GDF GBBC DIGITAL FINANCE

ISSA International Securities Services Association

Deloitte.

2023 | GDF, ISSA AND DELOITTE REPORT

DIGITAL ASSET CUSTODY DECIPHERED

A Primer to Navigating the Challenges of Safeguarding Digital Assets

INTRODUCTION

LEGAL, REGULATION, AND FINANCIAL CRIME

SETTLEMENT, FINALITY, AND ASSET SEGREGATION

DLT GOVERNANCE, KEY MANAGEMENT, STAKING AND INTEROPERABILITY

WHAT SHOULD ASSET OWNERS EXPECT

CONCLUSION

APPENDIX

REFERENCES AND RESOURCES

The views expressed and information set out in this report are the views of GBBC Digital Finance and International Securities Services Association and do not represent the individual views of specific member firms of contributing authors and chairs. The content reflects a broad range of experience and views communicated by individuals who occasionally disagree or have different views and opinions on the topic of DAC, as to be expected.

Foreword

Lawrence Wintermeyer
Chair of GBBC Digital Finance
Working Group Sponsor

Glen Fernandes
Co-Chair ISSA DLT and Digital Asset WG
Working Group Sponsor

As we near the first quarter of the 21st century, it is clear to many in business that digital technology is moving at a faster pace than executives, policymakers and governments, regulators and agencies, and even leading technologists, can often keep up with.

The impact of the 4th industrial revolution (i.e. internet, mobile and digital) through inexpensive and readily available computing technology connected to the network and in the hands of digital innovators and billions of consumers alike has profoundly changed many of our daily habits, routines and in some cases, changed our lives.

Blockchain technology has been with us for 13 years and the development of new ecosystems and digital assets is breathtaking. While showing great promise in playing a transformative role in the digital evolution of our global financial services infrastructure, the technology has often been mired in controversy, highly politicized, conflated through rhetoric and information asymmetry, and from all sides of the spectrum. Meanwhile current global financial system and regulations continue to lag in materially evolving to the new digital age.

Many in the industry leading this next era of digital transformation, from innovative FinTechs to established institutions, are committed to the potential benefits of new digital technologies. We understand the complexity of the risks and changes required, and have the experience to manage this transformation successfully.

It will take a lot of patience, understanding, hard work, and as seen, sometimes unfortunate failures, for these worlds to meet, and a significant commitment to work together is required by industry, policymakers, and regulators. More importantly, it will require us all to bring focus to the essence of what could take us forward and where we still need to put in more work. We are now well into this journey in our respective member associations. This is one of the most promising signals of nascent collaboration, and a humble attempt to distil the "substance" from the noise.

This report on digital asset custody (DAC), the "Gordian knot" of digital assets, sets out to provide financial services professionals, investors and policy makers of all experience and levels with a starting point to understand the risks and considerations involved in DAC and equip them to move forward with decisions, solutions, and execution – it is a practitioner's guide.

The report has been produced in a joint Custody Working Group, a collaboration between GBBC Digital Finance (GDF) – the financial services arm of Global Blockchain Business Council (GBBC) – and the International Securities Services Association (ISSA), supported by our member firms and the Working Group Secretariat, Deloitte.

We are grateful to all of our Working Group members and their invaluable contributions and resources, the Working Group co-chairs from Brown Brothers Harriman, Metaco, and State Street who led the development of the content of the report, and to Deloitte, the Secretariat and pen holder for the principal draft of the report. A special thanks as well to the GDF and ISSA team involved in the Secretariat support to produce the final version of the report. ■

Executive Summary

Seamus Donoghue
Chief Growth Officer, Metaco
Working Group Co-Chair

Swen Werner
Former Head of Digital Custody, State Street
Working Group Co-Chair

John Siena
Associate General Counsel and Co-Head Regulatory Strategy, Brown Brothers Harriman
Working Group Co-Chair

Ed Moorby
Partner, Deloitte
Working Group Secretariat - UK Lead

Roy Ben-Hur
Managing Director, Deloitte
Working Group Secretariat - US Lead

Distributed ledger technology (DLT) has the potential to transform financial services and impact capital markets and traditional market structures. To help realize this potential, investors need to know that their assets are safe. This requires a common understanding of how investor interests in assets recorded using DLT, known as DAC, are safeguarded, serviced, and executed securely. It also underscores the significance the role custodians play, even as technological advancements continue to reshape this sector.

Some activities required for DAC are recognized in traditional securities services as roles performed by a custodian or Financial Market Infrastructure (FMI), however it is broadly recognized that in relation to digital assets, new operating models, capabilities, and controls may be required to provide those services effectively. The tokenization of real-world assets has the potential to enable the further democratization of finance and contribute to the transformation of financial markets over the next decade.

This report presents an analysis into current trends and key considerations arising for investors establishing arrangements for the safeguarding and servicing of digital assets - DAC. These insights are intended to help establish a common understanding of DAC to help achieve investor assurance while reducing risks and increasing efficiencies though a better understanding of law, regulation, technology, and market developments.

The report is also intended to serve as a call to action for market participants and firms who would provide DAC services to support the kinds of market developments and legal and regulatory reforms that would help ensure broad, safe adoption of DLT in the financial services ecosystem.

The evolution of custody of "traditional" financial assets to custody of digital assets has signaled significant change in market structures and the delineation of roles, rules, regulations, and responsibilities. Like traditional capital markets, DAC refers to the safeguarding of an investors' assets, however, in this context, roles, rules, regulations, and responsibilities are far less settled and there is little legal precedent.

Digital assets may be bought on an exchange[1], with the blockchain's consensus mechanism assigning the asset to a digital wallet associated with the buyer. The wallet is accessed through the control of the private keys.

Custodians are responsible for securing these private keys to access the asset on behalf of the asset holder client. Corporate actions and other rights and entitlements may be managed via smart contracts or the ledger.

[1] Whether the function of the register is performed definitively by the DLT may or may not be supported in applicable law.

Many of the principles that apply in traditional custody can and should be applied to DAC. It is particularly important that the industry draws valuable lessons from recent industry failures and that firms offering DAC meet the standards and regulations that apply to custodians of traditional assets. The opportunity to rethink the financial market structures must be tempered with the understanding and commitment to the protection of investors' assets from fraud, malfeasance, misuse, misappropriation, or exposure due to operational or performance failures.

There are also challenges to be solved with the adoption and transition to DAC and a DLT environment, not least:

- There is little alignment to date from many market participants, including regulators, on a desire to facilitate a T+0 and 24/7/365 marketplace
- The technology must support a large-scale implementation to prove that it can be the transformative power
- Who will lead and bear the cost of this (significant) digital transformation should the financial markets move to DLT is unclear.

Given these challenges it is still unclear whether DLT will become the preferred technology for the entire, or some parts of the market, for example, the securities value chain. If it does become the preferred solution, this will take some time and have a (proven) period of co-existence even in an individual market. As with all technological changes, DLT is in competition with programs to shorten the settlement cycle, provide more data and analytics, and perennial cost pressures.

The report delivers an eight-point call to action to highlight the opportunities, risks, and risk mitigants that investors and service providers should understand and apply in connection with DAC:

1. Educate workforces on digital assets and their value chain as well as the risks and risk mitigation of elements such as key management and staking – particularly for asset owners and investment managers,

2. Engage with regulatory authorities to resolve uncertainties related to the development and growth of DAC and promote regulation through the lens of "same activity, same risks, same regulations",

3. Develop a common understanding of how asset owners and/or investment managers should ensure contractual terms that are clear, that address risks that are relevant to DAC and that delineate between the responsibilities of a digital custodian, and other market participants and service providers,

4. Support dialogue with anti-money laundering (AML) / know-your-customer (KYC) and sanctions authorities in order to achieve common aims so that requirements, money laundering and other criminal activity risks and sanctions enforcement are effectively addressed whilst allowing digital asset ecosystems to operate effectively,

5. Work with governors and/or operators of DLT networks to establish transparent finality rules and processes,

6. Work with the industry to establish principles and best practices for:

   i. Asset segregation
   ii. Ledger governance
   iii. Interoperability,

7. Advocate for bankruptcy remoteness of assets through statutory and regulatory reform, or litigation, to ensure jurisprudence,

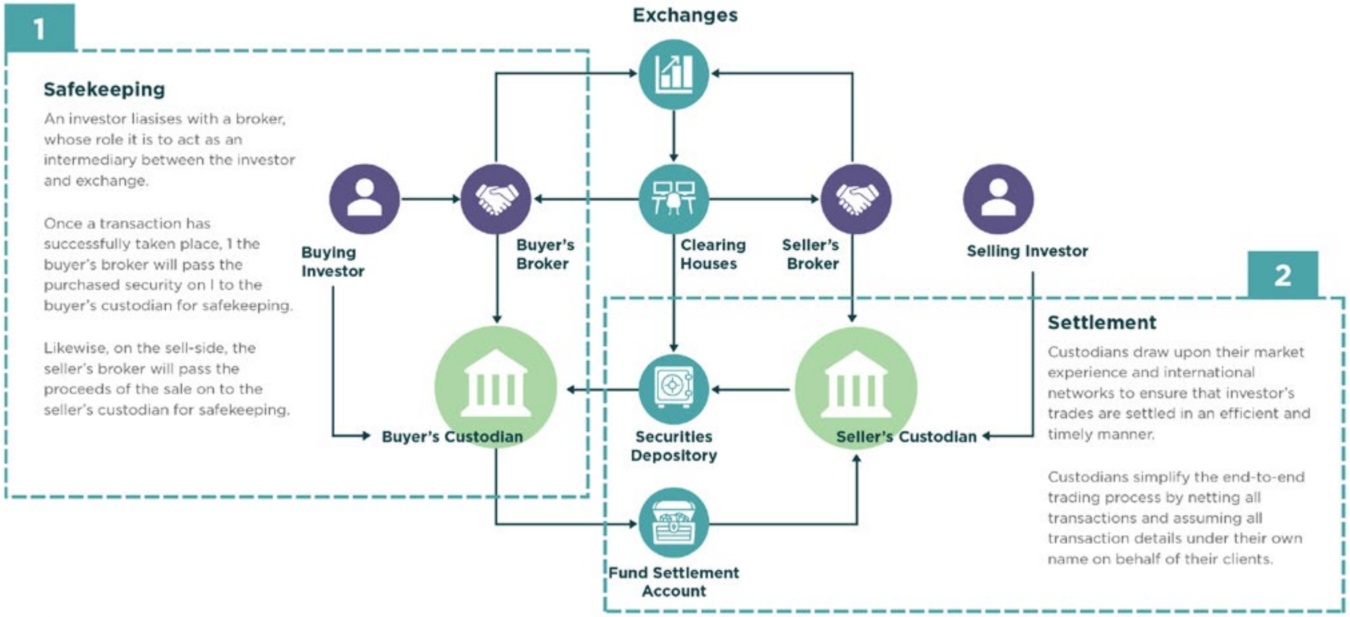
8. Support of the adoption of global legal standards to cover DAC. Standardization helps the market develop and creates less barriers. ■

INTRODUCTION AND BACKGROUND

From Traditional Custody to DAC and the Role of a Custodian

NB: Throughout this report the term “custodian” is used to denote all forms of regulated custody providers wherever that service is provided from i.e., globally, regionally, locally, and whether by a custodian, so-called “sub-custodian” or a Financial Market infrastructure (FMI) such as a CSD.

In traditional financial services custody, a financial asset is bought on an exchange, the legal register is at the local Central Securities Depository (CSD): once the buyer’s and seller’s custodians have matched instructions with the CSD, the custodians exchange cash for securities at the CSD (i.e., as reflected in their CSD participant accounts) and reflect these movements on their respective clients’ accounts. At the moment of this exchange (“settlement”) the custodian facilitating the purchase on behalf of its client has the asset in safeguarding on behalf of its client and services the asset (e.g., applying corporate actions, facilitating payment of dividends and income, paying withholding tax – all on behalf of the client) until the client wishes to sell the asset. The custodian then facilitates the sale.



Safekeeping

An investor liasises with a broker, whose role it is to act as an intermediary between the investor and exchange.

Once a transaction has successfully taken place, 1 the buyer’s broker will pass the purchased security on I to the buyer’s custodian for safekeeping.

Likewise, on the sell-side, the seller’s broker will pass the proceeds of the sale on to the seller’s custodian for safekeeping.

Settlement

Custodians draw upon their market experience and international networks to ensure that investor’s trades are settled in an efficient and timely manner.

Custodians simplify the end-to-end trading process by netting all transactions and assuming all transaction details under their own name on behalf of their clients.

Exhibit 1

© Deloitte 2023

The role of a custodian is to hold investors’ financial assets securely in exchange for a fee and facilitate dispositions such as sale on client instruction. This example may seem simple but it involves underlying complexities including complying with the local legal frameworks applicable to the custodians as well as the CSD, “finality” of settlement at the CSD, funding, matching and corporate event management – among other things. However, despite these various complexities, a long history of market practice as well as tested legal and regulatory environments have built up over decades to provide for relative safety, efficiency, stability and predictability.

As illustrated in Exhibit 1, a custodian’s role has traditionally consisted of a combination of three main functions:

1. holding physical securities and/or records of ownership rights in dematerialized ("book-entry") securities and fiat currency on behalf of a customer as an intermediary,

2. acting on instructions to facilitate the settlement (the change in ownership) of transactions in those securities on behalf of the relevant customer,

3. facilitating the exercise of other rights and entitlements associated with ownership of such securities (such as corporate actions, e.g., voting on shareholder or unitholder resolutions) or the fulfilment of obligations (such as processing the payment of withholding taxes).

The digital asset custodian is in the crucible of the adoption of DLT in financial markets

Like traditional capital markets, the function of a DAC custodian remains constant: it is responsible for the safeguarding of an investors' assets, however, as the digital asset industry has grown, how custodians may continue to deliver their service to the standard investors and regulators expect has been subject to close scrutiny.

Broadly, there are two categories of DLT network: public networks which are open to the public, and permissioned networks that operate within a closed ecosystem. The operating models, appropriate risk and control functions and available safeguards and governance can differ significantly between these two models. Additionally, within these two categories, are many different technology protocols which can behave and perform differently to each other and must also be considered.

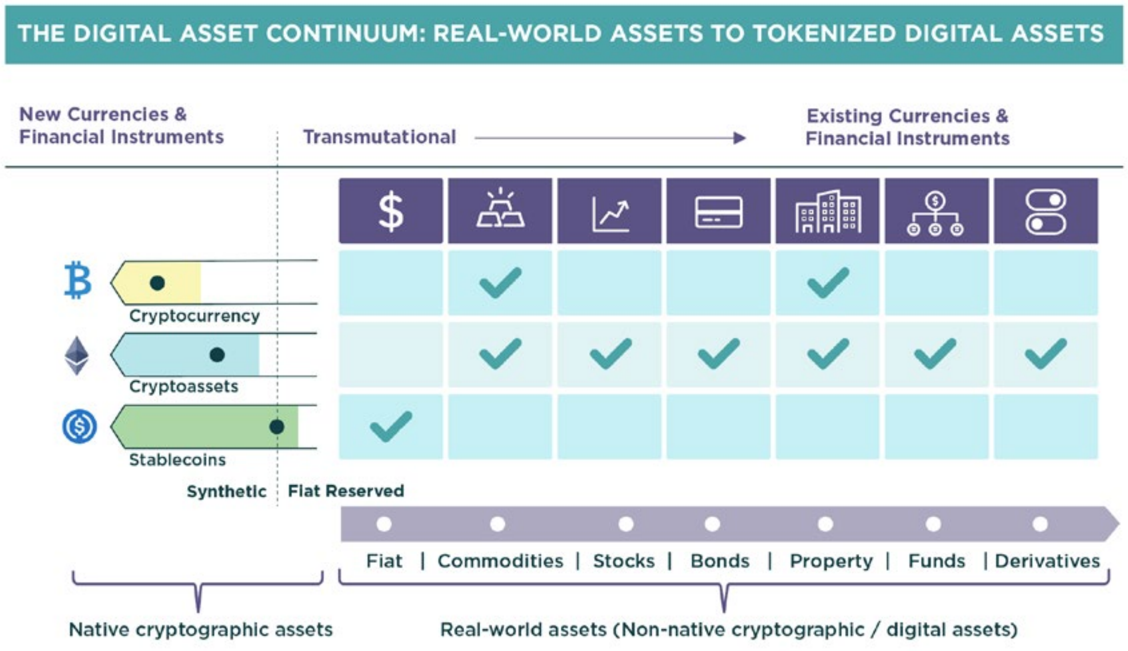
The use of the term 'DLT' throughout this report is used to denote all forms digital distributed ledgers including blockchain, mainnet, and Layer 2 solutions. The report focuses primarily on the challenges of DAC for public, permissionless blockchains unless explicitly stated otherwise.

The use of DLT is not limited to native cryptocurrencies and cryptoassets, like bitcoin or Ether, but also includes a wide variety of assets that are being represented on-chain and may not be native cryptographic assets.

Native cryptographic assets, often referred to as "cryptocurrencies" and "cryptoassets" such as bitcoin or Ethereum are issued on DLT through a "mining" and or "staking" process involving computing power, network validators, and in the case of staking, the use of collateral. Non-native cryptographic assets are "issued" using DLT typically using "smart contracts". These are often referred to as "crypto assets" or "cryptoassets", and in the case of some regulatory agencies, "virtual assets".

Stablecoins, such as USDT and USDC, which have fiat currency reserves (versus algorithm stablecoins which resemble synthetic derivatives) are an example of a non-native cryptographic asset with an underlying "real-world asset". These "digital assets" are typically constructed on DLT using a "smart contract".

Tokenized securities, such as equity and debt instruments, tokenized commodities, tokenized real estate, tokenized funds, and other representations of tokenized real-world assets, are examples of non-native cryptographic assets, that are also generally referred to as digital assets.



THE DIGITAL ASSET CONTINUUM: REAL-WORLD ASSETS TO TOKENIZED DIGITAL ASSETS

New Currencies & Financial Instruments
Transmutational
Existing Currencies & Financial Instruments
Synthetic
Flat Reserved
Native cryptographic assets
Real-world assets (Non-native cryptographic / digital assets)

	Fiat	Commodities	Stocks	Bonds	Property	Funds	Derivatives
Cryptocurrency		✓			✓		
Cryptoassets		✓	✓	✓	✓	✓	✓
Stablecoins	✓						

Exhibit 2

© GBBC Digital Finance 2023

Market Data - Tokenization Market Growth

With a variety of assets expected to be tokenized and the market for asset tokenization expected to grow exponentially, institutional investors are projected to allocate 5.6% of their portfolios to tokenized assets by 2026.[i] According to a recent survey conducted by EY-Parthenon, the global strategy consulting arm within Ernst & Young, 17% of respondents are already investing in tokenized assets, 25% planning to, and 35% expressing a keen interest in learning more about this asset class. Furthermore, 55% of the surveyed investors expressed plans to allocate funds to tokenized assets within the next one to two years.[ii]

The use of the term "digital assets" throughout this report is used to denote all forms of native and non-native cryptographic assets from cryptocurrencies to tokenized real-world assets such as fiat currencies or securities that issued on DLT (see Exhibit 2 for reference).

Exhibit 2 highlights the relationship between native and non-native cryptographic digital assets, collectively referred to as "digital assets" in this report, referring at all stages to both native and non-native cryptographic, as "digital assets", unless otherwise specifically referred to or referenced. The exception to this is non-fungible tokens (NFTs), a class of digital assets, which are not addressed in this report.

Ultimately, to fully unlock the benefits of DLT in financial markets, it is essential to implement institutional-grade custody solutions supported by arrangements that are bankruptcy remote. Growth in digital asset issuance from both public and private sector market participants is expected to further drive demand for DAC service. As a result of the high degree of variance in DLT and digital assets, custody providers must perform their own assessment on which assets, DLT networks, and technology protocols they are willing to service.

Tokenization of global illiquid assets estimated to be a $16 trillion business opportunity by 2030

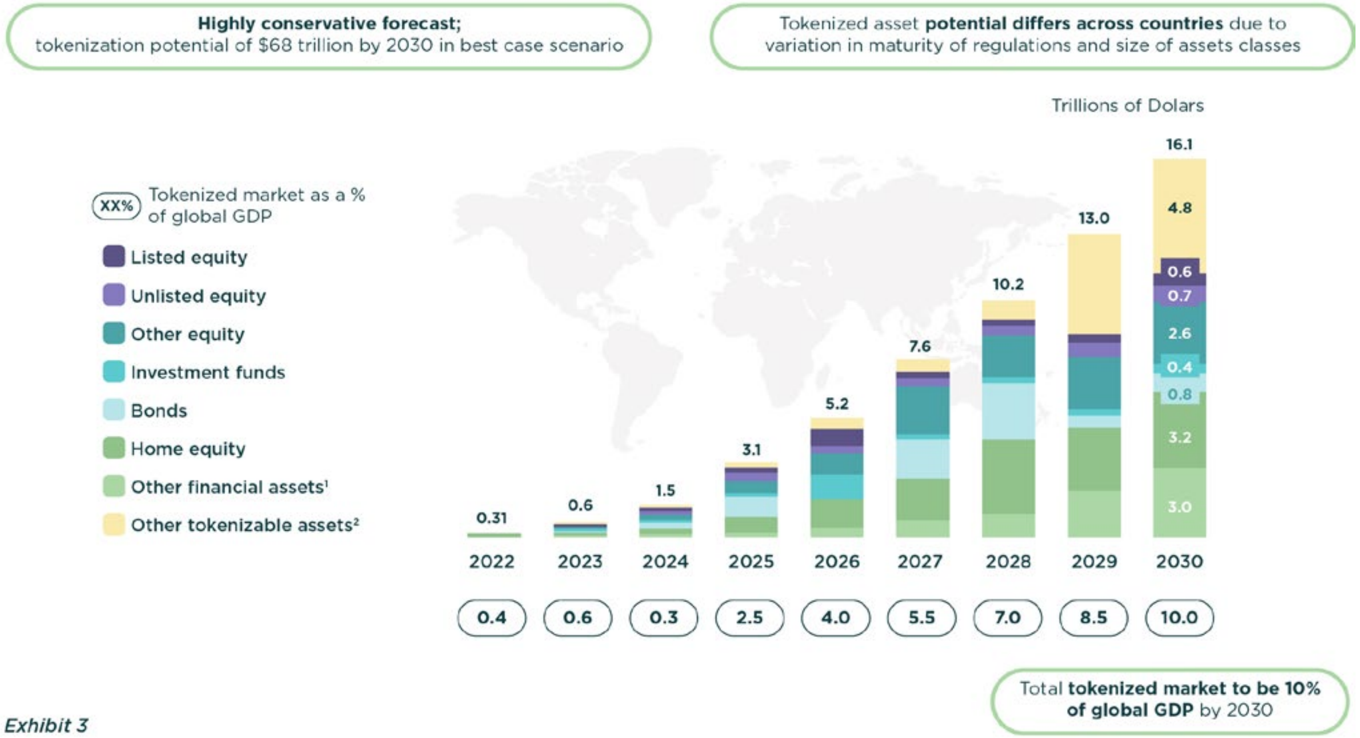


Exhibit 3

BCG and ADDX Report on "Relevance of on-chain asset tokenization in 'crypto winter', August 2022. ***Read the full report here.***

A major and further growth driver for this market depends on the industry's ability to meet institutional investors' expectations that the digital assets in their portfolio will have certainty that their ownership rights are protected and preferably the same level of protection that exists with their traditional asset classes. These investors will require to be protected through services that provide control, segregation of assets, bankruptcy protection and certainty of legal liability.

Benefits of DAC for market participants

Custodians have opportunities to enlarge the service offering for new products, as well as to offer new value-added services. This includes activities such as the development and application of smart contracts and enabling and ensuring interoperability between varying DLT networks and protocols.

Ideally, digital asset custodians (including existing FMIs) would be agnostic to specific technologies and driven by economic incentives to support a wide range of DLT networks. This characteristic positions them as ideal facilitators of market connectivity and interoperability, enabling increased scalability and seamless integration with FMIs, and playing a key role in development of any future digital FMI.

Additionally, by supporting tokens that represent voting rights, coupon payment entitlements, and more, custodians can enable workflow automation through smart contracts. This type of microservice automation could generate additional revenue, as importantly, enable new cost savings, and enable custodians to participate in upstream value generation.

For **investors**, ranging from single investors to large institutional investors, enhanced custody frameworks provide greater security and ease of transacting in digital assets. Leading custodians are attempting to address emerging considerations such as recourse for investors (subject to practical availability, legal agreements, and regulatory guidance), enhanced safeguarding (compared to digital asset exchange venues that typically have no bankruptcy remote client asset protections) and operational efficiencies in the digital assets market. Sophisticated security measures including multifactor authentication, encryption, and more, as well as regulatory compliant and accounting focused solutions will be required to drive wider acceptance of the digital asset recorded on public networks.

For **exchanges**, trading platforms and issuers of products, robust custody frameworks provide a combination of tangible and intangible benefits. Partnering with leading custodians offers exchanges increased reputational benefits with their end customers, as it assures the safe storage of assets. Integrating with custody solutions might also increase market liquidity and trading volumes for exchanges. Further, custodians might potentially mitigate conflicts of interest in certain jurisdictions (e.g., broker dealer entity also operating as custodian). Taken together, these benefits ultimately promote a fair and transparent market environment.

For **regulators** there is an opportunity to make headway in developing a robust regulatory framework for digital assets that addresses investor protection, market integrity, financial stability, compliance requirements, regulatory clarity, and international cooperation. By establishing a comprehensive legal and regulatory framework for DAC, regulators and policymakers can help foster the clarity and certainty on a global level and provide a solid foundation for the sustainable development of the digital asset ecosystem while minimizing risks and promoting responsible innovation.

Industry Challenges

The concept of DAC presents challenges to market structure, investor confidence, and regulation. The legal rights of digital asset owners pose the greatest challenge for custodians, with significant variations in approaches between civil law and common law jurisdictions. The safety of client assets requires that intermediaries follow applicable requirements imposed by law or regulation (e.g., maintenance of appropriate segregation and of appropriate levels of control), ensuring investor property can be identified as and when necessary.

Market Data - ISSA 'DLT in the Real World' Survey

A different challenge has been raised in the ISSA "DLT in the Real World" Survey and that is the one of business case. Given the competing priorities for investments is the business case of building out the new infrastructure and capabilities great enough to overcome the hurdle rates? At the moment, digital assets are relatively scarce and firms need to articulate the strategy for building the capacity to offer the service.

Access ISSA's DLT in the Real World Survey 2022 here

Digital assets and methods of transfer have struggled to integrate with existing legal systems. Each legal system, by and large, has addressed this challenge in its own way and time, thereby complicating the efforts for broader DLT acceptance as a solution to current inefficiencies. This fragmentation is likely to be problematic in the context of cross-border investments, holdings, and dispositions, especially if the law of more than one jurisdiction applies to the same investment. Unlike traditional securities there is little precedent and few recognized legal agreements to underpin the market norms.

Compliance with the evolving and often ambiguous regulatory landscape is a crucial aspect of exercising consumer protection. The structure of financial markets, combined with jurisdictional laws and regulations, and the role of custodians and market participants, contribute to significant complexity within the DLT ecosystem. Market participants will also have to assess and mitigate operational, financial, money laundering and strategic risks.

These challenges are seen in the traditional securities sphere and have largely been overcome through the creation of standards and market practices which have developed over decades. As the industry embraces technological innovation and transforms to leverage the opportunities of digital assets, there needs to be an acceleration in the creation and adoption of new standards. Until the markets and regulation for digital assets matures, caveat emptor remains sound advice.

It is also important to recognize that asset owners may have many different requirements for DAC, such as requirements for reporting and servicing of assets, digital or traditional, held by their custodians in a consolidated format. This report does not address these requirements (opportunities) nor does it address the ability of custodians to affect the transformation of traditional securities to digital assets and back again.

The transition from custody of "traditional" financial assets to the custody of digital assets has brought about a profound transformation in market dynamics. In this evolving landscape, market participants must reevaluate their understanding of the legal concept of custody as it stands today and consider three distinct types of DAC now available for investors:

- **Self-custody** - The investor is responsible for securing his own digital assets by making use of hardware, software, or paper wallets. This report does not address self-custody. There is a volume of information on this topic, which is less appropriate for many non-retail investors,
- **Third-party custody** - Investors entrust third-party service providers to safeguard their digital assets usually using institutional grade security measures,
- **Exchange wallets** - Investors give control over public and private keys to exchanges and are provided with access to a digital wallet. For an investor, this is similar in some respects to third-party custody but it involves different risks.

Purpose and structure of this report

This report endeavors to help establish a common understanding of how DAC providers may achieve investor assurance while reducing risks and increasing efficiencies though a better understanding of law, regulation, technology, and market developments.

This report will address DAC considerations relating to both, public decentralized DLT and permissioned DLT that operate within a closed ecosystem, however the principal focus of the report is oriented towards DAC on public DLT, where emerging (and required) standards are often glacial in development due to the complexities of global industry coalitions and or jurisdictional regulations.

It is broadly recognized that developments on permissioned DLT which are private networks with a level of control and governance exceeding public DLT can impose levels of standards that might expedite DAC solutions and ways of working that drive solutions that may be better aligned to investors, institutions, and regulators, particularly in non-retail markets.

The audience for this report is financial services executives, regulators, and policymakers. The report has been written to support discovery, discussion, and decisions on the topic of DAC by presenting the key concepts of DAC in relation to the key concepts of traditional custody and should be considered as a primer.

The report is a primer to help move the knowledge of DAC forward by bringing to the forefront, the opportunities and barriers DAC providers have to successfully navigate moving to these new digital technologies and ways of working.

To this end, the report covers nine factors in subsections across three section domains:

- Legal, Regulation, and Financial Crime
- Settlement & Finality, and Asset Segregation
- DLT Governance, Staking, Key Management, and Interoperability.

Each subsection is structured around four areas:

- **Factual differences –** between traditional custody and DAC
- **Risks to be addressed –** outlining the identified DAC key risks
- **Key risk mitigants –** outlining key DAC risk mitigation strategies
- **Execution barriers to risk mitigation –** outlining the identified barriers to DAC risk mitigation.

A fourth section 'What Asset Owners Should Expect' outlines consideration for asset owners as the evaluate their requirements for digital assets and DAC.

The subject of traditional custody has its complexities, as does the subject of regulated financial services. Adding to these two dimensions to new digital technologies such as DLT, cryptography, and digital assets, and, oftentimes unaligned, emerging jurisdictional regulations, makes DAC a very wide and seemingly complex topic. This presents nmany new risks to custodians, particularly from the perspective of serving investors in regulated markets.

The report has been sponsored by GDF and the ISSA with members of GBBC / GDF and ISSA coming together in a DAC Working Group to provide input in workshops, discussions and bilateral calls. The member Working Group co-chairs Brown Brothers Harriman, Metaco, and State Street have provided the content leadership and guidance, supported by the member Working Group Secretariat Deloitte, who held the pen for the creation of the body of the report, with final editing provided by the GDF and ISSA Secretariat members.

The views expressed and information set out in this report are the views of GBBC Digital Finance and International Securities Services Association and do not represent the individual views of specific member firms of contributing authors and chairs. The content reflects a broad range of experience and views communicated by individuals who occasionally disagree or have different views and opinions on the topic of DAC, as to be expected.

The content of the report has been curated by the co-chairs, the Secretariat and the Sponsors to incorporate individual views and opinions, where possible, and includes input from extant publicly data available on DAC best practices. All efforts have been made to ensure the report content is accurate.

Many industry practitioners believe that as these new digital technologies mature, in line with practitioner experience of working with these technologies, industry practitioners will converge on policy, operational and technical standards to ultimately, deliver the highest level of custody services to investors, counterparties and partners. ■

LEGAL, REGULATION, AND FINANCIAL CRIME

Legal

Factual differences

An understanding of "custody" of financial assets requires a foundational appreciation of how law and regulation underpin the application of "property" rights of asset owners. This is so not just in the traditional financial services sphere but equally in the digital asset environment.

Property tends to be categorized either as tangible (i.e., in physical form, such as materialized / certificated securities, precious metals, and the like) or intangible (e.g., in dematerialized or in uncertificated form, such as so-called "book-entry" securities). An individual's property rights in an asset are generally enforceable as against the whole world, whereas "contract" rights (e.g., OTC (over-the-counter-) derivative instruments, repurchase agreements, loans, etc.) are supported in the law only by and between the parties to the contract. Risks, rights and obligations of asset owners and others – which vary depending mainly on this distinction in legal characterizations - crystalize most visibly in the crucible of insolvency.

Before investing in a financial asset, it is therefore crucial to understand whether there are enforceable property rights in that asset. Characterization as "property" is particularly important in the event of the insolvency of a service provider or counterparty since proprietary rights that have been made effective against third parties are generally effective against creditors and an insolvency representative[2], where investors generally will be given priority over claims from third parties such as creditors. In addition to the investor having property rights in particular identifiable financial assets, it is also crucial that the service provider / counterparty effectively "segregates" the financial asset from its own assets in its books and records (such segregation is referred to in this report as "bankruptcy remoteness").[3]

The identification of enforceable property rights ("ownership") in an asset requires meaningful specification of the asset, which can be through the books and records of an intermediary, as well as the basis upon which the property right may be asserted. Where the property is intangible, a contractual arrangement is needed by which a custodian undertakes to hold and maintain the property on behalf of the investor, as well as clarity regarding which jurisdiction's law governs the arrangement and recognizes the existence of the asset and the client's property right in it.

The decentralized nature of the DLT on which digital assets are created can make it more challenging to determine the jurisdiction whose laws are relevant – or binding – with respect to these important questions. The novel nature of the constitution of some digital assets, and in some cases the pseudonymity of users, means that legal tools for recognizing ownership rights in those assets, and the mechanisms for transferring those rights to another person, may need adaptation, which has been an effort undertaken by legal bodies.[4] These complexities increase where the laws of more than one jurisdiction apply.

[2] *See,International Institute for the Unification of Private Law ("UNIDROIT"), Principles on Digital Assets and Private Law (Approved 12th May 2023) (the "UNIDROIT Principles"), Principle 19. Available at: https://www.unidroit.org/work-in-progress/digital-assets-and-private-law/*

[3] *The UK Law Commission, providing a detailed assessment of insolvency aspects in its recently published report on digital assets under the law of England and Wales, explained: "In a custodial intermediated holding arrangement involving segregated assets held in their totality on trust for (or otherwise subject to the superior title of) a third-party beneficiary or superior title holder, a custodial holding intermediary's general creditors will have no claim to those assets at all." UK Law Commission, Digital Assets: Final Report, Law Com No. 412 (2023) (the "Final Report"), Para. 7.26, p. 153. Available at: https://www.lawcom.gov.uk/project/digital-assets/*

[4] *Most notably UNIDROIT, the Hague Conference on Private International Law ("HCCH"), the U.S. Uniform Law Commission and the UK Law Commission.*

Where digital assets may be maintained and accessed using DLT but in more familiar frameworks – such as where there is a centralized governance via market infrastructure (e.g., a "permissioned"/"private" network) – the identification of property rights similarly will follow more familiar – and more settled – legal principles.

Custodial and client assets should be segregated to mitigate risk. Where segregation is not achieved, ensuring the bankruptcy remoteness of digital assets becomes more challenging, as the custodian may hold identical or similar assets for its own account, potentially commingling them with those of their clients.[7] This can arise for different reasons, including DLT's facilitation of continuous, round-the-clock execution of transactions, which means that updating of off-chain accounts and the performance of reconciliations not be in synch with what is reflected on the distributed ledger at a particular point in time.[8] Other complexities may be introduced, such as where commingled wallet addresses are utilized or staking, with intermediaries potentially taking proprietary positions themselves.

Understanding whether a particular digital asset in question constitutes "property", which offers the foundational advantage of providing for insolvency remoteness under the law, or whether it represents a "personal" claim, in which case the investor is left exposed to the creditworthiness of the party against whom it would assert the claim is a foundational element for any service provider seeking to provide DAC. A corollary to this first step is that, even if the asset is considered "property", it is also necessary to identify the party against whom a proprietary claim would be asserted, i.e., the "custodian" or other intermediary maintaining the asset as intangible property on an "insolvency remote" basis. This is because DLT offers the prospect of conferring property rights without a "custodian" as commonly understood in the traditional finance world[9], or conferring property rights in ways that are different from traditional approaches (e.g., focusing on control of private keys as a means of determining against whom a property right should be asserted).[10]

Regulatory Insights - UK vs EU Treatment of Tokenized Securities and Financial Instruments

Tokenized securities, for example, may be "opted in" to be treated as "securities entitlements" consistent with book-entry securities maintained by securities intermediaries in the United States. The UK Law Commission and UK Jurisdiction Task Force have made a similar distinction between those tokenized financial assets that may be treated as intangible property ("choses in action")[5] under existing English legal principles versus those that would be treated as a new form of property right ("digital objects"). The EU has also distinguished between cryptoassets falling under the Markets in Cryptoassets regulation (MiCA) versus tokenized "financial instruments" that instead will fall under the DLT Pilot Regime (under which DLT "market infrastructures" will provide the kind of centralized governance mentioned above).[6]

[5] "Legal rights (as opposed to digital objects) that are created within private, permissioned blockchain or DLT-based systems or multi-lateral contractual frameworks will be treated as things in action by the law." Final Report, para. 4.26(3), p. 64.

[6] While MiCA sets out a framework for the issuance, trading and "custody" currently largely unregulated crypto-assets, the DLT Pilot Regime seeks to provide a regulatory sandbox for specific authorizations for the trading and settlement of financial instruments (i.e., investments that would otherwise be regulated under MiFID as "financial instruments") that are based on distributed ledger technology ("DLT").

[7] Indeed, as the UK Law Commission further explained in its Final Report: "… where more complex structures are deployed, such as funds of commingled holdings held on behalf of a number of third parties and the intermediary itself, a portion of the value of such holdings representing the holding intermediary's co-ownership entitlement can fall into the bankruptcy estate and be subject to claims of general creditors." Final Report, Para. 7.26, p. 153.

[8] It should be noted that, even today, traditional custodians tend to consider their books and records not to be "final" until end-of-day processing has run its course following necessary reconciliations through the chain.

[9] Indeed, this is one of the main reasons why the UK Law Commission has recommended a "new" form of property right: a "digital object": the Law Commission explained that a new category or property is needed where there is no legal claim by a property holder against another legal person and which would exist "even if the law were to fail to recognise them as objects of personal property rights and even were a law to prohibit their existence", e.g., crypto-tokens native to the blockchain. Final Report, Para. 3.34, p. 42. An extreme example would include "digital bearer bonds". Id., para. 4.59, p. 75.

[10] [See, UCC Art. 12, UNIDROIT Principles, MiCA]

These crucial distinctions are most evident in most major markets, with consequences for investors in the context of insolvencies of platforms or intermediaries. The nature of the risk to which investors may be exposed must be clear and predictable under identifiable applicable law. Recent market events, and regulatory reactions to these events, bear out the importance of this.

Risks to be addressed

Asset ownership - difficulty or inability to demonstrate proprietary rights or undertake owner actions such as the exercise of rights or disposition (e.g., sale, pledging as collateral, etc.).

Gaps in bankruptcy remoteness - if assets are treated as part of the custodian's estate in the event of the custodian's insolvency, the asset owners will be treated as creditors of the custodian.

Business risk profile adjustment - Custodians will need to manage changes to their business risk profile in jurisdictions where the law imposes a different level or scope of liability for loss of client assets. This issue arises in the EU under MiCA which sets out a specific liability for custodians in the event of loss of client assets - custodians will need to understand and take new types of steps to prevent loss of digital assets when providing custody services to which MiCA applies.

Potential risk mitigants

The concept of control is recognized as a crucial common thread helping to determine whether any asset, regardless of technology employed, should be considered held in custody or not by a service provider. A service provider that is exercising control over the asset to the exclusion of others is generally acknowledged as having "custody" of the asset, and a transfer of such control to another is generally considered dispositive ("final"), so long as good-faith acquisition requirements are satisfied.

Often assets may be recorded in a service provider's books and records as an accommodation to an investor, not as a record of ownership or legal entitlement that can be asserted against the service provider as a "custodian" per se. In these cases, the investor usually has a contract claim against a counterparty (e.g., in the cases of over-the-counter (OTC) derivative instruments, investments in loans, repo arrangements, etc.). Here, the service provider lacks control, since these arrangements by their nature are bilateral between the investor and the counterparty, and there is no proprietary right to begin with in any case.

Regulatory Insights - Legal Developments in Luxembourg

By way of example, Luxembourg modernized its law with the Law of 22nd January 2021 on DLT[iii] and issuance of dematerialized securities by allowing for the issuance and recording of dematerialized securities through distributed ledgers / databases and creating the concept of an "Issuance account" under the 2013 Law. These developments proved immediately valuable, particularly in the context of issuing tokenized securities, in effect recognizing them as assets with assertable property rights.

Digital assets offer the prospect of a wider range of ways in which custody – or non-custody record-keeping and asset-servicing services - can be provided, with the potential for offering more variations. In the digital sphere, much depends on where exclusive control may or may not apply, with significant implications for both investors and service providers in terms of risks taken and protections available.

The question of which national law applies in a given scenario has proven to be the most difficult aspect that legal bodies such as UNIDROIT (International Institute for the Unification of Private Law) and the HCCH (Hague Conference on Private International Law) have had to grapple with. To a large extent, this depends on the type of ownership right: a consequence of "traditional" property is that – by definition – it has a location. Generally, almost all legal disputes identify the legal regime that applies with reference to the location of the property. Determining the location of property, however, is not entirely straightforward where the property is intangible. This has been the case for so-called book-entry securities long before DLT came on the scene. It is a question that national legal systems have each been trying to address with varying success for decades.

Nevertheless, acquirers of assets expect and believe that they can obtain exclusive rights with respect to a digital asset. UNIDROIT has attempted to address requisites of control in the Principles, namely in Principle 6, by providing that a person has control of a digital asset if (subject to certain exceptions) if the digital asset, or the relevant protocol or system, confers on that person:

i. the exclusive ability to prevent others from obtaining substantially all of the benefit from the digital asset

ii. the ability to obtain substantially all the benefit from the digital asset

iii. the exclusive ability to transfer the abilities mentioned in (i) and (ii) to another person (i.e., a change of control).

The digital asset, or the relevant protocols or system, must also allow that person to identify itself as having the abilities set out in (i), (ii) and (iii) above. However as long as key concepts are not aligned with existing notions, the co-existence and application of these principles could appear to be difficult. Control is to be understood as being a functional equivalent to possession. The situation is more complex as the notion is fragmented among national laws, refers to different criteria and cannot be limited to possession aspects. The debate co-exists with the differences between civil law and common law jurisdictions.

Regulatory Insights - UNIDROIT Principles

The UNIDROIT Principles are intended to facilitate harmonization of national law approaches regarding digital assets. Under the Principles, a digital asset is defined as 'an electronic record which is capable of being subject to control' – terminology which is intentionally ambiguous in order to ensure technological neutrality. However, due to the lack of a precise definition of a digital asset – as compared to MiCA or the notion of financial instrument under MiFID - there is no clear view on the type of assets that may fall within the scope of the UNIDROIT Principles and this is why there is still a debate.

Under the UNIDROIT Principles, it is recognized that a digital asset may state that it is linked to another asset such that any acquisition of it can be taken free of claims by third parties. This will largely depend on national law (the "Other Law of the State"). Consequently, the link between the digital asset and the other asset may vary depending on applicable law. This has significant consequences for asset owners and for custodians who provide asset servicing relating to a digital asset: not all states will provide for rights linked to the representation of an asset on the digital ledger in the same way. Consequently, asset owners and custodians may need to understand which law applies for this purpose, and whether the investors' rights associated with underlying assets also arise (or not) as a matter of law.

Ongoing legal reform is required, but it is equally important that investors develop a better understanding of how a custodian's contractual terms of service could impact their rights. Investor asset protection might improve if the insolvent intermediary is a bank, broker-dealer or CSD, since the applicable insolvency regimes are particularly engineered with this in mind.

Execution barriers to risk mitigation

Uncertainty around the effectiveness of asset segregation in protecting clients' rights to the asset in case of the default of a custodian (or purported custodian) is a major concern that could erode the trust of investors. A common understanding of segregation requirements that are effective under the law – especially in terms of protecting investors' ownership interests in the insolvency of a service provider – is therefore needed.

More broadly, it is essential that policymakers, regulatory authorities, and legislators are mindful of the risks of inconsistencies with other legal systems. Resolving uncertainty regarding choice of law – taking into account the overarching goal of technology neutrality – will foster cross-border interoperability and investment.

It is generally recognized that private law, commercial law, contractual law, and securities law have been fragmented for decades. The legal industry - from regulatory bodies to industry participants - should continue to work together with industry bodies and independent and non-governmental agencies, to identify the barriers to adoption, that new principles may cause, and suggest solutions to those issues. The UNIDROIT Principles are one example of a program that organizations might consider engaging with, as they set out to establish a conceptually sound set of principles for all jurisdictions to apply. ■

Regulation

Factual differences
Providers and users of DAC services face three key challenges:

1. **The differences in asset definition –** for example, the same asset viewed as a different asset class (e.g. a security) or something else in another jurisdiction, or in even within the same jurisdiction,

2. **The location-specific regulatory compliance obligations –** for example, challenges understanding obligations or achieving compliance in relation to specific locations of activity,

3. **The overall impact of regulatory incompatibilities or inconsistencies between jurisdictions.** As a result, this poses additional challenges for service providers who need to meet multiple requirements simultaneously.

For regulators, depending on the assets in question there could be potential structural differences in the way various market participants may want to interact with one another. For example, depending on market developments, there could be fewer intermediaries in the digital securities value chain. Regulators must grapple with how new governance, potential market structure changes and interaction models underpinning digital securities may evolve.

Risks to be addressed
There is currently a lack of clear interoperable regulatory frameworks for digital assets on a national and international level. Without progress, a patchwork of regimes, approaches and protections for investors and their assets will remain. By way of example, digital assets may be mis-classified where there are differences in classification taxonomy among jurisdictions.

Traditional regulation cannot be seamlessly applied to these new technologies and digital assets due to key differences in the process lifecycle of a product. For example, the potential 24/7 nature of DLT means there is often not a natural start and end-of-day position to record and reconcile balances. This raises questions regarding standardized processes such as regulatory reporting.

Regulatory Insights - Guidance of Supranationals on National Regulatory Authorities

Some regimes such as the EU DLT Pilot Regime[v] and the UK's forthcoming Digital Securities Sandbox[vi] aim to try to understand in greater depth whether and how some of these arrangements could work and how best to regulate them – including which participant(s) should take primary responsibility for the various aspects of the infrastructure, activities and services that constitute and support those arrangements.

Bodies such as the International Organization of Securities Commission (IOSCO) and the Financial Stability Board (FSB) recently have issued proposed recommendations and frameworks for guidance to regulatory authorities.[11]

[11] *[See IOSCO Consultation https://www.iosco.org/library/pubdocs/pdf/IOSCOPD734.pdf; and, FSB Global Regulatory Framework for Crypto-Asset Activities - https://www.fsb.org/wp-content/uploads/P170723-1.pdf]*

The specific characteristics of public DLT networks can lead to unique risk scenarios. For example, a significant DLT network fork event would have a considerable impact on asset ownership rights, and more work is needed to outline the practical response required of custodians in the event of a fork. The anonymity of ownership of some cryptoassets may also result in a range of risks that cannot be controlled using traditional control mechanisms (more information on this topic can be found Section 1.3.)

Potential risk mitigants

Regulatory framework enhancements

Regulatory frameworks for financial services are taking time to adapt to a new paradigm created by digital assets that will continue to change and evolve further. To close particularly high-risk regulatory gaps, authorities have prioritized:

- Denying the use of cryptocurrencies by bad actors / politically exposed persons (PEPs) as a means of bypassing AML and Counter-Terrorism Financing (CTF) regulation
- Addressing fraud involving cryptoassets by increasing enforcement and imposing strict regulatory requirements and limits to protect consumers
- Imposing licensing or authorization frameworks on those providing access to DAC services and investments, to bring these actors under regulatory supervision.

Regulatory Insights - SEC and EU Approaches to Supporting Investor Protection

Legislators and regulators have taken steps to place obligations on digital asset custodians to support investor protection:

On 15th February 2023, the SEC proposed a major overhaul of the investment adviser custody rule. This included a requirement that all assets – including digital / cryptoassets – that are subject to an investment adviser's investment discretion must be held with certain Qualified Custodians (which extends to "Foreign Financial Institutions" located outside the United States) who must ensure that such assets are 'clearly segregated from the bank's assets and easily identifiable as the client's assets.'[vii]

Meanwhile, in the EU, a distinction is made between assets which will fall within the new MiCA and those that will not. A consequence of MiCA's carefully drawn scope is that tokenized assets that may still be considered MiFID Financial Instruments are likely to be addressed using existing regulations and more traditional principles. Meanwhile MiCA explicitly recognizes some of the technological differences in the cryptoassets it covers, by providing for the custodian's liability for failure to perform or for failure to protect investors' rights and entitlements in an asset. Article 67 of MiCA provides that cryptoasset service providers ("CASPs") must take *'all appropriate measures to prevent the loss of, and ensure the safe return of, their clients' crypto-assets or means to those crypto-assets.'*[viii] The way in which important regulatory questions are addressed will impact on the interest from established institutional custodians to offer services in the relevant jurisdictions.

Clarifying custodian obligations in respect of digital assets

Safeguarding is a key obligation that custodians are required to satisfy. As described in the Legal Chapter, there are a range of complexities involved in ensuring the legal rights of digital asset owners. However, a common denominator is that a custodian is, at a minimum, expected to exercise reasonable skill and care in the safe custody of an investor's rights in their financial asset.

Determining whether certain risks are within the control of a custodian can be challenging in the context of digital assets on public DLT, because their operational performance partly depends on the distributed network. There are many complexities for custodians to consider, such as the effects of network congestion on transaction cost and confirmation time, or delays caused by technical considerations outside the scope of custodian control. Similarly, it is possible for erroneous actions to result in irrecoverable loss of assets. Whilst the outcome of a transaction can be checked and many failure scenarios identified in advance, the extent to which such checks should or must be performed by custodians (or other parties that may be in a position to do so) is unclear. This is due to the uncertainty of the existing custodial regulatory frameworks applicability to digital assets recorded on public DLT networks.

The challenge for regulators Is (as ever) in finding the balance between the exercise of control and investor protection on the one hand, and the need for an agile, innovative, and competitive marketplace on the other. Yet the recent failures of some digital asset service providers have demonstrated the need to close the gaps in areas where regulatory guidance is needed. The industry can play a part in identifying and self-managing these complexities by striving to address new and nuanced risks within counterparty contractual arrangements, so that expectations and risks are increasingly managed, and the corresponding risk of disputes is diminished.

Collaboration between regulatory bodies and digital asset custodians will help streamline enforcement and prevent non-compliance, while still allowing for innovation in the financial sector. There are a number of industry-led initiatives and standards emerging to address these challenges. These initiatives include:

- Industry bodies that promote higher standards of conduct for cryptoassets,
- The Bank of International Settlements (BIS) conducts extensive research to publish reports in collaboration with Tier1 Banks and Central Banks,
- Consultations issued by bodies like ISOCO and the FSB that invite stakeholders in the ecosystem to comment on proposed recommendations.

Execution barriers to risk mitigation

A lack of alignment from regulators and legislators in key jurisdictions, for example, the US (emerging), the UK (emerging), Europe (MiCA), Dubai (VARA Framework) etc.

Inherent anonymity in ownership of some digital assets, particularly native cryptocurrencies on public DTL such as bitcoin (on the Bitcoin Network).

The Impact of DLT forking on asset ownership rights and obligations and the practical responses required to investors and partners from custodians in the event of a fork.

The inability of a custodian to have exclusive control over assets on public networks due to the complexities of digital asset classes and or smart contracts, and the wide range of decentralized and mostly anonymous market participants. ■

Financial Crime

Factual differences

As with traditional financial services, the provenance of the identity and beneficial owner of a digital asset must be assessed in accordance with the same KYC / AML / CFT standards, including sanctions screening. In the case of private, permissioned DLT networks. It is of critical importance that users and commercial partners of the DLT network confirm that the appropriate KYC / AML / CFT standards and sanctions screening are in place and in line with the requirements outlined below. For public DLT networks, it is imperative that users and commercial partners understand the risks.

Consideration must be given to new requirements such as crypto sanctions and the new Financial Action Task Force (FATF) "Travel Rule" requiring CASPs to exchange customers' personally identifiable information (PII) before or concurrently with a transaction. FATF 2021b, updated the scope of standards and updates to include stablecoins, decentralized platforms, peer-to-peer (P2P) transactions, self-hosted wallets (also known as unhosted or non-custodial wallets), and the Travel Rule[ix].

It is important to note that the FATF travel rule is applicable to only cryptoassets and stablecoins and not tokenized securities.

The unique difference compared to traditional assets is the requirement to Know-Your-Asset (KYA). This describes the identification, recognition, and specification(s) of the underlying digital asset, from native cryptographic digital assets, such as cryptocurrencies, to non-native cryptographic digital assets, such as tokenized real-world securities including its antecedents – see Exhibit 4 for reference.

Risks to be addressed

Consequently, organizations providing DAC services must address new risks within the scope of existing KYC and AML obligations. Some of the leading non-compliance risks that custodians will need to navigate are:

- KYC - Implementation of KYC processes and controls for clients that hold digital assets along with existing procedures and control frameworks will be key for custodians. Additional considerations to be raised include the sufficiency of current customer identification requirements and the potential need to review on-chain activity and wallet addresses prior to client acceptance

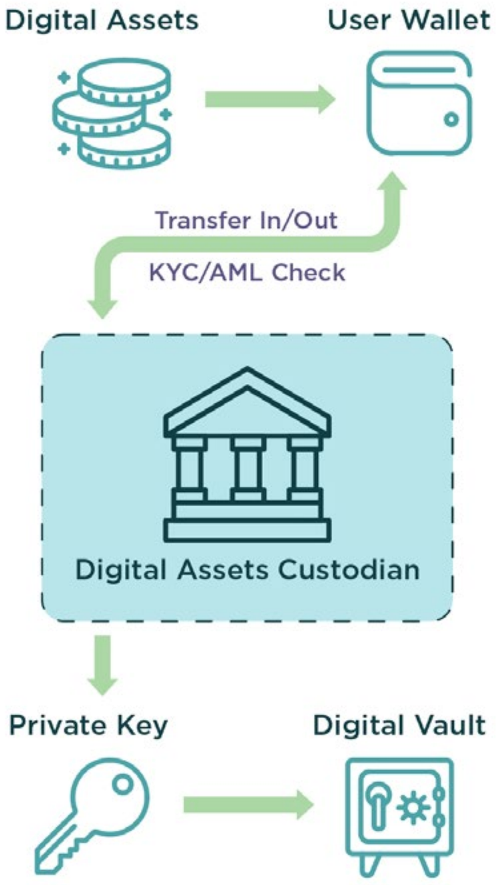


Exhibit 4

© Deloitte 2023

- **AML / CTF -** The combination of public DLTs and the diversity of the assets in themselves make AML obligations for digital assets difficult to implement. Custodians of digital assets have a responsibility to meet AML / CTF/ BSA and transaction monitoring obligations and to ensure that these processes are scalable, are occurring in near real-time, and that they are able to report suspicious activities to the relevant authorities per the jurisdiction's requirements

- **KYA -** Digital assets cannot easily be defined without specifying the network on which they reside (e.g., bitcoin on the Bitcoin Network is as different to a tokenized bitcoin on Ethereum akin to the difference between two different to an asset and a derivative of that asset). Whilst there are token standards (e.g., ERC20), they are not subject to the same controls concerning a securities issuance. This presents the need for custodians to perform digital asset assessments, in order to verify the asset they are holding. At present, there appears to be no specific regulatory requirements requiring a digital asset assessment for custody

- For some public DLT networks there is a **sanctions risk in the context of transaction fees -** Originators cannot predict which miner will be selected to confirm their transaction. There is uncertainty as to whether this fact could be seen as facilitating financial transactions with sanctioned parties in violation of the law if it turns out after the transaction was settled that the miner was a sanctioned party. Transaction fees do not create a direct payment from the initiator of a transaction to a miner. Whether this represents sufficient control is somewhat uncertain, but resolving this issue is critical to allow regulated financial firms to participate in this market

- **Overall monitoring and reporting -** A custodian might be unable to effectively monitor and detect suspicious transactions due to low maturity of AML monitoring tools in the market. As a result, this would affect the type and quality of data used for reporting back to the relevant authorities, however there is much more data available in DLT flows than in conventional flows. The chain is accessible to all, and data is available so the maturation of the tooling is likely to improve the situation.

Potential risk mitigants

The custody industry has a long and rich history in the development of best practices. To achieve a similar maturity in the digital asset market, the industry must focus on further education and expertise building:

- **Industry-wide wallet matching solutions** - The pseudo-anonymity of transactions in permissionless ecosystems creates not only AML challenges but also transaction processing risks. There are no specific entry controls determining participant access, which is one of the main AML concerns. This structure means that counterparty relationships cannot be completely mapped out within DLT networks, since off-chain activity is required to exchange such details at present. The industry needs a vendor agnostic method to exchange wallet addresses and confirm real-world identities.

- **Vendor solutions -** SMPG to support the effort, new vendors are emerging that provide on-chain transaction monitoring, identify wallet addresses and deploy behavioural analytics to determine illicit activities, such as money laundering, or other criminal activities. Additionally, many agencies have started to publish digital asset wallet addresses alongside real-world legal identities. Full-scale integration with existing compliance monitoring processes will be key to ensuring a robust process is in place to satisfy regulatory expectations and investor protection.

Execution barriers to risk mitigation

There are a variety of factors that make it difficult to perform these risk mitigations, including unclear and opaque address ownership, which can make it difficult to perform KYC checks. This lack of clarity extends to other issues, e.g. block miners may reside or operate in sanctioned jurisdictions, which could create further legal or regulatory issues and users who repeatedly change wallet addresses to hide their identity.

Today custodians can comply with KYC / AML rules as the beneficiary information travels with the instruction or is rejected for cash payments. Bitcoin, for example, does not require the beneficiary information but rather a wallet address and hence intermediaries in this value chain may not know the beneficiary. The requirements are addressed through the Travel Rule, changes but must be implemented properly.

Regulators have interpreted and applied the Travel Rule differently. Many jurisdictions have varying approaches to monitoring thresholds, Virtual Asset Service Provider (VASP) due-diligence, beneficiary customer information and transactions to / from non-custodial wallets.

If the beneficiary VASP or custodian is not ready to receive Travel Rule transfers, originator VASPs may not be able to comply with Travel Rule obligation, i.e., sending the required originator and beneficiary information alongside each transaction. So, depending on the VASP's policies and individual jurisdictional regulatory requirements, VASPs and custodians may not be able to process such transactions in a compliant manner. ■

Regulatory Insights - Travel Rule

Several global regulators, following the FATF guidance, stipulate that VASPs must transmit Travel Rule messages with any transaction over $1,000 involving another VASP. In contrast, current U.S. rules set the Travel Rule threshold trigger at $3,000 while some jurisdictions do not specify any transaction threshold figure. Additionally, the Travel Rule enforcement date has varied across jurisdictions: South Korea enforced it in March 2022 while jurisdictions such as Singapore began enforcing it in January 2020.[x]

Legal, Regulation, and Financial Crime
Key Takeaways

- Understanding custody of financial assets - both in traditional finance and the digital asset sphere - requires a grasp of how legal frameworks underpin property rights.

- Assets are categorized as tangible or intangible, with property rights having broad enforceability, while contract rights are limited to involved parties. These distinctions gain significance in insolvency scenarios, where investors typically have priority over creditors. Digital assets introduce complexity, potentially necessitating legal adaptations, especially in multi-jurisdictional contexts. Policymakers, regulatory authorities, and legislators must be vigilant about the risks of legal inconsistencies as the industry expands.

- Providers and users of DAC services face challenges related to varying asset definitions across jurisdictions, location-specific regulatory compliance requirements, and the lack of clear interoperable regulatory frameworks for digital assets on a national and international level, making it difficult for service providers to meet multiple requirements simultaneously.

- Adapting traditional regulations to digital assets presents difficulties due to differences in product lifecycle processes, notably the continuous operation of DLT networks. This raises questions about how to apply regulatory reporting and accounting practices effectively. Public DLT networks further introduce unique risk scenarios related to blockchain forks and the anonymity of cryptoasset ownership, necessitating the development of novel control mechanisms. Regulatory frameworks need to evolve to address these complexities, striking a balance between control, investor protection, and fostering innovation. Industry participants can also mitigate risks through contractual arrangements to manage expectations and minimize disputes.

- Digital asset custodians face several financial crime considerations, including the need for robust KYC processes, challenges in implementing AML, CTF, and BSA obligations, the necessity of performing digital asset assessments, potential sanctions risks related to transaction fees, and difficulties in monitoring and reporting suspicious transactions due to the limited maturity of AML monitoring tools.

SETTLEMENT, FINALITY, AND ASSET SEGREGATION

Settlement & Finality

Factual differences

Providing custody services generally refers to an agent or trustee safeguarding assets and preventing such assets from being stolen, lost or damaged. Closely linked to this are settlement and asset servicing, which might involve facilitating the settlement of purchases and sales as well as payment of interest income, dividends and withholding taxes.

Settlement finality is a legally defined concept used to represent the point at which the transfer of an asset is irrevocable. This ensures that transactions will, at some defined point, be complete and not subject to reversal even if counterparties to the transaction go bankrupt.

The associated risks of settlement generally span counterparty, liquidity, operational and legal considerations. In the world of DLT, the point of settlement finality might not be as evident and can lead to a mismatch between the operational and legal finality on a payment infrastructure operated within a given jurisdiction, introducing ambiguity. Within public DLT systems mainly used for cryptoassets, transactional information is first validated, then proposed within a block to network nodes, and finally accepted by network nodes, which then validate the next block.

The formation of a clear, technically specific 'point of finality' within such systems requires a custom approach that reflects the technical procedure involved and is capable of accommodating 'features' within the consensus process. For instance, this would include chain-tip reorganization, where a transaction may be validated by one node, accepted by a majority of network nodes, and may even be followed by new valid blocks, before being undermined and discarded during a chain re-org event (if another competing and 'preferred' series of valid blocks is discovered by a majority of network nodes).

It is worth noting that private permissioned DLT networks which tend to utilize more centralized consensus models and are far more comparable to model traditional settlement and finality rules, since the scope for competing validator updates and uncertainty of settlement finality timing and occurrence is greatly reduced.

Settlement finality holds significant importance in traditional securities custody, but the process differs for digital asset transactions as they go through various stages, starting from initial submission, then block inclusion, and ultimately reaching block finality, i.e. the transaction is no longer able to be reversed. Reconciliation processes need to clearly map to these states, which can widely vary depending on network protocols. Traditional markets have conventions such as Securities Market Practice Group (SMPG) market standards on how to deal with pending transactions.

Regulatory Insights - SEC Approach to ATSs

In September 2020, the SEC issued a no-action letter allowing registered alternative trading systems (ATSs) that settle trades involving digital asset securities to simplify the process for subscribers, allowing them to send their order to the ATS, and simultaneously send conditional settlement instructions to respective custodians if a match is made. Requiring buyers and sellers to send a separate instruction to their custodians after the match was cumbersome for ATS subscribers, increasing operational and settlement risks.

This approach echoes practice in traditional markets and whilst such guidance has been beneficial for the nascent digital asset industry, it also underscores that there is much to gain through re-use of existing, established process where appropriate.

The varying technical standards through which block authorization and settlement are achieved for different assets/chains can provoke further operational considerations:

- Private chains generally (and a small number of public chains) ensure absolute finality through semi-centralized control processes and the "Rulebook". The Rulebook refers to a set of regulations that govern and define the process and principles of settlement finality, outlining the specific procedures, standards, and rights involved in ensuring the conclusive and irreversible nature of settlement transactions in a given context,
- The Ethereum network's consensus mechanism incorporates a concept of finality through a formally defined process, roughly 15 minutes after block validation, when two thirds of the validators have agreed. Here finality is referenced from an economic and/or computer science point of view which does not necessarily equate to the definition in traditional markets which is predominantly a legal interpretation,
- The Bitcoin Network uses 'probabilistic finality', a concept of ever-increasing finality confidence which differs from classic absolute finality, and through which a transaction is generally considered final after 6 further blocks have been added to the chain. This is not defined by the Bitcoin Network, but rather the participants estimate that after 6 blocks, the probability of a re-org is too low to occur. This number could change (like it did from ETH, where it moved to 50).

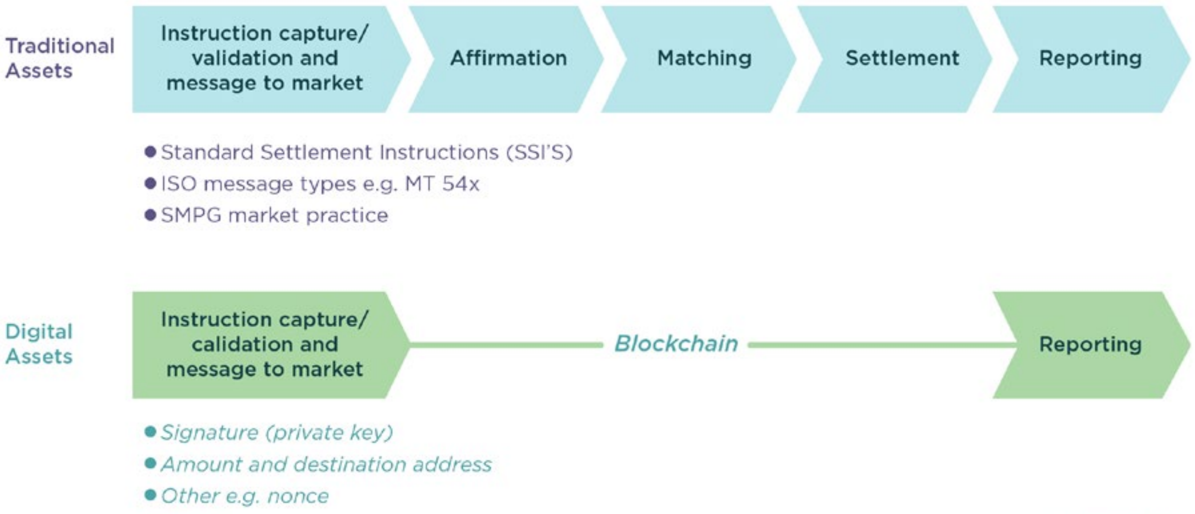

Traditional Assets
Instruction capture/ validation and message to market
Affirmation
Matching
Settlement
Reporting
● Standard Settlement Instructions (SSI'S)
● ISO message types e.g. MT 54x
● SMPG market practice
Digital Assets
Instruction capture/ calidation and message to market
Blockchain
Reporting
● Signature (private key)
● Amount and destination address
● Other e.g. nonce

Exhibit 5

© Deloitte 2023

Delivery versus payment settlement within a blockchain for digital securities involves the exchange of the digital security in return for cash or a cash equivalent token. The management of settlement requires the availability and liquidity of both the security and cash token. This may require the on-ramp of the asset or cash onto the ledger (if they exist on externally held accounts) and the off-ramp of the asset or cash from the ledger.

When it comes to custody, the complexity relies on the organization (the custodian) that must transfer the representation of an asset they hold by updating the blockchain. This can bring operational settlement risk as, until that custodian plays its role, settlement finality will not be achieved. This can be mitigated by an atomic swap capability of a smart contract but this is only effective when both assets are on the same chain.

Risks to be addressed

Regulatory focus across jurisdictions has generally been associated with:

- Depending on the digital asset in question, the point at which settlement finality is achieved may differ, and is more complex for public blockchains,

- Management of settlement and complexities associated with “forked” and “airdropped” digital assets (e.g., allocations across client accounts, conflicts of interest resulting from the fork or airdrop event),

- Operational settlement can be complex when ledgers, depending on the consensus mechanism, need to be updated and nodes need to be validated prior to achieving settlement finality,

- Custodians may struggle to complete Standard Settlement Instructions (SSIs) due to dynamic wallet addresses for some blockchain (UTXO / Bitcoin in particular). Dynamic wallet addresses are digital wallets whose addresses change frequently in order to add layers of security and obscure a wallet holder’s identity or holdings. These addresses raise challenges for KYC compliance and automation of settlement, but they do reduce cyber security risks,

- Additionally withdrawing cryptoassets from a (centralized) exchange that uses comingled wallets and returning the assets to the same address would render the assets inaccessible for the custodian without proactive support from the exchange. This is because a proxy address is used to determine to whom the incoming funds belong and cannot be associated with the owner when returned.

Potential risk mitigants

Custodians and market participants must ensure accurate books and records, including recording trading activity and asset transfers in accordance with recordkeeping requirements. Market participants, across jurisdictions may vary in reliability and consistency regarding settlement methods, and post-trade recordation and notification. Institutions should consider leveraging shared networks to ensure proper record keeping design. Redesign of operational and compliance procedures to reflect and mitigate digital asset specific risks is required. Participants need to understand the consensus mechanism and steps to achieving finality for each ledger they interact with.

Further, regulators should continue to provide greater clarity on rules for registered transfer agents, or others who play a similar role within the market structure, that are intended to facilitate prompt and accurate settlement of securities transactions and guidance on applicable transfer agent rules.

Execution barriers to risk mitigation

The complexity of defining the point of settlement finality with DLT arises particularly in public DLT networks where the control mechanisms that could govern a private network cannot be applied. As the ecosystem evolves, these factors will be overcome, and light will be shed on a common market understanding of what principles should be applied for determining settlement finality in a network where the asset is custodied.

Whilst the role of the custodian and its obligations generally remain the same, how this is achieved differs substantially. Transaction processing and settlement for DAC creates even higher dependencies on clients providing correct settlement instructions. Many steps currently requiring the involvement of a custody operations team are performed by software rules coded into blockchain (see Exhibit 5). ■

Asset Segregation

NB: When referring to wallets we are referring to wallet addresses unless explicated otherwise.

Factual differences

Asset segregation is a vital control process for assets under custody. The primary objective of segregation is to ensure that investor assets held by a custodian are protected in the event of insolvency, preventing them from being accessible to creditors of the insolvent custodian's estate. This key distinction sets investor assets apart from deposits or personal / contractual obligations. To make this clear, investors' property interests are therefore expected to be clearly demarcated in the records of the custodian.

Effective asset segregation requires a range of controls, typically in the form of account structure and reconciliations.

Whilst digital asset segregation is typically done on an aggregated basis, some digital asset custodians offer to hold fully segregated individual on-chain accounts on behalf of clients. This enables customers to view their positions by querying the on-chain account balance of their dedicated wallet.

Digital assets on public networks can present unique segregation challenges, particularly in contrast to traditional custody segregation that relies on separate internal and external accounts. On a public network, transactions are initiated from wallets, which are not equivalent to traditional custody accounts. Therefore, transaction records and wallet software are used to derive present balances.

Finally, standard trading day reconciliation processes do not fit digital assets networks. The 24/7 nature of some digital asset markets means the legacy concepts of official start of day or end of day for balance statements need to either be superimposed over constantly active markets or reconsidered entirely.

The node that creates a block will assign a timestamp to it, but node clocks may not be completely accurate. Therefore, the specific rules for inclusion/exclusion into given reporting or reconciliation batches require careful consideration.

Risks to be addressed

Due to the nature of the technology, the developing nature of property rights law concerning cryptoassets, and the range and activities of persons involved in providing custody services for cryptoassets, the application or effectiveness of traditional asset segregation techniques may be limited or ineffective. The aim of safeguarding client assets is key to the market's long-term success and suitable controls must be established.

Regulatory Insights - SEC Observation on DAC Specific Risks

The SEC's Office of the Chief Accountant (OCA) has observed "In connection with these services, these entities... may safeguard the platform user's cryptoasset(s) and also maintain the cryptographic key information necessary to access the cryptoasset. The obligations associated with these arrangements involve unique risks and uncertainties not present in arrangements to safeguard assets that are not cryptoassets, including technological, legal, and regulatory risks and uncertainties."[xi]

Further, DLT changes the nature of several existing risks that custodians must overcome to transition to a level of standard on par with regulated services. In the context of asset segregation, these include:

- Separation of owner assets from those of intermediaries (co-mingling)
- Assurance of services such as settlement when digital assets are redeemed
- The "closure" of wallets. A wallet exists forever and therefore the role of the custodian should be if assets are received on a "closed wallet" is undefined.

Potential risk mitigants

Digital asset custodians must operate robust, enterprise grade portfolio and custody management systems in order to maintain accurate client account and position data at all times.

Additional control processes are also recommended to ensure that off-chain (internal) and on-chain (external) records always remain consistent, comparable to the daily end of day reconciliations between a CSD and custodian.

In the short-term, the industry should additionally focus on further education and capacity building, as well as the development of best practices including, but not limited to:

- Provision of investor choice for assets to be recorded in a wallet address unique to the investor
- Elimination, evolution, or re-imagination of start-of-day or end-of-day balance statements
- Creation of standards around block timestamp differences and reconciliation
- Enhanced clarity on segregation as it relates to insolvency proceedings to minimize the risk of client assets being mistakenly classified as assets belonging to the custodian
- Enhanced clarity surrounding staked assets (see Section 3.3).

Execution barriers to risk mitigation

The resolution of the legal and regulatory barriers are key to ensuring the aims of asset segregation are achieved.

Other challenges to risk mitigation include:

- Timestamps should be omnipresent and consistent across all ledgers but are not and many technologists are unaware of the potential consequences of misaligned clocks
- Acceptance that where off-chain and on-chain records are maintained reconciliation is an important tool in identifying any errors or omissions. ■

Settlement, Finality, and Asset Segregation
Key Takeaways

- Settlement finality is a crucial concept that ensures the irreversible transfer of assets, minimizing risks related to counterparty, liquidity, operational, and legal considerations.

- In the realm of DLT, achieving clear settlement finality can be complex, especially in public DLT systems, where custom approaches are needed to accommodate technical nuances like chain-tip reorganizations. In contrast, private permissioned DLT networks with centralized consensus mechanisms resemble traditional settlement and finality rules, providing greater certainty in settlement timing and occurrence.

- Digital asset segregation presents unique challenges due to the nature of public networks, as transactions reference individual wallet addresses instead of traditional custody accounts. Additionally, the 24/7 nature of digital asset markets requires rethinking conventional reconciliation processes and careful consideration of timestamp accuracy for reporting and reconciliation batches.

- Digital asset custodians must maintain accurate client account and position data through robust portfolio and custody management systems, implementing control processes to ensure consistency between off-chain and on-chain records, akin to traditional daily reconciliations between a CSD and custodian.

DLT GOVERNANCE, KEY MANAGEMENT, STAKING, AND INTEROPERABILITY

DLT Governance

Factual differences
Traditional asset service providers rely on well tested protocols and procedures for governance and decision-making. To effect changes to the rules through which a company or service operates, governance is typically coordinated using hierarchical decision-making structures, including the potential for C-suite, Board or even shareholder votes in relation to important strategic events.

Private, access controlled DLT systems often also rely on centralized governance structures and traditional decision-making processes.

In contrast, public DLT communities tend to socialize governance and decision-making via open communities, opensource code repositories, and increasingly through Decentralized Autonomous Organizations (DAOs) that provide a method for both community-based decision-making, and the execution of financial commitments from the DAO treasury once agreed by the community.

Risks to be addressed
Custodians and market participants will have to address emerging risks associated with supporting or transacting in assets tied to permissionless blockchains:

- **Digital asset voting** - Low voter participation can undermine the legitimacy of decisions made through voting. Tightly coupled voting systems may be vulnerable to bribe attacks, where individuals with significant holdings manipulate the outcome for personal gain. Additionally, digital asset holders represent only one class of user, and their interests may clash with those of other users, raising concerns about the fairness and inclusivity of governance decisions.

- **Forked asset vs existing asset support -** Forks can have implications for blockchain governance and custodians since they can lead to the creation of new cryptoassets or networks, with the original and forked chains evolving independently. In such instances, custodians might need to make decisions on how to support the main chain, the forked chain or both and might require frameworks on decision-making and procedures to convey applicable decisions to investors in near real-time.

- **Smart Contract/Key/DLT hacks -** The risks of cybercriminals taking control of the blockchain through record manipulation, system corruption, attacks on the blockchain layer (such as block discard or block retention attacks), network-based attacks (such as DDoS attacks), and malware attacks are potential threats, which may impact custodians and investors. Time jacking attacks, where inaccurate timestamps are used to deceive nodes and enable double spending, are another risk. These risks might be applicable to both permissioned and permissionless blockchains.

Potential risk mitigants
By adopting the following mitigants, custodians can enhance the governance of digital assets, promote transparency, fairness, and security, and reduce the potential risks associated with decentralized networks and blockchain technologies. Custodians must educate investors on risks that client assets might face during governance related events, which might be beyond the control of the custodian.

These mitigants are not decided by the custodian but their implementation should be part of the assessment of whether the ledger will be supported by the custodian:

- **Digital constitutions** - This approach involves mathematically specifying the desired properties that the protocol should have. Any new code changes would require a computer-verifiable proof that they satisfy these properties. Digital constitutions provide a formal framework for governance and help ensure that protocol changes align with predetermined principles

- **Multifactorial consensus** - This approach involves multiple coordination flags and mechanisms, and decisions based on the collective result of these mechanisms. This approach includes coordination flags such as project roadmaps, consensus among core development teams, user votes, user votes through sybil-resistant polling systems, and adherence to established norms

- **Data access and governance** - Certain data, such as PII should be handled with utmost care and stored securely in alternative environments based on regulatory guidance (e.g., off-chain storage in an encrypted object storage). Additionally, custodians should validate the quality of data before it enters the blockchain to ensure accuracy and establish data governance policies, including access controls, metadata management, data quality controls, and security features. These policies should cover the entire data lifecycle involving on-chain and off-chain activities.

- In some networks ownership of assets on the network confers **voting ability** and custodians should consider whether they should invest in the assets to ensure that they have the ability to vote.

Execution barriers to risk mitigation

Managing risks associated with the governance of digital assets can be challenging due to several factors. For example, while digital governance constructs such as DAOs offer a formal framework for governance, expressing complex rules within code can be challenging. Value systems often require a degree of subjective interpretation, or adaption, making it hard to encompass them entirely through code-based governance mechanisms.

Designing governance mechanisms that align voters' actions with the common interest rather than self-interest can be challenging to achieve, with few precedents available. Achieving consensus between validating nodes and users on the network is crucial but complex.

Market Data - Effectiveness of On-Chain Governance

Ambitious examples of on-chain governance such as Tezos highlight the complex interplay of economic and other incentives that can undermine the effectiveness of code-based governance, particularly in scenarios where token distribution means a majority of voting power is concentrated among a small proportion of community members.

These factors demonstrate the complexities and challenges involved in implementing effective governance mitigations. Balancing the interests of diverse stakeholders, translating norms into code, fostering consensus, and avoiding conflicts are ongoing considerations that custodians and blockchain communities must navigate to ensure successful governance of digital assets.

In the case of regulated securities, custodians and CSDs must prepare for a world where some of the mechanisms related to validation, consensus, governance, and arbitration could have to be managed in a decentralized manner. ■

Key Management

Factual differences

The architecture of a typical blockchain introduces several areas of technical, operational, and commercial differentiation. Chief among these is the novel approach to digital asset ownership and control that arises within a distributed ledger environment.

Changes of ownership of digital assets can be executed directly by system users with DLT, but only following the submission and validation of an instruction (i.e., a transaction) that has been digitally signed. To digitally sign a transaction (i.e., to authorize a movement of funds), the specific private key that corresponds with the wallet address they want to transact from needs to be used. Anyone with access to the private key can initiate such a transaction, meaning assets can be lost if keys are compromised, thus underscoring the critical importance of keeping private keys secure.

With DLT, increasingly sophisticated methods for issuing, securing, managing, and using private keys have emerged. Approaches to enhance key management safety include multi-signature models (involving multiple keys), and the use of Hardware Security Modules (HSM), and more advanced threshold signature methods around which additional layers of authorization review and control can be arranged.

Certain private network deployments do not require participants to handle key management, where this is provided as a service by the platform operator.

The need for secure solutions contrasts with a desire for solutions that support faster performance. These competing priorities have led to the emergence of hot wallets and cold wallets as distinct solution components that address different custodial requirements – and are often used in combination ("warm wallets"):

DAC Building Blocks - Hot and Cold Wallets

- **Hot wallets** are typically connected directly to online infrastructure, and as a result carry a higher risk profile due to the threat of key loss through network or systems compromise. They are generally configured for high volume and / or low value transaction requests with low latency and focus on straight through execution. The funds stored within such wallets are typically of lower value intended to fulfil liquidity projections for typical transaction flow

- **Cold wallets** typically operate in offline and usually air-gapped environments, which involve security measures designed to ensure a computer network is physically isolated from unsecured networks, and in which there can be no possibility of remote compromise of keys. As a result, the security afforded by cold wallets is far superior to that of hot wallets. They are generally configured to fulfil the 'bank-vault' function, to secure the bulk of assets under the control of an institution, to which regular intra-day access is not required. The processes associated with executing cold wallet transactions often take longer (by design) and are more likely to require manual human involvement. As a result, cold storage is better suited to high value, low volume transaction scenarios, where security and oversight take priority over latency.

Risks to be addressed

Digital assets introduce new risks that must be managed effectively to provide a level of service that is superior or equivalent to traditional markets. Leading considerations include:

- **Poor key architecture** - Custody solutions and users rely on key management systems that offer a balance between usability and security. Some approaches may favor functional or performance needs (e.g., through use of hot wallets which permit rapid key access), at the cost of security

- **Liquidity risk** - The features associated with cold wallets mean that rapid access to assets in cold storage may not be possible. This could have the potential to create intraday or short-term liquidity risk

- **Human operational risks** - There are several risks that can result from human or operator error, including:

  i. *Poor operational design*: The construction of a robust multi-signature signing model can be undermined if the operational controls surrounding things like request verification or approval processes are compromised

  ii. *Ineffective key lifecycle management*: Keys typically pass through several lifecycle stages, including secure generation, allocation, storage, and usage, as well as rotation and decommission. These stages all introduce vulnerabilities and risks that if not properly managed, can jeopardize the security of a key

- **Inadequate incident response management** - In the worst-case scenario, where keys have been compromised, actions in the immediate aftermath may dramatically affect the overall impact of a compromise event. With appropriate enterprise incident response frameworks, corrective action to prevent or limit loss even after key compromise may be possible

- **Ineffective code review** - Solutions are not rigorously tested for flaws in the code, which may lead to keys being compromised

- **Lack of exclusive control, due to elements such as:**

  i. *DLT sharding* - dividing of a DLT network into smaller networks,

  ii. *Cryto key sharding* - dividing a single key into multiple pieces which can be recombined to recover and use the key for a signature and transaction,

  iii. *Multi signature wallets* - requiring multiple signatories to a transaction, and

  iv. *Multi-party computation (MPC)* - enables multiple independent parties to apply a mathematical computation on a part of the key share in order to create and sign transactions such that the key shares are with independent parties and randomly generated and no one party has the complete private key at any point in time), and others.

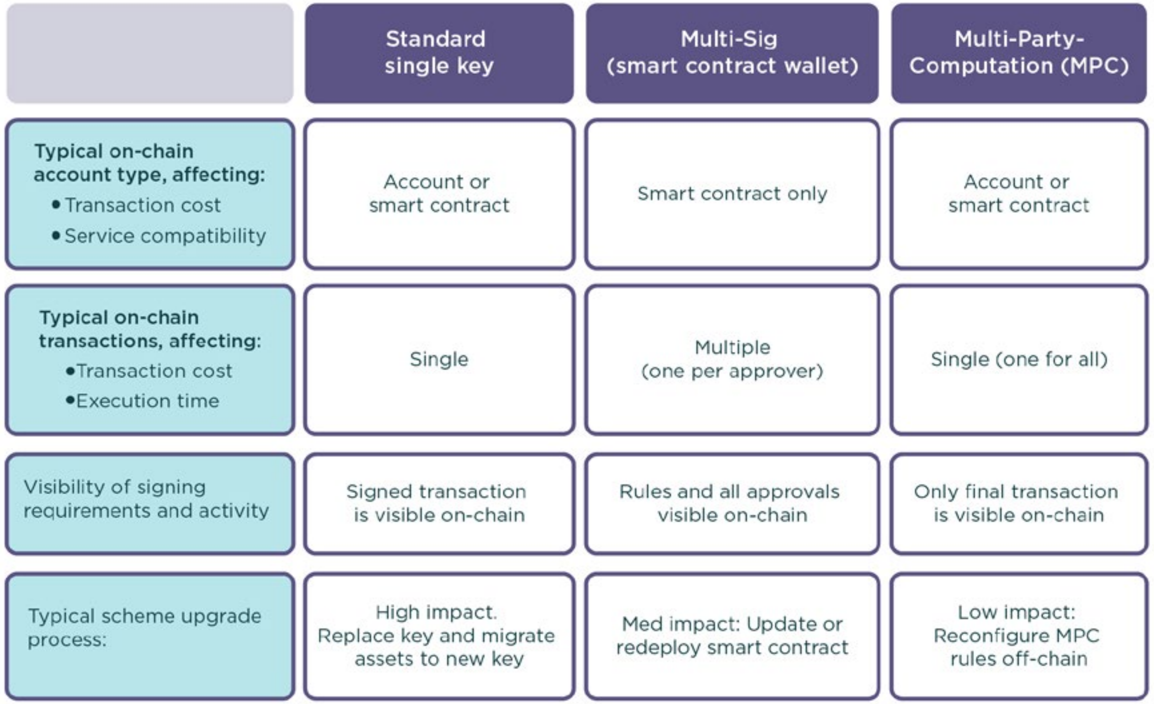
Blockchain creates a shared infrastructure, that does not enable exclusive control over assets as found in traditional markets. As a result, it does not allow digital asset custodians to provide the same guarantees as can be provided with traditional assets in terms of ensuring consistency and maintaining an operational service level. This is especially relevant while transacting the assets, and do not allow custodians to provide the same guarantees as can be provided with traditional assets. Popular MPC solutions propose a signature model where the secret key shares are split between the technology provider and the custodian, a model that was deemed acceptable for many of the industry’s early adopters.

Established regulated financial institutions responsible for providing third party custody of their clients, would require complete control over complete key share material or signatories. This includes where and how it is stored and managed, which conflicts with this shared-control model. A solution to this is that the shares are all held within different parts of the custodians' technology infrastructure, or all signatories are from the custodians organization.

Potential risk mitigants

First and foremost, organizations providing custody tools and services must adhere to the highest standards of security and risk management. This includes "standard" best practice certifications such as ISO27001 (an international standard regarding information security)[xii], specialist assurance reports such as SOCII[xiii]. Similarly, organizations procuring such services should apply extreme caution and rigor in their assessment of vendor maturity and suitability.

In addition, organizations seeking to implement key management should consider their own capabilities and needs for key management and implement arrangements that address their needs. This includes implementation and design of strong key architecture features, including multi-layered security, high level encryption, and other similar offerings.



	Standard single key	Multi-Sig (smart contract wallet)	Multi-Party-Computation (MPC)
Typical on-chain account type, affecting: • Transaction cost • Service compatibility	Account or smart contract	Smart contract only	Account or smart contract
Typical on-chain transactions, affecting: •Transaction cost •Execution time	Single	Multiple (one per approver)	Single (one for all)
Visibility of signing requirements and activity	Signed transaction is visible on-chain	Rules and all approvals visible on-chain	Only final transaction is visible on-chain
Typical scheme upgrade process:	High impact. Replace key and migrate assets to new key	Med impact: Update or redeploy smart contract	Low impact: Reconfigure MPC rules off-chain

Table 1: Example considerations relating to the evaluation of key management solution options.

© Deloitte 2023

Specifically, organizations without operational or technical experience managing keys or managing the custody of financial assets are often better suited to at a minimum outsource some element of the design, development, implementation of the service or alternatively purchase services in which key management is partly (or fully) outsourced to specialist providers. These service providers need to undergo the same due diligence as described above. Those who do choose to outsource should determine who is liable for various actions during the lifecycle of custody, including facilitating transactions for clients.

Organizations implementing custody solutions should ensure critical decision-making processes (such as product or vendor selection) are staffed by practitioners with access to sufficient specialist expertise. These specialists can help evaluate technical options, determine preferred options, and evidence decision-making rationale such as vendor assessment questionnaires.

As can be seen in Table 1 above, there are a variety of strategies that can help mitigate these risks, each with their own advantages and trade-offs.

Execution barriers to risk mitigation

There are a variety of considerations that custodians and market participants will have to navigate:

- **Technical skills –** Access to specialist technologists can be challenging for organizations without digital asset experience and will take time to embed. Specialist skills will likely be required across multiple domains spanning governance and oversight, technology, and operational teams

- **Organizational change capacity –** Beyond the availability of expertise, business change management related to custody, key management and to operate with digital assets in general requires coordinated activity across multiple domains including governance, technology, operations, and risk management. Large organizations can face challenges prioritizing resource allocation on large work programs against other strategic initiatives

- **Regulatory uncertainty –** Evolving standards and lack of consistent regulatory treatment may impede execution. For example, there may be uncertainty as to whether all the multiple key holders, or other participants in multi-signature schemes who can contribute to a transaction approval or signature generation process should be treated in the same way as parties that offer fully outsourced custodial control (i.e., as digital asset service providers – or equivalent in the respective jurisdiction). ■

Staking

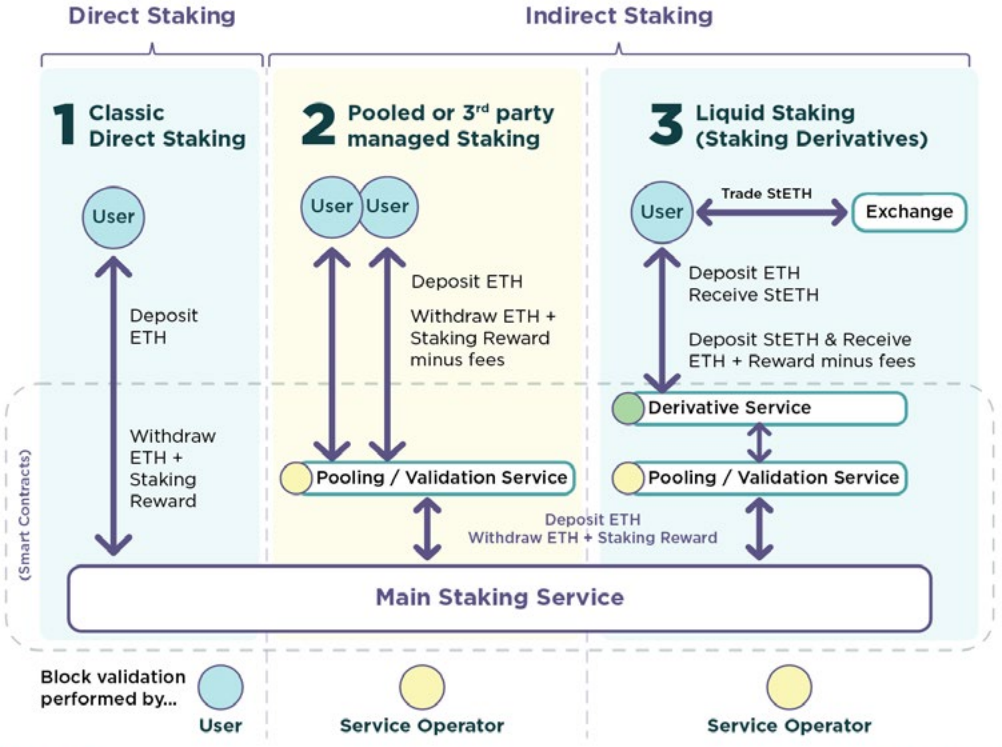

Direct Staking
Indirect Staking
1 Classic Direct Staking
2 Pooled or 3rd party managed Staking
3 Liquid Staking (Staking Derivatives)
User
Deposit ETH
Withdraw ETH + Staking Reward
User
User
Deposit ETH
Withdraw ETH + Staking Reward minus fees
User
Trade StETH
Exchange
Deposit ETH Receive StETH
Deposit StETH & Receive ETH + Reward minus fees
Derivative Service
Pooling / Validation Service
Pooling / Validation Service
Deposit ETH
Withdraw ETH + Staking Reward
Main Staking Service
(Smart Contracts)
Block validation performed by...
User
Service Operator
Service Operator

Exhibit 6

© GBBC 2023

Factual differences

There is no parallel for staking in the traditional financial models. This activity, outlined in Exhibit 6, is rarely seen outside of the cryptocurrency markets and so far, has not been seen in the tokenization of real-world assets. Transaction validation and new block creation within Proof-of-Stake (PoS) networks like Ethereum is typically performed by community members, who are in turn rewarded.

To ensure validators behave promptly and non-maliciously, parties must first transfer a quantity of assets into a 'staking' smart contract. This places the member at (a low) risk of significant and permanent loss of assets (e.g., "Slashing"), in which staked assets can be irrecoverably lost if validators' obligations are not fulfilled. Once a validator has placed assets into a staking service, they become eligible to participate in block validation to an extent proportional to the quantity of assets they have staked.

If a validator opts to stop validating, they must provide notice to the staking service (authorization smart contract) and wait for a specific holding period to expire, at which point their assets, plus any staking rewards, can be withdrawn and returned to the custody of the now ex-validator. In this way, staking can be undertaken to generate a yield on cryptoassets. Staking rewards are generally variable and designed to increase if overall participation reduces and decrease when participation increases.

Beyond the classic example of staking described above, numerous variants have emerged, the most common models are Direct Staking, and Indirect staking, which may include Staking-as-a-Service or Liquid Staking. A simplified illustration of common staking models is set out below (based on Ethereum ecosystem).

Risks to be addressed

While subscribing to staking services, investors must consider a variety of risks, especially pertaining to technical setup, penalties for node downtimes and liquidity of staked assets. Some considerations include:

- **Block validation risk** - If engaging in direct staking, depositors must recognize their obligation to participate in network block validation. This requires the correct technical setup and ongoing maintenance. Node services must be configured to operate in compliance with staking protocols. Failure to comply might lead to penalties, including slashing

- **Liquidity risk** - Different staking models present different risks to overall liquidity. Both direct and indirect staking involve relinquishing direct custody of staked assets until assets are successfully withdrawn or "unstaked". Direct staking further involves 'locking' staked assets for minimum time periods. Indirect services offer rules around asset withdrawal, whilst liquid staking options are designed to maintain liquidity in the form of transferrable tokenized staking derivatives

- **Third-party risk** - The decentralized nature of staking presents novel risks, as traditional risk management provisions are not relevant. Outsourced staking services might introduce further risks in relation to the smart contract services through which they operate, including risks regarding the deployment, maintenance, and upkeep of smart contracts. If these smart contracts are not properly maintained, they could present an attack vector for fraud, theft, or other risks.

Potential risk mitigants

Effectively mitigating risks associated with staking will require prior research and due diligence. Given the highly technical nature of the activity, participants will also have to conduct service due diligence to establish confidence in the team and technology and ensure risks are well understood and appropriately mitigated. Consideration should also be given to the availability of insurance in relation to each model considered.

Industry participants can also spread the allocation of assets across multiple staking services to help mitigate third-party risk associated with any one service. Similarly, participants are also considering staking services across multiple DLT networks (and therefore assets) to potentially reduce volatility risk associated with any single asset, however these actions do not necessarily reduce overall risk, and detailed evaluation is needed.

As previously mentioned, regulatory and legal due diligence must be performed.

Execution barriers to risk mitigation

The novelty of staking and rapidly evolving crypto landscape means there is limited data to analyze and predict future trends. This makes it challenging to develop risk models or forecast asset performance. It also means the regulatory landscape surrounding staking is still evolving and can vary greatly across jurisdictions. Uncertainty regarding regulations makes it challenging to establish consistent risk mitigation strategies.

Regulatory Insights - How Staking Falls under the Howey Test

Regulatory guidance across jurisdictions continues to be an evolving consideration. In the United States, the SEC contends that staking activities meet the criteria of a security per the Howey Test[xiv] since staking satisfies (i) Investment of money (i.e., Lock up of assets for potential returns), (ii) Common enterprise (collective efforts of validators) and (iii) Expectation of profits primarily from the efforts of others (i.e., via staking rewards received from staking service providers).

Despite a generally maturing industry, the digital asset ecosystem remains vulnerable to hacking and other forms of failure which can result in the loss of assets that are not properly secured. This risk applies equally to staking and underscores the increasingly important role of insurance, which is being increasingly offered in the space, in enabling staking services that can offer some level of asset protection., While insurance can offer asset protection, the short-term economics and costs of insurance may make it less feasible. ■

Interoperability

Factual differences

NB: This section considers technical interoperability and not other forms of interoperability (such as regulatory and legal interoperability).

Interoperability between DLT networks, applications and services across the digital asset marketplace is an important consideration to product developers and investors alike. It refers to the extent to which a custody solution can:

i) support multiple assets across multiple networks, and
ii) integrate with existing systems.

As set out below, interoperability considerations can be grouped logically, with different risk factors and mitigants per group.

Interoperability among off-chain services - Most custody services are off-chain. Whilst they connect to DLT, and submit transactions into networks, they predominantly operate within off-chain, often legacy technology, environments such as accounting and, reporting systems. These are likely to require integration for automation. Examples of required interoperability include:

- Ability of custody or portfolio management systems to detect and accurately interpret asset activity across multiple networks, and
- Compatibility of network activity monitoring services (such as AML transaction monitoring/ alerting services) with local blockchain nodes across different networks.

Interoperability within a DLT network - Interoperability within a network refers to different types of tokens that are configured in different smart contracts. Networks are supposed to ingest all these contracts in order for the transactions to be executed. This a key consideration due to how different process flows are able to span across multiple smart contracts. Examples of required interoperability include:

- Tokens on a blockchain with multiple smart contract elements (an ERC-20 fungible token with an embedded ERC-721 non-fungible token for additional data storage purposes)
- Smart contracts that are triggered based on live events resulting in the automatic minting of new tokens.

Interoperability between networks - The transfer of digital assets from one chain to another is known as “Cross-chain Bridging”. As various participants in an ecosystem may implement different networks, it is crucial that these networks are able to communicate with each other to affect the seamless transfer of assets or data.

When considering interoperability between networks, the consensus mechanism, smart contract language and authorization components are key factors in determining the settlement finality of the transaction. It would also ensure the records are appropriately updated on each ledger to display the ownership of each asset for the purposes of custody.

Examples of required interoperability include:

- Interoperability between public blockchain networks like Ethereum to Polygon, and
- Interoperability between private networks and public networks (and vice versa).

Risks to be addressed

Monitoring of activities on and off-chain - The interfaces and protocols through which off-chain and on-chain applications connect with nodes to send and receive information vary considerably across networks. This presents interoperability challenges to custody providers wishing to use common software to manage activity across multiple DLT networks. This introduces a risk of inadequate reporting due to various data source and network monitoring tools.

Cyber threats and incidents - Cyber threats and incidents have occurred because of vulnerabilities that were detected in smart contracts and interoperability protocols. As the development of this code is complex in nature with a limited number of experienced engineers, there is an inherent risk that assets on chain may be exposed to cyber hacks on public networks. This impacts the level of insurance a custody provider may purchase and offer as a mitigant to its client to safeguard their assets.

Compatibility - Assets that reside on one network may not be compatible with other networks making the transfer of those assets difficult to complete. In terms of data, different DLT networks utilize widely varying methods for structuring and storing data, typically requiring specific adaptation among off-chain services. It is also worth noting that DLT may not be compatible with legacy systems causing potential downtime and a huge consumption of resources to process all the data in a digestible format for reporting.

Complex technical components - There are various components within the networks that are very technical in nature and are not easily digestible. These include zero-knowledge proofs (ZKPs), oracles, virtual machine standards and contractual language differences. Institutional investors may not be interested in the detail of these technical concepts and therefore subject to a risk of reliance on third parties that have capabilities in these areas. The cryptographic methods utilized within system procedures such as digital signature generation and validation can vary between different blockchain networks. This affects the ease with which off-chain applications can interpret or validate data within such systems.

Potential risk mitigants

Risks could be mitigated by simplifying the investor strategy based on the offerings of one or two custodians. This would make it easier for the investor to classify counterparty risks. Given the large amounts of data noted within public networks, risks could be mitigated by adapting traditional monitoring tools to ingest data from the ledger. Data could also be easily transferred with the use of APIs. API are considered more mature and can easily be adapted for the use of blockchain interoperability. Entities can make use of various API standards like the open standards framework, JSON.RPC APIS, or Hyperledger Composer APIs for legacy integration.

Whilst there are new cyber threats introduced with smart contracts, there are many new participants in the market which focus on smart control audits and penetration testing to ensure that there are no bugs within the code.

Execution barriers to risk mitigation

There are various types of digital asset tokens (security, utility etc.) across various networks with different types of fungibility (fungible vs non-fungible). Due to the range and diversity of digital assets, an investor holding multiple different assets may foresee challenges in where and how all these assets would be custodied. There is no one size fits all solution and investors and custodians would be required to think about what solution fits best with their strategy.

Due to the volatility of the market and technical complexities of institutional grade custody, there may be a limited number of firms that offer custody services to institutional investors across multiple digital assets. This results in investors having a small group of custodians to choose from based on their portfolio. ■

DLT Governance, Key Management, Staking, And Interoperability
Key Takeaways

- Investors and custodians face cyber risks in both permissioned and permissionless DLTs, including the potential for cybercriminals to manipulate records, compromise system integrity, engage in network attacks like DDoS, and exploit vulnerabilities in smart contracts, keys, and blockchain layers, highlighting the importance of robust security measures. However, in the context of governance, custodians and market participants must hone in and address emerging risks tied to public permissionless DLTs, including concerns about low voter participation and potential manipulation in digital asset voting systems, as well as challenges related to governance fairness and inclusivity.

- In a DLT environment, changes in digital asset ownership raise concern around the concept of control - a crucial tenant of custody services. This has given rise to the development of various private key management methods, including single-key splitting models, multi-signature models, and the use of HSM, balancing the demand for security, performance and control.

- Staking is a highly technical in nature and presents unique risks pertaining to block validation risk, liquidity risk and third-party risk. In an attempt to mitigate, investors are encouraged to conduct extensive preemptive investigations and due diligence processes. However, the novelty of staking and rapidly evolving crypto landscape means there is limited data to analyze and predict future trends. This makes it challenging to develop risk models or forecast asset performance. It also means the regulatory landscape surrounding staking is still evolving and can vary greatly across jurisdictions.

- There are components within DLT networks that are very technical in nature, like staking and interoperability between networks, which may hinder institutional investors' appetite to weave through the technical concepts. In turn, this may expose them to risk that they may not have been exposed to in traditional financial markets where they may rely on standard and well-established due diligence processes. For investors, this risk is only amplified by the limited insurance DA custodians may purchase given the inherent risk that assets on chain. These limitations may include the effects of to cyber hacks on public networks, their susceptibility to compatibility issues as well as the risk of inadequate reporting due to various data source and network monitoring tools.

WHAT SHOULD ASSET OWNERS EXPECT

What Should Asset Owners Expect

Where an investment manager or similar service provider contracts for custody services in relation to assets it manages on behalf of underlying clients, considerations such as asset coverage, jurisdictional coverage, custody model offered within each jurisdiction (direct custody or third-party sub-custody), pricing, reputation etc.[12] will act as initial decision criteria for selecting a custody provider. Furthermore, the regulation applicable to the investment manager / service provider is likely to establish minimum standards for assurance as to conduct as well as the legal and technological security of the custody services to be procured.

These minimum standards will include considerations such as the creditworthiness and regulatory status of the custodian (e.g., qualification as a CASP under MiCA), the legal certainty of ownership and control of the assets under the relevant governing law (see Section 1.1) and the bankruptcy remoteness of the custody assets from the custodian's own assets (see Section 2.2).

As is the case with custody of traditional assets, the custody contract and related service agreement(s) are the primary mechanisms for setting out the parties' rights and obligations, representations as to good standing and capabilities, and any other important matters that form part of the basis on which the parties agree to deal with each other. This chapter attempts to summarize the considerations that investors should strive to clarify in their contracts when subscribing for the provision of DAC services. A non-exhaustive list of such critical considerations includes:

Ownership and bankruptcy remoteness

Whether and how an asset owner can obtain ownership of the digital financial asset and associated benefits and entitlements depends on a number of factors explained in earlier chapters. Some digital assets may not be considered as "property" in the jurisdiction of the asset owner or custodian who maintains it on the asset owner's behalf.

Regulatory Insights - Regulatory Approaches to DAC Concepts of Possession and Control

For example, the UK follows common law principles of possession and control, whilst French law appears to sidestep the role of a "custodian" in obtaining ownership by providing that investors own cryptoassets outright without regard to any other actors, including the sponsor or organizer of the platform (the so-called "DEEP").[13] Meanwhile, Luxembourg's Law of 22nd January, 2021 on distributed ledger technology and issuance of dematerialized securities modernized the Law of 6th April, 2013 on dematerialized securities by recognizing the possibility of issuing and recording dematerialized securities through distributed ledgers/databases and creating the concept of 'issuance account' in the 2013 Law. The law applies to 'securities that are deposited or held on a securities account with an account keeper that are or have been declared fungible' – this presumes they are held with an 'account keeper' and are transferred by book-entry ('book transfer'). This seems focused on "securities" and not on other kinds of assets that would be considered financial instruments under the Markets in Financial Instruments Directive (MiFID) or other kinds of 'digital' financial instruments to be covered by MiCA.

[12] *For a more comprehensive checklist, see table Exhibit 7 in Appendix*

[13] *See, Lehmann, M. (2021) 'National Blockchain Laws as a Threat to Capital Markets Integration', Uniform Law Review, Vol. 26, No. 1, p. 154, citing to Art. R211-5 of the French Monetary and Financial Code (Code monétaire et financier [CMF]), which excludes the trading of financial instruments on a trading platform that have a 'mandatorily nominative form' (a 'forme obligatoirement nominative'). This is the case for financial instruments recorded on a so-called 'dispositif d'enregistrement électronique partagé' (the DEEP), which roughly translates to 'shared electronic recording system.' See: Art. R211-2 CMF, available at https://academic.oup.com/ulr/article/26/1/148/6314582 (accessed 2nd September, 2022).*

As previously discussed, this has significant consequences in the insolvency of the custodian or potentially other providers such as platforms and exchanges. Even where the digital asset is considered “property”, the law may vary depending on jurisdiction in terms of how property interests are to be protected against whom they are to be asserted.

Establishing clarity on whether and how a custodian facilitates access to ownership rights and entitlements in financial assets for a client / asset owner is not a new concept. There is longstanding precedent in the industry on how this is achieved for “traditional” financial assets, including a relatively clear understanding of the limits of what custodians and other providers (such as FMIs) can “ensure”. Asset owners should seek to obtain as much clarity and legal certainty in these respects as possible, just as they would have done in the context of traditional finance.

Contracts should make clear whether a custody provider has the right to commingle client and proprietary assets in a way that may impact on ownership rights in the event of insolvency of the provider or some other party upon whom ownership rights depend (e.g., an FMI). Such arrangements often are acceptable in a traditional asset custody contract where bankruptcy remoteness is a key attribute on traditional custody (although this is not always the case, e.g., in the case of use of certain broker-dealers who are granted “right of use” of customer assets in the contract). If a client agrees to commingle assets, the potential impact on ownership rights should be clearly stated in the contract, together with any mitigants that the asset owner expect to see in relation to such arrangements.[14]

Within the contract there should be clarity of the liability provisions of the custodial relationship. If assets are lost, what is the custodian responsible for? Is the custodian liable for full liability and/or only for gross negligence? Particularly important is the context of assets lost for reasons outside of the control of the custodian. In traditional assets and private networks contractual recourse would normally be available but not for assets held on public networks.

Another important aspect to consider is insurance coverage. Asset owners should fully understand the extent to which their assets held at a custodian are covered through insurance and under what circumstances. These circumstances could for example relate to technical or operational issues at the custodian.

Finally, events arising that are external to the custody relationship, e.g., forking, protocol changes etc., could significantly impact on digital asset holdings of the asset owner. How these events are addressed by a custodian in “control” of the financial asset should be addressed in the contract as well.

Access and control

Intermediation structures differ and some digital asset service providers and infrastructure providers operate differently than those operating in traditional finance. For example, some providers, such as digital asset exchanges, may not be constituted as a legal person in an IOSCO-recognized jurisdiction. This may have impacts on the asset owner’s rights under the contract with the provider. Hence it is important that the asset owner conduct a thorough due diligence on the provider of DAC services and whether they have the necessary qualifications within the jurisdiction in question.

It should be noted that regulatory authorities have significantly increased expectations – and requirements – in this regard (see, e.g., MiCA’s provisions regarding criteria applicable to cryptoasset trading platforms, U.S. SEC proposed “Safeguarding Rule”, etc.).

[14] These mitigants may be imposed by law and regulation. See, eg., Rule 15c3-3 of the U.S. Securities Exchange Act of 1934 (“Customer protection - reserves and custody of securities”), applicable to U.S. broker-dealers in relation to customer assets.

Where applicable, custody documentation must incorporate any arrangements relating to hot and cold wallet storage, striking a balance between asset accessibility, security and speed. The basis on which assets are moved from hot to cold wallets, and the practical implications of those arrangements (e.g., time to execute and settle transactions is likely slower in the case of assets held in cold storage) need to be reflected accurately in contractual arrangements.

Control of assets throughout the trading cycle should also be documented, especially to understand if the custodian is able to offer off-exchange trading capabilities, ensuring full control and protection of assets as they remain stored within own custody accounts, and mirrored on exchanges, removing counterparty risk when clients trade.

In the case that the custodian uses multi-sig wallets (requiring multiple keys and therefore multiple signatories to authorize transactions) or more advanced encryption techniques (like MPC and geographically distributing those shares to protect against attacks and collusion), it is important for asset owners to determine and consent who the other actors are.

These actors would manage the computation of the part of their private keys, or who the other signatories are. It is imperative to understand the liabilities of the custodian if such an arrangement fails to safeguard the client assets or make the assets available for transacting in the necessary time.

The contract should clearly indicate whether the custodian has exclusive control of the client asset (meaning full control over the private key, key shares and governance policies) or and the necessary risk mitigants employed where there are gaps in control.

Intermediation models differ and at present there is little interoperability between DLT networks, whether public (permissioned / permissionless) or private. Asset owners should assess whether the firm wishing to provide the custody solution can access a broad range of networks and wallet providers and how they do this (i.e., manage a large number of relationships themselves or use a third-party technology provider to access the variety of networks).

Transacting

Network fees are highly variable on public chains and there is a tradeoff between such fees and transaction processing time and settlement finality. Custodians may wish to agree fee rates and have clients accept the impact of such maximum fees as part of service level agreements. Related, it is relevant to understand, if custodians execute every transaction on-chain, or if certain activities are handled in a virtual accounting layer, which would mean that DLT fees are not incurred on every transaction.

Following on, asset owners should understand if their assets are held in a segregated manner on-chain or if segregation is done in other systems proprietary to the custodian but not reflected on-chain. Both might be fully valid approaches, depending on the business and regulatory context.

As DLT markets can operate 24/7, the concept of end-of-day reporting needs to be re-defined by custodians. For asset owners, it is important to know how a custodian has designed this to have full transparency in what his reporting reflects.

Regulatory Insights - Liability of the Custodian under MiCA

In the EU, article 67 MiCA sets a specific standard of liability for the custodian in the event of loss of digital assets.

A further point of definition is, when a custodian treats a settlement system as legally binding and final for digital assets. The conditions and moment of legally binding settlement may not be clear for some digital assets and may differ among different digital assets. Therefore, asset owners should ensure they understand the custodian's approach to this.

Administration and financing

New asset administration approaches, which have been made possible by technology, like smart contract execution of corporate actions and lifecycle events (e.g., coupon payments), can raise questions about the governing law and legal jurisdiction in case of issues arising from smart contract operations.

Potential advancements in technology and standards

Where the development or availability of new service capabilities gives rise to a potential risk (e.g. smart contracts for lifecycle events), industry participants can come together to create industry standards. Areas where this could be possible include:

i. Service standards for transaction processing and related network fees,

ii. Standards for operation and issues arising from smart contract operation of digital asset lifecycle events such as corporate actions or coupon payments,

iii. Technological neutrality and agnosticism of a custodian should be credibly demonstrated.

Evolution in regulation

The rapidly developing nature of the digital asset environment and surrounding legal and regulatory regimes mean that the basis on which a contract is established is regularly shifting. Contract drafting needs to achieve a balance of reasonable certainty together with adaptability to accommodate new assets and technological capabilities.

The behavior of digital assets differs depending on the DLT protocol or on differences in smart contract design. This significant variation in the operation of the technology leads to a wide range of possible eventualities that are difficult to accommodate in contracts. A set of industry standard approaches (periodically updated and developed with feedback from key regulators) to which parties can cross-refer may be the most pragmatic way to accommodate this issue in the context of a rapidly developing and highly novel asset class. ■

What Should Asset Owners Expect
Key Takeaways

- When subscribing for the provision of DAC services, investors should consider risks pertaining to ownership and bankruptcy remoteness. Investors must understand when and how their asset may be considered property due to the significant consequences this has in the case of the insolvency of the custodian or other providers. Contracts should also make clear whether a DAC provider has the right to commingle client and proprietary assets in a way that may impact ownership rights in the event of insolvency of the provider or some other party upon whom ownership rights depend. In this context, contracts may need to make explicity the liability provisions of the custodial relationship and the extent to which investors' assets are insured if assets are lost.

- Intermediation structures in a DAC context may differ from those operating in traditional finance custody. Investors must seek to understand how their rights under the contract with the provider may differ from a traditional custody arrangement, furthermore emphasizing the importance of thorough due diligence and contractual clarity. Where applicable, custody documentation should also incorporate any arrangements relating to hot and cold wallet storage, document the custodian's control of assets through the trading lifecycle, and, when relying on more advanced encryption techniques, document who the actors responsible for distributing AuM and ensure investors consent to who these actors are.

- Investors must also take into account how the variance in network fees on public chains may impact a digital asset custodian's fee model and therefore the cost they bear for seeking DAC services. Investors must also reconcile with the concept of end-of-day reporting being revisited in DLT markets. In addition they must understand that the moment of legally binding settlement in has variables that do not exist in traditional financial markets. Investors must have visibility of all of these considerations when purchasing DAC services.

- Evolution in technology and the growth of the DAC market will drive standards creation and adoption across the market, and regulation will follow or evolve in jurisdictions where it has begun. Investors must take heed of these evolutions and seek to understand how it may influence the terms of their contractual agreements with their custodians and the safety of their assets in custody.

CONCLUSION

Conclusion

DAC will continue to play a critical enabling role in driving the market adoption of digital assets across client segments and geographies. There must be a clearer and deeper understanding by clients, providers, and regulators of the different types of digital assets and the different operating models for custody which can exist. A well designed and thoughtful custody service will not only safeguard investor assets but also foster greater trust amongst industry participants, ultimately allowing for greater innovation.

Efforts aimed at achieving greater regulatory clarity, including the MiCA package in the EU, the UK Jurisdiction Taskforce statement on English securities law, and Pilot/Sandbox projects in various jurisdictions, will continue to drive adoption of digital assets.

The lines between centralized exchange venues and decentralized wallets are increasingly blurred across a variety of asset classes (i.e., tokenized securities, cryptoassets, etc.), fulfilling an array of functions. Therefore security, regulatory compliance, and viability of the market structure, including profitability, are likely to remain important topics of discussion for years to come.

By establishing reliable custody services for digital assets, custodians can help create a secure and efficient environment for clients, investors, counterparties, and market participants.

The report delivers an eight-point call to action to highlight the opportunities, risks, and risk mitigants that investors and service providers should understand and apply in connection with DAC:

1. Educate workforces on digital assets and their value chain as well as the risks and risk mitigation of elements such as key management and staking – particularly for asset owners and investment managers,

2. Engage with regulatory authorities to resolve uncertainties related to the development and growth of DAC and promote regulation through the lens of "same activity, same risks, same regulations",

3. Develop a common understanding of how asset owners and/or investment managers should ensure contractual terms that are clear, that address risks that are relevant to DAC and that delineate between the responsibilities of a digital custodian, and other market participants and service providers,

4. Support dialogue with AML / KYC and sanctions authorities in order to achieve common aims so that know-your-customer requirements, money laundering and other criminal activity risks and sanctions enforcement are effectively addressed whilst allowing digital asset ecosystems to operate effectively,

5. Work with governors and/or operators of DLT networks to establish transparent finality rules and processes,

6. Work with the industry to establish principles and best practices for:
   i. Asset segregation
   ii. Ledger governance
   iii. Interoperability,

7. Advocate for bankruptcy remoteness of assets through statutory and regulatory reform, or litigation, to ensure jurisprudence,

8. Support of the adoption of global legal standards to cover DAC. Standardization helps the market develop and creates less barriers. ■

APPENDIX

APPENDIX A – **Key Report Takeaway By Sub-Section**

Section 1.1 - Legal

Understanding custody of financial assets - both in traditional finance and the digital asset sphere - requires a grasp of how legal frameworks underpin property rights.

Assets are categorized as tangible or intangible, with property rights enforceable against the world, while contract rights are limited to parties involved. These distinctions become crucial in insolvency scenarios.

Before investing in financial assets, it is vital to ensure enforceable property rights. In insolvency, investors typically have priority over creditors. Digital assets add complexity, as their decentralized nature may require legal adaptation, especially when multiple jurisdictions are involved.

As the industry grows, it is essential that policymakers, regulatory authorities, and legislators are mindful of the risks of inconsistencies with other legal systems.

Section 1.2 - Regulation

Providers and users of DAC services face challenges related to varying asset definitions across jurisdictions, location-specific regulatory compliance requirements, and the lack of clear interoperable regulatory frameworks for digital assets on a national and international level, making it difficult for service providers to meet multiple requirements simultaneously.

Applying traditional regulations to digital assets is challenging due to differences in product lifecycle processes, such as the continuous operation of DLT networks, which raises questions about regulatory reporting and accounting.

Public DLT networks have unique characteristics that can lead to specific risk scenarios, including the potential impact of blockchain forks on asset ownership rights and the challenges posed by the anonymity of some cryptoasset ownership, necessitating the development of new control mechanisms.

The challenge in the context of digital assets on public DLTs is determining which risks are under a custodian's control, given the network's distributed nature and complexities. This uncertainty highlights the need for regulatory frameworks to adapt to digital assets. Regulators must strike a balance between control and investor protection while fostering innovation. The industry can also contribute by addressing risks through contractual arrangements to manage expectations and reduce disputes.

Section 1.3 - Financial Crime

KYC: Custodians need to implement robust KYC processes and controls for clients holding digital assets, including the review of on-chain activity and wallet addresses, and ensuring a minimum of customer identification requirements.

AML / CTF: Custodians must navigate the challenges of implementing AML, CTF, and BSA obligations in the context of diverse digital assets and public blockchains. Compliance processes should be scalable, real-time, and capable of reporting suspicious activities to relevant authorities.

KYA: Custodians need to perform digital asset assessments to verify the assets they hold, even though specific regulatory requirements for such assessments may be lacking.

Sanctions risks: In some public DLT networks, there is a risk of sanctions violations related to transaction fees. Originators cannot control which miner confirms their transaction, potentially leading to concerns about facilitating transactions with sanctioned parties. Resolving this issue is crucial for regulated financial firms' participation in the market.

Monitoring and reporting: Custodians may struggle to effectively monitor and detect suspicious transactions due to the limited maturity of AML monitoring tools in the market. This affects the quality of data used for reporting to authorities, but the accessibility of blockchain data offers the potential for tooling maturation to improve monitoring capabilities.

Section 2.1 - Settlement & Finality

Settlement finality is a crucial concept that ensures the irreversible transfer of assets, minimizing risks related to counterparty, liquidity, operational, and legal considerations.

In the realm of DLT, achieving clear settlement finality can be complex, especially in public blockchain systems, where custom approaches are needed to accommodate technical nuances like chain-tip reorganizations.

Private permissioned DLT networks, with centralized consensus mechanisms, tend to resemble traditional settlement and finality rules more closely, reducing uncertainty in settlement timing and occurrence.

Section 2.2 - Asset Segregation

Digital asset segregation presents unique challenges due to the nature of public networks, as transactions reference individual wallet addresses instead of traditional custody accounts. Additionally, the 24/7 nature of digital asset markets requires rethinking conventional reconciliation processes and careful consideration of timestamp accuracy for reporting and reconciliation batches.

Digital asset custodians must maintain accurate client account and position data through robust portfolio and custody management systems, implementing control processes to ensure consistency between off-chain and on-chain records, akin to traditional daily reconciliations between a CSD and custodian.

Section 3.1 - DLT Governance

Public permissionless DLTs carry a heavier risk profile than private permissioned systems for custodians and market participants.

Investors and custodians face cyber risks in both permissioned and permissionless DLTs, including the potential for cybercriminals to manipulate records, compromise system integrity, engage in network attacks like DDoS, and exploit vulnerabilities in smart contracts, keys, and blockchain layers, highlighting the importance of robust security measures.

However, in the context of governance, custodians and market participants must hone in and address emerging risks tied to public permissionless DLTs, including concerns about low voter participation and potential manipulation in digital asset voting systems, as well as challenges related to governance fairness and inclusivity.

Section 3.2 - Key Management

In a DLT environment, changes in digital asset ownership raise concern around the concept of control - a crucial tenant of custody services. These changes in ownership occur through user-initiated transactions digitally signed by the custodian(s) using a specific private key, emphasizing the critical need for secure private key management to prevent asset loss.

This has given rise to the development of various private key management methods, including single-key splitting models, multi-signature models, and the use of HSM, balancing the demand for demand for security, performance and control.

Section 3.3 - Staking

Staking is an activity which, thus far, has rarely been seen outside of the cryptocurrency markets and not yet in the tokenization of real-world assets. A such, this is a unique risk that investors seeking DAC services must consider, with considerations including but not limited to:

i) **Block validation risk** - where if depositors are engaged in direct staking, they must recognize their obligation to participate in network block validation,

ii) **Liquidity risk** - where both direct and indirect staking involve relinquishing direct custody of staked assets until assets are successfully withdrawn or "unstaked", and

iii) **Third-party risk** - where outsourced staking services might introduce further risks in relation to the smart contract services through which they operate, including risks regarding the deployment, maintenance, and upkeep of smart contracts.

Staking is a highly technical in nature and requires extensive prior research and due diligence processes to mitigate the risks that it may give rise to. However, the novelty of staking and rapidly evolving crypto landscape means there is limited data to analyze and predict future trends. This makes it challenging to develop risk models or forecast asset performance. It also means the regulatory landscape surrounding staking is still evolving and can vary greatly across jurisdictions.

Section 3.4 – Interoperability

Technical interoperability in the context of DAC refers to the extent to which a DAC solution can 1) support multiple assets across multiple networks, and 2) integrate with existing systems.

There are components within DLT networks that are very technical in nature which may hinder institutional investors' appetite to weave through the technical concepts and thus expose them to risk that they may not have been exposed to in traditional financial markets where they may rely on standard and well-established due diligence processes. For investors, this risk is only amplified by the limited insurance DA custodians may purchase given the inherent risk that assets on chain may be exposed to cyber hacks on public networks, their proness to compatibility issues as well as the risk of inadequate reporting due to various data source and network monitoring tools.

Section 4 – What Should Asset Owners Expect

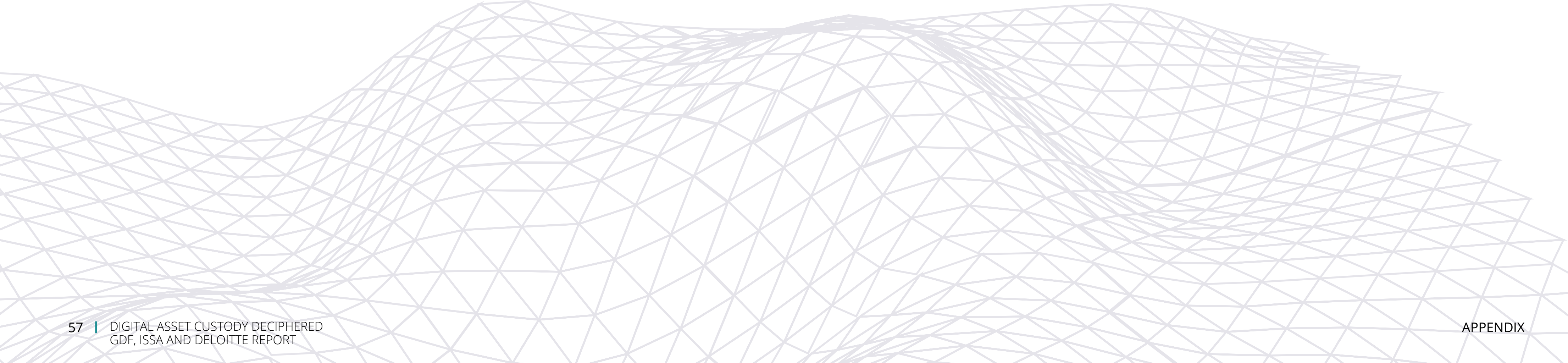
Section 4 summarizes the considerations that investors should strive to clarify in their contracts when subscribing for the provision of DAC services, including but not limited to:

Considerations pertaining to **ownership and bankruptcy remoteness** focus on how and where an investor's digital asset may be considered property. This has significant consequences in the insolvency of the custodian or potentially other providers such as platforms and exchanges - even if the asset is considered property. It is crucial investors seek to obtain as much clarity and legal certainty in these respects as possible, and contracts should make clear whether a DAC provider has the right to commingle client and proprietary assets in a way that may impact ownership rights in the event of insolvency of the provider or some other party upon whom ownership rights depend. This also emphasizes the need for contacts to clarify the liability provisions of the custodial relationship and the extent to which investors' assets are insured if assets are lost.

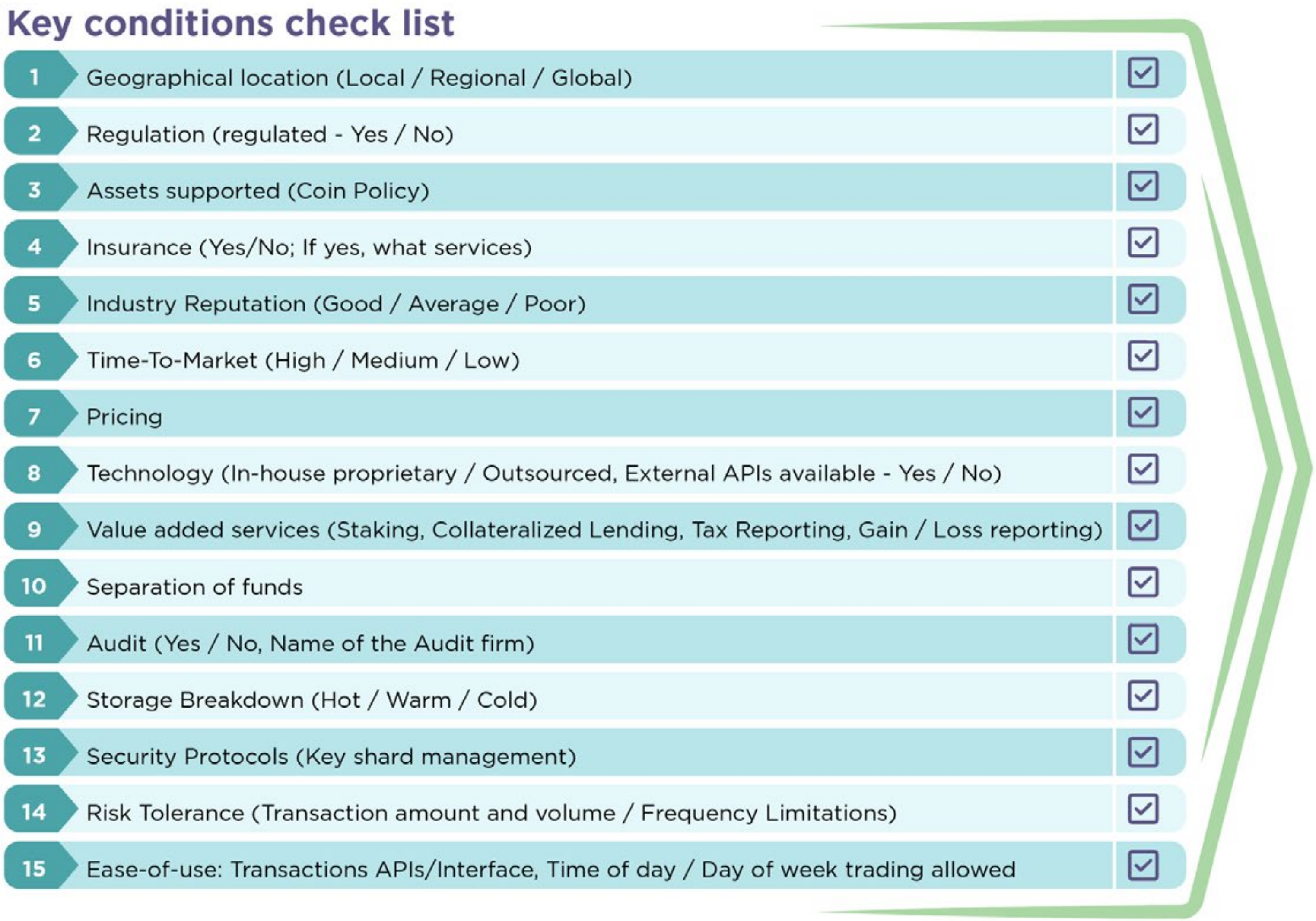
Considerations pertaining to **access and control** hone in on how intermediation structures in a DAC context may differ from those operating in TradFi and how this may impact the investor's rights under the contract with the provider, furthermore emphasising the importance of thorough due diligence and contractual clarity. Where applicable, custody documentation must incorporate any arrangements relating to hot and cold wallet storage, document the custodian's control of assets through the trading lifecycle, and, when relying on more advanced encryption techniques, document who the actors responsible for distributing to assets under management and ensure investors consent to who these actors are.

Considerations pertaining to **transacting risks** emphasise how the variance in network fees on public chains may impact a digital asset custodian's fee model, how the concept of end-of-day reporting may need to be revisited in DLT markets, and lastly how the moment of legally binding settement in DLT markets has variables that do not exist in traditional financial markets and will therefore also be subject to being reconceptualised. Investors must have visiblity of all of these considerations when purchasing DAC services.

Evolution in technology and the growth of the DAC market will drive **standards creation and adoption** across the market, and regulation will follow or evolve in jurisdictions where it has begun. Investors must take heed of these evolutions and seek to understand how it may influence the terms of their contractul agreements with their custodians and the safety of their assets in custody.



APPENDIX B – **Key Consideration Checklist**



Key conditions check list

1 Geographical location (Local / Regional / Global) ☑

2 Regulation (regulated - Yes / No) ☑

3 Assets supported (Coin Policy) ☑

4 Insurance (Yes/No; If yes, what services) ☑

5 Industry Reputation (Good / Average / Poor) ☑

6 Time-To-Market (High / Medium / Low) ☑

7 Pricing ☑

8 Technology (In-house proprietary / Outsourced, External APIs available - Yes / No) ☑

9 Value added services (Staking, Collateralized Lending, Tax Reporting, Gain / Loss reporting) ☑

10 Separation of funds ☑

11 Audit (Yes / No, Name of the Audit firm) ☑

12 Storage Breakdown (Hot / Warm / Cold) ☑

13 Security Protocols (Key shard management) ☑

14 Risk Tolerance (Transaction amount and volume / Frequency Limitations) ☑

15 Ease-of-use: Transactions APIs/Interface, Time of day / Day of week trading allowed ☑

Exhibit 7

© Deloitte 2023

APPENDIX C – **Endnotes**

NB: This page lists the sources that were referenced intra-text throughout the report.

[i] *Markets Media Group, "Institutions to Allocate 5.6% to Tokenized Assets by 2026" (September 2023), by Shanny Basar.*

[ii] *EY-Parthenon, "How tokenization in asset management is driving meaningful opportunity" (August 2023):*

[iii] *Luxembourg publishes law of 22 January 2021 on distributed ledger technology and issuance of dematerialized securities (Deloitte)*

[iv] *Digital Assets and Private Law (UNIDROIT)*

[v] *Report on the DLT Pilot Regime (European Securities and Markets Authority)*

[vi] *Regulatory Sandbox (Financial Conduct Authority)*

[vii] *SEC Proposes Enhanced Safeguarding Rule for Registered Investment Advisers (SEC)*

[viii] *Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (MiCA)*

[ix] *Financial Action Task Force, Updated Guidance for a Risk-Based Approach To (Virtual Assets and Virtual Asset Service Providers, 2021)*

[x] *Travel Rule Requirements by Jurisdiction (Notabene)*

[xi] *Staff Accounting Bulletin No. 121 (SEC)*

[xii] *https://www.iso.org/standard/27001*

[xiii] *https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report*

[xiv] *https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets*

APPENDIX D – **Glossary**

Term	Definition
Airdrop	It is a process of sending newly minted tokens to hundreds or thousands of different wallet addresses with the hope recipients will be more inclined to engage with the corresponding project even if it's only to learn how to cash out the free tokens into something else.
Asset owner sovereignty	It is concept of hybrid custody that sits between self-custody and custody provided by an intermediary
Automated Market Makers	Automated market making protocols are smart contracts on a DLT that automatically provide a price to exchange digital assets.
Automatic Programming Interfaces (API)	Known as Application Programming Interface. A set of sub-routines definitions, communication protocols and tools for sharing data between different systems.
Bankruptcy remoteness of assets	A bankruptcy-remote entity is typically prohibited from incurring debt or other obligations and is limited in its purpose and the activities in which it may engage.
Basel Committee on Banking Supervision Standard (BCBS)	The Basel Framework is the full set of standards of the Basel Committee on Banking Supervision (BCBS), which is the primary global standard setter for the prudential regulation of banks.
Cryptography	A technique using codes and ciphers to encrypt and decrypt sensitive information, messages, or data. The art of privatizing and ousting unwanted actors from information.
De minimis principal	De minimis is a legal principle which allows matters of insufficient importance or small scale to be exempted from a rule or requirement.
Decentralized Autonomous Organizations (DAOs)	A DAO is a decentralized autonomous organization, a type of bottom-up entity structure with no central authority.
Decentralized custody	It uses a novel security model reliant on a network of private and randomly grouped nodes to ensure privacy instead of relying on single custodian
Deed polls	A deed poll (plural: deeds poll) is a legal document binding on a single person or several persons acting jointly to express an intention or create an obligation.
Digital asset(s)	In the digital asset space, custodians operate in a similar fashion to traditional financial markets in that their primary role remains the responsibility for, and the safeguarding of customer's digital assets. They act as participant in network nodes which are connected via consensus mechanism.
Digital Ledger Technology (DLT)	(DLT) is a system of electronic records that enables independent entities to establish a consensus around a shared ledger without relying on a central authority to provide or authenticate the authoritative version of the records.
DLT network nodes	Every device on a distributed ledger network stores a copy of the ledger.
DVP transaction	Delivery versus payment (DVP) is a securities industry settlement method that guarantees the transfer of securities only happens after payment has been made.

Term	Definition
Ethereum Virtual Machine (EVM)	The Ethereum Virtual Machine (EVM) is a core piece of Ethereum that helps power the DLT and smart contracts. It is vital in assisting Ethereum to achieve user adoption and decentralization
Ethereum	A public DLT network launched in 2016 and a cryptoasset that aims to compete with fiat currencies as a means of exchange. It has no intrinsic value, asset backing or links to other projects and is not backed by any authority such as a central bank. Ethereum is not a security but a commodity (at least within the USA)
Forking	A fork happens whenever a community makes a change to the DLT's protocol, or basic set of rules.
Generative Artificial Intelligence	ChatGPT and other AI tools to aid growth of Digital assets
Group 1 cryptoassets	Those that meet a full set of classification conditions. Group 1 cryptoassets include tokenized traditional assets (Group 1a) and cryptoassets with effective stabilization mechanisms (Group 1b), which would be subject to at least equivalent risk-based capital requirements based on the risk weights of underlying exposures as set out in the existing Basel capital framework
Group 2 cryptoassets	Those that fail to meet any of the classification conditions. As a result, they pose additional and higher risks compared with Group 1 cryptoassets and consequently would be subject to a newly prescribed conservative capital treatment.
Insolvency-remote	it determines whether a claimant has a claim to property that is ringfenced from anyone else's balance sheet
Interoperability between DLT networks	DLT interoperability refers to the ability of different DLT networks to communicate with each other, enabling the seamless transfer of messages, data, and token
Miners	Miners are found in Proof-of-Work (PoW) DLT networks and are required to solve complex mathematical equations to compete for the chance to verify transactions.
Non-Fungible Tokens (NFTs)	Non-fungible tokens (NFTs) are assets that have been tokenized via a DLT. They are assigned unique identification codes and metadata that distinguish them from other tokens.
Peer-to-Peer (P2P) protocol	Peer-to-peer refers to the direct exchange of some asset, such as a digital currency, between individual parties without the involvement of a central authority.
Permissioned DLTs	A permissioned DLT is a distributed ledger that is not publicly accessible. It can only be accessed by users with permissions. The users can only perform specific actions granted to them by the ledger administrators and are required to identify themselves through certificates or other digital means.
Permissionedless DLTs	A permissionedless DLT is a distributed ledger that is publicly accessible and has limited controls on the participants.
Proof-of-stake (PoS)	Proof of stake (PoS) is a consensus protocol in DLTs. It is a way to decide which user or users validate new blocks of transactions and earn a reward for doing so correctly.
Proof-of-Work	Proof-of-work is the consensus algorithm used by the Bitcoin Network. Miners provide an external resource – computer power – in order to participate in the block validation process.

Term	Definition
Qualified Custodians	Holding, directly or indirectly, client funds or securities, or having any authority to obtain possession of them. As it relates to cryptocurrency, custody commonly refers to holding a client's private keys.
Real-world assets	Real-world assets (RWAs) are tangible assets or financial primitives with the potential to serve as collateral in the Decentralized Finance industry
Ren	Decentralized protocols that enable the movement of digital assets from one chain to another
Standard settlement instructions (SSIs)	Standard settlement instructions (or SSIs) are one of the most important reference data sets in the financial industry. For a given trade or cash movement, they identify the accounts that assets and money should be credited to, the market or place of settlement and through which custodians/intermediaries the communication should flow
Stop-Loss	A stop-loss or stop-loss order is the automatic liquidation of assets when the market price reaches a certain level. Users stipulate the price at which a stop-loss occurs.
Token Standards	Token standards are the set of rules, conditions, and functions that dictate how a crypto token works. Common token standards include- ERC-20, ERC-721, ERC-777, ERC-1155
Tokenization	Tokenization refers to a process by which a piece of sensitive data, such as a credit card number, is replaced by a surrogate value known as a token. The sensitive data still generally needs to be stored securely at one centralized location for subsequent reference and requires strong protections around it.
Validators	Validators are responsible for verifying the validity of transactions of Proof-of-Stake (PoS) DLT networks, which employs the help of validators through a selection process.
Wallet	It's a storage facility for cryptocurrencies. A software that allows users to store their cryptocurrencies in a UI/UX friendly way. Abundant in formats; paper wallet, web wallet, desktop wallet, hardware, and mobile wallets.
Wash Trading	Wash trading is a process whereby a trader buys and sells a security for the express purpose of feeding misleading information to the market
Wholesale CBDC	CBDCs designed for use among financial intermediaries only

REFERENCES AND RESOURCES

Report References

NB: This page lists all the sources that were referenced in the footnotes of the report, where further explanation - usually legal analysis - was provided to better the understanding of the reader

BCG and ADDX Report on "Relevance of on-chain asset tokenization in 'crypto winter', by Sumit Kumar, Rajaram Suresh, Darius Liu, Bernhard Kronfellner and Aaditya Kaul, published in August 2022.

Digital Assets: Final Report, UK Law Commission

FSB Global Regulatory Framework for Crypto-Asset Activities, Financial Stability Board (FSB)

'National Blockchain Laws as a Threat to Capital Markets Integration', Uniform Law Review, Matthias Lehmann

Policy Recommendations for Crypto and Digital Asset Markets Consultation Report, The International Organization of Securities Commissions (IOSCO)

Principles on Digital Assets and Private Law, International Institute for the Unification of Private Law ("UNIDROIT")

U.S. Securities Exchange Act of 1934

Industry Report Repository

NB: This page is a short repository of other industry reports that broach the topic of DAC that were not referenced in the report

2022 Digital Asset Outlook, The Block

A Market Overview of Custody for Digital Assets: Digital Custodian Whitepaper, Deloitte

Custody of Cryptoassets: Moving Towards Industry Best Practice, Clifford Chance

Digital Asset Custody: An AIMA Industry Guide, The Alternative Investment Management Association (AIMA)

Digital Asset Custody Paper, Hogan Lovells

Digital Digest: Symbiotic Solutions: The Role of Industry, Technology and Regulations in Meeting the Challenges of a Digital Future, State Street

Hot Topic: Digital Assets: Evaluating custody of digital assets, KPMG

Institutional Investing 2.0: Migration to Digital Assets Accelerates, BNY Mellon

Report: Institutional Digital Asset Custody, GSR

State of digital asset custody: Understanding and implementing digital asset custody for institutional investors, PWC

Swiss Digital Asset Custody Report 2023, Home of Blockchain.swiss

GDF HEADQUARTERS:
Kemp House
160 City Road
London
EC1V 2NX
United Kingdom

FOLLOW GDF:
𝕏 @GlobalDigitalFi
in Global Digital Finance
M @GlobalDigitalFinance

CONTACT GDF:
e: hello@gdf.io
w: www.gdf.io

ISSA HEADQUARTERS:
c/o SIX Group AG
Hardturmstrasse 201
P.O.Box CH-8021
Zurich
Switzerland

FOLLOW ISSA:
in ISSA - Intl Securities Services Association

CONTACT ISSA:
e: issa@issanet.org
w: www.issanet.org

DELOITTE HEADQUARTERS:
1 New Street Square
London, EC4A 3HQ
United Kingdom

FOLLOW DELOITTE:
in Deloitte

CONTACT DELOITTE:
e: ukfsnetwork@deloitte.co.uk
w: www.deloitte.co.uk

The information contained in this report is based on sources believed to be accurate but is subject to change or correction at any time without notice – accordingly, the accuracy of any information contained herein cannot be guaranteed and neither the individual named as sponsor of or author of or contributor to this report nor any of GBBC Digital Finance, the International Securities Services Association or their member firms, as well as State Street, Metaco, Brown Brothers Harriman, and Deloitte, including partners, employees or associates, shall be liable for any errors in the event of reliance on this information. The material contained in this report is for general information and reference purposes only and is not intended as legal, tax, accounting, investment, financial or other professional advice on any matter, and is not to be used or relied upon as such.

This report, and the statements contained herein, are not an offer or solicitation to buy or sell any products (including financial products) or services mentioned or to participate in any particular strategy and should not be construed as such. This report is not intended for distribution to, or use by, any person or entity in any jurisdiction or country in which such distribution or use would be contrary to local law or regulation.

Any discussion of tax matters contained in this publication is not intended or written to be used, and cannot be used, for the purpose of avoiding penalties under the U.S. Internal Revenue Code or promoting, marketing or recommending to another party any transaction or matter.