



2023 | GDF, ISSA AND DELOITTE REPORT

DIGITAL ASSET CUSTODY DECIPHERED

Key Takeaways

Preface

GBBC Digital Finance (GDF) and the International Securities Services Association (ISSA) have published a report on digital asset custody (DAC). This report has been produced in a joint Custody Working Group, a collaboration between GDF and ISSA, supported by their member firms and the Working Group Secretariat, Deloitte.

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.

This document outlines the key takeaways from the report's three section domains and each of their respective subsections:

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

These takeaways condense the key considerations for 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.

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.



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

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

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

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 explicit 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.

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. As 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 proneness 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 settlement 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 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. ■



GDF HEADQUARTERS:

Kemp House
160 City Road
London
EC1V 2NX
United Kingdom

FOLLOW GDF:

 @GlobalDigitalFi
 Global Digital Finance
 @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:

 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:

 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.