AIMA

Digital Asset Custody

An AIMA Industry Guide

Sponsored by:

DISCLAIMER

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

This industry guide does not intend to give specific legal or commercial advice. Although care has been taken as to what is contained in this guide, no attempt has been made to give definitive or exhaustive statements of law or any opinions on specific legal or regulatory issues and no representation is made or warranty given that the information is complete or accurate. Furthermore, the applicable laws and regulations may change over time. As more legislation and regulatory guidelines are issued or updated, the accuracy of the information contained in this guide may alter.

This guide does not constitute or offer legal, regulatory or other advice and users of this guide should not rely on it as such advice. Neither AIMA nor the members of the Working Group accept any liability to any user of this guide who does rely on the content sof this guide. 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 or any member of the Working Group, or any of their respective employees, agents, service providers or professional advisers assumes any liability or responsibility, 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 this guide. Neither AIMA nor members of the Working Group 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) this industry guide.

Users of this guide are responsible for complying with all applicable copyright laws. AIMA permits users of this guide to make copies of this guide as necessary and incidental to users' viewing of it; users of this guide may take a print of so much of the guide as is reasonable for private purposes. Users of this 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 this 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 this guide and AIMA or any member of the Working Group in relation to this guide and users of this guide submit to the exclusive jurisdiction of the English courts.

Table of Contents

Foreword

The past year witnessed an upsurge of interest relating to digital assets among mainstream institutions and investors. 40% of nearly 300 clients interviewed by Goldman Sachs declared that they currently have exposure in some form to cryptocurrencies, with 61% expecting their holdings to increase over the next 12 months.[1] 21% of hedge funds are currently investing in digital assets with 26% of hedge fund managers, who are not yet investing, confirming that they are in late-stage planning to invest or looking to invest.[2] With BNY Mellon, State Street, Citi, JPMorgan and Deutsche Bank in the process of launching their digital asset custody service and Visa and Mastercard announcing they will support crypto payments, signs point to an increasing level of confidence in, and further institutionalisation of, this nascent technology.[3]

New digital asset classes are carving out an increasingly important role for the financial sector as potential investment opportunities in a fast-moving technology sector as well as diversifiers within portfolios. Though it is not just "traditional" cryptocurrencies that are forging the way ahead. The distributed ledger technology that gave rise to Bitcoin has yielded distinct advantages and use cases, such as stablecoins, tokenisation, central bank digital currencies and non-fungible tokens. Moreover, this same technology can eventually be applied to traditional financial instruments such as debt and equity – including in a decentralised manner through decentralised finance, or "DeFi".

Sitting at the heart of this technology in its simplest and broadest sense is the cryptographic key, conferring control of a digital asset to its holder. The private key – essentially a very large random number – is mathematically used to derive a unique public address, in some ways similar to an account held with a bank. The nature of the pairing makes it computationally very easy to prove control of a digital asset, but very difficult for someone to guess the paired private key, making the digital asset that they control difficult to acquire maliciously. However, as mathematically secure as that relationship is, it does impose a number of requirements in relation to the security of the private key.

Whereas traditional finance relies on identity-based frameworks, supporting either individuals or corporate entities, digital assets rely on the custody and control of the private key. Generation, control and management of these private keys are very different to the way in which assets have been traditionally controlled and managed. It is the control and management of these private keys which have given rise to the frameworks supporting the custody of digital assets as a distinct and specialist service offering.

While keeping a private key safe is fundamentally a technical need entailing specific hygiene protocols, when embedded within a commercial service offering, potential users of that service need to consider the terms upon which the service offering is provided, the regulatory framework sitting around the custody provider, any insurance provisions that are required or are in place and the legal basis upon which the assets are held. All of these factors are extremely important, both in the context of the security of the assets themselves, but more broadly in the context of setting standards for the industry as a whole which are robust, properly applied and represent current thinking.

1 Goldman Sachs, Global Macro Research Issue 98 (21 May 2021).

2 PwC, Elwood and AIMA, Third Annual Global Crypto Hedge Fund Report (24 May 2021).

3 *See, e.g.,* Mastercard Newsroom, Why Mastercard is bringing crypto onto its network (10 Feb. 2021).

This Guide is the initiative of AIMA's Digital Assets Working Group (the "AIMA DAWG").[4] The Guide aims to provide industry guidance on sound practices and key considerations for institutional investors determining whether and how to custody their digital assets. It has been written by a cross section of practitioners, as the custody of digital assets is cross-functional in nature, ranging from technologists and cyber security professionals to legal and compliance teams. The Guide has been primarily designed for those who are seeking the services of a Digital Asset Custodian ("DA Custodian") or, to the extent legally permissible, a custodial infrastructure provider.

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, this 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 A**), all of whom have generously volunteered their time and expertise to produce.

4 The AIMA DAWG is a cross section of senior industry experts including institutional investors, custodians, exchanges and other 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 https://www.aima.org/regulation/keytopics/digital-assets.html.

Glossary

AIFMD	the respective EU and UK versions of Directive 2011/61/EU of the European Parliament and the Council of 8 June 2011 on Alternative Investment Fund Managers, as amended (as applicable)
AML	anti-money laundering
Bitcoin	a particular type of decentralised cryptocurrency
blockchain	a system of records that are connected using cryptography to protect data
board	a board of directors for an entity established as a company or, with respect to other types of entities, the body performing similar functions, which, depending on the legal structure, could include a management company, trustee or general partner and, in certain circumstances, includes an "independent review committee" under applicable Canadian law
CBDC	a central bank digital currency, which is a digital form of money established by government regulation
CFTC	the U.S. Commodity Futures Trading Commission
cryptography	the conversion of data into private code using encryption algorithms, typically for transmission over a public network
DA Custodian	a digital asset custodian
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 on decentralised public blockchain networks and that do not involve intermediaries, such as banks
DLT	distributed ledger technology, which uses multiple independent computers to store information and transactions rather than a single centralised database
Ether	the name of the cryptocurrency tokens used for payment on the Ethereum network
Ethereum	a blockchain network that is similar to Bitcoin. It has its own cryptocurrency, called Ether or ETH, and can be used to build, publish and monetise decentralised digital applications on the network
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 U.S. dollar or the Euro
hosted wallet	a wallet typically held by a third-party provider
HSM	hardware security module

institutional investor	for the purposes of the Guide, an institutional investor may be: (i) a family office; (ii) an investment manager investing on behalf of a client or a fund; or (iii) an investment manager investing for its own account
investment 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. An investment 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; (v) an alternative investment fund manager under the AIFMD; and/or (vi) an external management company under the UCITS Directive. 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 investment managers
ISO	the International Organization for Standardization
ISO27001	the international standard for information security
miners	people creating new cryptocurrency through the process of solving computational problems that validate transaction blocks and work to maintain the blockchain ledger
MPC	multi-party computation
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
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 non-mining platform 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 blockchain protocol that involves miners solving complex mathematical problems/algorithms in order to place a block of transactions on the chain
Qualified Custodian	under U.S. Securities and Exchange Commission's custody rule for investment advisers, a qualified custodian can be a bank, registered broker-dealer, futures commission merchant, or certain foreign entity. With certain limited exceptions, an investment adviser is required to maintain client funds and securities with a qualified custodian
smart contract	a programmatically executed transaction coded into a blockchain network based on predefined terms
SOC	Service Organization Controls

SOX	the Sarbanes-Oxley Act of 2002 is the U.S. law meant to protect investors from fraudulent accounting activities by corporations
UCITS Directive	the respective EU and UK versions of Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to Undertakings for Collective Investment in Transferrable Securities, as amended (as applicable)
unhosted wallet	a wallet held by the user
VASP	virtual asset service provider
wallet	an application or device for storing the private keys providing access to the digital asset
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

Digital assets are digital records of value or contractual rights that can be stored, tracked and transferred using DLT or blockchain technology. The underlying technology enables secure peer-to-peer transactions without the need for a central or governing entity, and without requiring transactors to rely on trusting each other. While there is not a universally accepted definition of digital assets, the CFTC defines them as "*anything that can be stored and transmitted electronically and has associated ownership or use rights*". [5]

A distinguishing factor among blockchain technologies is Layer 1 (L1) and Layer 2 (L2) solutions. L1s are base layer networks like Bitcoin, Ethereum, Algorand, Stellar, Solana and Cardano.

L1s like Bitcoin and Ethereum, which both run Proof of Work consensus mechanisms, are generally more decentralised and secure; however, they take longer and it can become expensive to process transactions during times of network congestion. Ethereum experiences this through an increase in "gas" fees, which make it more costly to send or transmit tokens and NFTs or deploy smart contracts. Similarly, it can take several hours to get the necessary number of confirmations to receive a transaction on the Bitcoin network.

Developers build L2s on top of L1s to solve this scalability problem. They enable several smaller transactions to be processed on a "sidechain" (i.e., a separate blockchain that has fewer nodes and can confirm transactions more quickly) which are then batched together and confirmed as one transaction on the main L1 chain. Examples of L2s include Polygon, Arbitrum, Optimism for Ethereum and Lightning Network for Bitcoin.

The most common types of digital assets include:

- **Cryptocurrencies** are digital assets which typically are not "backed" by other assets. These tokens can be a payment mechanism (e.g., Bitcoin) and may be used to pay for using, and govern, a blockchain network that runs smart contract applications (e.g., Ethereum "gas").

- **Stablecoins** are designed to mirror the price of an asset such as a fiat currency like the U.S. dollar. The price "stability" of such coins with respect to the fiat currency can be achieved through different types of mechanisms such as the backing of issuance (i) by the fiat currency or some form of liquid collateral denominated in that currency or (ii) through collateralisation by other cryptocurrencies.

- **Tokenised assets** are an "on-chain" (i.e., blockchain) representations of assets that exist "off-chain", such as real estate, securities, etc. Tokenised assets differ from protocol-native assets like Bitcoin, since the asset exists in both physical and digital form.

- **CBDCs** use an electronic record or digital token to represent the virtual form of a currency issued and regulated by the monetary authority of a particular country or group of countries.

5 CFTC, Digital Assets Primer, Dec. 2020.

- **DeFi assets** are the functional components of a broader finance application existing on a blockchain. DeFi applications use smart contracts, which are trusted pieces of software whose veracity, security and execution are governed by DLT. DeFi applications can provide peer-to-peer financial services, such as lending, without a central entity. DeFi assets are usually governance tokens, similar to equity instruments, whose holders participate in the design and implementation of the various DeFi applications.

In traditional financial models, institutional investors rely on a depositary or custodian to secure their financial assets to reduce the risk of theft, loss and insolvency and, in many cases, to satisfy regulatory requirements which limit their ability to custody their own assets. In the digital asset environment, this is generally no different. Similar to traditional financial products, for many investors, a digital asset needs to be held and custodied by a regulated depositary or custodian (i.e., a DA Custodian).

The concept of digital asset custody revolves around the safekeeping of a private key. However, as the private keys are used to store, manage and transfer digital assets by the owner and help with the decryption of messages and authentication of transactions, they represent a single point of failure in the system. Therefore, private keys require sophisticated technologies to prevent theft, loss or destruction.

An institutional investor looking for a DA Custodian to custody its digital assets should seek a DA Custodian who has the ability to support the types of digital assets that align with the investor's investment strategy. The institutional investor will need to determine if they need to use a DA Custodian that is maintaining appropriate authorisation and/or licences and supervised by regulatory authorities (e.g., a depositary or "Qualified Custodian") or a custodial infrastructure provider used only to secure public and private keys and to enable the institutional investor to self-custody its own digital assets. Not all jurisdictions allow self-custody solutions or allow them for all types of investors.

When evaluating DA Custodians, institutional investors should consider the following:

- **Asset safekeeping** – What structure and/or mechanism does the DA Custodian use to safeguard clients' ownership rights and to prevent the use of client assets by the DA Custodian for its own account or from becoming part of the bankruptcy estate of the DA Custodian upon insolvency?

- **Track record** – For how long has the DA Custodian been custodying the relevant type of digital assets at scale with no loss of client assets and what is the DA Custodian's assets under custody market share in the relevant type of digital assets?

- **Financial strength** – What are the financial resources the DA Custodian can call on to make good on its client obligations?

- **Insurance** – What are the size, type and quality of the DA Custodian's insurance programme?

- **Security** – Does the DA Custodian have capabilities in physical and cyber security and security-first software development practices, including, for example, the ability to mitigate human error through strong controls, as well as segregation of client keys?

- **Disaster recovery protocols or similar** – Does the DA Custodian offer the capability to recover the assets in case of a major technical or operational issue either on the custodian or investor side?

- **Asset servicing** – Will the client be benefiting from forks, airdrops, staking, governance and lending?

- **Third party oversight** – Are there independent third parties (e.g., regulators and auditors) supervising the DA Custodian's operations?

- **Range of support** – What are the number of Layer 1 blockchains and digital assets supported and the frequency of adding new assets?

- **Accessibility** – How quickly can clients retrieve and move assets?

- **Control** – Can the DA Custodian unilaterally control the assets? If yes, under what circumstances and what contractual protections are in place for the investor?

- **Reporting** – Does the DA Custodian offer reporting capabilities such as NAV, balances, transfers and orders?

Although the relative importance placed on each of these factors may differ, institutional investors interested in a third-party custody arrangement should seek to understand the capabilities of the various DA Custodians in the market and work with the DA Custodian that aligns with their own particular strategy and requirements.

There are many players in the digital asset custody space. These include Virtual Asset Service Providers ("VASPs") as well as traditional custodians who are expanding their offerings. In some jurisdictions, traditional custodians may also have to register as a VASP (or equivalent) to offer digital asset services.

Secure custody of digital assets is fundamental to meeting the needs of the various market stakeholders within the digital asset ecosystem. At its heart sits the digital asset itself, with a range of technical and security features that will determine the framework that needs to be applied. The most important and frequently encountered asset is likely to be Bitcoin, followed by Ethereum. However, with over 18,000 digital assets at the time of writing, the principles associated with the custody of these assets need to be flexible enough to securely cater for all classes.

Sale and purchase of assets are typically achieved through an exchange of some kind, which may be fully or partially regulated. A fully regulated exchange implies that all aspects of the exchange fall under the auspices of a regulatory framework, whereas a partially regulated exchange may only require certain operational standards to adhere to a given regulatory framework, such as AML regulations.

In terms of holders of these assets, strong demand for qualified custody is evident from hedge funds, venture capital firms, private equity firms, asset managers, asset owners, exchanges, corporate treasuries, sovereign wealth funds, family offices, fintechs, miners and high net worth individuals. Emerging areas of custody demand include the need to store stablecoins and/or CBDCs which are expected to increase significantly over the coming months and years. Similarly,

demand for the custody of security tokens is expected to increase, coupled with support for NFTs. As demand for these services increases, it is inevitable that external oversight will be called upon to validate the proper custody of these assets. This will emerge in the form of audit and assurance offerings from professional service providers. There are instances where frameworks have been applied, for example SOC reports[6] or other international accreditations such as ISO27001 in relation to digital asset exchanges or custodians.[7] But progress is relatively slow, driven principally by risk appetite.

2. Custody options – an overview of technologies

At the highest level, a number of custody options are available today to institutional investors with each having its own characteristics:

- Self-custody:[8]
    - includes hot (browser-based), warm (software-based) and/or cold (offline-based) wallets/ storage;
    - provides for greater control of digital assets;
    - allows for a broad range of protocol and token support;
    - if means of access to assets held in self-custody using traditional approaches (including software/hardware wallets, etc.) are lost, assets will become irrecoverable;
    - assumes responsibility for assets, asset servicing and associated risks (compliance and financial crimes, technology and cyber risks); and
    - requires digital assets expertise within the institutional investor (technology, security, development capabilities).
- Exchange hosted wallet:
    - investor gives control and management of public and private keys to an exchange, but maintains access via an online wallet;
    - ease of access;
    - counterparty risks with the exchange;
    - security risk associated with exchange hacks;
    - commingling of client assets; and
    - not operationally or capital efficient if the investors trade (and therefore custody) on multiple exchanges;
    - need for on-chain transfers in times of high volatility across multiple exchanges to manage collateral; and
    - potential rehypothecation of client assets.

6 Note that these are U.S. and not international reports (although in general they are recognised internationally).

7 See **Section 5** of the Guide for a further discussion of SOC reports and ISO certifications.

8 Note that in certain jurisdictions there might be a regulatory requirement under relevant legislation to appoint a depositary, a Qualified Custodian or a similarly regulated third-party service provider.

- Third-party custody:
    - stores digital assets on behalf of customers using clearly defined features and controls to provide certainty over the safekeeping of the assets;
    - institutional grade technology stack and security;
    - likely to be insured;
    - can be hot, warm or cold;
    - assumes responsibility for assets, asset servicing and associated risks;
    - assumes the burden of managing a complex and ever evolving tech stack;
    - could provide regulatory compliance;
    - sub-custody where institutional investors can outsource custody operations to a digital asset custody provider in an omnibus or segregated set-up (custodian would not know the end investor); and
    - may be subject to regulatory oversight.

DA Custodians and custodial infrastructure providers can use hot wallets, warm wallets, cold or air-gapped storage to hold digital assets. Hot wallets' private keys are stored online which is a convenient and easy way to access assets and is more suitable for high-frequency trading (HFT) type use cases but has increased vulnerability and security concerns. Cold storage is the most traditional storage in digital asset custody, more suitable for longer term strategies like buy and hold but typically involve longer customer service level agreements for withdrawals. To retrieve assets, manual human intervention is required, and for traditional private key custody it can take anywhere from a few hours to a few days to process the request depending on the provider. However, MPC cold wallets can be accessible within a few hours or less. Due to the human security layers, there is a reduced onset of fraud and risk of being hacked with a greater risk of human error or coercion. However, these risks can be managed and mitigated through robust processes and controls. Warm storage is a mix of a cold and hot infrastructure.

DA Custodians may hold investors' long-term investments in air-gapped wallets or cold storage to maximise security and actively manage the percentages of assets kept in hot wallets as well as to facilitate any necessary rapid withdrawals. Some custody solutions combine the speed of a hot wallet with the security of an air-gapped wallet or cold storage by using more modern, proven technology solutions than legacy cold storage.

A successful transfer of digital assets on the blockchain network requires the digital signing of the transaction with the private key. All blockchain networks are decentralised and any transfer of assets on the blockchain network is irreversible, which implies that the holder of the private key is in full control of the account and therefore the assets themselves. Therefore, while the generation and storage of the wallet's private key is the cornerstone of all custody solutions, access to the keys (in the form of user permission management, client policy administration, DA Custodian's own fraud detection safeguards or address whitelisting) should be subject to the same level of security and protection.

Protocols adopted to safeguard the private key can be highly sophisticated or as simple as writing the private key on a document and storing it securely. This Guide assumes a more institutional grade approach to custody and ignores the most basic approaches.

2.1 Cold storage or air-gapped storage

The concept behind "cold" or "air-gapped storage" is that the private key cannot be hacked or stolen by a malicious actor over the internet as the keys are stored in appliances that are not connected to the internet. While conceptually simple, there are a number of considerations involved in implementing an institutional grade cold storage solution including:

- **Key Generation Ceremony** – The process of generating a master seed (**see Section 3.1**) from which all wallets will be derived from. The key ceremony must be audited to ensure that no party is able to access the master seed. The key ceremony material must be either destroyed or securely backed-up (and sharded) for recovery.
- **Wallet Generation** – The private key must be generated in a secured appliance (hardware or software) and should never be exposed to any party or extracted from the appliance. The corresponding public key is the external representation of the wallet.
- **Entropy** – The degree of randomisation utilised in generating the private key, which impacts how easy it would be to guess the private key sequence.
- **Air Gapping** – The process of isolating the computer used to generate key pairs from any physical or electromagnetic communication networks to prevent unauthorised access.
- **Key Sharding** – Splitting the private key or master seed into multiple components, presumably for separate storage by separate parties, thus increasing the threshold for the number of parties required to regenerate the private key.
- **Shamir's Secret Sharing** – A form of cryptography that enables the DA Custodian to regenerate the private keys and/or master seed if in possession of n–1 shards, ensuring that there is no single point of failure if a particular shard is lost or damaged.

The primary benefit of cold or air-gapped storage is that the private key is offline, and therefore unlikely to be copied or obtained by hackers, though this method necessitates robust consideration of physical security requirements, as well as back-up and redundancy planning. The main drawback of traditional cold storage is that access to assets is unlikely to be immediate, which may make it a less attractive method of custody for active trading or any case where funds must be settled expediently.

2.2 Hardware security module

The concept behind utilising a hardware security module ("HSM") is that the private key is generated within a secure device from which it cannot be extracted without damaging the device. The private key is never exposed, even to the holder of the device, and therefore cannot be copied or hacked. The most simplistic version of this technology is a hardware wallet device, though this generally implies that the device would be possessed by a single party. A more robust institutional solution would be to build an HSM in which the private key is generated within multiple devices, effectively requiring the involvement of multiple parties to sign a transaction. HSMs often comply with internationally recognised standards to verify the secure creation and storage of private keys.[9] HSMs have also been used in securing private keys for many traditional applications such as secure communications, the security of the internet and key national infrastructure.

9 For example, the U.S. Federal Information Processing Standard (FIPS) 140-2 is a governmental security standard used to approve cryptographic modules. These recognised standards have been widely used in the commercial and military sectors for decades.

Given it relates to back-up and redundancy (as with the cold storage method of custody), the key to a multi-party HSM approach would be for the quorum, necessary to sign a transaction, to be less than the total number of signatories to avoid a single point of failure. Storage and recovery of a master seed are equally important as securing the wallet's private key. The process to recover the master seed (and all wallets) should be documented under a resolution mechanism by the DA Custodian. The sharding and storage process of the master seed must be extremely robust to prevent fraudsters, hackers or rogue employees from gaining access. Meanwhile, if using a simplistic hardware wallet controlled by one party, there is typically a recovery seed phrase that enables a transfer of assets associated with the hardware wallet to a new device. Storage of this recovery seed phrase is equally important to storage of the private key itself since the holder of the recovery seed could simply transfer assets to a new device.

The main drawback is that HSM may not be natively supported by a blockchain and similar to that with MPC – there is a reliance upon the code supporting the HSM technology, and therefore the code management/governance techniques of the DA Custodian.

2.3 Multi-party computation

Multi-party computation ("MPC") utilises technology that uses algorithms and multiple servers to generate a private key in such a fashion that no one server hosts the entire private key at any point through the lifetime of such key. For instance, if one server held the value of X = 3, a second the value of Y = 4 and a third an algorithm that is XY2, a value of 144 would be returned as the private key without any of the multiple servers knowing all of the components of the private key. In this example, two of the three component parts would be required to consent to the signing of a transaction, avoiding a single point of failure.

MPC enables a custodial solution in which a multi-signatory requirement replaces the need to store the private keys offline. This gives users immediate access to their digital assets provided the quorum is available, which is the key benefit of an MPC custodial arrangement. As with HSM technology, MPC also reduces physical security risk as it relates to any single piece of information. The main drawbacks of MPC include reliance on coding produced by developers, as well as limitations inherent in the complexity of the code which can result in a quorum of two parties. Benefits of MPC only hold where the shards are geographically and architecturally distributed. Splitting a key between a few parties sitting in the same room and using the same infrastructure is limited versus a simple password-protected interface for consensus approvals. Another common area of concern is the lack of standardisation on multi-party threshold (cryptographic) schemes.[10]

3. Key generation and management

As indicated in Section 2 of the Guide, key generation and management is perhaps the most important element of custody for digital assets. This section aims to highlight key considerations and sound practices (beyond the assumed adherence to general sound practices for information security) that should be evaluated when weighing the risks of a custody solution for digital assets. Note that this section assumes adherence to general sound practices for information security.[11]

10 Workshops such as the NIST Workshop on Multi-Party Threshold Schemes (Nov. 2020) provide a forum for discussions and a step in the right direction towards international standardisation. However, at present, there are no well-cited, international standards for MPC schemes.

11 AIMA's Guides to Sound Practices comprises the widest body of sound practice output and guidance on the alternative investment management industry. For example, AIMA's Guides on Cyber Security and on Operational Risk Management contain guidance around sound practices for information security.

3.1 Main considerations for key generation

A deterministic wallet is a system of deriving keys from a single starting point known as a master seed. The master seed allows a user to easily back-up and restore a wallet without needing any other information and can in some cases allow the creation of public addresses without the knowledge of the private key.

A master seed is simply a random number which needs to be securely generated and backed-up so that a wallet can always be 're-generated' in the event of a loss or destruction. One way a master seed can be reconstituted is via a mnemonic passphrase which is a method of creating a back-up of the master seed by mapping the data of the master seed to a dictionary of words. The secrecy of master seeds or mnemonic passphrases is paramount as possession of these artefacts would enable the regeneration of all public and private keys of a deterministic wallet and to transact with the blockchain(s) as the wallet owner.

Master keys are randomly generated strings that are typically used to encrypt sensitive information. In the context of master seeds, a master key may be used to encrypt a master seed, thereby allowing the master seed to be securely stored without the concern of it being seen or copied. Master keys can be sharded so that they can only be reconstructed if multiple shards are brought back together.

When private keys or master seeds are generated, they may be exposed to the parties participating in their generation. This necessitates a rigorous documented key generation process that ideally involves multiple parties. If the keys are generated on an internet-connected device, the private keys may also be accessible by malicious actors to the extent that the internet-connected device is infected with malware or other data security vulnerabilities. Additionally, consideration must be given to back-up and redundancy planning to avoid a total loss of assets should that the primary storage solution becomes unavailable. Custody solutions may utilise key sharding: the process of breaking the private key into multiple components that must be reassembled to reconstitute the private key prior to processing an egress transaction. In such instances, consideration must be given to employing a form of encryption technology which avoids a single point of failure. The key ceremony must be strictly governed.

- Participants:
    - Safety, security and due care are prioritised over speed.
    - Access controls (e.g., entry logs, cameras) are in place to ensure no unauthorised entry to locations where HSMs are stored.
    - Employee background checks and four-eyes principle checks on all steps of key generation and withdrawal ceremonies.
    - No one individual has control or knowledge of the end-to-end process to reinforce segregation. Information is shared with participants strictly on a need-to-know basis.
    - Segregation of duties and independence are reiterated through the selection of individuals from independent functions for key roles. This approach additionally deters collusion through the introduction of professional liability.
    - Multiple practice sessions are required to rehearse the process. Back-up individuals are fully trained and carefully selected to minimise information leakage.

- Auditors:
  - External reviewers should be carefully selected so that information sharing is minimised.
  - An external review of the process design should be conducted to provide independent assurance over process steps.
  - External attendees at the key ceremony process as an additional deterrent for collusion.
- Sharding of key/seed and safekeeping of shards:
  - The master seed should be split into separate components and dispersed storage such that it is sufficiently challenging for a malicious actor to retrieve the component shards.
  - Artefacts should be geographically dispersed, split into N of M combinations, which require a minimum number to recreate the private keys, and securely stored with separate custodians.
  - Shamir's Secret Sharing or equivalent cryptographic techniques should be used such that the key can be recovered if any individual shard is lost or damaged.
  - Artefacts should be examined periodically to ensure that they are in place and not damaged.
- Resolution process:
  - Retrieval processes should be contractually agreed in advance with the custodians storing the artefacts.
  - Consideration should be given to involving an independent third party in the retrieval process.
  - In the event artefact retrieval is required, the requestor and receiver should not be the same individual. This should be contractually agreed.

3.2 Sound practices for key generation

For certain blockchain networks, keys may be generated within HSM, other hardware wallets or using MPC technology. If designed correctly, these approaches imply that the private key will never be exposed to any one party. This mitigates inherent risks during the key generation process while introducing key management risks as discussed further below. Assuming key generation is performed without HSM or MPC technology, practices adopted should entail some or all of the following:

- **Surveillance** – A key generation ceremony should be subject to a combination of surveillance techniques, including a combination of video cameras, third-party oversight or participation in the key generation process, documentation of steps taken and attestation to adherence to the required elements of the process.
- **Air Gap** – Consideration should be given to whether the private keys are to be generated on an internet-connected device. A device that is not connected to the network is commonly referred to as an "air-gapped" device. Using an air-gapped device reduces the risk of a remote attacker breaching the confidentiality of the key generation process and increases the likelihood that only the parties involved in the key generation process will have access to the keys.

- **Entropy** – This is known as the degree of randomisation involved in generating the private key. Ideally, at least dual entropy would be employed to minimise the likelihood of correctly "guessing" the private key.

- **Hard Drive** – To the extent that the device used to generate the private keys is not equipped with a hard drive, the computer cannot retain information between reboots, which limits a perpetrator's vectors of attack. If the device is equipped with a hard drive, inherent risks can be mitigated by utilising a new device for each key generation ceremony, wiping the hard drive clean at the end of each process or by destroying the local hard drive on the device itself.

- **Sharding** – The process of splitting the private key into multiple components for separate storage typically enhances security as it would make it significantly more challenging for a malicious actor to retrieve the private key. The key sharding process should utilise Shamir's Secret Sharing or an equivalent mode of cryptography to ensure that the key is recoverable if any individual shard is lost or damaged (i.e., three of four shards are required to regenerate the private key). Key shards should ideally be encrypted and stored separately in locations with strong physical security protections (i.e., safes) that are accessible by different individuals in such a manner that no one party has access to all of the individual shards.

- **Redundancy** – The private key or the private key shards need to be stored in a secondary location (or locations if necessary) as a back-up in case the primary solution becomes unavailable. Any copier used to print copies of the keys should be air-gapped and memory-free, while the mode of transportation of the keys to the back-up location needs to be assessed for appropriate security protocols.

- **Hardware wallets** – Where hardware wallets are utilised, as the private key exists within the hardware device itself and is typically not observable itself, risks involved in generating keys may be considered lower. However, redundancy also needs to be considered in case the hardware wallet is lost or damaged. Certain hardware wallets would enable a recovery process using a seed phrase or seed words. The recovery seed should be written down on paper and stored offline in a secure location that is separate to the hardware wallet itself to ensure recovery. Where possible, multiple parties should be involved in storing and accessing the seed recovery phase, with careful attention paid to ensuring there is no key-person risk inherent in the seed recovery process.

Assets should not be distributed to an address until successful completion of the risk management procedures have been verified.

3.3 Key management considerations

Equally important to the security framework built around the generation of private keys is key management, particularly at the time of any transaction on the blockchain network since the private keys may be exposed to the internet when signing a transaction. Note that the private keys may also be exposed when participating in governance protocols. Key management considerations also extend to HSM and MPC technologies as the safekeeping of devices or key shards can be considered akin to safekeeping of private keys.

3.4 Key management sound practices

A consideration that may impact key management is the required accessibility of the assets. An elaborate multi-party cold storage solution may not be possible for an active trading strategy, unless separation of execution from settlement is carried out. Whether private keys or private key

shards are stored in an HSM, using an MPC solution, on exchange, in a hot wallet or cold storage, some of the sound practices include:

- Thought should be given to segregation of duties between authorised signatories for fiat currency and authorised signatories for digital assets, in order to implement multi-party involvement to fund a trading venue prior to transacting.

- If using a DA Custodian that is responsible for the custody of private keys, initiation of the egress process should feature multi-party authentication on the institutional investors' part following the same principles used to initiate and approve a fiat cash disbursement.

- Assets should only be left on an exchange, in a hot wallet or at a counterparty, in the case of over-the-counter transaction, for as long as necessary. When not actively planning to trade, assets should be swept into secure custody on a frequent basis. This may not be possible when trading derivatives. Hence a third party such as a prime broker might be appropriate to mitigate counterparty credit risk versus exchanges.

- Assets should be split across multiple addresses to minimise the impact of any operational failure.

- Private keys stored in cold storage should ideally only be accessible to the extent that multiple parties are involved, with enhanced controls in place governing the decryption of private keys.

- If using a third-party HSM solution, ideally a quorum that consists of at least two parties should be required to perform any action, including an egress of assets or to make account-level changes. Ideally the quorum would not be 100% of participants to avoid key-person risk.

- If the institutional investor is required to employ self-custody practices using hardware wallets, physical security protocols put in place to safeguard the hardware device should be robust and involve a combination of video surveillance, safes, and keycard access controls. If possible, implementing segregation of duties – so that multiple parties would be required to access the hardware wallet – would improve security.

- If the institutional investor is required to employ self-custody practices using private keys that are generated outside of a hardware wallet, the private keys should be stored offline in a secure fashion (i.e., in a safe) and in a format that protects against damage from flooding or smoke. Controls should be robust to limit the number of parties that have access to the private keys. The institutional investor could use sharding techniques to increase the number of parties that would be required to reconstitute the private keys, though if Shamir's Secret Sharing or an equivalent form of cryptography is not utilised, this may introduce an element of key-person risk that needs to be weighed carefully. This solution, while popular for retail individual investors, should never be encouraged for any institutional investor due to the (very) high risk it carries.

- If employing an MPC solution, the key shards should never be stored in the same place or be accessible by the same individuals, both of which would defeat the purpose of an MPC solution. This should be true at all points in time even at the point of key generation by the DA Custodian. Failure to do so may compromise the assets.

Note that the custody of digital assets is continually evolving, and readers should expect new technological solutions to emerge, some of which may entail additional consideration when assessing custody.

4. Due diligence

With various options for the custody of digital assets, institutional investors are advised to invest time to go through a thorough due diligence process carefully evaluating the DA Custodian's policies, procedures and internal controls. The due diligence questions and level of detail will differ for every individual DA Custodian. For example, those using self-storage will want to investigate aspects around technology and/or media used to store the asset. When using a third-party storage solution, institutional investors should conduct a thorough third-party due diligence process. If this is a generic third-party diligence plan, it is wise to ensure it covers specific points around digital assets. Institutional investors should also be cognisant of the risk and mitigation tactics for each.

4.1 Governance

Any workable system or organisation of a custody operation may be acceptable as long as the relevant legal and compliance requirements are being met, and the DA Custodian's board and management, are fully aware of and, are fulfilling their responsibilities.

Capable management and appropriate staffing with knowledge of digital assets are essential to effective risk management. Experienced management and staff with appropriate autonomy, adequate training and the ability to manage turnover play a major part in offering high quality and consistent performance in custody services. Ensuring that the right people are in a position to mount the right challenge. A DA Custodian must carefully compare its staffing levels with the volume of business and the complexity of the services offered. If staffing is not adequate to handle the volume of business, transactions may be poorly executed and the DA Custodian may lose both assets and clients.

The depth of experience of the information security team at the DA Custodian is key.

4.2 Legal and compliance

The DA Custodian's board and management are responsible for ensuring that the custody activities comply with applicable laws and regulations. All applicable laws and regulations relevant to the custody business should be identified and communicated to the appropriate personnel. The DA Custodian should have an adequate system in place to monitor for compliance with applicable laws and regulations.

Some of the compliance issues that may arise for DA Custodians are compliance with local laws, including, but not limited to, recordkeeping and confirmation requirements, shareholder communication, AML, asset protection, investor protection and fiduciary obligations.

DA Custodians, particularly if operating globally, may be affected by a variety of laws and regulations.[12] Local laws may address such issues as:

- **Fiduciary capacity** – A DA Custodian may be considered to be a fiduciary under the law of some jurisdictions.

12 For example, in addition to U.S. federal laws and regulations, the DA Custodian may be subject to State laws, and laws of foreign countries in which they offer services. In foreign countries, the global DA Custodian will typically rely on its sub-custodian network to understand and comply with local laws and regulations.

- **Unclaimed property** – Globally, unclaimed property laws vary widely. In the U.S., for example, most States have unclaimed property laws. These provisions may require a DA Custodian to escheat unclaimed property to the State. The U.S. Employee Retirement Income Security Act of 1974 pre-empts State unclaimed property laws for retirement plan assets.

- **Taxation** – Countries' tax policies on investment income and capital gains differ.

- **Money laundering or suspicious activity** – To prevent money laundering and other illegal activities, a wide range of laws and regulations exist that may require DA Custodians to identify customers and report suspicious activities.

- **Reporting and recordkeeping** – A DA Custodian may be subject to regulatory reporting and recordkeeping requirements in the countries in which it offers its services.

Global DA Custodians operate in multiple, fast-evolving regulatory environments. They must have an effective process in place to identify regulatory and market changes as they arise and ensure continued compliance.

A strong compliance program should include monitoring the variety of laws and regulations that may affect a DA Custodian's business and reporting any material changes to the institutional investor. Global DA Custodians must be aware in particular of the multiple overlapping (and potentially conflicting) regulatory environments in which they operate. Institutional investors who choose a custodial infrastructure provider carry the compliance risk, as they are considered the custodians of these assets. Compliance risk may be heightened in foreign markets because different markets have different rules and regulations. These differences make supervision more challenging.

DA Custodians are subject to a wide array of regulations, including in most cases those which address money laundering and terrorist financing and which address consumer privacy issues. These, among other regulations, may pose challenges to DA Custodians due to such regulations' lack of contemplation of the digital asset industry and technical difficulty in complying with the black letter of certain provisions. A specific area to consider would be the applicable conduct compliance considerations, including conflicts of interest, fiduciary compliance, etc., which would apply depending on respective business models.

4.3 AML and Fraud

An important risk to consider is digital assets association with illicit activity. Some, however, argue that the blockchain acts as an immutable record and thus makes it very difficult to cover up illicit activity. For example, recent law enforcement cases demonstrate using transaction monitoring on blockchain to clamp down on illicit activity long after the crimes have occurred.[13] That being said, cryptocurrency money launderers represent a major component of the illicit activities and institutional investors should verify that the DA Custodian is taking steps to ensure this risk is properly assessed and mitigated.

Failure to sufficiently address this risk can lead to severe reputational damage with major business implications. The importance of a DA Custodian's reputation cannot be overstated. The ability of the DA Custodian to deliver services as promised and maintain the security of digital assets under custody is critical to maintaining its reputation.

13 See, Recovery of Colonial Pipeline ransom funds highlights traceability of cryptocurrency, experts say (June 2021).

DA Custodians should be evaluated on steps taken to deter cryptocurrency usage in illicit activities through comprehensive onboarding programs, AML programs, clear know-your-customer (KYC) processes and compliance with regulatory reporting requirements (suspicious activity reports, etc.).

4.4 Cyber security and incident planning

The cyber security posture of a DA Custodian is arguably the most important area of its IT operations. For DA Custodians, not having a good handle on virtual hygiene, handling and exchange of digital assets could lead to devastating consequences such as theft, fraud and loss.

In keeping with sound governance practices, DA Custodians should have detailed cyber security written policies and procedures implemented. These plans should be in line with all legal and regulatory compliance obligations applicable to the DA Custodian's business. These plans should also be auditable and reviewed periodically as well as being tested at least annually and updated after any significant organisational changes. Investors should consider seeking third-party audits specifically relating to cyber security.

Likewise institutional investors looking to invest in digital assets must be cognisant of these risks, have effective hygiene protocols in place as well as a contingency plan for each scenario should disaster strike. Following industry governance closely, most intuitional investors should align to frameworks for sound cyber security sound practices. AIMA has published a series of Guides to Sound Practices, including one on cyber security.[14]

4.5 Financial and counterparties

Financial (or backing) risk represents the notion that, due to its capital structure, a DA Custodian may not be able to withstand certain business shocks, leading to impact on clients, up to and including the custodian's insolvency. Typical capital structure, liquidity and funding concerns present in traditional markets also exist for DA Custodians, but with the added wrinkle that many of these companies operate outside the standard banking apparatuses. Although the sentiment has lately been diminishing, there are several major financial institutions that still refuse to engage digital asset companies on either a deposit or investment banking basis.

Investors looking to place their digital assets with a DA Custodian should examine not just the custodian's balance sheet structure and size, but also its underlying ownership commitment and provenance.

Counterparty risk is the risk or likelihood that a counterparty in a financial transaction will default on its contractual obligation. In addition to the balance sheet risk previously mentioned, this failure could also be caused by operational breakdowns.

To assess these risks, investors have begun assigning Counterparty Risk Scores to various DA Custodians. Counterparty Risk Scores rely on both quantitative and qualitative factors which can include a review of:

- legal entity structure and ownership;
- management's track record and tenure;

14 AIMA, Guide to Sound Practices for Cyber Security (2022).

- quality of risk management, security and compliance departments, as well as relevant controls;
- business reputation, relevant news and headlines, competitor analysis;
- entity status (sanctioned or unsanctioned), political affiliation (politically exposed persons), internet community activity (associations with darknet markets), etc.;
- historical and current financial performance inclusive of in-depth reviews of profitability, liquidity, leverage and capital adequacy; and
- legal and regulatory risks.

Another tool in counterparty analysis is a SOC report or ISO27001 certification. While SOC reports are not required by law, they provide a strong base on which institutional investors may build confidence in their DA Custodians. See **Section 5** of the Guide for a further discussion of SOC reports and ISO certifications.

4.6 Insolvency

Within the digital assets ecosystem, insolvency risk poses a key concern for constituent firms up and down the value chain. Unlike the custody of traditional assets, which in some jurisdictions may fall under protection, digital assets sit more or less at the mercy of their DA Custodians.[15]

Institutional investors evaluating the implications of an insolvency on custodied assets should consider whether those assets are held in omnibus or segregated accounts or a combination thereof.

- **Omnibus** – Client accounts are comingled, pooled or otherwise combined and the DA Custodian holds the key. In this case, the DA Custodian will appear on the chain as the owner of the asset. This is also the most common custody offering by exchanges.
- **Segregated** – Assets are held in distinctly demarcated accounts under the name of the actual owners, not in the DA Custodian's name.

The difference between these two can play a significant role in the event of a DA Custodian's insolvency and the subsequent legal proceedings.

Assets that are held in a comingled or omnibus account are not easily tracked back to the original depositors. While on-chain analysis may be able to track back certain assets in a comingled setting, courts may not differentiate between assets within an account. There are, however, ways to identify clients through on-chain solutions such as proxy wallets, which essentially are 'pass-through' wallets associated with specific clients for the sole purpose of identifying where deposits into an omnibus structure come from. Overall, it is much simpler for courts to unwind ownership interest in segregated accounts.

Courts have not clearly established (and certainly not in DeFi cases, where those assets are being lent, hypothecated or otherwise held as loan collateral) where the chain of custody or the transfer of ownership begins in the world of comingled digital assets. In an insolvency, creditors may claim that comingled assets under the control and potential ownership of the DA Custodian are the DA

15 In the U.S., an independent agency of the federal government, the Federal Deposit Insurance Corporation, generally insures up to $250,000 per person, per bank. It covers all checking accounts, savings accounts, money market deposit accounts and certificates of deposit. It currently does not cover cryptocurrency.

Custodian's assets, not the institutional investor's, and should not be considered as insolvency remote.

A blockchain lends itself to clear and transparent demarcation of ownership and can be used to clearly segregate accounts in a way that even third parties can view.

Key control is of paramount importance in the event of insolvency. Whoever has control of the key has control of the asset, so due diligence needs to explore a DA Custodian's private key controls in the event of insolvency.

4.7 Operational risk

Transaction risk, which falls under operational risk is the risk to current or projected financial condition and resilience arising from inadequate or failed internal processes or systems, human errors or misconduct, or adverse external events such as cyber attacks. This type of risk is inherent in efforts to gain strategic advantage, and in the failure to keep pace with changes in the financial services marketplace.

Transaction risk is inherently high in digital asset custody services because of the high volume of transactions processed. Although it could be argued that transaction risk is lower than in the traditional space (e.g. Equities and Futures) where processes tend to be a lot more manual in nature (including reconciliations across various databases). Nevertheless, ensuring the DA Custodian has effective risk management tools, policies and procedures, a strong and robust control environment, and efficient use of technology is essential. Meaningful reporting, based on accurate and reliable data, is needed to provide management with monitoring tools. The risks may be magnified with a global DA Custodian where transactions occur around the clock in a variety of different markets.

When reviewing DA Custodians, institutional investors should assess the following aspects of the digital assets custody offering:

- turnaround time for transactions in/out of the wallet, including fraud detection tools, compliance and coin provenance checks;
- key-person dependability risk, especially when human intervention is required to access and/or operate the wallet's private key;
- connectivity to other DA Custodians and exchanges for seamless settlement; and
- compliance with the "travel rule" (Financial Action Task Force recommendation 16) or plans to comply.[16]

Another key operational risk consideration is the single point of failure. DA Custodians who run a trust-less architecture are better placed to cope with operational risks. This requires elimination of single points of failure such as handling private keys and seed phrases. In addition, best-in-class operational procedures would also eliminate the ability of any single party to compromise the wallet (including the DA Custodian itself) due to internal errors.

16 See, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf.

Examples of Due Diligence Questions:

- How many digital assets does the DA Custodian support for custody?
- Does the custody solution provide insolvency remoteness for custodied client assets? Explain how.
- Does the DA Custodian provide custody solely for digital assets, or fiat currencies as well?
- Describe wallet and safekeeping options offered through the custody solutions (e.g., hot, cold, warm).
- Are clients' assets held in commingled wallets or segregated wallets and explain why?
- What is the contractual or legal duty of care and standard of liability owed by the DA Custodian to its clients?
- Does the custody solution allow for, or enable, the rehypothecation of client digital assets under custody? If so, what collateral and/or risk control requirements govern such activities?
- Does the DA Custodian plan to add support for additional digital assets? If so, please describe the new asset onboarding evaluation, timeline and due diligence process.
- Describe the deposit and withdrawal process for digital assets in custody and associated time frames.

5. Application of SOC reports and ISO certifications

As the digital asset industry continues to mature, SOC reports and ISO certifications are differentiators that signal a DA Custodian upholds strong controls aligned with industry standards and best practices. The controls and processes that SOC reports and ISO certifications cover are key elements to a secure and effective digital asset custody practice and are important to evaluate when reviewing DA Custodians.

While SOC reports are one of many pieces in the process of vetting service providers, they establish a basis for placing trust in a DA Custodian given the independent third-party assurances and transparency they provide. Institutional investors can leverage SOC reports to reduce their own costs of compliance and, in certain cases, choosing service providers that undergo routine SOC assessments can even help them meet the needs of their own stakeholders, such as auditors and regulators. SOC reports can also provide institutional investors with a standard framework and set of criteria to compare service providers to one another.

5.1 Applicability of SOC 1 and SOC 2 reports

SOC 1 reports provide assurance over controls and processes that impact user entity financial statements and reporting. Specific processes covered by SOC 1 reports for DA Custodians may include digital asset onboarding, asset valuation, reconciliation and private key management controls.

An institutional investor that has digital assets on its balance sheet and/or within its revenue stream, and whose financial statements are externally audited, requires financial services and custody service providers that regularly procure SOC 1 reports to facilitate financial statement audits and/or meet SOX compliance obligations. Financial statement auditors are key stakeholders that expect user entities to select service providers that provide SOC 1 reports.

Besides financial statement auditors, other stakeholders interested in SOC 1 reports may include internal audit and risk management teams, business partners and regulators of the DA Custodian.

SOC 2 reports may not satisfy the requirements of these stakeholders as they do not provide specific assurance over controls relevant to financial statements and reporting.

SOC 2 reports provide assurance over controls and processes relevant to (i) the security, availability and/or processing integrity of the systems a service provider uses to process clients' data; and (ii) the confidentiality and privacy of the information processed by these systems. Specific to digital asset custody, SOC 2 reports can provide a DA Custodian's clients with assurance around the security, availability and exclusive control of their digital assets.

SOC 1 and SOC 2 reports can be further categorised into Type I and Type II reports. A Type I report is an attestation of controls at a DA Custodian at a specific point in time, whereas a Type II report is an attestation of controls at a DA Custodian over a specified period of time (typically a minimum period of three to six months). Type I reports contain the independent auditor's opinion on the fairness of the design of internal controls. Type II reports are generally more comprehensive as they incrementally include the auditor's opinion on the operating effectiveness of the controls over the audit period, a detailed description of the tests the auditor performed to evaluate the controls and the results of these tests.

5.2 Questions to ask when evaluating SOC reports

There are certain considerations to be aware of when reviewing SOC reports. It is not enough to know that a DA Custodian has received an attestation report from an audit firm, nor is it enough to take the opinion presented by the service auditor at face value.

- **Is it a SOC 1 or SOC 2 report?** Institutional investors should ensure their DA Custodian produces reports that meet their needs, as the two reports provide different assurances. SOC 1 reports may contain tests of controls related to the security and/or processing integrity criteria covered in SOC 2 reports.[17]

- **Is it a Type I or Type II report?** A Type I report should be considered as a 'light' attestation or a snapshot of controls at a certain point in time. A Type II report is more comprehensive as it covers a defined amount of time and includes the service auditor's opinion on the operating effectiveness of the controls as well as a detailed description of the tests of controls and the results of those tests.

- **Is the auditor's opinion unqualified or qualified?** It is strongly preferable if a DA Custodian obtains a report with an unqualified (or clean) opinion. This means that the auditor believes the system was suitably designed and there was reasonable assurance that the DA Custodian achieved its control objectives and/or service commitments over the time period specified in the report based on the controls tested. If the auditor provides a qualified opinion, the auditor may have identified concerns during the reporting period that prevented the DA Custodian from meeting its objectives.

- **Are there any exceptions related to control activities?** Institutional investors should evaluate the sections that highlight the auditors' tests and results of tests to determine whether they noted any exceptions or qualifications related to individual control activities. Certain control activities may be more critical for one user entity versus another, so institutional investors should evaluate exceptions in light of their own risk appetite thresholds.

17 SOC 2 reports are relevant to a broad variety of third-party service organisations – the underlying thread is that service organisations handle, process and/or maintain sensitive data of their customers. If a SOC 1 report is not available or applicable, DA Custodians that store and process sensitive data of end-users can leverage SOC 2 reporting to offer specific assurances.

- **Does the service auditor have expertise in the industry?** Practitioners should have adequate knowledge of the industry of the DA Custodian they are evaluating.

5.3 Applicability of ISO certifications

ISO/IEC 27001 is globally recognised as the premier international standard, providing the specifications and requirements for implementing an information security management system. Conforming to an internationally recognised standard enables DA Custodians to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties. The standard is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to institutional investors. With the ISO 27001 certification, which involves undertaking regular reviews and internal audits of the information security management system to ensure continual improvement, a DA Custodian would be strengthening the protection of assets under custody.

In the nascent digital asset industry, the role and scope of service providers is quickly expanding (exchanges have become de facto custodians) and the magnitude of what is at stake is unique (digital asset transactions are probabilistically irreversible). Service providers in the space recognise that they can use SOC reports and ISO certifications to (i) differentiate themselves relative to the marketplace, (ii) win the business of institutional investors that expect a certain level of assurance, and (iii) set higher industry standards for the status quo.

Appendix A: AIMA Working Group Members

- Haydn Jones – **PwC**
- Rich Itri – **ECI**
- Asen Kostadinov – **Copper**
- Daniel Andemeskel – **UI Enlyte**
- Divya Dattani – **Barclays Investment Bank**
- Evan Kohn – **Anchorage Digital**
- George Kirchner – **NYDIG**
- Jack Neureuter – **Fidelity Digital Assets**
- John D'Agostino – **Dagger Consulting LLC**
- Jonathan Gilmour – **Travers Smith LLP**
- Lauren Abendschein - **Coinbase**
- Maxime de Guillebon – **Zodia Custody**
- Nitin Khanapurkar – **Apex Group**
- Robert Cooper – **Digivault**
- Simon Zais – **Capco**
- Steven D'Mello – **Albourne Partners**
- Vaïk Müller – **CMS Switzerland**

Appendix B: 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 $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 $600 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 C: About the Sponsors

ECI

ECI is the leading provider of managed services, cyber security and business transformation for mid-market financial services organisations across the globe. From its unmatched range of services, ECI provides stability, security and improved business performance, freeing clients from technology concerns and enabling them to focus on running their businesses.

More than 1,000 customers worldwide with over $3 trillion of assets under management put their trust in ECI.

We are headquartered in Boston and have offices across the United States, Europe and Asia.
For further information, please visit www.eci.com.

PwC

At PwC, our purpose is to build trust in society and solve important problems. Whether you're an innovator, an investor, or a global financial services provider, our teams are here to help. Changing customer expectations and major macroeconomic forces continue to challenge the financial services industry to leverage technology, to stay relevant and get ahead. We firmly believe that collaboration and partnerships are key to the future of the industry, so how can the ecosystem come together to create commercial success and good customer outcomes? We help clients across the financial services industry to navigate the digital ecosystem, deliver on their ambitions and to do so at speed:

- we help incumbent institutions harness the power of technology as they shape their businesses for the future;
- we help digitally native challengers as they seek to disrupt the traditional market;
- we help B2B FinTechs of all shapes and sizes on their journey as they scale and grow; and
- we help investors in FinTech to create and capture value across all stages of the deal lifecycle.

We're a network of firms in 155 countries with over 284,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at https://www.pwc.com/gx/en/about/new-ventures/crypto-center.html.

aima.org