

Hogan
Lovells

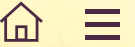
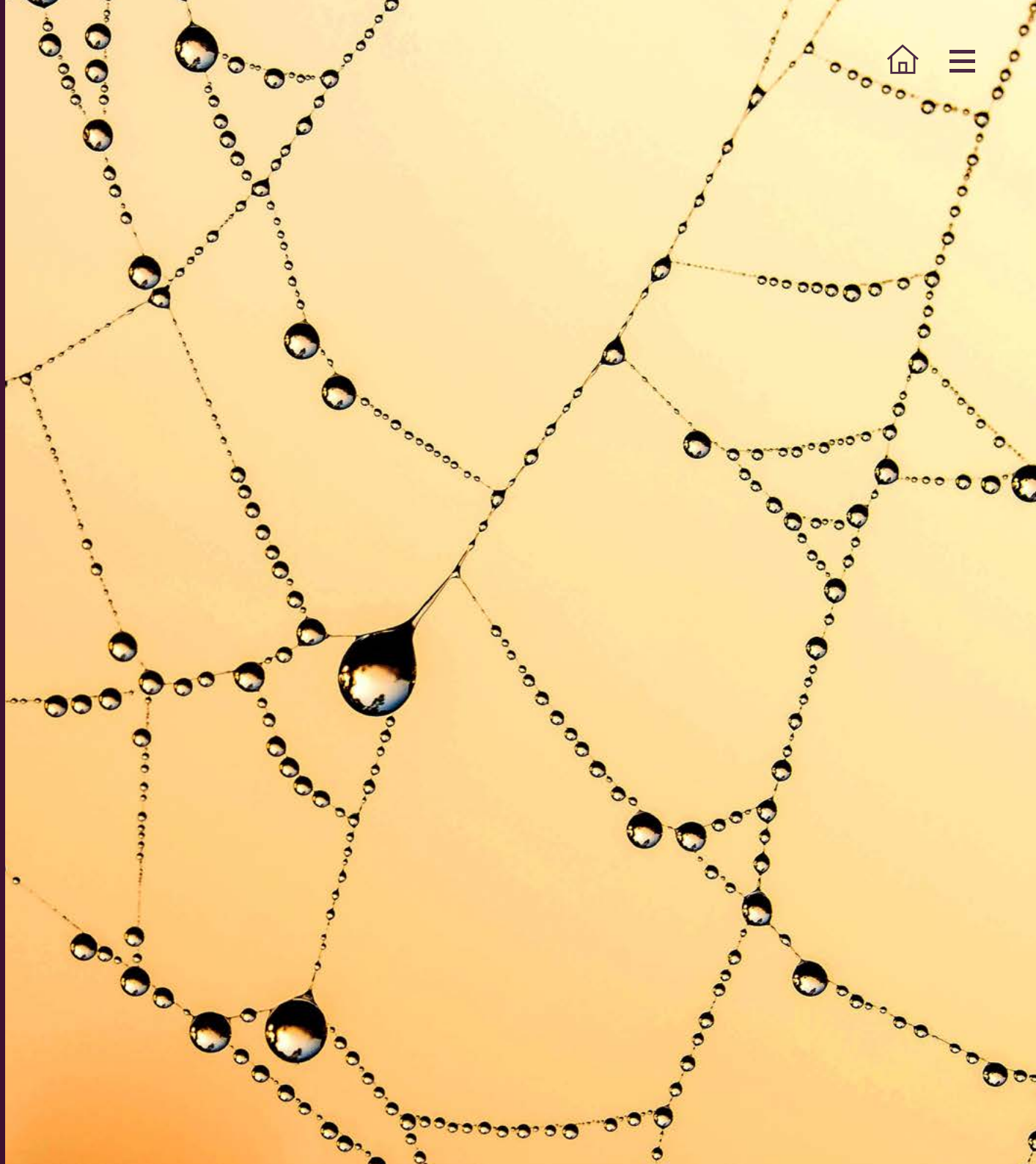


Digital Asset Custody Paper

Open document >

Contents

- ① Background to this paper
- ② An overview of traditional custody
- ③ Differences in digital asset custody
- ④ Current legal approaches to digital asset custody
- ⑤ A proposed way forward
- ⑥ About Hogan Lovells
- ⑦ About Zodia Custody
- ⑧ Contacts



Background to this paper

With increasing levels of capital continuing to flow into digital assets globally, an ever-growing pool of asset holders, and even governments exploring various digital asset projects, the need to examine custody services in the digital assets industry has never been more essential and relevant. Individuals and institutions need to understand how the custody of digital assets works, how custody is achieved, and what risks to be mindful of when navigating the possible opportunities surrounding digital assets.

New exciting projects are being explored and piloted and increasingly, institutions – once reserved and hesitant – are dipping their toes into this exciting world. With new projects, come new challenges, but we often find that it is the fundamentals of storing, safeguarding and administering digital assets that pose the biggest stumbling block for these projects.

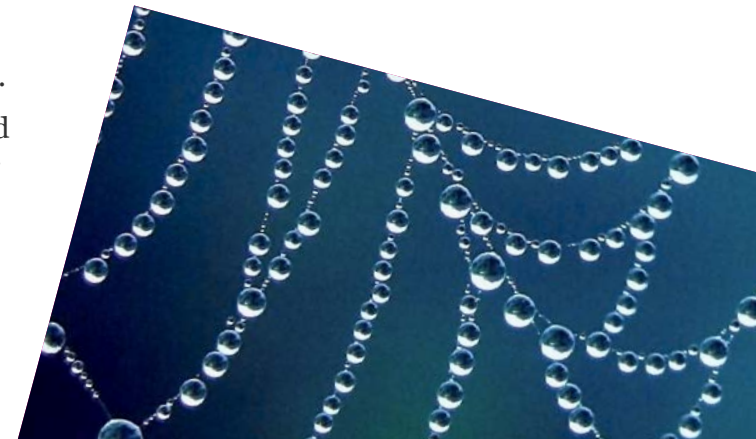
This paper will be of particular interest to corporations and institutions hoping to get to grips with the complexities of digital asset custody, and what this means for them when seeking to appoint a custody provider to facilitate their digital asset projects. We hope, however, that this will also be an interesting study for anyone with a genuine interest in digital assets and the associated opportunities.

Hogan Lovells and Zodia Custody have worked together to produce this paper, combining our collective legal, technical and operational knowledge. For further details on the

organisations and authors please see the “About Hogan Lovells” and “About Zodia Custody” sections of this paper. This paper is not designed to endorse the services or products of either Hogan Lovells or Zodia Custody. Rather, it is intended to act as an informational tool for institutions and companies to make their own assessments of custody arrangements.

We have sought to provide some clarity on the world of digital asset custody, touching upon the origins of custody before the emergence of the digital assets industry, and comparing the custody of more traditional assets with the custody of digital assets. In this exercise, our aim is to demystify digital asset custody and to highlight key questions that should be asked when exploring custody service options.

Events unfolding at the time of writing this paper have alarmed many in the digital assets industry and highlighted the importance of custody services that are reliable and robust. The need for focus on the potential risks involved in certain custody solutions has never been more evident.






An overview of traditional custody

What is traditional custody, and how does it work?

In the context of financial services, the word “custody” refers to the service of safekeeping assets belonging to clients and providing related administration services in relation to those assets. Although custody can be provided in relation to several different asset classes, custody is typically undertaken in relation to financial instruments and often offered by custodian banks. The precise way in which assets are held in custody depends on the nature of the asset in question. In this section, we outline how custody is generally administered for financial instruments (hereafter referred to as “traditional assets”).

Custodians are service providers that offer to clients, which may be institutional or retail clients, services that allow for the safeguarding and administration of certain assets owned by those clients.

The custody market in relation to financial instruments in particular tends to be dominated by commercial and investment banks, though some brokers may also act as custodians of these kinds of asset. The custodian market in relation to traditional assets is well established, and a small number of firms remain the custodians of choice for the many institutions that make use of custody services. Custody arrangements are generally offered as a standardised service, on terms defined by the custodian, which need to be consistent with the various regulatory requirements focused on ensuring there are adequate protections for the client’s assets. There is often very minimal room for negotiation, as a result.



Why are custodians necessary?

The safeguarding and administration of traditional assets carries certain risks and operational burdens, which many asset-owners are not well equipped to manage themselves. An institution may not be familiar with the processes required to undertake transactions (i.e. buy or sell) in assets that it holds and will likely require a third party to manage these processes. Additionally, membership of particular financial market infrastructures (“**FMI**s”) including settlement systems and Central Securities Depositories (as described later in this paper) is often required in order for a person to hold and transfer title to certain assets.

For instance, UK securities that are settled through the CREST system must be held through entities that are members of CREST (which excludes most asset-owners). Custodians also play an important role for investment managers that require custodians to hold assets that are managed on behalf of clients.

A professional custodian will have experience in handling these processes, and should have robust controls, checks and balances in place to ensure appropriate safeguarding and administration of these assets. Custodians are established to manage the ongoing operational and compliance requirements that are necessary in order to safely hold assets, including managing settlements and reconciliations. Administrative tasks, such as exercising rights pertaining to custodied assets (e.g. receiving dividends, or utilising voting rights) can be undertaken by a custodian. A custodian will also generally have the necessary regulatory licences or memberships with FMIs that are required in order for the custodian to hold assets on behalf of its clients (or will have relationships with sub-custodians that have such licences or memberships).

Ultimately, custodians provide a certain peace of mind to clients that assets are held safely and securely, with a third party providing a custody service that is subject to certain regulatory protections (described further later in this paper). This is particularly important in relation to client asset segregation and the maintenance of books and records, which should reduce the risk of theft, loss or mishandling of assets.

What kind of assets may be held by a custodian?

Custodians are responsible for safeguarding and administering both physical and electronically held assets on behalf of their clients. Traditional assets that are held in custody cover a broad range of asset classes, and may include securities certificates (such as share and bond certificates), commodities (e.g. gold) and other records (e.g. real estate documentation).

A brief history of custody and its evolution

Historically, banks were well placed to offer custodial services for client assets as they had ready-made safe spaces (i.e. bank vaults) which could hold client securities certificates in physical form as well as other valuable assets, such as gold.

The rapid growth of computers and the internet and the steady digitalisation of financial systems and processes has resulted in a considerable evolution of the custody industry since this point.

Keeping with the example of shares in publicly listed companies, the inefficiencies of transacting through physical documentation led to the introduction of two mechanisms designed to ease operational difficulties in a digital world:

(a) “dematerialised” (i.e. electronic form) financial instruments, title to which is often recorded in book entry form.

(b) “immobilised” assets, which are physical assets held in a centralised depository on account of the beneficial owner. In order to track changes in ownership, asset transfers are documented through records held by a centralised intermediary.

Central Securities Depositories (“**CSDs**”) are financial market infrastructure providers that play a key role in recording the ownership of certain traditional assets such as shares in a publicly listed company. There are a range of CSDs operating across different jurisdictions. Prominent examples of CSDs include Euroclear (which operates multiple securities settlement systems in Europe, including the UK’s CREST system) and Clearstream. These are mostly private entities which are themselves directly regulated, often by a jurisdiction’s central bank.

Other providers operate in relation to other asset classes. For example, in relation to physical commodities, immobilisation may also be performed by the entities that are involved in the holding or transfer of such assets, such as the operators of warehouses.

The result is a complex web of market participants and intermediaries that play central roles in the smooth operation of traditional asset markets. In today’s traditional financial markets, custodians play a critical role in providing clients with not only safe custody and administration of their assets, but also established connections with market infrastructure providers (including CSDs) which are more difficult for clients to establish themselves.



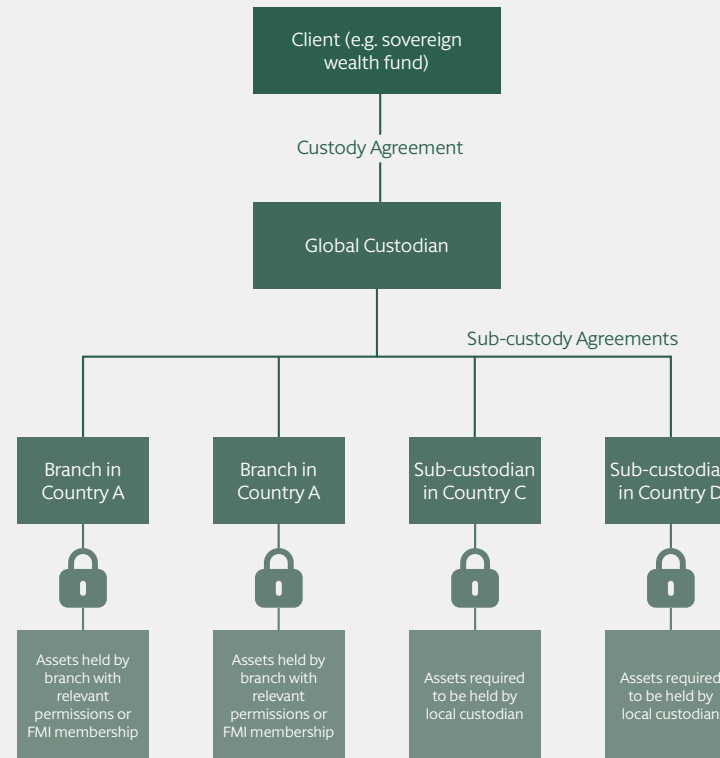
Are there different types of custodian?

A key point to paper is that generally the custody of certain traditional asset types requires a presence in the location in which the relevant asset is held. This is required to ensure that control or safekeeping can be provided to clients in accordance with local law requirements governing that traditional asset.

For physical assets, this may involve a custodian operating a vault in the relevant jurisdiction. For non-physical assets, it may involve working with a local custodian entity that is able to hold title to the traditional asset in accordance with local laws. As such, custodians may be categorised in two ways:

(a) Global Custodians – These are global banks which offer an all-inclusive and cross-border custody service, with significant market coverage around the world. Global custodians may have a physical presence, or be direct members of a CSD, in certain key jurisdictions, but will often rely upon a large network of sub-custodians that are located in jurisdictions where the global custodian does not have a branch. It would represent a significant investment cost and operational burden for global custodians to maintain a presence, and CSD connectivity, in each jurisdiction in which it wishes to operate – hence the need for sub-custodians.

An illustrative example of a traditional custody model



(b) Sub-Custodians – These are custodians which may have a legal entity and expertise in a specific home market (single-market custodians), or may provide additional cross-border services to multiple markets (multi-direct custodians). Typically, sub-custodians provide local market expertise, proximity and connectivity to local institutions, including CSDs, which global custodians may not have in a specific jurisdiction. Sub-custodians also offer regulatory expertise which would be difficult for global custodians to maintain across all jurisdictions in which they operate.

The manner in which traditional assets are held is often heavily intermediated: an individual client may hold their entire securities portfolio with a bank, which may then procure custody services from its affiliate custodian. Its affiliate custodian may effect registration of title with a “home” CSD, and procure services of a global custody provider for securities issued by issuers located in other jurisdictions. The global custodian may employ a network of sub-custodians that have the requisite memberships of their national CSD to enable the recording of title, and transfers of title, to the asset in that jurisdiction.

What do custodians do?

Custodians provide the following services:¹

(a) Safeguarding – Custodians safeguard legal title to their clients’ assets, for example by registering them in the name of a nominee company and undertaking reconciliation processes to ensure that the amount of assets that the custodian ought to be holding for its clients (as indicated in their books and records) is at all times reflected by its actual holdings (including, where applicable, in line with the holdings reflected in the records of a central intermediary such as a CSD).

(b) Settlement – Custodians are responsible for settling transactions into which their clients enter. In some instances, this may involve effecting settlement through the books of a CSD’s central register, where dematerialised traditional assets (such as shares in a publicly listed company) are involved. In other instances, Custodians will be responsible for any other formalities applicable to other categories of regulated traditional asset.

(c) Asset Services – Custodians may provide a range of services enabling clients to exercise their rights and obligations arising under the traditional assets that the client owns. This may not be relevant to all asset types, but some examples include:

- (i) the collection of dividends (for shares) or interest (for bonds);
- (ii) payment and reclaim of tax; and
- (iii) exercising voting rights at shareholder or bondholder meetings by proxy.

How do custodians hold traditional assets?

Depending on the market in question or the preference of the client, there are broadly two models of custody that we will explore in this paragraph: “omnibus” and “segregated”.

The description below is necessarily high level and general and is intended to introduce the concepts of asset segregation and commingling which are important considerations in the world of digital assets.

Segregated models – Under segregated models, a custodian separates clients’ assets, so that client assets are not commingled with the assets of another client or of the custody provider. This segregation will be reflected in the custodian’s own records, and this approach will also need to be flowed down to the records of any central intermediary (e.g. a CSD in the case of shares in publicly listed companies).

Omnibus models – In contrast, the omnibus model allows the custodian to commingle all of its clients’ assets in a single account (including in the records that any applicable central intermediary, such as a CSD, may maintain). The custodian that holds the omnibus account which contains the clients’ assets will be the only entity to appear in the register as holder of legal title. The omnibus model is considered to be more operationally efficient as only one account is required, though client consent is usually required if a custodian is to hold a client’s securities in an omnibus account as the commingling approach may increase the client’s risk (e.g. in an insolvency scenario affecting the custodian).

1. Further details in the European Central Bank Occasional Paper Series 2007 - <https://www.ecb.europa.eu/pub/pdf/scpops/ecbocp68.pdf>.

The proper administration of custody services is paramount to client confidence. As such, custodians must implement policies, controls and procedures to ensure that any orders that are settled on behalf of their clients are processed in accordance with the instructions of the client. These include, for example, the requirement to maintain internal books and records, and segregation of assets, to ensure that a client's assets are safeguarded. Having secure processes to identify authorised individuals that can issue instructions in relation to a client's assets is also crucial. A custodian often seeks to mitigate risks by:

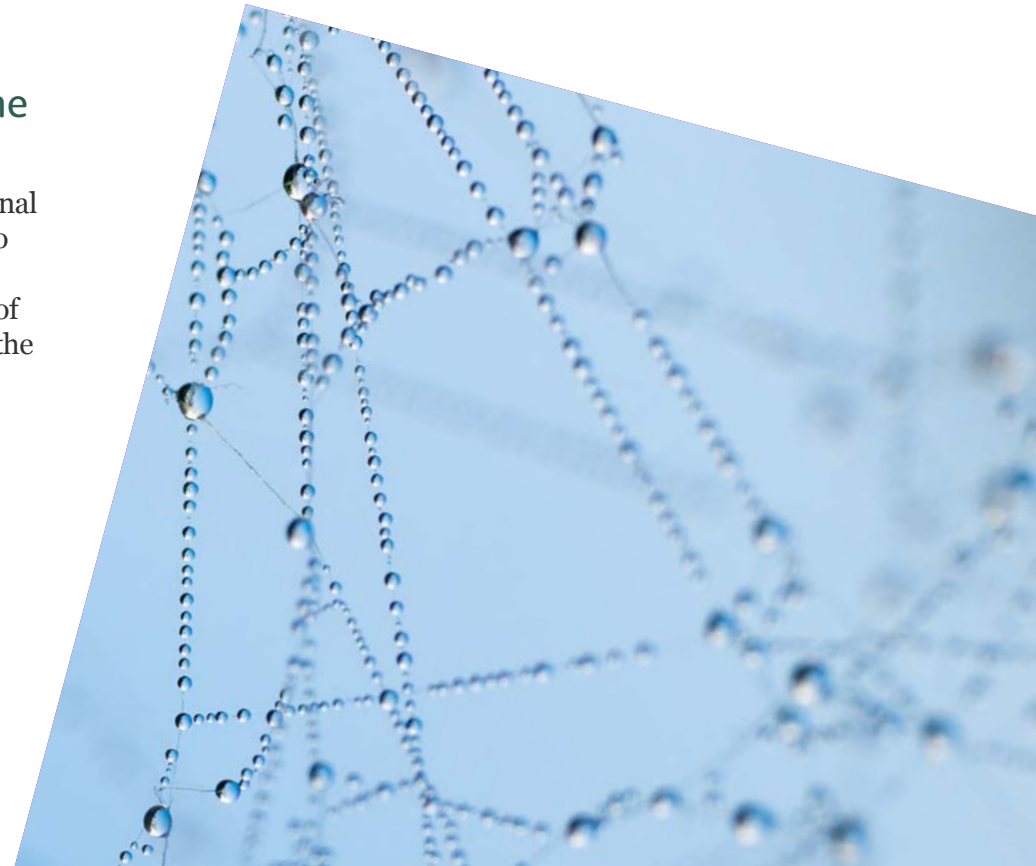
(a) ensuring that it has clear policies and procedures - and, often, specific platforms or portals to act as an operational safeguard - regarding who can (and cannot) issue instructions in relation to custodied assets. If instructions are issued by a non-authorised person, a custodian that acts on those instructions may be liable for acting without the client's authority. Similarly, if the custodian does not act on instructions that are authorised by a client, this may result in a loss to the client and liability on the part of the custodian; and

(b) seeking security interests over custodied assets (for example, pledges or liens over assets that the custodian holds for the client). As a result of the services that a custodian provides, custodians are themselves exposed to a certain level of credit risk. For example, custodians may incur fees from third parties, such as settlement systems, when facilitating the settlement of transactions on the client's behalf. Custodians would typically pass such costs through to their clients, but they are primarily liable to the third party for the payment of the relevant fees and security interests are sought to address this risk.

How is custody regulated in the UK and EU?

As described above, the custody of traditional assets presents certain levels of risk both to custodians themselves, but also to clients. As such, custodians are subject to a range of regulatory requirements depending upon the nature of assets that a custodian holds in custody, and the jurisdictions in which the custodian operates.

The scope of this paper is intended to be global, but for the purposes of this subsection we will briefly focus on the position close to home – both under applicable EU legislation and in relation to the UK regime. We aim to provide a very high level summary of the key regulatory principles underpinning the custody of traditional assets, which provide an interesting point of comparison in later sections of this paper.



Key principles under the EU Framework

At an EU level, Directive 2014/65/EU (also known as the second Markets in Financial Instruments Directive or “**MiFID II**”) characterises the safekeeping and administration of financial instruments, including custodianship and related services (e.g. cash and collateral management), as an “ancillary service”.² The custody service does not itself trigger a requirement for regulatory authorisation as an “investment firm” if it is the sole activity that an entity undertakes. Such requirement, however, is typically present in local implementations.

Without delving too deeply into MiFID II,³ the key principles that can be drawn from MiFID II and the Delegated Regulation supplementing MiFID II,⁴ include:

- (a) that custodians make adequate arrangements:
 - (i) to safekeep a client’s ownership rights in financial instruments, particularly in the event of the firm’s insolvency;
 - (ii) to safekeep client funds; and
 - (iii) to prevent use of the client’s funds or instruments on the custodian’s own account; and
- (b) the provision of information to clients to ensure that they are clear on the nature of the custody service offered by the custodian. This includes informing clients where instruments or funds may be held by a third party, or in an omnibus account, and informing clients of the resulting risks.

Key principles under the UK Framework

In the UK, the safeguarding and administration of certain specified investments is a regulated activity under the Financial Services and Markets Act 2000. A custodian will require authorisation in the UK where it provides custody services, even if that custodian does not perform any services that would require it to be authorised as an investment firm under MiFID II. There are a wide range of custody rules applicable to firms that safeguard and administer specified investments, and in this paper we have sought to summarise the key themes which are most pertinent to our later analysis of custodianship in the digital asset industry.

Entities that are authorised to perform the regulated activity of safeguarding and administration of investments in the UK are subject to specific regulatory requirements under the FCA’s client assets (“**CASS**”) rules relating to custody. Overall, the CASS rules are designed to ensure that client assets are safeguarded appropriately, such that those clients will not find that custodied assets are not available to them in the event of a custodian’s insolvency. Having appropriate records, and clear distinct legal structures without any commingling of assets, is a means of mitigating such risk.

CASS sets out detailed rules and requirements, which can broadly be summarised as requiring a custodian to do the following:

- (a) protect client assets;
- (b) put in place adequate organisational measures to minimise the risk of loss or diminution in value of custodied assets;
- (c) comply with specific rules in relation to the proper registration of legal title;
- (d) exercise due skill and care before depositing any client assets with any third parties;
- (e) enter into a written agreement with any third parties that act as sub-custodians; and
- (f) maintain appropriate records to enable it to distinguish between the assets belonging to different clients.

CASS includes specific requirements as to the registration or recording of legal title to a client’s safe custody asset. Such registration must be in the name of: (i) the client, or (ii) a nominee company controlled by the custodian, or its affiliates, a recognised exchange or a sub-custodian (unless local traditions or laws require a different approach).

2. MiFID II, Section B of Annex I.

3. MiFID II, Article 16.

4. Commission Delegated Regulation (EU) 2017/565.

Custodians subject to CASS must also ensure that their own assets are not comingled with the assets of their clients (with some limited exceptions, such as where this occurs incidentally), and are not used for other purposes (such as, for example, proprietary trading by the custodian) except where expressly authorised by the client. Clear records and audit trails are necessary to keep track of client assets, including internal records for each client's assets and reconciliation processes to ensure that actual assets held match the levels required under those records. Any shortfall should be covered by the custodian using its own assets as a temporary measure.

These rules are designed to ensure that there is clear separation between the assets of a custody client, and the assets of the custodian. There are also detailed rules in CASS that apply to firms that hold money on behalf of their clients. These rules establish a statutory trust under which the firm holds money as trustee for their clients (with an exclusion for banks holding funds as part of their banking service, where such funds are treated as a debt owed to the client). The FCA expects custodians to provide a notification in the event of material failures or breaches in complying with CASS rules.

Key takeaways

The provision of custody services, whilst necessary and beneficial to clients, raises a number of risks for custodians and clients alike. Any third party taking custody of the assets of another party holds a significant amount of control in relation to those assets. As such, regulatory regimes covering the custody of traditional assets are largely focused on ensuring that, as a base level, client assets are safe, separated and are not used for a custodian's own purposes.

This section of the paper has been intended to set the scene in relation to traditional custody and the industry that many are aware of, and even involved with, but perhaps have not reflected on in detail for some time. After all, the custody of traditional assets is a well-established industry. With this background in mind, we turn now to the evolution of the digital assets industry and what custody of digital assets means, both technically as well as legally, with a view to outlining the key questions that clients or potential clients should be asking when exploring digital assets.



Differences in digital asset custody

Before discussing the particular features of digital asset custody, we have included below some explanations of the key concepts related to digital assets that run through the remainder of this paper. An understanding of the vocabulary used to describe digital asset custody services is an important first step to understanding the nature of digital asset custody.

The classification of digital assets continues to evolve with the introduction of new regulatory regimes around the world and, challengingly, it is not consistent across different jurisdictions. International harmonisation appears to be some way off, but the need for consistency continues to gain recognition among global regulators.⁵ Despite this lack of harmonisation, it is possible to identify how certain terms are generally understood. In this paragraph we highlight several of such terms and the meaning that we give them in this paper.⁶

Distributed Ledger Technology (“DLT”) –

A technology which enables the operation and use of a digital store of information or data that is shared (i.e. distributed) among a network of computers (known as nodes) and may be available to other participants. Participants approve and eventually synchronise additions to the ledger through an agreed consensus mechanism.

Digital assets – Also commonly referred to as “cryptoassets” or “virtual assets”. Most definitions of “digital asset” cover digital representations of value or rights recorded to a public address on a distributed ledger as part of a DLT System (or similar technology). This is intended to be a broad term, and for the purposes of this paper we use “digital assets” as an umbrella term to encompass all digital assets, including stablecoins, security tokens, utility tokens and even to some extent non-fungible tokens.

5. Financial Stability Board (2022), *International Regulation of Crypto-asset Activities*, 11 October, p. 4.

6. These terms, and the precise details contained in these definitions, may vary depending upon the manner in which a specific digital asset or DLT system works (meaning that some generalisation is necessary for the purposes of this paper).

Within the broad category of “digital assets”, there are a number of sub-categories which include:

(i) Cryptocurrency: a type of digital asset that can be digitally traded and functions as a medium of exchange; and/or a unit of account; and/or a store of value. It is not issued nor guaranteed by any central bank or public authority, is not backed by another asset, and fulfils the above functions only by agreement within the community of its users.⁷

Notable examples include bitcoin and ether.

(ii) Stablecoins: a type of digital asset which purports to maintain a stable value relative to a specified asset (which includes fiat currencies), or a pool or basket of assets.

(iii) Utility token: a type of digital asset which is exclusively intended to provide access to a good or a service supplied by the issuer of that token.

(iv) Security token: a type of digital asset which represents traditional financial instruments (e.g. share certificates, units in a bond) in tokenised form. In this paper, we have focused on the characteristics of digital asset custody generally, and the challenges that exist across all sub-categories of digital assets. In relation to security tokens, there is an additional

layer of challenge as, in many cases, regulatory requirements applicable to traditional assets will apply in the case of their security token equivalent. This should be kept in mind when exploring projects which involve the custody of security tokens – and while these additional challenges are not explored in detail in this paper, we hope to explore this topic further in future publications, particularly in the context of tokenisation and the custody of tokenised assets.

(v) Non-fungible tokens (“NFTs”): a type of digital asset which is unique and created for use in specific applications which cannot be divided and is not fungible (i.e. interchangeable) with other tokens.

Public key and public address – Public keys are strings of data that are often stated to be comparable to a bank account number in certain respects. It is a string of data that can be shared with anyone publicly, and which will be used by third parties to send transactions to you. In short, if one person is sending digital assets to another person, the person sending digital assets will send those assets to the recipient’s public key. A public address is a version of the public key that has been hashed. Public addresses can be created very quickly and others can share to that public address rather than the public key. This is similar, for example, to certain technology offerings in the market today which allow for disposable virtual debit cards to be created and deleted after a small number of transactions.

7. This should not be confused with the characteristics of conventional or “fiat” currencies.





Private keys – Private keys are strings of data bearing a unique mathematical relationship to the public key where ownership of digital assets is recorded on a distributed ledger. It is in many cases mathematically impossible for the private key to be reverse-engineered from the public address. Private keys are used by owners of digital assets to “sign” or authenticate outbound transactions in digital assets from the public address of the private key holder to another person with a public key. Private keys are, therefore, the key component enabling a person to establish and exercise ownership rights in relation to their digital assets.⁸

Wallet – Wallets are the bundle of systems and processes that store and control deployment of the suite of private keys used to operate a person’s public address. In essence, the wallet is the technology through which keys are managed, thereby forming a key aspect of any digital asset custody offering.

Why is digital asset custody different to custody of traditional assets?

Digital assets have emerged as a widely-discussed asset class, particularly during the 2010s and onwards. Indeed, many digital assets are no longer mere speculative investments, but rather form part of a tokenised economy that has recently, albeit briefly, surpassed US \$3 trillion in market value.⁹

This asset class differs from traditional assets in that the ownership of a digital asset relies upon cryptographic techniques, and is typically (though not always) reliant upon an underlying infrastructure known as DLT. This can be distinguished from traditional financial instruments, whose existence has some tangible form (for example, a share certificate), albeit immobilised and dematerialised. When we refer to digital assets, we are essentially referring to intangible data that are reflected on a DLT system, in an encrypted form, the ownership of which is demonstrated by, and transferred through, the deployment of the private keys in relation to the DLT system.

The widespread adoption of digital assets has resulted in an equally prevalent demand for effective digital asset custody solutions. Digital asset custody is a fundamental necessity; every user, whether existing, new, institutional or retail, needs a safe way to store and manage their digital assets.

8. The processes governing the deployment of private keys associated with public addresses, which are used when posting transactions to the distributed ledger (the “original private key”), can themselves incorporate additional protective layers of private keys which govern the deployment of the original private key. In this paper, references to “private keys” means those *private keys* associated with public addresses (i.e. the *original private key* referred to in this paragraph).

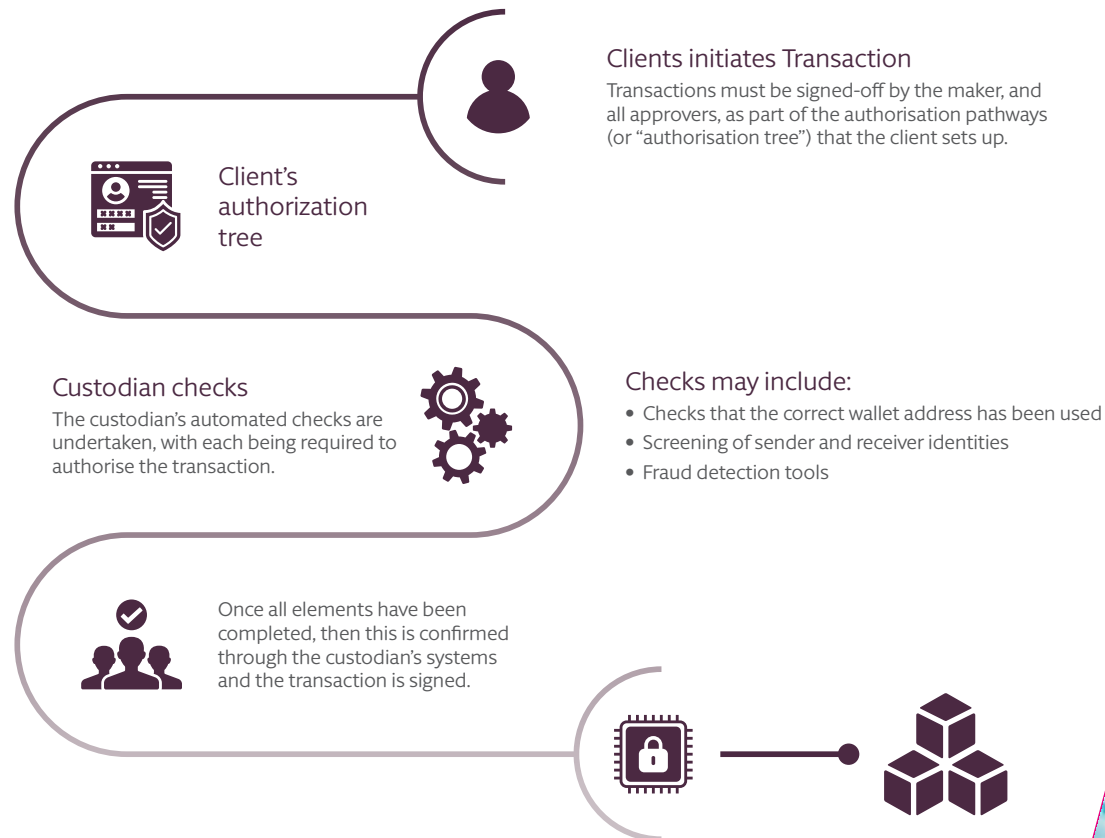
9. [Bitcoin.com](https://www.bitcoin.com), November 8 2021

This is not an asset class, however, that traditional custodians are used to safeguarding or administering for clients. Where traditional custodians offered connections to various stakeholders within the traditional financial markets, digital asset markets involve a range of different stakeholders and institutions which are connected in a different way. Traditional custodians have started to advance on the technology-side but deploy risk management frameworks based on traditional regulated standards of custody in order to operate in the same market. Some, notably Standard Chartered Bank and Bank of New York Mellon, have established operating subsidiaries that provide custody services for digital assets. This is a key challenge for institutions that are seeking to launch digital asset projects – often, the first hurdle is finding a suitable custodian that operates in line with institutional expectations associated with traditional asset custody.

What do we mean by custody of digital assets?

When we refer to digital asset custody in this paper, from a technical perspective we are referring to the custody or storage of the private key or keys associated with the public addresses where the clients digital assets are recorded and the ability to control the operation of the client's wallet by posting transactions to the distributed ledger, all in accordance with instructions provided by the client. In general, we are therefore referring to custody and controlled deployment of private keys when we refer to digital asset custody.

An illustrative example of a digital asset transaction involving a custodian



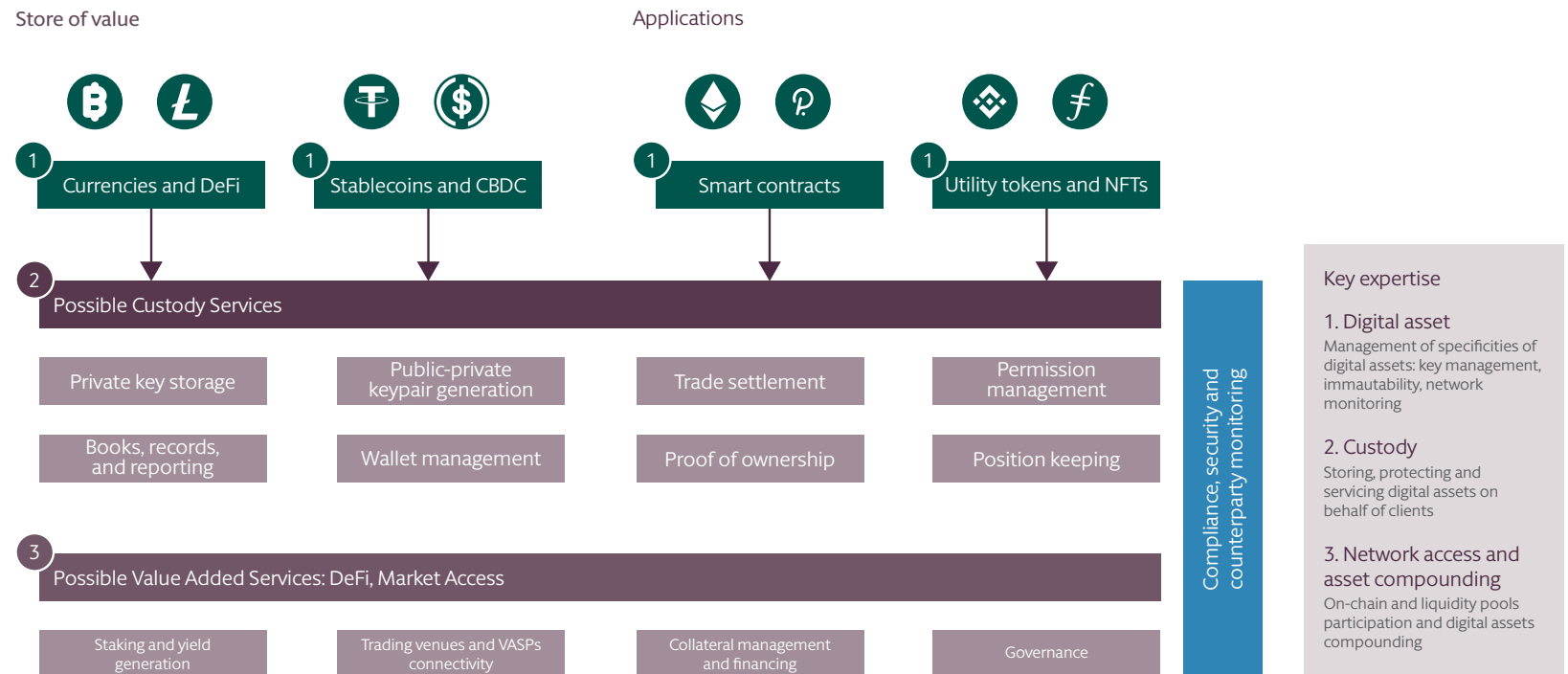
The above diagram represents only one possible custody model

A distinction can be drawn between a third party that stores and deploys the private key (true, or direct, custodians for the purposes of this paper) and what may better be described as technology services where the client is provided with the private key to authenticate transactions.

It should be noted that there is also a distinction to make between what may be termed a custodial wallet service, and a full digital custody service. The key differences are that custodial wallet services are often more simplistic and focused around ease of access for users, while a digital custody service will be more institutionally focused – allowing for multiple users to access private keys (i.e. where a corporate or institution requires multiple personnel to have access), and often focusing on institutional-grade security.

An example of current/future custody services offered to institutional investors (subject to applicable regulation)

With a wide range of possible services and solutions available, the type of service being provided will impact the nature of legal title and risk analyses that clients should undertake and these will be distinctive in each case – there is no “one size fits all” approach. Solutions that deliver the private key to clients are self-custody or non-custodial wallet solutions and may not meet the financial crime protection, security and/or deployment needs of today’s sophisticated institutional clients. Similarly, there is a broad spectrum of services that would consider themselves to be “custody services” but it is important to assess whether these solutions are closer to a custodial wallet service or an institutional-grade custody service.



The above diagram represents only one possible custody model

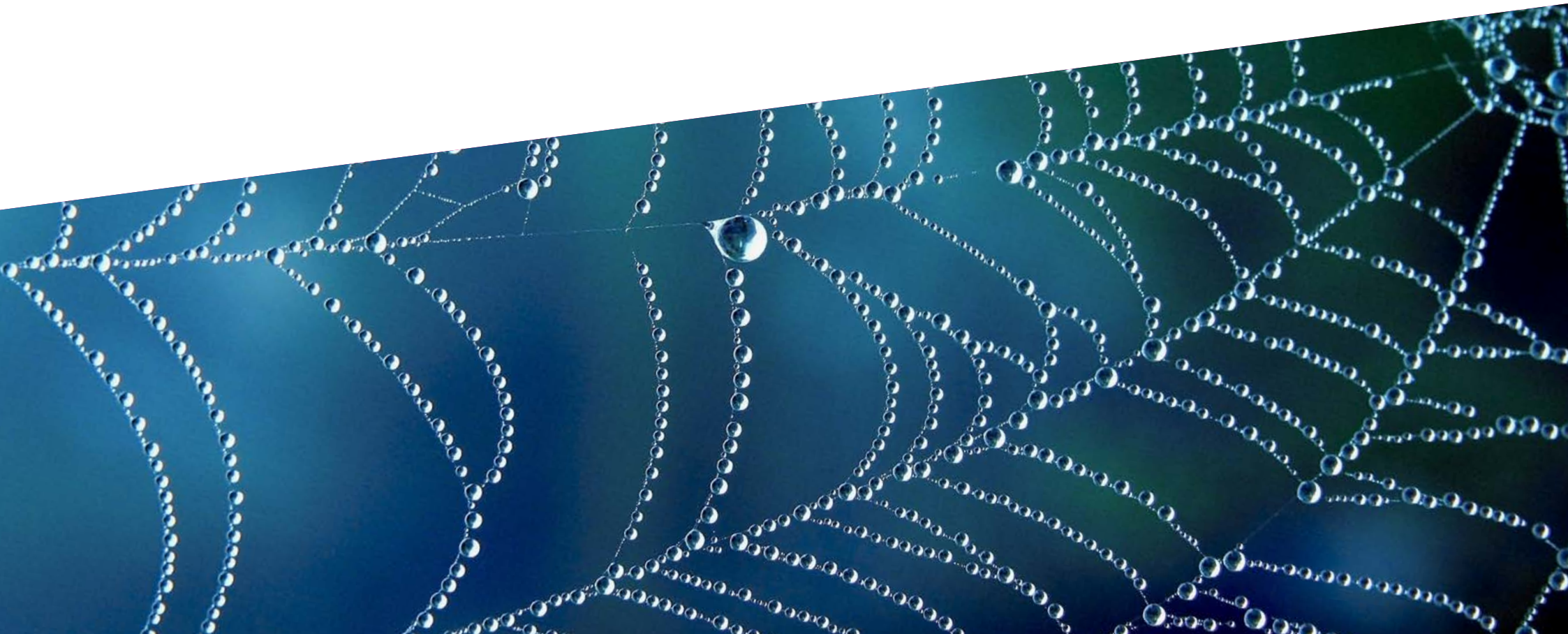
Technical and operational differences between digital asset custody and traditional custody

As described above, there are a number of differences between traditional asset custody and digital asset custody, not least due to the nature of digital assets themselves as a form of data which is stored on a decentralised system. While the overall role of the custodian remains the same in general terms, and the intended outcome of custody is also the same, the means of safeguarding and administering digital assets is inherently different in many ways.

A key difference is that the decentralised nature of most DLT systems means that a central ledger is maintained on a distributed basis amongst all participants in the DLT network. As such, there is no strict operational requirement for a central intermediary, such as a CSD, to keep this central trusted record.

Another distinction is in the requirement for local sub-custodians. In general, digital assets are not currently subject to specific custody-related regulatory requirements which require a custodian to have a legal presence in the jurisdiction in which the digital assets were issued. In fact, the nature of DLT and

digital assets mean that many digital asset ecosystems are decentralised and global in nature. The position in relation to security tokens, however, is likely to be different and may require the more traditional sub-custodian approach.



Approaches to digital asset custody

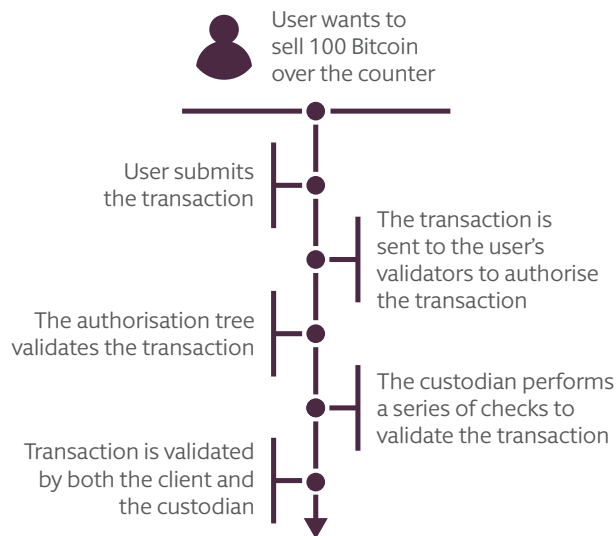
In any digital asset custody arrangement, the security of the private key is paramount and important decisions need to be taken about the form and environment in which the private key is stored and the processes and timelines associated with its deployment in support of authenticating transactions.

Broadly speaking, the choices are for the key to be stored:

- (a) by the client, in what can be termed “self-custody” or a “non-custodial” arrangement; or
- (b) by a custodian, in a “custodial” arrangement.

In this paper, we are focusing upon custodial arrangements offered by third-party custodians to clients.

An illustrative example of the custodian’s role in digital asset transaction settlement



The above diagram represents only one possible custody model

Two common types of institutional custody offering are Multi-Party Computing or “MPC” solutions and Hardware Security Module or “HSM” solutions. The distinction between the two offerings will often lie in the cryptographic standards applied to the private key and the storage solution for the private key or sharded private key. In either case institutional clients should satisfy themselves as to:


- (a) the source of the cryptographic algorithm used in the solution and whether it is bespoke or supported by recognised international certifications or validation; and
- (b) whether or not the storage solution for the private key or private key shards is secure and independently certified against key extraction techniques.

Different types of wallet

Regardless of the choice of custody model, there are different methods of private key storage employed in both non-custodial and custodial wallet arrangements. Private keys may be stored in a physical or digital environment. If the private keys are held in physical form, for example purpose-built hardware wallets, then the private keys will be stored in an environment disconnected from the internet – this is termed a “cold” wallet, as the wallet is offline. This approach is often seen as a more “long-term” wallet storage solution but there are hardware solutions that permit disconnected storage with very low latency. These “warm wallet” solutions are referred to below.

If the private keys are held in a digital environment, then the key may be held in a connected environment – this is termed a “hot” wallet, as the wallet is connected to the internet.

One other type of wallet to highlight is the so-called “warm” wallet, whereby the private keys are stored in a secure enclave that is disconnected from the online environment. Users are able to access the private keys through hardware intermediary devices that extract data packets received from one environment and reconstruct them in the other environment (to avoid an online connection to the storage environment).



The level of risk associated with the environment in which private keys are held (i.e. the safeguarding element), together with the processes associated with deployment of the private key (i.e. the administration element), should be assessed by users prior to selecting a preferred custodian. Put simply, the system design must eliminate single points of failure (whether due to people, processes or location) and encryption of the private keys is essential.

For example, if the private key is held in physical form in a cold or warm wallet, it is important to ensure that a single loss or fraud event cannot compromise the security of the private key. The same applies to private keys held in digital form in a hot wallet – it will not be satisfactory if private keys can be deployed due to the compromise of a single system password, or can be lost due to the loss of functionality of a single unit of hardware or software.

Key sharding and multi-signature wallets

In order to reduce operational and cybersecurity risks and challenges that exist in relation to digital assets, certain technical mechanisms have been developed. A sharded environment or multi-signature user policy are two examples of mechanisms that are often deployed as a means of mitigating the risk of a single point of failure. It should be borne in mind that sharding alone is not a

complete security solution. Private key shards are sensitive and equal rigour should be applied to storage of private key shards as to whole private keys.

Sharding is a concept that is often referred to in relation to private keys, and is seen as a way of mitigating the risks of a single point of failure. Quite literally, sharding means the splitting and distribution of a data set into multiple pieces. In the context of private key storage, sharding can be applied to the customer's encrypted private key itself (in either physical or digital form). Sharding can also be applied to the encrypted master seed, which is a data string from which a client's public keys and private keys are derived. Encryption standards, security of physical shard artefacts, geographic distribution, redundancy and secure access/deployment protocols are core features of any sharding plan.

In practical terms, sharding may be used as a means of avoiding a single point of failure – a private key can be sharded into multiple pieces, with a combination of those pieces (or of some of those pieces) being sufficient to constitute a single private key capable of facilitating transactions in a client's digital assets.

Multi-signature wallets are similar in that multiple signatures are required prior to a transaction being approved, and prior to a client's digital assets being transferred.

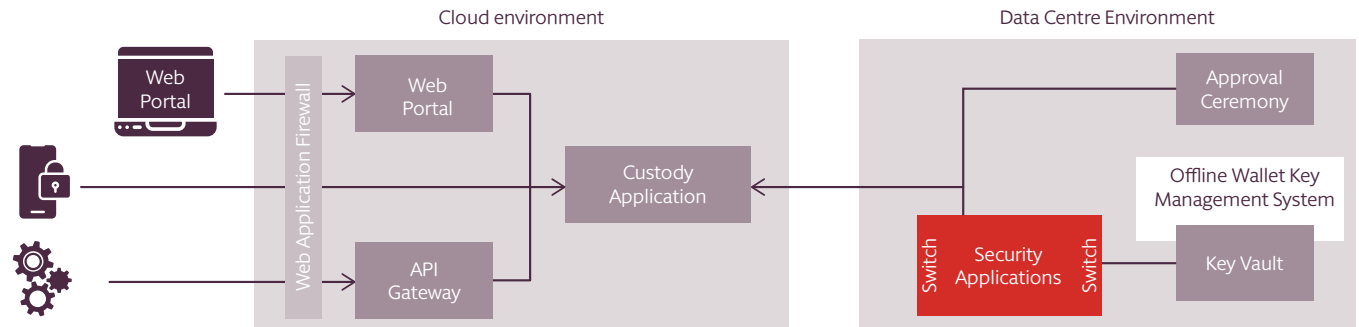
Risks and challenges in digital asset custody

Fundamentally, and as many market participants have recognised over the last several weeks, the segregation of duties between the custodian and the market infrastructure with which they interact is an important risk mitigant. If assets are custodied by the same entity that also provides pricing and execution services, and that entity assumes market risk itself, then a failure in its liquidity or risk management can have catastrophic consequences for the holders of assets custodied with that provider. A dedicated, third-party custodian that takes no liquidity or market risk is a substantial client protection.

There is no substitute for good old-fashioned due diligence by clients on providers of custody services, their management team and risk management frameworks. Is the custodian licensed or registered in a preferred jurisdiction? What custody model does it utilise? Recent events may indicate that these matters have not been probed to the extent required.

Where a third party provides custody services to clients, it is crucial for clients to understand not only the technology solution used by the provider, but also the legal overlay or characterisation that applies to the storage of the key, its deployment and the digital assets that are controlled by deployment of the private key. If the wrong characterisation is applied by the digital

An illustrative example of how an institutional-grade custody wallet may work



The above diagram represents only one possible custody model

asset custodian, then clients are at risk of losing control of their private keys and, potentially, the digital assets that are controlled by those private keys.

In addition to safeguarding digital assets, digital asset custodians are also responsible for security maintenance, which is complex and burdensome. Digital asset custodians have been subject to a spate of recent hacks, which in many cases have resulted in the looting of customers' digital asset wallets. Cybersecurity risk is not a new concept, but the manner in which hackers are able to access and misappropriate assets and funds has evolved alongside the technology itself.

In these cases, customers are reliant on the terms presented by the digital asset custodian, and to some extent the custodian's goodwill to make whole the stolen assets. Importantly (and in general terms), there is no regulatory obligation upon the custodian to make whole the customer in this scenario. While there may be some legal principles that apply in certain jurisdictions in such scenario, those principles may not neatly apply in the digital asset context. Over US \$6.2 billion worth of digital assets were lost to hackers and scammers¹⁰ in digital asset-related scams in 2021, demonstrating the extent of this issue, and therefore the market opportunity for digital asset custodians with best-in-class security measures.

10. *Financial Times*, 19 September 2022

The differences between the traditional model of custody and digital asset custody have become clearer in recent times. The importance of the role of custody has never been greater for clients that own digital assets, whether they be retail or institutional. The harsh fallout of the “crypto winter” – a reduction of the price of numerous digital assets, which triggered financial instability for a number of digital asset companies – has shone a light on the poor outcomes of asymmetric risk management practices and wallet structures that were not designed or optimised for client asset protection. Entities providing custody to clients have gone into insolvency in a number of high profile cases, and in some such cases clients have reportedly ranked as unsecured creditors of the provider alongside the provider’s other general creditors.

The wake of the crypto winter serves to highlight both: the various risks associated with the holding of digital assets; and the need to better distinguish industry offerings that take client protection seriously. The continued move towards the use of regulated digital asset custodians will need to take into account and address the specific features and risks associated with digital assets.



There are a number of challenges that exist today from a client's perspective which it is important to examine prior to establishing an appropriate way forward. Below we have drawn together our suggestion for the key areas that client and potential clients should evaluate prior to appointing a digital asset custodian. This is a non-exhaustive list, but it is hoped that these points will enable a more streamlined due diligence process and avoid unexpected challenges in relation to digital asset projects.

Lack of client protections (e.g. against insolvency of custodian)

Client protections in relation to private key storage are not currently commonplace. Nor are digital assets or private keys recognised for special treatment in custodian insolvency.¹¹

This contrasts with other forms of asset that clients may be used to dealing with. One example would be “e-money” in the EU and UK, which benefits from a Special Administration regime for payments and e-money firms, designed to facilitate the return of customer funds as soon as reasonably practicable. Broadly, such protections are not available in relation to digital assets that are not regulated as regulated instruments (for example, as e-money is regulated in the EU and UK).

It is not an absolute truth to say that private key storage is always unregulated. In Japan, for example, the Japan Financial Services Agency mandates the offline storage of private keys corresponding to the majority of a client's digital assets due to security concerns resulting from notable exchange collapses (see further details in our later section of this paper regarding regulation in Japan). There are certain examples of direct and specific operational requirements being specified by regulators in this way. Such examples, however, are reasonably limited. As a result, in most cases it will be important to derive assurance that conventional legal or contractual (as distinct from regulatory) mechanisms can be relied upon to protect client assets.

If assets have been transferred to a third party custodian's wallet on the basis of outright title transfer to that custodian, but the client has not agreed appropriate contractual terms to govern that relationship and to ensure that the client's interests are protected and that the assets are properly segregated from the custodian's own assets (e.g. via a trust arrangement), then there is a risk of the relevant client ranking with unsecured general creditors in the event of insolvency of the third party custodian – meaning that the client sits much lower in the pecking order when the insolvent party's assets are distributed to its creditors. As a result, the client is less likely to receive the full amount of its digital assets upon the insolvency of the digital asset custodian.

11. Compare the UK Special Administrative regime for e-money providers, which prioritises the expedited return of investor assets relative to rescuing the business of the entity as a going concern.

Furthermore, if a third party custodian were to become insolvent, practical issues associated with identification of the private key as belonging to a given client, and the ease with which those keys could be deployed by an administrator to effect a transfer of the client's assets, are an important consideration. In speaking to one leading administrator about how an insolvency of a party holding digital assets might contrast in practical terms from an insolvency of a party holding traditional assets, the most important factor cited was people. This means that an early and primary objective of the administrator would be to secure people with sufficient technical expertise able to assist with retrieval and deployment of the private keys. When conducting due diligence on any proposed third party custody provider, clients should satisfy themselves that business contingency planning would equip an administrator with a methodology for the recovery of private keys without compromising their security and that these could be understood by people within the business or externally, brought in by an administrator in such a situation.

A key question arising here – what mechanisms can be put in place to address these risks from a client's perspective?

From an English law standpoint, in relation to traditional assets a relationship of debtor/creditor can be avoided if the assets are controlled by the transferee on the terms of a trust. Trust law principles differ worldwide, but this view may be applicable globally to other jurisdictions that have a trust concept. Remaining with the English law example, common law has established¹² that digital assets meeting well-established tests of:

- (a) what may constitute property; and
- (b) what is required to establish a trust, are capable of constituting trust property.

In the case referred to in footnote 12, the English court established that trusts in relation to digital assets which meet the tests for trust formation will not form part of the insolvent estate available to general unsecured creditors.

Additionally, if the private keys are held by the custodian on a fiduciary basis, then prior to their deployment by an administrator in an insolvency situation, clients can benefit from an additional layer of protection in that they are entitled to demand specific performance or at least to ensure that their interests are taken into account by the company administrator as part of the insolvency proceedings.

Key takeaways

While there are similarities between traditional asset custody and digital asset custody, there are material differences which necessitate a different perspective and different approach to risk assessment. In the next section of this paper, we explore the ways in which regulators are seeking to address the similar and different risks that digital asset custody can present to clients.

¹². *Ruscoe v Cryptopia Ltd (in Liquidation)* [2020] NZHC 728.



Current legal approaches to digital asset custody

Before considering a proposed way forward for investors, it is helpful to touch upon certain examples of the approach to the regulation of digital asset custody currently seen in the market. In general, we can see a trend towards regulating digital asset custody but this is very much at different stages in different jurisdictions.

In this section, we describe (at a high level) the regulatory approaches in the United Kingdom, Germany and Japan in this area. We also touch upon the European Union's Markets in Crypto-assets Regulation ("**MiCA**") and the impact that this will have upon digital asset custody services provided from or into the European Union. First, however, it is helpful to touch upon the Financial Action Task Force ("**FATF**"), and the steps that have been taken through anti-money laundering regulations as one of the first key regulatory developments relating to digital assets.

Anti-money laundering regulations

FATF, an intergovernmental body focused upon the development of standards and policies intended to reduce financial crime (and particularly money laundering and terrorist financing), issued guidance and recommendations in October 2021 with a focus on virtual assets, and the potential risks from a financial crime perspective. FATF recommended that virtual asset service

providers engaged in the safekeeping and/or administration of virtual assets¹³ or instruments enabling control over virtual assets (i.e. private keys) on behalf of another person should fall within the scope of anti-money laundering regulations and be required to conduct customer due diligence checks (among other obligations).

In relation to custody services relating to virtual assets, FATF clarified in its guidance that, in simple terms, safekeeping and administration includes the service of holding a virtual asset or the private keys to the virtual asset on behalf of another person. Administration, in this case, could include the concept of managing virtual assets on behalf of another person. FATF specified that this activity would capture most custodial wallet service providers as they hold and/or keep virtual assets on behalf of another person. Although FATF guidance is not legally binding, it is often seen as a roadmap for regulatory updates in most jurisdictions with developed legal systems and therefore the recommendations set out in FATF's guidance will usually be implemented shortly after being published.

FATF's guidance has been implemented in many jurisdictions in a variety of different forms. The regulatory regimes detailed below all implement regulatory requirements that have been set out in FATF guidance on virtual assets.

13. FATF defines a "virtual asset" as "a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations."

In the EU, the Fifth Anti-Money Laundering Directive (“**AMLD5**”) represented the EU’s initial answer to FATF’s virtual asset guidance. AMLD5 implemented FATF’s recommendations by bringing “virtual currencies”¹⁴ within the scope of the EU’s anti-money laundering and counter-terrorist financing regulatory regime. AMLD5 regulates two key categories of virtual asset service: (i) virtual asset exchange providers, and (ii) custodian wallet providers – being entities that provide services to safeguard private cryptographic keys on behalf of customers, to hold, store and transfer virtual currencies. AMLD5 required that EU Member States implemented local legislative amendments and this has now broadly been completed across all EU Member States.

The United Kingdom

Other than the implementation of the requirements of AMLD5 in relation to custodian wallet providers, the UK has not yet implemented a specific digital asset custody regulatory regime. The UK is currently in the process of developing a new regulatory framework in relation to digital assets which, among other things, seeks to bring a broader range of digital assets within the scope of regulation. While there does not appear to be specific digital asset custody regulation on the short-term horizon, it is possible that the United Kingdom could introduce such regulation in response to regulatory initiatives in other jurisdictions.

The current regime

The primary form of regulation that is relevant to digital asset custody exists under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (“**MLRs**”). The MLRs regulate all custodian wallet providers offering safeguarding and administration services in relation to digital assets (which includes both regulated tokens and many unregulated tokens). The FCA has confirmed that custodian wallet providers will need to obtain a registration with the FCA even if the custodian wallet provider is already registered or authorised by the FCA for other purposes (such as electronic money institutions, payment services and FSMA-regulated firms)¹⁵. Digital asset custodians that fall within the definition of “custodian wallet provider” and that have business operations located in the United Kingdom will therefore be required to obtain this registration prior to being able to offer digital asset custody services from the United Kingdom. The registration under the MLRs differs to the FCA’s financial services regulatory regime, as it is not a full regulatory authorisation and does not result in subsequent FCA supervision.

Whether FSMA and the FCA’s conduct rules will apply to digital asset custodians depends upon the nature of the digital assets that a custodian safeguards and administers for its clients. The FCA has provided its view on the categorisation of digital assets, and the current position is that existing financial services regulations will be applied to digital assets that would fall within the scope of existing regulated financial instruments in traditional finance.

The FCA’s Policy Statement 19/22 sets out the FCA’s assessment of the application of the existing regulatory perimeter to digital assets. Not all digital assets are regulated – those that are regulated are referred to by the FCA as “regulated tokens”, which are divided into two categories: (i) security tokens, i.e. digital assets with specific characteristics that result in the relevant digital assets meeting the definition of a “specified investment” as defined in the Regulated Activities Order (under the Financial Services and Markets Act (“**FSMA**”) 2000) such as shares or bonds; and (ii) e-money tokens, i.e. digital assets that meet the definition of “electronic money” in the Electronic Money Regulations 2011.

14. Under AMLD5, “virtual currencies” are defined as “a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically.”

15. Crypto-assets: AML/CTF regime: Register with the FCA | FCA

Digital assets that fall outside of these categories are known as “unregulated tokens”, and this category includes exchange tokens (i.e. digital assets which are not issued or backed by a central authority and which are intended and designed to be used as a means of exchange including bitcoin and ether) and utility tokens (i.e. digital assets that grant the holder access to a current or prospective service, but which do not grant the holder rights the same as those granted by specified investments and are not used as a means of exchange).

Only custodians that provide clients with custody services in respect of “regulated tokens” are required to obtain Part 4A permission from the FCA or PRA, in the same way that a traditional custodian would be required to seek authorisation. It is only custodians that are regulated in this way which are required to comply with, for example, CASS requirements such as segregation of client assets from the custodian’s own assets. Custodians of exclusively “unregulated tokens” (such as bitcoin or ether) may safeguard and administer such digital assets without requiring regulatory authorisation and without being obliged to comply with CASS requirements.¹⁶

A proposed future regime

4.10 The United Kingdom is moving to keep pace with other jurisdictions that are implementing digital asset-specific regulation. The Financial Services and Markets (“**FSM**”) Bill was introduced

to Parliament in July 2022, and at the time of writing this paper is at the Committee Stage in the House of Commons. The FSM Bill seeks to bring activities facilitating the use of stablecoins within the regulatory perimeter in the United Kingdom.

The FSM Bill introduces the concept of “digital settlement assets”, defined as: “a digital representation of value or rights, whether or not cryptographically secured, that — (a) can be used for the settlement of payment obligations; (b) can be transferred, stored or traded electronically; and (c) uses technology supporting the recording or storage of data (which may include distributed ledger technology).”

Currently contemplated reforms include empowering HM Treasury to create new digital asset regulatory regimes, as well as bringing digital settlement assets within the remit of existing financial regulations. If passed, this legislation will grant HM Treasury the power to establish an FCA authorisation and supervision regime to mitigate conduct, prudential and market integrity risks for issuers and payment service providers using digital settlement assets, which is likely to have a knock-on effect upon digital asset custodians and expand the number of custodians that will require some form of regulatory authorisation.

It should be noted for completeness that the Law Commission in England and Wales has proposed the creation of a new category of personal property in response to concerns that digital assets do not neatly fit within the two existing concepts of personal property under English law. This new third category of personal property rights: “data objects”, would be distinct from the two existing personal property rights that exist in English law, which apply to “things in possession” and “things in action”.

Should the Law Commission’s proposals become law, this will have significant implications for digital asset custodians, namely that it will grant customers of custodians with proprietary rights over their digital assets which is currently not completely clear under English law. Unlike contractual rights, which exist only between the parties to the contract, proprietary rights can be asserted against the rest of the world. This would give the clients of custodians stronger recourse in instances of insolvency and fraud, as an unsecured creditor with a personal contractual claim will rank behind a creditor with a proprietary claim. This is one example of a jurisdiction proposing key reforms to established legal principles in order to enable more positive outcomes for digital asset owners and address some of the challenges faced by those owners at this point in time.

16. Note that this analysis may differ where the custodian is an FCA-authorised entity and that authorised entity also offers custody of unregulated tokens. In this case, the FCA may expect that the authorised firm will apply regulatory requirements such as CASS requirements even in relation to unregulated tokens.



Germany

In contrast to the approach taken in the United Kingdom, Germany has implemented a robust and specific regulatory regime targeting digital asset custody, which goes beyond simply expanding the remit of existing anti-money laundering regulatory requirements.

Germany implemented the requirements of AMLD5 through the amendment of the German Banking Act (the Kreditwesengesetz, or “KWG”) and other relevant laws. While AMLD5 required that EU Member States reformed anti-money laundering regulations to ensure that those undertaking the safeguarding and/or administration of “virtual assets” came within scope of anti-money laundering regulations, Germany used this as an opportunity to reform its approach to the regulation of digital asset custody in general. Germany’s amendments to the KWG result in the regulation of “cryptoasset custody business” as a financial service, with “cryptoassets” being regarded as a form of financial instrument.

“Cryptoassets” as a new category of financial instruments under the KWG is a broader definition than is seen in other EU Member States. This definition captures those digital assets which are (based on agreement or in practice) accepted as a means of exchange or payment, or serve investment purposes. The definition is likely to capture most digital assets that are used as a form of “cryptocurrency”, including bitcoin and ether. Pursuant to guidance provided by Germany’s financial services regulator, Bundesanstalt für Finanzdienstleistungsaufsicht (“BaFin”), the definition excludes certain utility tokens (i.e. where these represent a mere voucher). With that said, it is not fully clear whether all utility tokens would be out-of-scope of the KWG.

Additionally, the Electronic Securities Act (the Gesetz über elektronische Wertpapiere, or “eWpG”) dated 3 June 2021 opened the possibility for electronic securities under German law. The eWpG differentiates between central register securities and crypto securities. The eWpG contemplates that electronic securities may be issued using various different technological approaches, and, in the case of crypto securities, this includes the use of blockchain and cryptographic techniques. Under the eWpG, the keeping of crypto securities registers is a regulated activity and requires a BaFin licence.

In light of the broad definition, many digital asset custody providers will be required to obtain a full regulatory licence, and possibly multiple licences, from BaFin under the KWG (and eWpG as applicable) in order to offer digital asset custody services in Germany. Digital asset custodians will therefore be supervised in a manner broadly consistent with other regulated financial services firms.

This approach can be seen from multiple different lenses – for digital asset custodians, this could be regarded as an additional regulatory burden (resulting in higher operating costs on an ongoing basis to ensure compliance). Other custodians, and particularly clients, may view this as a beneficial move which ensures a higher required benchmark for the quality of service offered by digital asset custodians than may be found in other jurisdictions.

● Japan

We have also examined the regulatory position in a non-EU jurisdiction in which very specific custody-focused regulatory change can be seen and which provides an interesting middle ground between the UK and Germany.

In Japan, existing regulations were initially expanded so as to capture the exchange of digital assets and to ensure that those entities facilitating exchange activities would be subject to regulation. The narrow approach to such expansion, however, meant that the position in relation to digital asset custody was not necessarily clear and it appeared that custody activities were not necessarily captured under the expanded regulations.

In response to this, Japanese legislators amended two key pieces of legislation: the Payment Services Act, Japan's payment regulations which had been expanded to capture exchange service providers originally, as well as Japan's securities regulation, the Financial Instruments and Exchange Act. This ensures that the custody of digital assets are regulated either under the payment services regime or securities regulatory regime (as applicable to the digital assets in question).

The approach taken in the Payment Services Act in relation to digital asset custody providers is particularly interesting, as Japan opted to specify specific granular obligations for digital asset custodians to comply with which are not seen in many other similar regulatory regimes.

Digital asset custodians must be registered as a "cryptoasset exchange provider" with Japan's Financial Services Agency, and must comply with a number of internal organisational requirements applicable to all "cryptoasset exchange service providers", as well as specific digital asset custody operational obligations. Particularly notable requirements that apply specifically to digital asset custody providers include:

- (a) an obligation to hold client funds in a separate trust account;
- (b) a requirement that client digital assets are segregated from the custody provider's own assets;

(c) an obligation to hold digital assets in cold wallets (or equivalent) other than an amount of 5% or less of the aggregate value of client digital assets which may be held in hot wallets to facilitate exchange services; and

(d) an obligation for the custodian to hold digital assets (of the same kind and quantity) on its own account in an equivalent amount to any customer assets that are held in hot wallets on behalf of clients.

This is a rare example of a regulator applying specific requirements as to the ratio of client assets that must be held in hot and cold wallets, with the additional protection of the custodian's own reserves to mitigate the increased cybersecurity risk that is associated with hot wallets. We can also identify familiar concepts that are similar to those found in the UK's CASS requirements and (as noted below) in the upcoming MiCA regulation as well.



Having considered the position in the UK, Germany and Japan as it stands today, we also wanted to highlight the impact that MiCA will have upon digital asset custodians established in, or offering services into, EU Member States. MiCA includes specific obligations relating to the custody of “crypto-assets” which will be familiar to those that are acquainted with MiFID II.

MiCA is an EU regulation that aims to provide a harmonised legal framework for regulating certain digital asset-related activities that are provided from or into EU Member States. The final text of MiCA was agreed in early October 2022 after two years of negotiation amongst the EU institutions. The final text of MiCA will be adopted into law after following the drafting of the MiCA delegated acts, and it is likely to be published in the Official Journal of the European Union by early 2023. The full implementation of MiCA is not expected to take place prior to 2024.

MiCA is applicable to all digital assets that fall within the definition of “crypto-asset” being “a digital representation of value or rights, which may be transferred and stored electronically, using distributed ledger or similar technology”. Notably, MiCA explicitly excludes NFTs from scope, other than in certain scenarios (for example, where NFTs are de facto used for payment or investment purposes). MiCA will apply to issuers of “crypto-assets”, as well as crypto-asset service providers (including custodians) and crypto-asset markets.

MiCA regulates activities including (among others) the custody and administration of crypto-assets on behalf of third parties, which is defined as “safekeeping or controlling, on behalf of third parties, crypto-assets or the means of access to such crypto-assets, where applicable in the form of private cryptographic keys”.¹⁷ As a result, custodians of crypto-assets are classified as crypto-asset service providers (“CASPs”) and required to obtain regulatory authorisation with the relevant national competent authority under MiCA.

As CASPs, crypto-asset custodians are subject to general requirements (which apply to all CASPs) as well as custody-specific requirements (applying to crypto-asset custodians only) under MiCA. The final draft of the agreed text of MiCA includes the following requirements applicable to crypto-asset custodians.¹⁸

General requirements

A number of general requirements applying to all CASPs will be applicable to custodians holding crypto-assets, including:

- (a) minimum capital requirements that the custodian must retain;
- (b) certain governance requirements including ensuring that the custodian’s management are in sufficiently good repute and possess the requisite knowledge and skills to run the custodian;
- (c) requirements to act honestly, fairly and professionally in accordance with their clients’ best interests; and

¹⁷. MiCA, Article 3(1)(10).

¹⁸. Note in particular, MiCA Articles 59, 60, 61, 63, 67 and 80a.

(iv) an obligation to put systems in place to prevent market abuse and insider dealing.

There are also general requirements for CASPs that hold crypto-assets or funds belonging to their clients, ensuring that adequate arrangements are made to safeguard clients' ownership rights (particularly in the case of CASP insolvency), to prevent the use of their clients' funds for their own account, and to place client funds in a central bank or credit institution within a certain period following receipt.

Custody-specific requirements

There are additionally specific requirements for CASPs providing custody and administration services, which broadly reflect equivalent requirements that we are familiar with in relation to the custody of investment products discussed briefly earlier in this paper. In particular, custodians must:

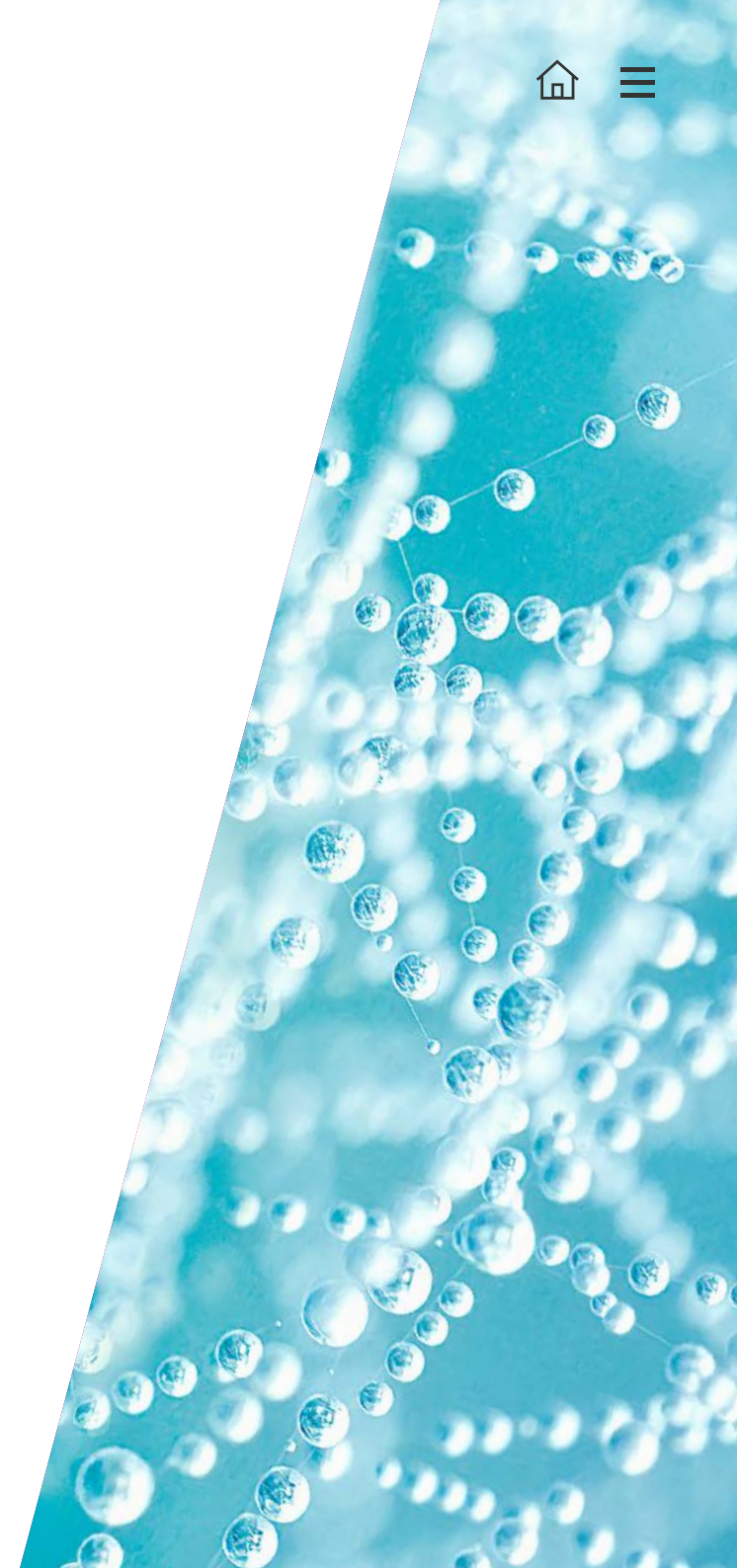
- (i) enter into an agreement with their clients specifying duties and responsibilities, which should include details such as the means of communication between the CASP and the client, a description of the security systems used by the CASP and include a "custody policy";
- (ii) keep a register of positions;
- (iii) establish safekeeping procedures;
- (iv) facilitate the exercise of their clients' rights;
- (v) provide their clients with a "statement of position" at least once every three months;

(vi) ensure necessary procedures are in place to return crypto-assets; and

(vii) segregate their own proprietary crypto-assets from those of their clients.

It is clear that MiCA represents a shift in the regulatory obligations of digital asset custodians. It is a substantial regulation that will have a fundamental impact upon the digital asset industry and all related service providers. While a detailed review of MiCA is beyond the scope of this paper, the key takeaway from a custody perspective is that the regulatory landscape continues to shift in the direction of greater consumer protection and the protection of client assets.

For clients or potential clients of digital asset custodians, this can be seen as a positive move from a risk perspective. In contrast, digital asset custodians will be required to rapidly get to grips with the new regulatory regime that will result in regulatory requirements applying to custodians in a manner akin to the regulation of traditional custodians.



A proposed way forward

This paper has explored the origins of the custody industry, identified the continued evolutionary journey into the digital world and has sought to provide details of some of the key differences between traditional custody and digital asset custody that clients should ensure they are familiar with when engaging with digital assets and selecting a custodian.

The fundamental question remains, however – what is the way forward for institutions seeking to enter this space and what are the legal and operational opportunities and pitfalls to bear in mind when considering how best to custody digital assets?

To answer this, we would advise a particular focus on the following aspects in order to ensure a smoother custody experience:

- (a) assessing the legal structure of the applicable custody arrangement, to ensure this is appropriate for an institution's requirements;
- (b) digging into the custodian's operational processes, including its approach to ensuring that it offers a resilient service;
- (c) considering the security mechanisms that the custodian implements to ensure that its client's digital assets are not unnecessarily at risk; and
- (d) above all, scrutinising the approach to regulatory compliance that the custodian is implementing.

We delve into each of these below in more detail with the aim of assisting institutions in getting to grips with these considerations and moving forward with these assessments to increase the likelihood of success for innovative digital asset projects.

Legal structuring of custody arrangements

Ultimately it is important that the legal relationship between the client and the custodian be effective to vest legal and/or beneficial ownership and control of the digital assets in the client. To avoid loss, it is important for clients who are concerned with managing their risk exposures to carefully segment custody providers and work through all asset flows to understand the vulnerability of their assets before choosing a custodian. Not all custodians are alike and the choice made should be informed and align with a client's risk appetite.

Questions to ask include:

- (a) does the custodian segregate client assets and funds from its own?
- (b) does the custodian segregate each client's assets from the assets of each other client, and offer a segregation of assets with different private keys associated with each client's assets?
- (c) how does the custodian purport to manage its client's digital assets, or those of their customers? Is there a trust arrangement, or do the client and its customers maintain a beneficial interest in those digital assets? Remember, control of the private key is critical here and in many jurisdictions legal principles have not caught up with technical advancements, meaning that the custodian potentially has far more legal freedom with your digital assets than would be the case with a traditional custodian.

Operational approach to custody and resilience

A key consideration here relates to the model of custody offered by the custodian, which is tied to the questions raised above. If the custodian has segregated the assets of each client, then this presents a higher level of protection for clients, though may result in certain operational inefficiencies in relation to the ability of the custodian to execute a client's orders. In contrast, certain custodians may employ an omnibus model which offers operational efficiencies but may increase the risk for clients of either a security breach or custodian failure or insolvency. In this case, client assets are at higher risk than where each client's assets are segregated – an assessment to balance this risk with the potential operational and commercial benefits should be undertaken in such cases.

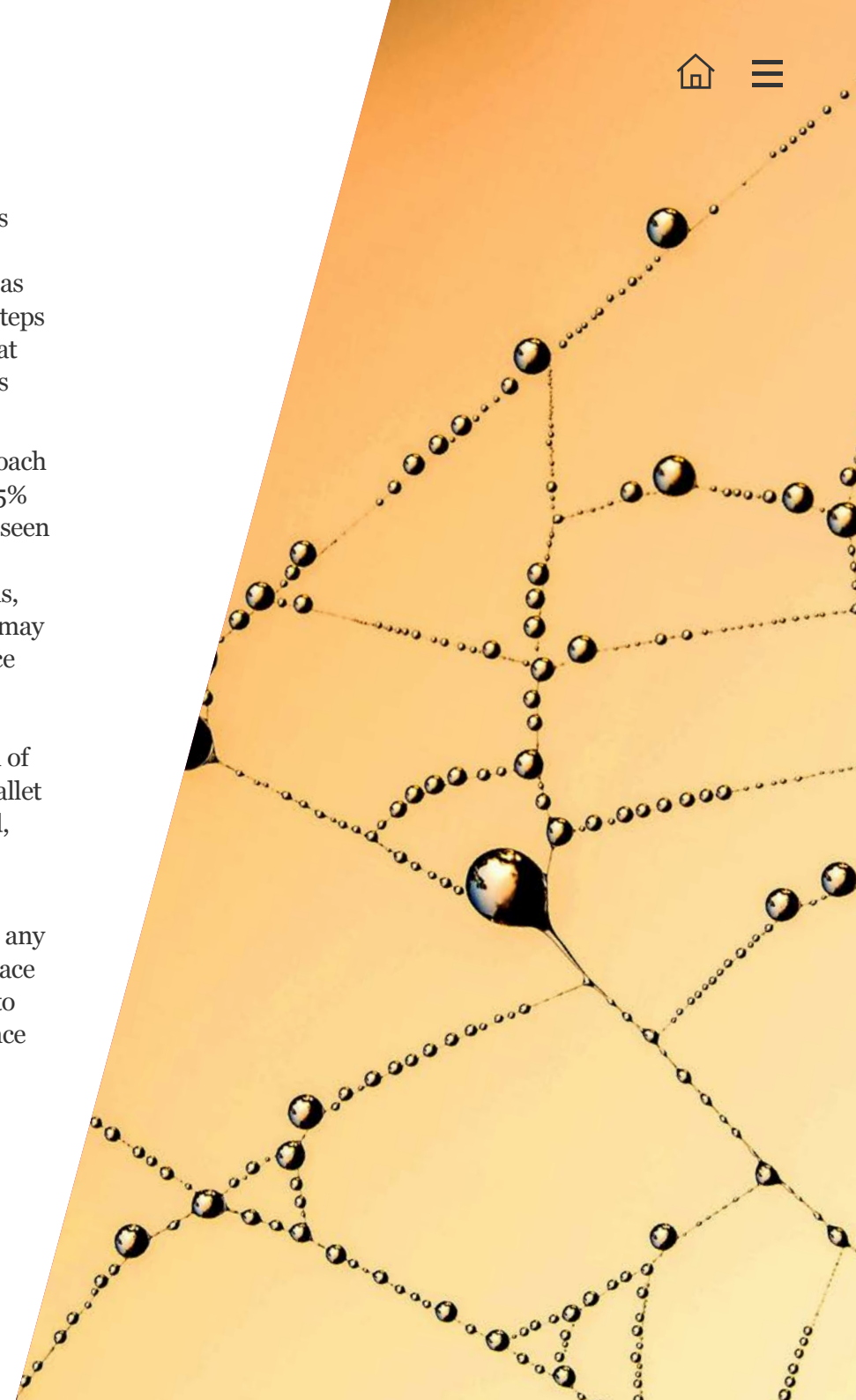
For institutions that are evaluating digital asset custodians, existing principles relating to the evaluation of critical outsourced service providers may prove to be a useful tool. In particular, considering the custodian's approach to information security, business continuity and disaster recovery will provide some additional comfort to clients that key technology can be restored or replaced in the event that disaster strikes. This exercise will also be somewhat indicative of the level of sophistication that a custodian can offer to the institution and whether this is up to institutional standards.

Security mechanisms

A key consideration relates to the custodian's approach to hot and cold wallet storage, and other applicable security mechanisms (such as sharding or multi-signature wallets). What steps has the custodian implemented to ensure that the ratio of hot-to-cold digital asset storage is appropriate? Is this ratio clear to clients?

Our examination of Japan's regulatory approach to digital asset custody has highlighted that 5% of digital assets stored in hot wallets may be seen as the maximum percentage that regulators would consider to be safe in Japan. From this, we can extrapolate that a higher percentage may be indicative of a higher level of risk tolerance shown by the custodian in question. Japan's regulatory approach also raises the further question – does the custodian have any level of reserve to cover the possibility that its hot wallet storage is hacked or otherwise compromised, such that clients would be put whole in this scenario?

Clients should assess these factors alongside any mechanisms that the custodian has put in place to safeguard private keys and digital assets, to build a picture of the custodian's risk tolerance and the potential worst case scenario.



Regulatory compliance

Digital asset custody regulation is not uniform at this point in time by any means, and the level of regulatory obligation expected in different jurisdictions can vary greatly. There are many digital asset custodians in the market, each situated in different jurisdictions and subject to different regulatory regimes.

In this sense, it is important to consider whether the regulatory standards in the jurisdictions in which the custodian is regulated are sufficiently robust. Does the custodian apply a standard of best protection across all jurisdictions, even if not strictly required? Is the custodian aware of upcoming developments and ahead of the curve in relation to the regulatory requirements that it will need to comply with not only presently, but in the short and medium term?

To be more specific, custodians need to demonstrate to clients as a minimum that, in order to provide assurance of continuity of service to clients, they either have the core regulatory building blocks in place, or a roadmap that is as clear as the evolving regulations allow for, to acquire those regulatory building blocks. Particular considerations that should be in the minds of custodians today include (as required):

- (a) local money laundering and counter-terrorism registrations – and the implementation of appropriate controls, measures, policies and procedures in order to comply with ongoing regulatory obligations relating to anti-money laundering and counter-terrorist financing;

- (b) local licensing requirements applicable to digital asset custody providers, as appropriate for the category (or categories) of digital assets that the custodian will safeguard and administer, along with systems and controls to meet the requirements for firms with such licences; and

- (c) effective operationalisation of Financial Action Task Force recommendation 16 “travel rule” requirements – ensuring that certain specified information in relation to the sender and receiver of digital assets is obtained.

The continued evolution of the digital asset industry and applicable regulation

More broadly, it is important to be mindful that the regulatory environment in which digital asset custody services will be delivered in the near future continues to evolve at pace. What lies ahead is greater clarity as to the regulatory characterisation of digital assets, the precise nature of legal property rights associated with the asset class and clarity on the approach to regulation of the services relating to digital assets, including custody.

These initiatives are driven by the objectives of protecting clients and the broader financial system from risk. We have already discussed the UK government's signposting that stablecoins used as a means of payment will be brought within the regulatory perimeter by way of the FSM Bill, as well as the EU's MiCA regulation, which will regulate digital asset custody providers.

Additionally, at an international level - and from a broader policy perspective - the Financial Stability Board (FSB) has proposed¹⁹ a global approach to regulation of digital assets based on the principles of "same activity, same risk, same regulation." The regulatory community may have taken its time to keep up with the digital asset industry, but regulators are now firmly in the rear-view mirror and digital asset custodians in particular must ensure that they are ready for the wave of regulation that is on the horizon to meet those standards.

But more broadly, as the digital asset market rapidly professionalises and institutionalises, clients' expectations will exceed that of simply meeting minimum regulatory standards. They will include the adoption of business-wide risk management frameworks that accommodate and drive adoption of new regulatory standards and meet or exceed those of regulated institutions operating in traditional financial markets. We hope that this paper equips clients and prospective clients with the tools necessary to make these kinds of assessments, and to further understand the industry and environment that they are considering moving into. Custody is a key building block for any digital asset and tokenisation project, but if approached in the wrong way (without the correct questions being asked) these projects may never get off the ground, or could lead to real issues and challenges down the road.

19. Financial Stability Board (2022), International Regulation of Crypto-asset Activities, 11 October, p. 4.

About Hogan Lovells

Hogan Lovells is an international law firm with one of the most experienced Digital Asset and Blockchain practices in the legal sector, and has deep expertise advising on complex, first-in-kind matters. Hogan Lovells is at the forefront of change and its lawyers play a leading role in the development of the emerging regulatory frameworks. Clients benefit from the firm's expertise and knowledge of the regulators and key market players.

Hogan Lovells is a strategic partner with a number of industry bodies and networks, including Global Blockchain Business Council Digital Finance (formerly Global Digital Finance), an industry body promoting the development of best practices and conduct standards for the digital asset industry. The firm is an active member of GBBC's prominent industry Working Groups, including the Patron Board, Advisory Counsel, MiCA, Tax, Sanctions and DeFi. In addition, the firm is a strategic partner with Innovate Finance, UK Finance and Payments20, and Hogan Lovells takes an active role in the development of policy and regulation.

Hogan Lovells recognise that the regulatory position relating to the issuance and utilisation of digital assets is still evolving. The firm has been at the heart of global education and lobbying efforts around digital assets for many years, speaking to regulators and policymakers across the world, including the White House, U.S. Treasury, HM Treasury, OECD, NYDFS, European Parliament, World Bank and IOSCO.

The firm's experience, partnerships and diverse client base means it is perfectly placed to deliver commercial and innovative solutions for its clients.

Additionally, Hogan Lovells has created a range of digital tools such as its [Cryptoasset Activity AML Registration Toolkit](#) and the [Digital Assets and Blockchain Hub](#) to help financial institutions navigate the legal and regulatory landscapes; both arguably the most comprehensive toolkits of their kind created by a law firm. Hogan Lovells has also developed its own technology platforms for clients, including most recently DriveChain, a blockchain-enabled automated technology solution, designed to drive efficiencies within commercial transactions across all industries.

About the authors



John Salmon
Partner, London

John leads the Hogan Lovells Digital Assets & Blockchain practice and has played a leading role in many cutting-edge developments and solutions in this space. He advises a full range of market players, from start-ups to major global banks. He spends a great deal of time educating regulators, policy makers and clients in the area of blockchain and crypto and has spoken to the OECD, European Parliament, IOSCO and many governments on this area. John's active engagement in a number of industry initiatives places him at the forefront of regulatory evolutions in relation to digital assets. He has a wealth of experience advising financial institutions and technology companies on the implementation and operation of digital assets and blockchain projects, across a range of industry sectors. In addition, John has extensive experience of drafting and negotiating both customer and supplier IT services contracts, including for development projects, software licensing, cloud, and systems integration.



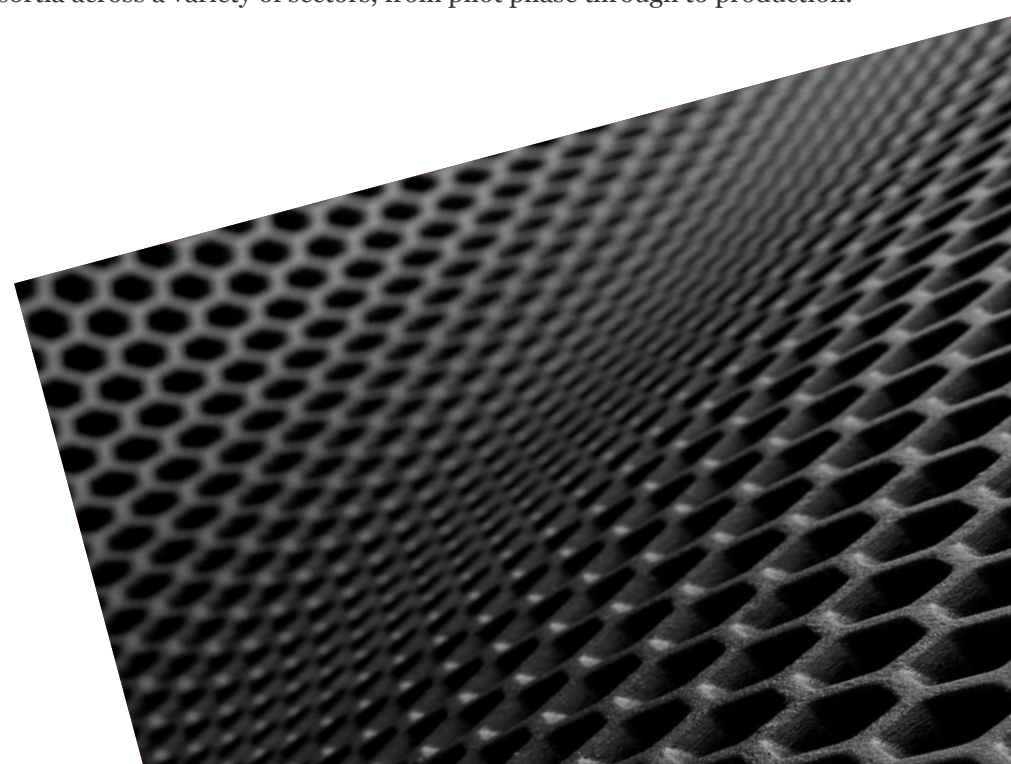
Michael Thomas
Partner, London

Michael leads our Investments & Markets practice in the UK. He has spent over 20 years advising all types of financial institutions on regulatory, governance and commercial matters. Michael has extensive expertise in advising trading platforms and financial market infrastructure, which provides a critical technical understanding of how the financial markets operate. His extensive regulatory experience has enabled Michael to understand and steer the development of a wide range of cutting-edge projects in the arena of digital assets, including the world's first issuance of company shares on a blockchain; advising on the feasibility and implementation of a wide range of digital asset business models; and assisting clients to launch their digital asset businesses in multiple jurisdictions. His digital asset expertise ranges from: advising blockchain start-ups, to advising existing financial institutions seeking to apply the new technology, to assisting the development of new models of operation for FMIs seeking to apply digital asset and blockchain ledger technology.



James Sharp
Associate, London

James is an associate in the Technology Team, with a focus on advising financial institutions, technology providers and FinTech companies on their strategic technology projects, digital and technology solutions and regulatory risk. James particularly specialises in all matters relating to blockchain, digital assets, NFTs, and Web 3.0. James's focus on blockchain and digital assets means he understands the complex range of commercial and regulatory issues facing clients that are seeking to participate in the space and struggling with the ever-evolving regulatory hurdles. He has advised clients on a range of projects, from anti-money laundering regulatory queries to co-operations, partnerships and restructurings relating to digital asset custody arrangements and tokenised asset projects (including in relation to tokenised art). Additionally, James has experience advising clients on the often-complex contractual and structuring arrangements related to the establishment and operation of blockchain consortia across a variety of sectors, from pilot phase through to production.





Mark Orton
Senior Associate, London

Mark Orton is a senior associate in the Hogan Lovells Financial Institutions Group and advises a range of clients, including banks, asset managers, insurers, FMIs and FinTechs in relation to financial services regulation at both the UK and EU level. A particular focus of Mark's practice is on tokenisation and digital assets and the deployment of distributed ledger technology in the provision of financial services. Mark has significant experience advising on the regulatory implications related to a wide range of digital assets and blockchain projects and helps clients to structure their offerings in a manner that is compliant with relevant regulatory requirements. This experience includes advice in relation to the tokenisation of traditional financial instruments and regulated products, as well as advice on the regulatory implications of the provision of custody and other services in relation to 'unregulated' cryptoassets (such as lending and staking). Mark has also advised on the contractual arrangements underpinning blockchain-based FMIs.



Joseph Scott
Trainee solicitor

Joseph Scott is a trainee solicitor working in Hogan Lovells Technology Team. He works on a range of matters regarding digital assets and the regulatory challenges relating to the associated technologies, and has in particular focused his attention to the digital asset custody field. He also has experience in corporate litigation, fraud and investigations.



About Zodia Custody

Zodia Custody provides digital asset custody services to corporate and institutional clients. Zodia Custody Limited is a subsidiary of Standard Chartered plc with a minority interest held by Northern Trust. In respect of its cryptoasset activities it is registered with the UK FCA for anti-money laundering and counter terrorism purposes (Firm Reference Number 928347), with FinCen as a Money Services Business and has an Irish subsidiary registered with the Central Bank of Ireland under the Criminal Justice Act (Firm Reference Number C453603).

Zodia's mission is to combine the technology and agility of a start-up with the risk management framework of a leading global financial institution. Client asset safety is the core consideration.

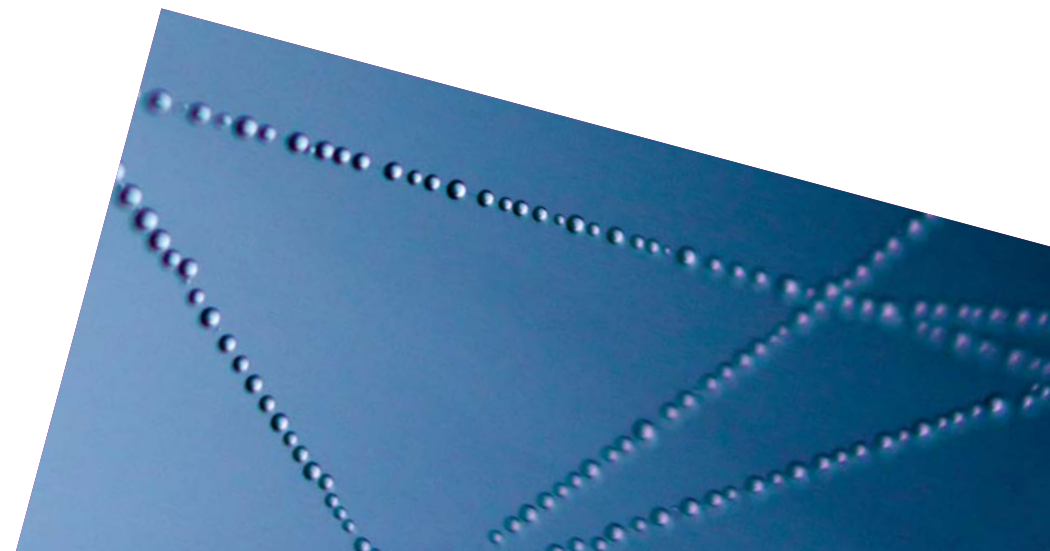
Zodia addresses the following digital asset servicing needs:

- **Safekeeping:** tailored custody models for risk diversification and global coverage. Cold storage with 24x7 real-time availability, and zero central points of compromise.
- **Exposure to asset classes:** Bitcoin, Ethereum, Bitcoin Cash, Litecoin, Chainlink, Uniswap, Wrapped Bitcoin, and USD coin.
- **Better yield generation:** support for staking and DeFi financing protocols.
- **Native understanding of cash management,** securities services, wealth and markets products, and applications (not just custody!).

- **Management of structured products: end-to-end lifecycle management for structured products.**

- **Real-time access to liquidity:** seamless exchange of value from transfers in/out to order execution via (de-)/centralized exchanges and brokerages.

Zodia is committed to delivering secure and robust technology infrastructure that will enable corporate and institutional clients to safeguard and service their digital assets. Contact Zodia for a demonstration of the system.





Julian Sawyer
CEO
julian.sawyer@zodia.io

Julian Sawyer is the CEO (subject to FCA approval) at Zodia Custody, the Standard Chartered and Northern Trust backed digital asset custodian joining the business in November 2022. Prior to that he was Chief Executive Officer at Bitstamp, the worlds oldest crypto exchange with over 4 million customers. He has been an advisor to the board of the leading Australian challenger bank, Volt and an advisor to a number of financial services business in Europe, US and Dubai. Prior to joining Bitstamp Julian worked for Gemini as MD for Europe and he also co-founded Starling Bank, where he was COO with responsibility for running customer services, AML & Fraud, Payment Operations, HR and Supplier Management. He also held P&L responsibility for the B2B arm, Starling Banking Services. Prior to Starling, he was a management consultant at Accenture and EY and set up and ran his own financial services consultancy, Bluerock, for 13 years before selling it. Julian is an Honorary Senior Visiting Fellow at Bayes Business School's Faculty of Management.



Richard Clark
Head of Sales & Partnerships
richard.clark@zodia.io

Richard joined Zodia in June this year. Richard spent more than 15 years at Merrill Lynch in various roles but mainly as a Sales Director of Futures & Options, Fixed Income PB, FX PB and OTC Clearing. Richard is based in London.



Alasdair Pitt
Head of Legal
alasdair.pitt@zodia.io

Before joining Zodia in 2020, Alasdair spent 11 years supporting the Greater China and North Asia Financial Markets business for SCB based in Hong Kong. Before that he worked in Equity Capital Markets origination for Citigroup in Tokyo and for Credit Suisse based in London, New York and Tokyo. He is studying for a Masters in Entrepreneurship at Judge Business School, University of Cambridge.



Hogan Lovells



John Salmon
Partner, London
T: +44 20 7296 5071
john.salmon@hoganlovells.com



Sharon Lewis
Partner, Paris, London
T: +33 (1) 5367 4704 (Paris)
T: +44 20 7296 2474 (London)
sharon.lewis@hoganlovells.com



Elizabeth (Liz) Boison
Partner, Washington, D.C.
T: +1 202 637 5624
elizabeth.boison@hoganlovells.com



Dr. Leopold von Gerlach
Partner, Hamburg, Frankfurt
T: +49 40 419 93 144 (Hamburg)
T: +49 69 962 36 0 (Frankfurt)
leopold.vongerlach@hoganlovells.com



Wataru Kamoto
Partner, Tokyo
T: +81 3 5157 8163
wataru.kamoto@hoganlovells.com



Andrew McGinty
Partner, Hong Kong
T: +852 2840 5004
andrew.mcgintry@hoganlovells.com



Michael Thomas
Partner, London
T: +44 20 7296 5081
michael.thomas@hoganlovells.com



Dr. Jochen Seitz
Partner, Frankfurt
T: +49 69 96 23 6700
jochen.seitz@hoganlovells.com



Bryony Widdup
Partner, London
T: +44 20 7296 2000
bryony.widdup@hoganlovells.com



Luke Grubb
Consultant, London
T: +44 20 7296 2912
luke.grubb@hoganlovells.com



Mark Orton
Senior Associate, London
T: +44 20 7296 2000
mark.orton@hoganlovells.com



James Sharp
Associate, London
T: +44 20 7296 5765
james.sharp@hoganlovells.com

Zodia Custody



Julian Sawyer
CEO
julian.sawyer@zodia.io



Alasdair Pitt
Head of Legal
alasdair.pitt@zodia.io



Richard Clark
Head of Sales & Partnerships
richard.clark@zodia.io

Contacts

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dublin
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami

Milan
Minneapolis
Monterrey
Munich
New York
Northern Virginia
Paris
Philadelphia
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.

*Our associated offices
Legal Services Centre: Berlin

www.hoganlovells.com

"Hogan Lovells" or the "firm" is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses.

The word "partner" is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.

For more information about Hogan Lovells, the partners and their qualifications, see www.hoganlovells.com.

Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney advertising. Images of people may feature current or former lawyers and employees at Hogan Lovells or models not connected with the firm.

© Hogan Lovells 2023. All rights reserved. CT-REQ-2080