30 September 2022

Basel Committee on Banking Supervision
Bank for International Settlements
CH-4002 – Basel
Switzerland

Via Electronic Submission at www.bis.org/bcbs/commentupload.htm

RE: Consultative Document, Second consultation on the prudential treatment of cryptoasset exposures (Issued 30 June 2022)

Ladies and Gentlemen:

The Bank of New York Mellon Corporation, State Street Corporation and Northern Trust Corporation (collectively, the Custody Banks) appreciate the opportunity to comment on the *Second consultation on the prudential treatment of cryptoasset exposures* (Second Consultation) published by the Basel Committee on Banking Supervision (Committee) on 30 June 2022.[1]

The Custody Banks have participated in various trade association responses to the Second Consultation (Joint Trade responses). These responses address important aspects of the banking industry's general interest in cryptoassets and highlight the unique ways in which the industry can support responsible innovation and thereby mitigate existing and potential risks resulting from such assets. The Custody Banks' response is intended to complement the Joint Trade responses by providing the perspective of banks that specialize in the provision of safekeeping and asset administration services. The safe custody of client

[1] The Bank of New York Mellon Corporation is headquartered in New York, New York (United States) and delivers wealth management and investment services to institutions, corporations, and individual investors. As of June 30, 2022, The Bank of New York Mellon Corporation had US $43 trillion in assets under custody/administration and US $1.9 trillion in assets under management.
State Street Corporation is headquartered in Boston, Massachusetts (United States) and specializes in the provision of financial services, including investment servicing, investment management, data and analytics, and investment research and trading, for institutional investor clients. As of June 30, 2022, State Street Corporation had US $38 trillion in assets under custody/administration and $3.5 trillion in assets under management.
Northern Trust Corporation is headquartered in Chicago, Illinois (United States) and provides asset servicing, asset management and banking for personal and institutional clients. As of June 30, 2022, Northern Trust had US $13.7 trillion assets under custody/administration and US $1.3 trillion in assets under management.

assets, including cryptoassets, is critical to customer protection and the stability of the financial system – key considerations for cryptoasset regulation.

I. Overview

The Custody Banks support the Committee's goal to establish minimum standards for the prudential treatment of cryptoasset exposures and the incremental steps which the Committee has taken in the Second Consultation to clarify its approach. At the same time, we believe that the intended framework is unnecessarily conservative in its treatment of the custody function and as such will impede rather than support the many benefits that distributed ledger technology (DLT) and related innovations provide, specifically: more resilient, transparent and efficient financial transactions. The prudential framework for cryptoasset exposures should recognize these benefits, striving in the process to align responsible innovation with safety and soundness.

To further that effort, we recommend the following changes to the framework:

1. Revising the proposed definition of "exposure" in section SCO60.4 to align with existing Basel definitions of exposure, which do not include assets held in custody;
2. Removing the proposed infrastructure risk add-on for Group 1a cryptoassets as the risks it seeks to address are adequately covered in other sections of the Second Consultation; and
3. Eliminating assets under custody from the proposed Group 2 exposure limit to allow banks to safekeep Group 2 cryptoassets at an operationally and economically viable level.

These points are explained in greater detail in parts II through IV of this letter. Without these changes, the intended framework for the prudential treatment of cryptoasset exposures will most likely dampen the ability of bank custodians to support the responsible development of the cryptoasset market and also discourage the types of technological improvements to market structures that prudential regulation should seek to support.

II. The proposed definition of "exposure" in section SCO60.4 should be revised to align with existing Basel definitions of exposure, which do not include assets held in custody.

The Second Consultation sets forth the following definition of "exposure" that is within the scope of the proposed cryptoasset exposure framework:

60.4 For the purposes of this chapter, the term "exposure" includes on- or off-balance sheet amounts that give rise to credit, market, operational and liquidity risks. It includes activities, such as non-fiduciary custodial services, that may only give rise to operational risk.[2]

[2] Second Consultation, page 7.

This definition is fundamentally at odds with the current legal and regulatory framework for banks' custody services, and disadvantages DLT-based custody systems as compared to traditional custody systems.

Legal and Regulatory Framework for Custody

Banking organizations are the primary providers of custodial and fiduciary services and also may safeguard cryptoassets when holding collateral or margin in secured financing and other client transactions. Depending on the scope of the definition of "exposure", some or all of these core, traditional banking services may fall within the proposed cryptoasset framework and therefore be subject to the infrastructure risk add-on, the Group 2 asset exposure limit and other provisions of the intended framework. We strongly oppose this approach. The resulting impact to capital from such an expansive definition of "exposure" would limit or even preclude banking organizations from providing these core services for cryptoassets, which would in turn impede responsible cryptoasset innovation.

The Custody Banks have a long history of providing safekeeping services for their clients, and their role as a trusted intermediary is well-understood by the market as essential in safely supporting client assets in an increasingly complex global financial system. The US Office of the Comptroller of the Currency (OCC) describes this role at length in an interpretive letter declaring that national banks are authorized to engage in digital asset custody activities, noting that "safekeeping services are among the most fundamental and basic services provided by banks…..OCC guidance has recognized that banks may hold a wide variety of assets as custodian, including assets that are unique and hard to value."[3]

The business relationship between a custody bank and its client is established according to a negotiated contract which sets out the scope of the services to be provided, key terms and conditions relevant to those services, the standard of care that the custody bank will exercise in carrying out its duties and the governing law of the contract.[4] The core components of a custody contract remain the same whether the services are being provided on a fiduciary or a non-fiduciary basis, although the commercial terms may vary. Assets held in custody by the banking organization belong to the client and are segregated at all times from the bank's own assets and those of its other clients, to ensure that the assets are bankruptcy remote and cannot be used to satisfy the claims of the custodian's creditors.

There is a clearly defined body of law that supports the client's ownership rights over assets held in custody. For instance, in the US, Article 8-503(a) of the Uniform Commercial Code (UCC) provides that financial assets held by a securities intermediary (*i.e.,* a custodian) for a customer (*i.e.* the entitlement holder) are not property of the securities intermediary and are not subject to claims of creditors of the securities intermediary. Furthermore, Article 8-102(9) of the UCC specifies that a 'financial asset' includes any property that is held by a securities intermediary (*i.e.* a custodian) for another person in a 'securities account', if the parties have expressly agreed that the property is to be treated as a financial asset under

[3] OCC Interpretive Letter 1170, Authority of National Banks to Provide Crypto-Currency Custody Services for Clients (July 22, 2020).

[4] See OCC Comptroller Handbook on Custody Services (January 2002), page 11: "Custody relationships are contractual in nature and are essentially directed agencies. The customer is the principal, and the custodian is the agent. The custody agreement is important as a risk management tool. The agreement should clearly establish the custodian's duties and responsibilities. Custody agreements should be standardized when possible, and any deviations from the standardized agreement should be reviewed prior to acceptance."

Article 8. More recently, there are active efforts underway to further clarify the treatment of cryptoasset exposures in the UCC, specifically by confirming that cryptoassets that fall within the scope of Article 8 and new Article 12 do not constitute property of the securities intermediary.[5] It is, in turn, a well-established principle of US bankruptcy law that assets held in custody are not available to the creditors of an insolvent bank. As an example, US courts have repeatedly affirmed that the Federal Deposit Insurance Corporation, in its role as receiver for failed banks, takes no greater rights in the property of the bank than the rights that the insolvent bank itself possessed.

Industry practice relating to the safekeeping of client assets has developed over time based on UCC requirements and other legal mandates. This includes Section 17(f) of the Investment Advisors Act of 1940, which requires mutual funds offered in the US to maintain their securities and other similar investments with entities under conditions designed to maintain the safety of fund assets. This also includes Rule 206(4)-2 of the Investment Advisors Act of 1940 (*i.e.* the custody rule) which specifies that if an investment advisor is deemed to have custody of client assets, the advisor must use a 'qualified custodian' to maintain those assets.

Additionally, industry practice for the safekeeping of client assets incorporates three core principles, which are designed to manage the potential risk of misappropriation or loss; they are as follows:

- Safekeeping operations must be functionally separated from trading and other similar activities;
- Client assets must be segregated at all times from the bank's proprietary assets and the assets of other clients; and
- Proper control over client assets must be maintained at all times, including in the case of cryptoassets, by control of the private keys in order to eliminate any 'single point of failure' in the record of ownership.

Based on these considerations, it is well-established as a matter of law and regulation that assets held in custody are not an exposure of the bank and therefore do not create risks that require capitalization outside of the existing framework for operational risk. Indeed, it is altogether unclear whether it is even appropriate to characterize assets held in custody as an off-balance sheet exposure as suggested in proposed section SCO60.4, since this implies the presence of potential credit, market or liquidity risk that does not exist. It is also worth noting, in this respect, that the Basel III Accord does not refer to assets held in custody as an off-balance sheet item.[6] Furthermore, any such characterization would trigger leverage capital requirements that are wholly inappropriate for the custody related activities of a bank, including the safekeeping function.

For these reasons, we believe that it would be inappropriate for the Committee to use the Second Consultation to fundamentally alter the existing capital treatment applied to assets held in custody. We therefore urge the Committee to remove the reference in proposed SCO60.4 to "non-fiduciary custody activities." Furthermore, we also request express confirmation that the add-on for infrastructure risk for Group 1a cryptoassets and the Group 2 exposure limit (discussed in section III and IV, respectively) do not apply to the safekeeping of client assets.

---

[5] See 'UCC Digital Asset Amendments Finalized', Cleary Gottlieb, July 21, 2022.

[6] Basel Committee on Banking Supervision, Basel III leverage ratio framework and disclosure requirements (January 2014).

III. The proposed infrastructure risk add-on should be eliminated, as the risks it seeks to address are already well covered in other sections of the Second Consultation.

The Second Consultation proposes to include a 2.5% risk weighted asset (RWA) add-on to all Group 1 cryptoassets to cover various 'unforeseen risks' that the use of DLT infrastructure by banks may pose. While we acknowledge that DLT infrastructure is relatively new and evolving, the proposed, sweeping add-on is inconsistent with the Committee's principle of technology neutrality, overlaps with requirements that are found elsewhere in the Second Consultation and risks several negative consequences.

As the Committee acknowledges, Group 1a cryptoassets are simply digital representations of traditional assets where the record of ownership is established and accounted for using blockchain-based systems rather than the electronic data systems most commonly used today. Blockchain is a shared immutable chronological record of assets (*i.e.* a digital ledger) that uses cryptographic techniques to securely record transactions. Blockchain provides distributed control, a shared version of the truth and a time-stamped archive of all activities. Blockchain systems incorporate identity management functionality, a consensus based decision-making process and smart contract capabilities. The design, structure and governance of blockchain are key to defining the appropriate operational model for cryptoassets, including, in the case of the Custody Banks, the organization of the safekeeping function. In today's environment, permissioned-based blockchain systems offer the greatest level of security due to carefully defined governance structures, restrictions on access to specifically designated parties and the presence of a ruleset to control user participation. As a result, permissioned-based blockchain systems are the 'back-bone' of ongoing industry efforts to reinvent, and thereby enhance, efficiencies and reduce risk, in core financial market processes, such as collateral management and securities settlement.

Consistent with their essential role in the financial ecosystem, banks are subject to comprehensive prudential mandates designed to ensure that their activities are conducted in a safe and sound manner. This extends to the use of new technologies, which banks are required to support with robust firm-wide risk management programs designed to properly identify, manage and control pertinent risks throughout the deployment lifecycle: from the initial project stage, to assessment, validation and testing, to implementation and integration within the technology environment, to the ongoing monitoring and review of outcomes. This rigorous control framework is implicitly recognized by the Committee in proposed section SCO60.130 where it lays out detailed expectations for banks regarding the management of 'cryptoasset technology risk.'

These expectations are broken down by the Committee into four discrete categories covering: (i) the stability of the blockchain, including among other matters, the reliability of the source code, organization of the protocol, capacity constraints, systems scalability, testing protocols and the organization of the consensus mechanism, (ii) core design features, notably whether the blockchain system is permissioned or permissionless, (iii) service accessibility and control of the private cryptographic keys, and (iv) trustworthiness of node operators and other system participants.[7] Furthermore, proposed section 60.130 specifies additional considerations for banks relative to the management of information, communication and technology risk, cyber-risk, legal risk, money laundering and other financial crimes compliance

[7] Second Consultation, pages 32-33.

expectations, and considerations regarding the valuation of assets.[8] In effect then, a bank cannot as a practical matter make use of blockchain-based systems or engage in financial activities involving tokenized versions of traditional assets (*i.e.* Group 1a cryptoassets) unless it demonstrates to the satisfaction of its prudential regulators that it fully understands and has the ability to properly manage the resulting risk.

The Committee adds an additional layer of conservatism to its approach by requiring in proposed section 60.26 supervisory approval of all classification decisions made by banks, including 'reviewing and assessing bank's analysis and risk management and measurement approaches, and approving bank's demonstrations of whether and how a cryptoasset qualifies (as a Group 1a cryptoasset)'.[9] Furthermore, the Committee specifies that cryptoassets 'must be classified as Group 2 cryptoassets, unless the bank demonstrates to the supervisor that the cryptoasset meets all the required classification conditions.'[10] As such, the control framework which the Committee prescribes in the Second Consultation for activities involving Group 1a cryptoassets is already prescriptive and there is no compelling reason to add an additional layer of conservatism through the imposition of an infrastructure risk add-on. This is especially true since under proposed section 60.132, the Committee explicitly affirms the ability of regulators to apply an additional capital charge, or other similar quantitative limit, on any cryptoasset- related activity of a bank 'upon the identification of capital inadequacy or shortcomings in the bank's risk management.'[11]

While the use of a highly conservative approach to the treatment of Group 1a cryptoassets may seem entirely prudent, this approach has the potential for a series of unintended outcomes with important implications for the banking industry and the financial system as a whole. We strongly urge the Committee to bear in mind, in this respect, that recent instability in the cryptoasset market was not caused by any material lapse or failure of DLT itself, but rather by the inappropriate conduct an unstable business models of the entities operating in this space today, often without appropriate oversight. This includes unsustainable lending practices, inadequate customer disclosure, inappropriate commingling of various business functions and the systematic failure of entities to properly segregate client asset from their own assets. More broadly, this speaks to the imperative of ensuring that prudential solutions draw an appropriate distinction between the technology underlying cryptoassets (*i.e.* DLT or blockchain) and the various financial products which make use of this technology, where the prudential risks are not the same.

The Custody Banks would draw the Committee's particular attention to the following unintended outcomes that may result from the intended treatment of Group 1a cryptoassets.

Disruption of the Regulatory Capital Framework

The infrastructure risk add-on envisioned by the Committee is a novel metric without precedent in the regulatory capital framework for global banks. Its implementation would be transformative for the industry, compelling it to fundamentally reconsider the assumptions which drive risk-based capital today, including the role of information technology risk in the capital estimation process. Furthermore, the implementation of an infrastructure risk add-on could undermine the operation of core banking functions, including the provision of safekeeping services, which are offered today at scale and which are heavily reliant on technology solutions to drive efficiencies, reduce risk and control costs. We do not believe that

[8] Second Consultation, pages 33-34.
[9] Second Consultation, page 13.
[10] Second Consultation, page 13.
[11] Second consultation, page 34.

this is an appropriate outcome, especially when there is no evidence of any material failure by the banking industry to manage the risks that result from activities involving tokenized versions of traditional assets.

Similarly, the decision to deploy an infrastructure risk add-on for DLT systems will create a potentially disruptive precedent for the industry, opening the door to its broader use by prudential regulators in the context of other new technologies that are crucial to the continued reinvention of core systems and processes. This includes, for instance, the use of cloud-based solutions to better and more seamlessly manage data storage, data integration and data architecture needs, as well as the use of artificial intelligence solutions to strengthen anti-money laundering and financial crimes enforcement capabilities. Again, we do not believe that the Committee's approach to the regulation of Group 1a cryptoassets should create this broad-based uncertainty with respect to technology and innovation, especially in the absence of any demonstrated failing by the banking industry.

Internal Books and Records

Banking institutions and the broader financial services industry have for some time recognized that DLT is a secure and often superior method of recordkeeping. The benefits of DLT extend to the internal recordkeeping function of banks, many of which have spent considerable resources to implement solutions that drive efficiencies and reduce risk. As such, if adopted broadly, DLT and other similar technological innovations have the potential to materially strengthen the resilience of the financial system. However, proposed section SCO60.4 threatens to undermine this outcome by subjecting these uses of DLT to capital requirements that do not apply to financial activities using more traditional books and records systems.

The proposed cryptoasset framework should not create regulation that limits the design option for banks' internal books and records systems. Internal uses of DLT by banks are subject to existing risk management expectations and supervisory examination to ensure that the technology solution is sound and deployed in a manner that properly accounts for potential risks. Furthermore, internal uses of DLT do not present the same potential risks as transactional activities conducted on a public-facing blockchain. DLT-based systems that are fully controlled by a bank (via permission set-ups, node control or other restrictions on use and access) should be viewed as similar to the internal books and records systems currently in use across the industry. Transactional errors on a bank's internal books and records may be unilaterally corrected by the bank in a manner similar to any other intra-bank book entry mistake (*e.g.*, corrections can be made by the banks with the use of forks). Similarly, the relevant bank has control over third-party access to such systems, so that third parties are unable to direct the movement of assets through the system, just as they are unable to direct movements on traditional bank books and records systems. As such, the decision by banks to use DLT and other similar innovations as part of their internal books and record systems should not be subject to the requirements of the proposed cryptoasset framework since such an approach is unnecessary to ensure ongoing adherence by banks to core principles of safety and soundness.

Efficiency of Post-Trade Systems

The transformative implications of DLT for the financial system are well-understood and market participants have and continue to deploy new solutions that fundamentally re-imagine the way in which financial services and products are offered today. This includes the use of DLT in private equity administration, the automation of collateral management processes and the tokenization of traditional

assets. This effort to harness the innovative potential of new technologies also extends to post-trade processes, which are conducted at scale and which involve multiple counterparties, each with their own systems and records, that must continuously validate and reconcile key financial information until the transaction is complete. While this may occur on a bilateral or even trilateral basis, post-trade transactions are often conducted through centralized infrastructure, such as central securities depositories and national payment systems, that help support settlement finality and the resulting transfer of the record of ownership. Final settlement may take several days to complete, exposures which are mitigated through the exchange among counterparties of significant amounts of financial collateral.

Post-trade processes are complex and there are strong incentives for market participants to deploy new technologies to drive greater efficiencies and reduce risk. For instance, the advent of instantaneous settlement made possible by DLT would substantially reduce the need for intra-day credit, rationalize the role played today by various financial intermediaries, reduce complexity by eliminating multi-party reconciliations and substantially mitigate potential operational errors. In some cases, the efforts of market participants, including centralized infrastructure, to reinvent core post-trade processes are well-under way. For instance, the Australian Securities Exchange is actively working to replace the existing technology that supports the Clearing House Electronics Sub-Register System (CHESS), which serves as the central book of record in the local market, with a blockchain-based alternative. Similarly, the US Depository Trust and Clearing Corporation is working on a prototype (Project Lithium) to explore how a central bank digital currency might be used to facilitate clearing and settlement using blockchain technology, an initiative that is expected to: (i) reduce counterparty risk and trapped liquidity, (ii) increase capital efficiency, (iii) create a more efficient and automated workflow, (iv) better guarantee the delivery of cash and securities, and (v) improve transparency to regulators.

We are concerned that the implementation of an infrastructure risk add-on for Group 1a cryptoassets will have the effect of undermining these essential initiatives by creating unnecessary barriers to banking industry participation. While there appears to be a predisposition on the part of some regulators to view cryptoassets and their underlying technology only as a source of risk, the reality is much more complex, especially in the case of Group 1a cryptoassets (*i.e*., tokenized versions of traditional assets), which have the potential to drive vast improvements in core processes, an outcome that prudential regulation should actively support.

Dislocation of Financial Markets

As a general matter, the Committee defines Group 1a cryptoassets as tokenized versions of traditional assets which are equivalent in every material respect, including in the legal and economic rights which they convey. Consistent with this approach, the Committee emphasizes in proposed section SCO60.33 and 60.34 the importance of ensuring that the liquidity characteristics and market value of the tokenized asset remains consistent with that of the underlying traditional asset so as to mitigate any potential unforeseen credit or market risk. While we fully agree with the Committee's policy goal, we note that the implementation of an infrastructure risk add-on for tokenized versions of traditional assets will, as a practical matter, create the very bifurcation in market liquidity and value that the Committee wishes to mitigate. This reflects the greater costs that a bank will necessarily incur when transacting in the tokenized version of an asset relative to the underlying traditional asset due to the impact of the proposed infrastructure risk add-on. As such, the Committee's approach would result in a natural arbitrage opportunity for non-banks as they aggressively seek to exploit differences in market pricing caused by the

use of a novel risk add-on in the prudential framework. We believe that the Committee should seek to discourage such an outcome, especially in view of its negative implications for the consumer.

Recognizing these various considerations and outcomes, we urge the Committee to eliminate the use of an infrastructure risk add-on for Group 1a cryptoassets, relying instead on the existing Pillar II supervisory review process to address any residual concerns regarding 'unforeseen risk' in the new technology. Alternatively, the Committee could clarify that the infrastructure risk add-on does not apply to bank activities involving Group 1a cryptoassets *(i.e*. tokenized versions of traditional assets) undertaken using a controlled DLT system operated by either one or more prudentially-regulated entities or a financial market utility, due to the even more limited technology and systems-related risks which these structures entail. In any event, the infrastructure risk add-on should never apply to the use of DLT by banks in the design of their internal books and record systems.

IV. The proposed Group 2 exposure limit should not apply to safeguarding Group 2 cryptoassets.

The Second Consultation proposes the implementation of an exposure limit for Group 2 cryptoassets equal to 1% of a bank's Tier 1 capital at all times. When combined with the proposed definition of 'exposure' in proposed section 60.40, this has the potential to drastically limit the ability of banks to safeguard Group 2 cryptoassets on behalf of their clients.

The provision of custody and related services by banks enables clients to safely access and participate in various financial markets globally. Such services are critical to the functioning of the financial markets, and in some cases are required by law or regulation for investor protection.[12] Custody banks provide such services today on a cost-effective basis largely because of the economies of scale they can achieve. The proposed exposure limit, if applied to assets held in custody, would preclude the Custody Banks from supporting the safekeeping of Group 2 cryptoassets, as it would be economically and operationally unviable for the bank to do so at such a small scale. We do not believe that such an outcome is in the best interest of the financial system as it would continue to force clients to rely on non-bank providers that are outside the regulatory and supervisory perimeter to custody their cryptoassets, thereby increasing, rather than helping, to mitigate potential systemic risk.

V. Conclusion

While the Custody Banks support the Committee's efforts to develop a framework for the prudential treatment of cryptoasset exposures, we believe that the intended approach is unnecessarily conservative and incorporates features that would undermine the role of bank custodians in safely and efficiently supporting client assets in an increasingly complex financial ecosystem.

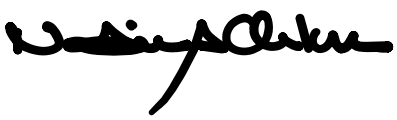
[12] In the US, the Investment Company Act of 1940 requires mutual funds to ensure the proper segregation of fund assets, which is usually achieved through the use of custodians. EU rules regarding the Undertakings for Collective Investments in Transferable Securities (UCITS) and Alternative Investment Funds (AIFs) require the use of custody services; assets of each UCITS or AIF must be held at a single depositary or custodian.

In particular, we strongly oppose the incorporation of the term 'non-fiduciary custody services' in the definition of a cryptoasset exposure and the implementation of an infrastructure risk add-on for Group 1a cryptoassets. Furthermore, we urge the Committee to confirm that a bank's internal book and records systems are not within the scope on the prudential framework for cryptoassets and also that assets held in custody are not subject to the Group 2 exposure limit.

We respectfully request that the Committee's final standards reflect the general principles of "same risk, same activity, same treatment" and simplicity, built in turn on established safety and soundness tools for banks to promote responsible innovation, and the protection of the client's interest. We look forward to further engagement with the Committee in regard to this important work.

Yours Sincerely,





Roman Regelman	Peter B. Cherecwich	Nadine Chakar
CEO of Securities Services and	President of Asset Servicing	Executive Vice President
Digital	Northern Trust Corporation	Head of Digital
BNY Mellon Corporation		State Street Corporation