosures for controls around custody management may include considerations for four key areas that could be summarised at a high-level without imposing additional security risks, include:

Private key and wallet generation: controls surrounding how keys and wallets are generated in a secure manner with adequate segregation of duties and oversight

Access management: controls surrounding how keys and wallets are accessed on an ongoing operational basis with appropriate segregation of duties, approvals and reviews

Physical and virtual security: controls surrounding how keys and wallets are stored securely

Incident response: controls surrounding a designated team that responds to various identified disaster recovery scenarios based on the custody architecture

Disclosures around exposure to different digital asset products and strategies would serve the purpose of helping investors and other parties in understanding different degrees of risk exposure a given firm or counterparty may be exposed to. For instance, disclosing significant exposure to staking or DeFi applications would indicate additional exposure to smart contract risk, the risk that a given smart contract may have bugs in its code, that is out of the control of the firm or counterparty beyond appropriate initial due diligence. While the above primarily focuses on enterprise risk management in the digital asset space, appropriate disclosures for investment risk and counterparty risk should also be considered.

4.2 Counterparty risk

Digital asset investors will face counterparty risks with their custodians and prime brokers, the exchanges, venues and OTC desks where they trade and any counterparties to whom they pledge or lend assets. Many counterparties for digital assets are comparatively new and may not have credit ratings, making traditional credit risk assessment difficult. As most digital assets companies are private, there is additional opaqueness when compared to traditional finance. Also, most digital assets are not cleared, meaning that there is no central counterparty to assume the credit risk on the other side of the trade. Finally, because digital asset trades settle very quickly after execution, most exchanges require prefunding the order. This feature embeds credit risk for all users with assets deposited on the exchange – as shown with FTX, if the withdrawals halt and the exchange fails, one may become an unsecured creditor in bankruptcy. In contrast, settlement with OTC desks is generally daily, but exact terms are determined between parties. With OTC there are bilateral counterparty credit exposures and a default may leave an organisation with unhedged exposure or loss of returns.

Digital asset investors will face counterparty risks with their custodians and prime brokers, the exchanges, venues and OTC desks where they trade and any counterparties to whom they pledge or lend assets.

In managing these risks, institutional investors should:

- look for counterparties with financial strength, credit ratings, access to financial support from a reputable parent entity, guarantees and assurances where possible, and balance sheet, collateral or other ability to fund their obligations;
- seek out counterparties that have controls and processes relevant to their financial stability (e.g., ICFR controls); and
- submit themselves to applicable industry audits and certifications, (e.g., SOC reports).

Also, certain trading venues may offer intra-day credit to avoid prefunding digital asset trades, or otherwise enable simultaneous "DVP-like" settlement. As a matter of sound practice in relation to selection/due diligence, the institutional investor should:

- if possible, create a formal process for onboarding a new counterparty that is governed by a senior member of staff other than the portfolio manager, the Chief Investment Officer and any member of the investment team. The process should include the minimum level of due diligence required for differing types of agreements (e.g., execution only or prime brokerage arrangement);

- monitor indicators such as credit ratings, balance sheet strength, credit default swap spreads, stock prices, tier 1 capital ratios, market news (including social media) and deposit inflows and outflows. Monitoring should occur on a frequent (likely no less than weekly) basis;

- demonstrate through written records that due diligence has been performed both at the initial stage and on an ongoing basis, especially if the counterparty undergoes a material change of business, including records of the institutional investor's due diligence a review of the historical and current regulatory standing of the counterparty in the country(ies) that regulate their business activities;

- consider requesting that each counterparty complete the AITEC-AIMA Illustrative Questionnaire for the Due Diligence of Vendor Technology and Cyber Security as an aid to due diligence and the related need for documentation;

- investigate counterparties organisational structure, how business lines are capitalised or supported by the overall business, IT and personnel investment in the business lines; and

- review and understand the disaster recovery and business continuity plan for the counterparty.

Counterparties should be monitored for signs of deterioration in creditworthiness. Relevant information on the counterparty and its associated parent/affiliate companies should be monitored closely.

An institutional investor may look to reduce counterparty risk through diversification. They should weigh the benefits of diversifying counterparty risks against increases in cost and complexity of operational processes. Although diversification among counterparties may help to materially reduce idiosyncratic risk, the same level of benefit may not hold during country-specific or global events that may adversely affect a group of counterparties. Like traditional finance, historically, digital assets have seen high levels of contagion and interconnections with major industry participants should be assumed (i.e., hedge funds having exposure to major lenders and exchanges, where one entity failing can ripple across participants).

4.3 Market and liquidity risk

Digital assets have had higher volatility and often more fragmented liquidity than traditional asset classes like stocks and bonds. In terms of risk management, limited asset lending means that short-selling is not yet mature, and derivatives (i.e., perpetual swaps and futures) are available but much of the liquidity is concentrated in less-regulated venues.

Institutional investors in digital assets should:

- make thoughtful use of multiple venues, as well as consider when to use agency and/or principal trading models;
- look for trading counterparties and venues with clearly documented trade acceptance, routing and execution procedures, and separation of agency and principal activities;
- assess potential order sizes in terms of venue and market volumes; and
- look for trading counterparties and venues with strong capabilities and controls around pricing, order/execution communication and integration, and availability (e.g., rolling uptime).

Compared to traditional electronic markets, many digital assets lack the same level of standardisation and reliability, as well as effective communication for maintenance, downtime and protocol changes. Historically, high trading levels, especially around market and economic events, have increased risk of bringing down exchanges or causing unacceptable latency. Access to multiple exchanges and/or liquidity providers is critical to an investor's risk management strategy, both for accessing liquidity and reducing technology and counterparty risk.

Some investment management strategy measures to mitigate market and liquidity risk might include:

- **Diversification:** Diversifying the portfolio across different digital assets and asset classes can help to reduce the impact of market volatility and concentration risk. Increasing access to venues and OTC desks reduces operational and liquidity risk.
- **Hedging strategies:** Using hedging strategies, such as futures contracts, options, perpetual swaps or other derivatives, can help to manage market volatility and protect against potential losses and increase access to liquidity.
- **Regular rebalancing**: Regularly rebalancing the portfolio can help to maintain the desired risk/return profile and minimise the impact of market volatility. This also includes having sufficient balances in hot wallets to trade as needed in situations of increased volatility.

4.4 Operational risk

Digital asset operations – trading, settlement, custody, security and other functions – use different providers, systems and technologies compared to traditional asset classes. Institutional investors could potentially be exposed to operational risks stemming from areas such as technology issues, volume spikes, inconsistent processes and malicious activity.

Key areas to assess include onboarding, identity management, access security, handling of cryptographic keys, pricing and valuation, transaction authorisation, transaction monitoring, settlement and transfer instructions.

Institutional investors should seek out trading, custody and derivatives partners with holistic, integrated, documented and tested procedures aimed at preventing and mitigating operational risks. Such procedures usually combine procedural, cryptographic technology and physical protocols to detect and prevent errors. Key areas to assess include onboarding, identity management, access security, handling of cryptographic keys, pricing and valuation, transaction authorisation, transaction monitoring, settlement and transfer instructions. Institutional investors should assess trading counterparties and venues' data management and security and overall business resiliency policies, and look for industry certifications of operations/ technology controls such as SOC 1 and 2 reports.

Operational risk in 24/7 trading of digital assets refers to the potential for loss or damage caused by inadequate or failed internal processes, systems, human errors or external events. Below are some examples:

- **Technical failures:** software bugs, network outages, exchange outages, withdrawal outages, or system crashes can cause disruptions in trading and result in significant losses.

- **Human error:** mistakes made by traders, administrators or other personnel can lead to incorrect trades, missed opportunities or other errors that cause financial loss.

- **Data breaches:** digital assets are valuable targets for hackers, and exchanges and other trading platforms are prime targets for cyber attacks. Data breaches can result in the theft of funds or confidential information.

- **Security risk:** digital assets are vulnerable to hacking and theft, and exchanges or digital wallets that store these assets can be targeted by cyber criminals.

Figure 6

The following practices are designed to manage operational risk:

Procedural measures

These procedures can help mitigate risk and improve operational resilience:

- Regular software updates, backups and disaster recovery planning can help to minimise the impact of technical failures and protect against data breaches.
- Implement automated risk management systems, such as algorithmic trading strategies and real-time monitoring, which can help to respond quickly and effectively to market volatility events, even when support staff are not available. Using a smart order router can increase market access, reducing the risk of not being able to trade if an exchange is down.
- Access management that avoids single point of failure. Some procedures that may be implemented include trading lifecycle/process, trading and asset movement approval hierarchy, wallet initiation and recovery procedure and wallet key storage.
- Have whitelisted protocols and counterparties in place for responding to market volatility events can help to ensure that the appropriate actions are taken quickly and consistently, regardless of the time of day.
- Have a clear communications in place, including the designated point of contact for market volatility events. This can help to ensure that all relevant parties are kept informed and updated in a timely manner.
- Ensure that, for all criteria functions, one or more individuals with relevant permissions and knowledge is reachable 24/7.

Operational team and system infrastructure

Some key considerations for operations and infrastructure include:

- Utilise a robust performance management system with the ability to maintain an audit trail and implement appropriate permissions and segregation of duties is essential. This could assist in monitoring the performance and ensuring that all transactions are recorded accurately and transparently. Implementing drop copies or another form of reconciliation is critical. Ideally, a two or three way reconciliation should be set up between parties.
- To help provide 24/7 coverage, leverage tools that can generate alerts in case of any unusual activity. This includes monitoring real-time market data, price movements and trading volumes, as well as keeping track of any suspicious activity. Some examples include monitoring software, trading bots and SMS/email alerts.
- Have an on-call support team available to respond to market volatility events can help to ensure that necessary actions are taken in a timely manner, even outside of normal working hours.
- Provide remote access to trading systems and market data to allow for rapid response to market volatility events, even when support staff are not physically present. As many exchanges are jurisdiction limited, it is essential to confirm that relevant support staff can assist ahead of a major event.
- Implementing a clear segregation of duties among team members helps in reducing the risk of fraud and human error. This involves assigning different responsibilities and permissions to different team members to minimise the risk of unauthorised transactions.
- Having a robust business continuity plan in place helps in mitigating the impact of any unexpected events. This includes planning for potential disasters such as power outages, internet connectivity issues or system failures.

The following practices are designed to manage operational risk:

Asset management and controls

Key considerations for management and controls for digital assets are:

- Implement effective asset management and control procedures is crucial, and institutional investors should strive to incorporate:
    - wallet whitelisting;
    - multiple user authorisation (dual at a minimum);
    - segregation of duties; and
    - MFA throughout collateral management process.
- **'High risk' counterparties**: consider increased monitoring and limiting the use of 'high risk' counterparties since not all digital asset trading partners may be able to provide the necessary controls. To achieve the desired controls, institutional investors may need to split up MFA between users and implement API alerts for any collateral movements.
- **DeFi ecosystem**: utilise a multi-signature or MPC wallet provider when transferring assets within the DeFi ecosystem in order to provide added security and reduce the risk of loss or theft. Institutional investors can utilise signature wallets; however, in such cases, institutional investors should adopt stringent hardware wallet management procedures, including physical safe storage protocols and sharding of ledger passcodes to ensure that no one individual can transfer the digital assets.
- **Regular reviews:** regularly review collateral management and control procedures to ensure they are up-to-date and effective. This includes regular assessments of counterparties, wallet providers, user access, as well as monitoring of internal processes and systems.

Training and education

Education and training strategies to improve operational resilience include:

- Human error prevention: train staff on human error prevention, including regular training on processes, checks and balances and oversight to minimise mistakes.
- Cyber security training: train staff on cybersecurity sound practices, including data protection, secure passwords and avoiding phishing scams. AIMA has published a Guide to Sound Practices for Cyber Security setting out principles that a manager should consider when developing a cyber security programme as part of its overall compliance and operations.
- Technical training: provide technical training for staff on the trading platform, risk management systems and other software and systems used in digital asset trading.
- Risk management training: train staff on risk management processes, including the use of stop-loss orders, position limits and other risk management tools and practices.

In conclusion, institutional investors face significant challenges when it comes to operational risk management. By following sound practices and implementing effective controls and monitoring systems, institutional investors can reduce their exposure to risk and ensure the integrity of their funds. Because the business of institutional investors can vary considerably, the methods they use to manage and mitigate identified operational risks may also differ. The suggestions set out in this Guide are just that – suggestions. They are not by any means the only possible or the only appropriate methods which may be employed. Institutional investors should consider any additional risks that may be introduced by the methods chosen to monitor and mitigate identified operational risks.

While the Guide presents a helpful collection of jurisdiction neutral guidance on operational risk management for institutional investors in digital assets, it should not be taken as exhaustive or necessarily complete with respect to the considerations that would be important to any specific investor's operational risk management policies and processes.[2]

4.5 Personal account dealing and personal trading policies

Institutional investors should establish written policies and procedures designed to help employees to avoid situations in which the investor is in a conflict of interest or implicated in a market abusive trade. The personal trading policy should reflect each relevant jurisdiction's specific regulatory requirements. Depending on the size of the institutional investor and volume of personal transactions, the institutional investor should consider implementing efficient technological solutions for pre-approval and to monitor employees' personal securities transactions effectively.

2 AIMA has published a separate Guide to Sound Practices for Operational Risk Management, which sets out principles that small- to medium-sized fund managers should consider when developing an Operational Risk Management programme as part of their overall compliance and operations.

5 Global Regulatory Landscape

Businesses often struggle with digital asset regulation being different from one jurisdiction to another. It takes valuable time, money and plenty of resources to remain compliant with so many different laws. To remain compliant across the current global regulatory landscape, a huge amount of effort needs to be devoted to legal and compliance matters. In addition, complying with new rules every time a digital assets firm looks to enter a new country — and with it, a new jurisdiction — can slow down the globalisation process significantly. That being said, this is not materially different from the challenges facing traditional financial services providers in terms of cross-border services and products compliance, licensing and/or local requirement.

To maintain compliance, digital assets firms including exchanges may choose to set up separate legal entities to help them operate more efficiently across borders. Many of these firms are continuing to forge ahead, increasing their revenues and expanding further, even in spite of market downturns.

Despite the regulatory protections aiming at insulating retail clients from more risky or speculative financial services and products, unfortunately, some smaller digital asset businesses, particularly those at an early stage without significant funds, may be tempted to cut corners when it comes to compliance. Ultimately, this puts end users in danger and at risk, which is exactly what regulation aims to protect against. A delicate balance has yet to be found between regulation, enforcement and facilitation of innovation, without exposing investors and markets to uncontrolled risks. It is going to be extremely important for investors and businesses alike to understand local market regulations and how to interact safely with digital assets.

Unsurprisingly regulators are struggling to keep pace because of the speed of innovation within the industry. Applying an identical set of laws designed for traditional financial institutions to digital asset providers may stifle innovation and lead to regulators attempting to force the square peg of digital assets into the round hole of regulations adopted over half a century ago.

Getting the world to harmonise on regulation relies on future involvement from global standard setters, such as the International Organization of Securities Commissions and the Financial Stability Board. Domestic responses to the increased use of digital assets vary tremendously and as such, regulation differs from region to region. Some countries have forged ahead by embracing digital assets regulation.

On the contrary, other jurisdictions have lagged behind with their regulatory efforts or chosen to ban digital assets completely, seeing it as a threat to their own economies — China is one example of this, taking the decision to prohibit cryptocurrencies and mining in 2021. Most problematic have been the jurisdictions that take no stance at all; those that have not banned cryptocurrencies, but equally, have not imposed any clear regulatory standards either. While such regions may not be deliberately facilitating regulatory arbitrage, by handing out different regulatory licences to various digital assets players, they have highlighted the necessity of setting clear standards for digital assets regulation across the globe.

Harmonising on attitudes towards regulation around the world will only benefit the digital assets space and open up new opportunities for the industry. In the future, this could see nations with prohibitive laws reverse their decisions to ban or limit the potential for digital assets, and nations which are regulating digital assets firms unclearly being required to clarify their stance. That being said, this will largely depend on the adoption of widely-enforced, global regulatory standards that protect investors and businesses from the negative aspects of unregulated digital assets.

A delicate balance has yet to be found between regulation, enforcement and facilitation of innovation, without exposing investors and markets to uncontrolled risks. It is going to be extremely important for investors and businesses alike to understand local market regulations and how to interact safely with digital assets.

6 Conclusion

Institutional investors are increasingly looking at how digital assets may be incorporated into existing and new strategies. Meanwhile, the digital asset markets and associated infrastructure continues to evolve and look to shake up decades old financial protocols.

As discussed in this guide, there are different ways to access the digital assets markets. Every investor is different and has a unique approach and set of tools that they might rely upon to monitor and effectively trade the fast-moving digital asset markets.

The trading counterparties and venues landscape may have contracted throughout 2022 and into 2023, but there remain many liquidity providers and exchanges from which to choose. Some have more narrow specialisations while others offer a wider swath of services. As with any other transaction, proper due diligence must be conducted to ensure the institutional investor understands and is comfortable with the risks associated with both the strategy and counterparty.

After a tumultuous year or so for the digital asset markets, increased diligence standards by users of venues and exchanges have led to greater transparency, including voluntary proof of reserves by most exchanges. There has also been raised awareness across the industry around key considerations for enterprise risk management. The industry has learned many lessons on the importance of mitigating credit risk after the collapses of major trading firms, exchanges, lenders, and stablecoins.

Clearly, regulatory clarity is coming, both through enforcement actions and new legislation globally. The numerous cases by regulators against major

crypto exchanges, token issuers, lenders and other participants will set precedent for impermissible actions by entities and their directors. Longer term, rather than regulating through enforcement, governments will likely pass better-defined legislation. Regulatory arbitrage across jurisdictions by large global centralised exchanges could soon end and perhaps the next battleground will be on-chain as regulators comprehend permissionless and censorship resistant code running on decentralised infrastructure. Regardless, it is safe to say that curiosity about this emerging technology will persist and the ecosystem will likey continue to be built, despite recent challenges.

APPENDIX A: Examples of Due Diligence Questions

Institutional investors should engage in proper due diligence when onboarding new trading counterparties and venues. Choosing trading counterparties and venues is one of, if not the most important decision an investor will make. Asking the right questions and conducting proper counterparty due diligence is imperative. Simply choosing counterparties who are well-known or have strong marketing (e.g., FTX) may not protect against counterparty risk. Below are examples of due diligence questions to consider:

Document request list:

- Provide copies of each of the following with respect to the trading counterparty:
    - AML/KYC/client onboarding policy, including on-chain analytics to monitor crypto asset deposits;
    - Cyber security policy;
    - SOC2 and/or ISO27001 Report (if applicable);
    - Last 2 years of audited financials;
    - Most recent balance sheet (audited is preferred); and
    - Corporate structure and organisational chart, including parent and subsidiaries (and affiliated companies if applicable) and ultimate beneficial owners.

Organisation overview:

- Provide copies of each of the following with respect to the trading counterparty:
    - Countries of business operations;
    - All applicable licenses and regulatory approvals; and
    - List of all associated entities and details of business activities.

Regulatory:

- Provide copies of each of the following with respect to the trading counterparty:
    - Any material regulatory changes over past two years;
    - Licenses received in any jurisdictions under laws regulating commodities, derivatives, securities, banking, lending or financial products;
    - Any warnings, suspension/termination of registration/licensing/ membership, imposed terms and conditions or sanctions by financial services regulators, self-regulatory organisations (or similar organisations);

- Any civil proceedings against the organisation, its directors, current or former key employees; and
- Any on-going inquiries or investigations from any regulators currently ongoing.

Compliance:

- Does the trading counterparty use third-party vendors for AML/KYC?
- Provide a list of the countries from which the trading counterparty prohibits onboarding (beyond sanctioned countries if applicable).
- Can unverified users withdraw from the platform? Are there different levels of withdrawals/trading volume based on different levels of KYC?
- Does the trading counterparty have policies and procedures to identify and report suspicious transactions?

Information security:

- Has the trading counterparty ever experienced a hack or security breach? If so, when did it occur and what was the scale of the breach?
- Does the trading counterparty have standard operating procedures in the event of a security breach?
- Is the trading counterparty SOC and/or ISO 27001 compliant? If yes, please provide the report/certification and if not, then please outline the organisation's plans to obtain these certifications.
- Has the trading counterparty conducted penetration testing internally or with external experts?

Controls:

- Does the trading counterparty maintain internal custody and private key management? If yes, provide information on security measures in place to generate and backup private keys. If no, provide detailed information on the controls in place at the third party custodian (including SOC reports if available).
- What types of environments are used to store private keys (i.e., hot, cold and deep cold storage)?
- What percentage of assets are typically stored in hot and cold wallets? Do percentages vary by asset or blockchain? Are hard limits in place?
- Does the trading counterparty utilise multi-signature or multi-computation wallets? If multi-signature, what is the m of n structure for cold wallets? If MPC, how many shards is the private key divided into?
- Does the trading counterparty maintain a withdrawal policy for transferring digital assets to/from hot and cold wallets? If yes, please provide a copy or describe the process.
- Does the trading counterparty maintain an insurance policy to cover the loss of any digital assets?

Independent governance:

- Is there an independent internal audit team and/or enterprise risk function? If yes, do they perform annual control testing?
- Does the trading counterparty have a governing body? If so, please provide a complete list of members of the governing body and how many are considered independent?
- Is an external audit of controls performed on an annual basis? If so, by whom?

Financial management and risk:

- Are regular audits/assessments (internal or external) conducted to verify the existence of digital assets held on the platform?
- Does the trading counterparty conduct a proof of reserves? If so, is it completed internally or externally? Is the proof of reserves real-time? If not, what is the frequency? Please provide more information on the methodology of the proof of reserves, including the procedures implemented and the assumptions made if applicable.
- Please provide a breakdown of all assets and liabilities for digital assets, including any outstanding loans or other obligations.
- Please outline products offered to clients that involve leverage, including the max leverage available for each product.
- Is credit offered to clients via the internal treasury or via rehypothecation?
- Do any clients have non-liquidation provisions?
- Has the platform experienced socialised losses in the past?
- What is the current size of the insurance fund? Please provide a website link to monitor the insurance fund in real-time if applicable.
- Is there an independent risk team? If so, what is the size of the team? Does the trading counterparty have a Chief Risk Officer?

APPENDIX B: AIMA Working Group

Jacob Prudhomme and Kareem Sadek	KPMG
James Delaney	AIMA
John D'Agostino	Co-Chair, AIMA's Digital Assets Working Group
Steven D'Mello	Albourne Partners Limited
Diogo Mónica	Anchorage Digital
Oliver Lynch	Bittrex Global
Katy Allen	BlockFills
Yelena Nemenko	Coinbase
Dave Weisberger	CoinRoutes
Eva Gustavsson	Copper
Konstantin Shulga	Finery Markets
Eva Sanchez	GSR
Haydn Jones	Kroll
Fedor Poskriakov	Lenz & Staehelin
Bennett Moore	RSM
Sarah Crabb	Simmons & Simmons
Thomas Barton	Trovio Group

We would also like to thank AIMA's Digital Assets Committee for their involvement and the following reviewers of the guide: Olga Romanova (Aaro Capital), Martin Palotai (Alphemy Capital), Nicola Harte (Archax Capital), Parker Merritt (Coin Metrics), Nicholas Dimitriou (Great South Gate Asset Management), Ilya Paveliev (Haruko) and Alexander Grieve (Tiger Hill Partners).

APPENDIX C: About AIMA

The Alternative Investment Management Association (AIMA) is the global representative of the alternative investment industry, with around 2,100 corporate members in over 60 countries. AIMA's fund manager members collectively manage more than US$2.5 trillion in hedge fund and private credit assets.

AIMA draws upon the expertise and diversity of its membership to provide leadership in industry initiatives such as advocacy, policy and regulatory engagement, educational programmes and sound practice guides. AIMA works to raise media and public awareness of the value of the industry.

AIMA set up the Alternative Credit Council (ACC) to help firms focused in the private credit and direct lending space. The ACC currently represents over 250 members that manage US$800 billion of private credit assets globally.

AIMA is committed to developing skills and education standards and is a co-founder of the Chartered Alternative Investment Analyst designation (CAIA) – the first and only specialised educational standard for alternative investment specialists. AIMA is governed by its Council (Board of Directors).

For further information, please visit www.aima.org.

APPENDIX D: About the Sponsor

About KPMG

KPMG firms offer a wealth of experience in the digital asset space, having collaborated with numerous industry clients and governments, including Central Banks, Exchanges, and leading Financial Institutions. The global network of KPMG professionals, present across 143 countries and territories, is equipped to provide advice and support across a broad range of cryptoasset and blockchain services spanning Advisory, Audit, and Tax. With a proven track record of delivering effective services and technology solutions in the digital asset-related projects space, KPMG firms have a deep understanding of the complexities and nuances involved.

KPMG professionals in Audit, Tax and Advisory are specialist in their fields and have deep experience of the issues and needs of the investment management businesses. KPMG firms' clients include investment managers, wealth managers, family offices, fund administrators and service providers who focus on mutual funds, hedge funds, private equity funds, infrastructure funds and real estate funds, and institutional investors for pension funds and sovereign wealth funds.

KPMG firms aim to provide tailored services of the highest standard. KPMG professionals are focused on building trusted relationships and delivering quality output through project teams that can support you from anywhere in the world, whatever your investment activity.

Acknowledgements

Laszlo Peter
KPMG Australia
E: laszlopeter@kpmg.com.au

Kunal Bhasin
KPMG in Canada
E: kbhasin@kpmg.ca

George Djuric
KPMG in Canada
E: gdjuric@kpmg.ca

Mitchell Nicholson
KPMG in Canada
E: mitchellnicholson@kpmg.ca

Kareem Sadek
KPMG in Canada
E: ksadek@kpmg.ca

Barnaby Robson
KPMG China
E: barnaby.robson@kpmg.com

Catherine Philippe
KPMG in France
E: cphilippe@kpmg.fr

Yosi Biton
KPMG in Israel
E: ybiton@kpmg.com

Julio Ferron
KPMG in Spain
E: jferron@kpmg.es

Gautam Ganeshan
KPMG in the Cayman Islands
E: gautamganeshan@kpmg.ky

Andrew Schofield
KPMG in the Cayman Islands
E: aschofield@kpmg.ky

Mikael Johnson
KPMG in the US
E: majohnson@kpmg.com

Jacob Prudhomme
KPMG in the US
E: jacobprudhomme@kpmg.com

Christopher Seigle
KPMG in the US
E: cseigle@kpmg.com

James Suglia
KPMG in the US
E: jsuglia@kpmg.com

Anthony Tuths
KPMG in the US
E: atuths@kpmg.com

About KPMG International

KPMG is a global organization of independent professional services firms providing Audit, Tax and Advisory services. KPMG is the brand under which the member firms of KPMG International Limited ("KPMG International") operate and provide professional services. "KPMG" is used to refer to individual member firms within the KPMG organization or to one or more member firms collectively.

KPMG firms operate in 143 countries and territories with more than 265,000 partners and employees working in member firms around the world. Each KPMG firm is a legally distinct and separate entity and describes itself as such. Each KPMG member firm is responsible for its own obligations and liabilities.

KPMG International Limited is a private English company limited by guarantee. KPMG International Limited and its related entities do not provide services to clients.

For more detail about our structure, please visit kpmg.com/governance.

Representing the world's hedge fund industry