Digital asset custody deciphered: A primer to navigating the challenges of safeguarding digital assets

Received (in revised form): 9th November, 2023

Colin Parry
Chief Executive Officer, International Securities Services Association, Switzerland

Colin Parry

Colin Parry *is Chief Executive Officer of the International Securities Services Association (ISSA). He is responsible for creating and executing the ISSA strategy, growing the membership and ensuring that ISSA continues to help shape the future of the securities services industry through developing solutions and reducing risk. He also runs his own consulting business. Prior to joining ISSA in September 2019, Colin co-founded a FinTech (Atomic Wire) and set up his own consulting business after almost 25 years at UBS. At UBS he held a number of senior roles in the US, UK and Switzerland in both operations and finance, including running the global investment banking operations and creating finance shared services. Colin holds a Bachelor's degree in money, banking and finance from Birmingham University (UK) and graduated from the Royal Military Academy Sandhurst.*

International Securities Services Association, c/o SIX Group Services AG, Pfingstweidstrasse 110, CH 8005 Zurich, Switzerland
Tel: +44 (0)7398 752014;
E-mail: colin.parry.issa@six-group.com

Journal of Securities Operations & Custody
Vol. 16, No. 2, pp. 106–117

1753-1802

ABSTRACT

The International Securities Services Association (ISSA), Global Digital Finance and Deloitte have co-authored a report on Digital Asset Custody. This paper gives a synopsis of one element of the report and provides a brief explanation of digital asset custody (DAC) and the key facets that should be considered when looking at a DAC solution. DAC is different from traditional asset custody but it is not totally different. There are complexities that occur uniquely within DAC, and it is imperative that managers understand those aspects and the implications, such as permissioned versus permissionless ledgers, key management, etc. There are also a number of familiar terms used in DAC in a different way from traditional markets and is necessary for managers to challenge the existing wisdom for both DAC and traditional custody. To progress the opportunities that DAC — through distributed ledger technology (DLT) and tokenised assets — offer financial markets, however, the industry should not throw away all the learnings from traditional custody offerings. Custodians (in the widest sense) should merge their knowledge of safekeeping principles with the new abilities offered by DAC to ensure that they can manage the risks of operating in this new environment. An example of a new risk is that DLT evangelists will say 'Blockchain is instant and immutable and therefore guarantees finality', but is it true in all or any circumstance? Risk management starts with risk awareness and the purpose of this paper is to explain the risks that occur in the scenarios of providing or purchasing DAC.

Keywords: DLT, custody, digital asset custody, safekeeping

INTRODUCTION

As we near the end of the first quarter of the twenty-first century, it is clear to many that digital technology is moving at a faster pace than executives, policymakers and governments, regulators and agencies — and even leading technologists — can keep up with. Digitally dematerialised assets safely and legally bought, sold and settled across jurisdictional borders 24/7 by investors is something that the current global financial system and regulations were not designed to do.

The impact of decentralised innovation through inexpensive and readily available

computing technology connected to the network, and in the hands of digital innovators and consumers alike, has profoundly changed many of our daily habits, routines and, in some cases, our lives.

We spend an average of over three hours a day on our smartphones: communicating, reading and watching content, shopping, banking, booking our travel, working and more. This supercomputer in our hands allows us to access the ubiquity of global knowledge and services on offer on the web and digital financial services are the heart of this digital economy.

Distributed ledger technology (DLT) has been with us for 15 years and the development of new ecosystems and digital assets is breathtaking. While showing great promise in playing a significant role in the digital transformation of our global financial services infrastructure, the technology has often been mired in controversy, highly politicised and conflated through rhetoric and information asymmetry from all sides of the spectrum.

Many of us leading this next era of digital transformation, from innovators to 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, however, take a lot of patience, understanding, hard work and, as seen, failures for this transformation to be successful. A significant commitment to work together is required by industry, policymakers and regulators.

This paper is a synopsis of the recently issued ISSA, GDF and Deloitte report[1] and provides a brief explanation of digital asset custody (DAC) and the key facets that should be considered when looking at a DAC solution. It should be noted that, throughout this paper, the terms 'custodian', 'traditional custodian' and 'digital custodian' are used to denote all forms of regulated custody providers wherever that service is provided from, ie both a custodian or a financial market infrastructure (FMI) such as a central securities depository (CSD), whether in traditional asset custody or DAC.

DAC has been described as the Gordian knot of digital assets — without solutions the market will not gain traction and liquidity. It is the author's view that without solving for DAC, many investment funds across the world will be unable to invest into digital assets.

DLT has the potential to transform financial services and have an impact on capital markets and traditional market structures (see Figure 1). To help realise 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.

DEFINITION OF DAC

A custodian's role has traditionally consisted of a combination of three main functions:

- Holding physical securities or records of ownership rights in dematerialised ('book-entry') securities and fiat currency on behalf of a customer.
- Acting on instructions to facilitate the settlement (the change in ownership) of transactions in those securities on behalf of the relevant customer.
- Facilitating the exercise of other rights, entitlements and obligations associated with ownership of such securities.

Like traditional custody, DAC refers to the safekeeping, settlement and asset servicing of an investor's assets. With DAC, however, roles, rules, regulations and responsibilities are far less settled and there is little legal

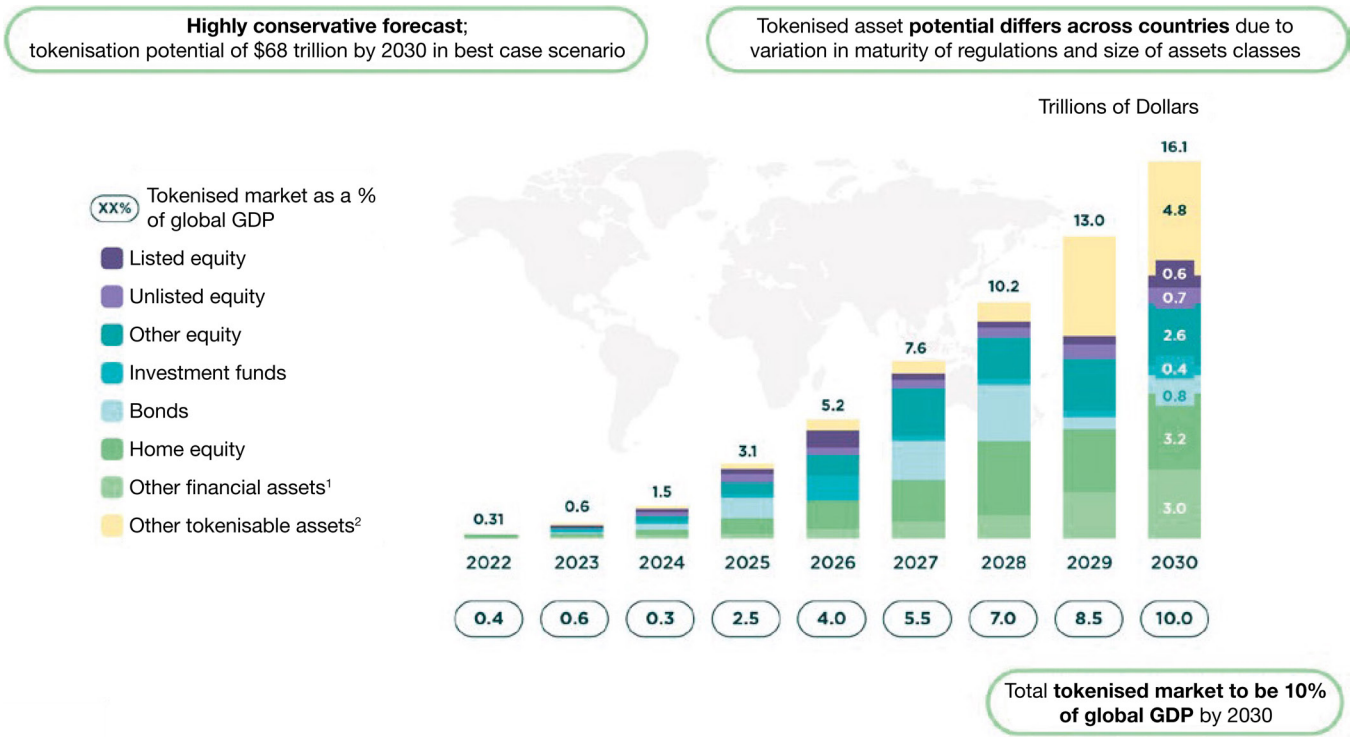

Figure 1 Tokenisation of illiquid assets to be US$16tr worth opportunity globally
Source: BCG and ADDX[2]

precedent. Digital assets can be bought on an exchange, 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. Digital custodians are responsible for securing these private keys to access the asset on behalf of the asset holder. Corporate actions and other rights and entitlements can be managed via smart contracts or the ledger. Ledgers are either permissioned or permissionless and may (or may not) use third parties to establish consensus. Additionally, within these two categories, are many different technology protocols which can behave and perform differently to each other and must also be considered.

As the explanation above shows, DAC is different from the legal act of custody as commonly understood today. Furthermore, there are different types of DAC available for investors:

- *Self-custody*: The investor is responsible for securing its digital assets by making use of hardware, software or paper wallets. The author believes this is inappropriate for institutional 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 get access to a digital wallet. For an investor, this is similar to third-party custody, but it involves different risks.

While many of the principles that apply in the context of traditional custody should also be applied to DAC, it is important that

the lessons from recent industry failures are learned and that an organisation offering DAC should 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.

Some activities required for DAC are recognised in traditional securities services as roles performed by a custodian or FMI. It is broadly accepted, however, that in relation to digital assets, new operating models, capabilities and controls may be required to provide those services effectively. The tokenisation of 'real-world' assets has the potential to enable the further democratisation of finance and contribute to the transformation of financial markets over the next decade.

The use of blockchains is not limited to cryptocurrencies; it also includes a wide variety of assets that are being represented on-chain, including the tokenisation of existing asset classes and digitally native assets such as tokenised real estate, etc. (see Figure 2). In addition to different types of digital asset, the particular characteristics of the DLT which is used is also relevant to provision of custody. Broadly, there are two categories network: public decentralised and permissioned private networks. The operating models, appropriate risk and control functions and available safeguards and governance differ significantly between these two models. Within these two network categories, the specific technology protocols used have an impact. As a result, custody providers need to perform their own assessment on which assets, networks and technology protocols they are willing to service.

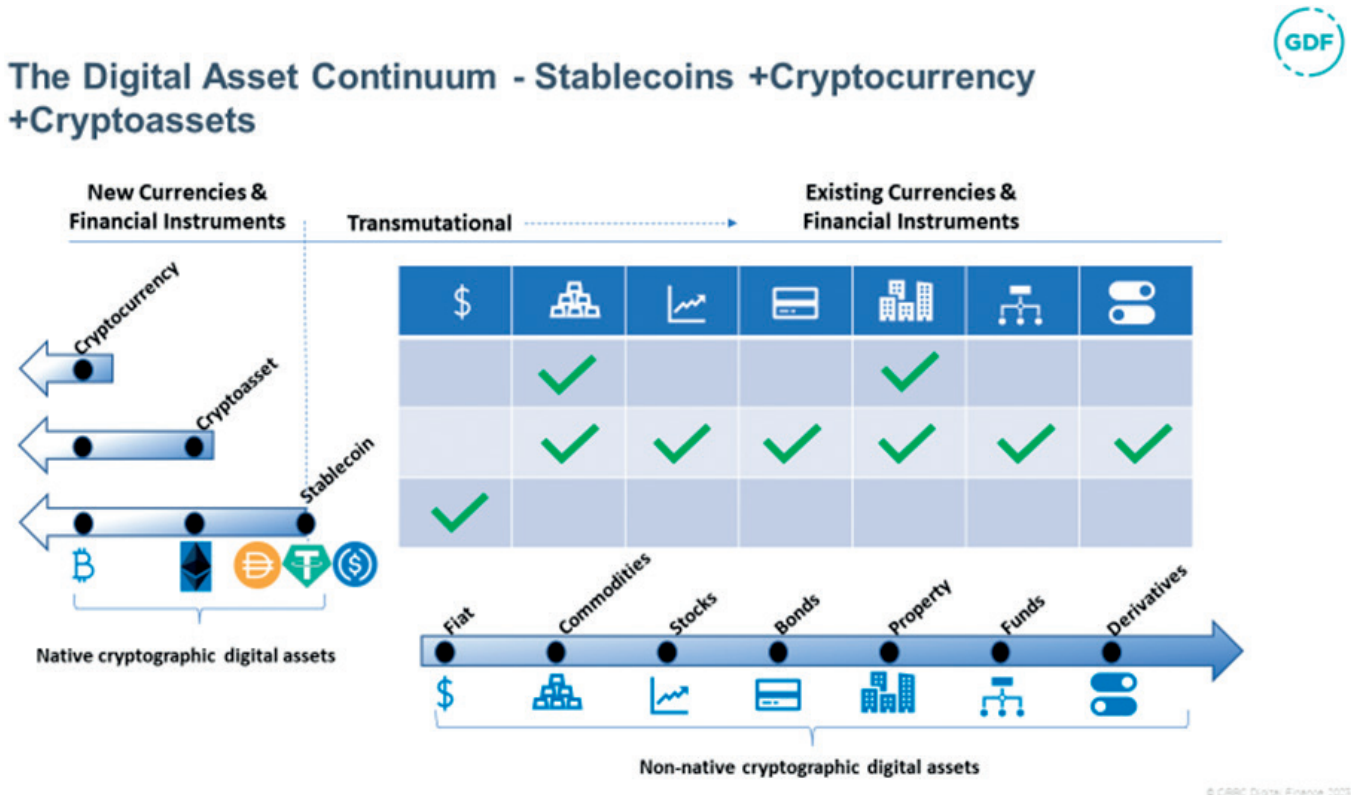

Figure 2 The digital asset continuum

It is also important to recognise 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 paper does not address these requirements (opportunities), nor does it address the ability of custodians to effect the transformation of traditional securities to digital assets and back again.

DAC ENVIRONMENTAL CHALLENGES

There are, inevitably, challenges that need 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 for the markets.
- Who will lead and bear the cost of this (significant) digital transformation should the financial markets move to DLT is unclear.
- 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 (eg maintenance of appropriate segregation and of appropriate levels of control), ensuring investor property can be identified as and when necessary.
- 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 recognised 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.

Many of these challenges are seen in the traditional securities sphere and have largely been overcome through the creation of standards and market practices that 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.

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) and over what time frame adoption may occur. If it does become the preferred solution, this will take some time and will need to have a (proven) period of co-existence even in an individual market. As with all technological changes, DLT is in competition with programmes to shorten the settlement cycle, provide more data and analytics and achieve cost savings.

SUMMARY LEVEL RISKS AND RISK MITIGATION

The author proposed a number of points regarding high-level risks and mitigants that investors and service providers should understand and apply in connection with DAC. These can be categorised as:

- Legal and regulatory considerations.
- Settlement finality and asset segregation.
- Other risks relevant to custody.

These risks are further explained below.

To ensure that the above are addressed, the industry — both custodians and investors — should look to:

- 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.
- 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'.
- 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.
- Support dialogue with anti-money laundering (AML)/know-your-customer (KYC) and sanctions authorities in order to achieve common aims so that KYC requirements, money laundering and other criminal activity risks and sanctions enforcement are effectively addressed while allowing digital asset ecosystems to operate effectively.
- Work with governors and/or operators of public DLT networks to establish transparent finality rules and processes. In these context governors refers to the legal entity or digital autonomous organisation (DAO) that controls the network behaviours.
- Work with the industry to establish principles and best practices for:
  - asset segregation;
  - ledger governance; and
  - interoperability.
- Advocate for bankruptcy remoteness of assets through statutory and regulatory reform or litigation, to ensure jurisprudence.
- Support of the adoption of global legal standards to cover DAC. Standardisation helps the market develop and creates less barriers.

EXPLORATION OF RISK FACTORS TO BE AWARE OF AS A DAC

Legal, regulatory and financial crime considerations

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

Property tends to be categorised either as tangible (ie in physical form, such as materialised/certificated securities, precious metals and the like) or intangible (eg in dematerialised or in uncertificated form, such as so-called 'book-entry' securities). An individual's property rights to an asset are generally enforceable as against the whole world, whereas 'contract' rights (eg over the counter (OTC) 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 characterisations, crystallise 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 to that asset. Characterisation 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, where investors generally will be given priority over claims from third parties such as creditors. In addition to the investor having property rights to 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').

The decentralised 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 recognising 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. These complexities increase where the laws of more than one jurisdiction apply.

In addition, 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. 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 may not be in synch with what is reflected on the distributed ledger at a particular point in time. Other complexities may be introduced, such as pre-funding where omnibus wallets are utilised or validation staking, with intermediaries potentially taking proprietary positions themselves.

Providers and users of DAC services face three key challenges in respect to regulation:

(1) The differences in asset definition — for example, the same asset being viewed as a different asset class (eg a security) or something else in another jurisdiction, or in some cases 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.

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 standardised processes such as regulatory reporting.

Safeguarding is a key obligation that custodians are required to satisfy. As described

previously, there are a range of complexities involved in ensuring the legal rights of digital asset owners. A common denominator, however, 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. While 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.

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/combatting the financing of terrorism (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.

One 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 tokenised real-world securities including its antecedents (see Figure 3).

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 the participant in the network facilitates financial transactions with sanctioned parties in violation of the law, but there is also no way to demonstrate that they are indeed facilitating financial transactions with sanctioned parties in violation of the law. Transaction fees do not create a direct payment from the initiator

Figure 3 Digital asset custodian

of a transaction to a miner. Whether this represents sufficient control is somewhat uncertain, but resolving this issue is critical to allow regulated financial companies to participate in this market.

Settlement finality and asset segregation

Providing custody services generally refers to an agent or trustee safekeeping 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 crypto-assets, 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 reorganisation, 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 utilise more centralised consensus models, 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.

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.

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 that reference individual wallet addresses using public keys, which are not equivalent to traditional custody accounts. Therefore, transaction records and wallets 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.

Other custody risks

Traditional securities services 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 centralised governance structures and traditional decision-making processes.

In contrast, public blockchain communities tend to socialise governance and decision making via open communities, opensource code repositories and increasingly through 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. This generates a number of novel risks in relation to digital constitutions, voter participation and asset forks, as well as the more usual cyber challenges.

Another atypical risk is that 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 (ie a transaction) that has been digitally signed by the asset owner. To digitally sign a transaction (ie to authorise a payment or execute an on-chain trade), the asset owner must use the specific private key that corresponds with the account they want to transact from. 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 include single-key splitting models, multi-signature models (involving multiple keys) and the use of hardware security modules (HSM), around which additional layers of authorisation review and control can be arranged. In an additional variation, certain private network deployments do not require participants to handle key management, and this is provided as a service by the platform operator (see Figure 4).

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 (wallets that are connected to the DLT infrastructure and available at any time) and cold wallets (wallets that are store keys off any network, such as in a safe or piece of paper, and therefore are not available in real time) as distinct solution components that address different custodial requirements, and are often used in combination.

There is no parallel for staking (see below) in the traditional financial models. This activity is rarely seen outside of the cryptocurrency markets and, so far, has not been seen in the tokenisation of real-world assets. Transaction validation and new block creation within proof-of-stake (PoS) networks, such as 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 (low) risk of significant and permanent loss of assets (eg '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.

An area where there is more commonality with the traditional markets is

	Standard single key	Multi-Signature (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	Medium impact: Update or redeploy smart contract	Low impact: Reconfigure MPC rules off-chain

Figure 4 Example considerations relating to the evaluation of key management options
Source: Deloitte

in interoperability or the lack of it. The 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 DAC solution can: (a) support multiple assets across multiple networks; and (b) 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. While 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.
- *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 multiple smart contracts. An example of required interoperability is for 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).
- *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 effect the seamless transfer of assets or data. When cyberattacks are cited as affecting DLT, it is the breaching of the security on these bridges that is generally being exploited.

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

Risk management starts with risk awareness and the purpose of this paper was to explain the risks which occur in the scenarios of providing or purchasing DAC. There are solutions of varying complexity and cost to these challenges and the full report describes a number of those mitigants.

CONCLUSION

For DAC to solve the issues of asset safety in digital assets, the whole industry needs to:

- 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.
- 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'.
- Develop a common understanding of how asset owners and/or investment managers should ensure contractual terms that are clear, address risks that are relevant to DAC and delineate between the responsibilities of a digital custodian and other market participants and service providers.
- Support dialogue with AML/KYC and sanctions authorities in order to achieve common aims so that KYC requirements, money laundering and other criminal activity risks and sanctions enforcement are effectively addressed while allowing digital asset ecosystems to operate effectively.
- Work with governors and/or operators of public DLT networks to establish transparent finality rules and processes. In these context governors refers to the legal entity or DAO that controls the network behaviours.
- Work with the industry to establish principles and best practices for:
  - asset segregation;
  - ledger governance; and
  - interoperability.
- Advocate for bankruptcy remoteness of assets through statutory and regulatory reform, or litigation, to ensure jurisprudence.
- Support the adoption of global legal standards to cover DAC. Standardisation helps the market develop and creates less barriers.

Further work is needed on these topics not just by individual companies but through collaboration, connecting and change in order to shape the future of securities services.

References

(1) GBBC Digital Finance (GDF) (2023), 'GDF, ISSA and Deloitte Report: Digital Asset Custody deciphered :A Primer to Navigating the Challenges of Safeguarding Digital Assets', available at https://issanet.org/content/uploads/2023/10/Custody-Report_07.10.2023.pdf (accessed 9th November, 2023).

(2) Kumar, S., Suresh, R., Liu, D., Kronfellner, B. and Kaul, A. (2022), 'Relevance of and on-chain asset tokenization in "crypto winter"', Boston Consulting Group (BCG), available at https://documents.addx.co/relevance_of_onchain_asset_tokenization_in_crypto_winter.pdf (accessed 9th November, 2023).