By Electronic Mail

March 3, 2023

The White House Office of Science and Technology Policy (OSTP)
Eisenhower Executive Office Building
725 17th Street NW
Washington, DC 20006

Re: Request for Information: Digital Assets Research and Development Agenda

To Whom It May Concern:

The Securities Industry and Financial Markets Association ("SIFMA")[1] appreciates the opportunity to comment on the request for information ("RFI") issued by the White House Office of Science and Technology Policy ("OSTP") to help identify priorities for research and development related to digital assets, including various underlying technologies such as blockchain, distributed ledgers, decentralized finance, and smart contracts. The RFI also solicits comment on several related issues such as cybersecurity and privacy, programmability, and sustainability as they relate to digital assets.[2]

SIFMA welcomes the OSTP's interest in seeking additional information on the research and development ("R&D") opportunities that could arise from digital assets. In particular, the OSTP's interest in understanding the "goals, sectors, or applications that could be improved with digital assets and related technologies," as well as the "goals, sectors, or applications where digital assets introduce risks or harms."[3] SIFMA's response to the RFI focuses on the opportunities and possible risks associated with digital assets and distributed ledger technology ("DLT") in the context of capital markets products and applications.

[1] SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's nearly 1 million employees, we advocate for legislation, regulation and business policy, affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA).

[2] *See* Office of Science and Technology Policy, 88 Fed. Reg. 5,043 (Jan. 26, 2023).

[3] *Ibid.* 5045.

New York 140 Broadway, 35th Floor | New York, NY 10005
Washington 1099 New York Avenue, NW, 6th Floor | Washington, DC 20001
www.sifma.org

SIFMA believes that these new technologies can drive substantial efficiency, security, transparency, and financial inclusion benefits to U.S. capital markets, providing that their associated risks are appropriately managed. The best way to ensure that these potential risks are appropriately managed, and that experimentation and innovation more generally occurs in a responsible manner that protects investors, is to have such activities occur within the existing regulatory frameworks that govern U.S. capital markets. As such, this response is focused on the opportunities, risk management issues, and regulatory considerations associated with the application of DLT to existing financial instruments, payment instruments and payments infrastructures (in contrast to its use in other types of native digital assets, such as cryptocurrencies).

Executive Summary

SIFMA is submitting this response to highlight the following issues:

- ***Potential Capital Markets Use Cases***: There are a variety of capital markets focused DLT use cases that SIFMA members are exploring and discuss their potential benefits. These include:
  - Blockchain infrastructure applications that could improve the speed, security, and/or efficiency of existing processes;
  - The tokenization of "traditional" securities and the issuance of "natively" digital securities, which could offer significant benefits to a wide range of market participants;
  - The tokenization of non-security assets (*e.g.,* tokenized deposits or fiat currency); and
  - Ways in which DLT can be used to make cross-border payments faster, less costly, less risky and more broadly accessible.

- ***Understanding Technology Differences:*** Policymakers and market participants need to understand the distinct risks and benefits that arise from differences in the underlying technology infrastructure that enables digital asset products and services. Specifically, it is important to understand:
  - The differences between technology infrastructures that are accessible only to a private or restricted network versus those that are publicly available.
  - The differences between the control privileges for users of the network, whether those networks are "permissioned" or "permissionless". Regulated financial institutions are looking at both "private-permissioned" and "public-permissioned" networks. Each type of network has its own valuable features that offer substantially more embedded controls and risk management functionality than "public-permissionless" networks, such as those that drive the Bitcoin network.
  - The risk of a DLT application needs to take into context the features of the technology itself, the product or operational process it drives, and the broader risk management frameworks provided by the institution(s) operating it.

- ***Building on Existing Risk Management Programs at Regulated Institutions*-- Capital Markets:** DLT applications can benefit by leveraging existing risk management control functions at regulated financial institutions. Mature risk management frameworks capturing a range of technology and operational risks already exist at these institutions. This framework provides financial institutions the ability to assess and identify which technology configurations present the least risk, and layer additional controls on top of those offered by

the DLT platform itself. This process of managing risks when deploying new DLT infrastructure is similar to the processes that financial institutions have used to manage decades of technology innovation and address risks associated with legacy systems.

- ***Regulatory Modernization:*** It is crucial that the regulatory framework be modernized to support, or clarify that current regulations allow for, innovation in the digital assets space and maintain the inherent competitive advantage of U.S. markets in regulated digital products. This is best accomplished by applying existing, well-developed, and broadly understood regulatory frameworks at both the federal and state level to digital asset-oriented entities and products, with appropriate updates, including through interpretive guidance or commentary, that reflect the unique features of blockchain technology. As policymakers update existing rulebooks, they should also prioritize investor protection, adopt a "technology neutral" approach, and follow the principle of "same risk, same activity, same regulatory outcome."

- ***Updating Standards:*** It is vital that existing technology and operational standards supported by the Federal government be updated to accommodate DLT, *e.g.,* through continued investment in research and projects being conducted by the National Institute of Science and Technology ("NIST").

- ***Development of a U.S. Central Bank Digital Currency ("CBDC"):*** We highlight existing work that SIFMA has conducted in this area, with a focus on the possible benefits of a wholesale CBDC for certain capital markets applications. SIFMA underscores the importance, however, of conducting additional research and study before moving forward with the adoption of any form of U.S. CBDC.

- ***Public-Private Partnerships:*** SIFMA recommends that policymakers establish public-private task forces and working groups to drive research and support responsible development in the digital assets space.

* * *

SIFMA appreciates the OSTP's consideration of these comments and would be pleased to discuss any of these views in greater detail if it would assist with their deliberations. Please contact Charles DeSimone at cdesimone@sifma.org and Peter Ryan at pryan@sifma.org if you wish to discuss the points raised in this letter further.

Sincerely,

Kenneth E. Bentsen, Jr.
CEO and President
Securities Industry and Financial Markets Association

1. Benefits of Digital Assets and Frameworks for Understanding Risk Management

SIFMA and its members believe that the application of digital asset technology has the potential to drive substantial improvements in the U.S. capital markets. Digital assets innovation by regulated entities in regulated products arguably offers the best venue for digital assets experimentation and innovation; building on existing regulatory frameworks and protections. In this letter, SIMFA discusses the opportunities and regulatory and risk management issues associated with the application of DLT to regulated financial products, such as equity and debt securities.

Notably, these products and applications are distinct from other types of digital assets, such as those commonly referred to as "cryptocurrencies." While a range of taxonomies and terminology are used to categorize DLT-based assets, the framework adopted by the Basel Committee on Bank Supervision ("BCBS") differentiates between three broad categories: tokenized traditional assets, which often create efficiencies within the well-established banking framework; cryptoassets with effective stabilization mechanisms (*i.e.,* stablecoins); and unbacked cryptoassets, such as Bitcoin.[1] The Global Financial Markets Associations ("GFMA"), of which SIFMA is a member, has developed a taxonomy that further differentiates digital assets into six categories: 1) value-stable digital-assets, including CBDCs, financial market infrastructure ("FMI") tokens, tokenized commercial bank money, and stablecoins; 2) security tokens; 3) cryptocurrencies; 4) settlement tokens; 5) utility tokens; and 6) other crypto-assets (*i.e.,* those not structured as value-stable crypto-assets).[2]

The absence of consistent definitions or a nuanced taxonomy of different digital asset types used by regulators creates major challenges and stifles innovation. Unclear or inconsistent definitions create obstacles for firms who are looking to apply DLT infrastructure to create efficiencies and carry out well established and already permissible activities. For example, many digital asset activities being explored by capital markets participants are simply using new infrastructure to record ownership of existing registered products, yet regulatory definitions often fail to distinguish between this type of activity and non-traditional applications of digital asset technology. The lack of consistency in taxonomies internationally also creates challenges for market participants, leading to differential treatment for certain classes of assets and activities depending on jurisdiction. Continued U.S. leadership in digital assets innovation and in the capital markets more broadly will be contingent on ensuring greater harmonization of taxonomies across major jurisdictions and on U.S. policymakers taking a more nuanced approach to definitional issues than has been shown to date.

In addition to being mindful of the distinctions between different types of digital assets, policymakers also need to understand the important differences in configurations of the underlying digital ledger technology and the impacts of those differences (see section 3 below). These distinctions between digital assets and between blockchain infrastructures should shape the type of oversight and investor protections that an activity, asset, or entity should be subject to. Research into the broad category of "digital assets" needs to be cognizant of these

[1] Basel Committee on Banking Supervision, "Prudential treatment of cryptoasset exposures" December 2022, available at: https://www.bis.org/bcbs/publ/d545.pdf

[2] The full taxonomy is provided in Annex 1 to the GFMA response to the Financial Stability Board's (FSB) questions for consultation on "International Regulation of Crypto-Asset Activities – A Proposed Framework," December 2022, available at: https://www.gfma.org/wp-content/uploads/2022/12/gfma-response-to-fsb-crypto-asset-consult-15-december-2022.pdf

foundational differences in features and applications and produce policy recommendations that appropriately reflect these distinctions.

As policymakers conduct further research, SIFMA furthermore encourages them to focus on discrete digital asset types that are designed and issued in compliance with existing capital markets regulatory frameworks, and on specific infrastructure configurations that best enable regulated financial entities to manage risk, maintain fair and orderly markets, and protect the interests of clients and investors.

2. Potential Use Cases and their Benefits for Regulated Entities

Below, SIFMA highlights several applications of digital asset products and services and discuss the potential benefits they could offer capital markets participants and the broader economy. These include blockchain based infrastructure; native digital security issuance; tokenization of existing financial instruments; tokenized non-security assets such as commercial bank deposits; and cross-border transfers.

A) Blockchain Infrastructure Applications

Market participants continue to explore and implement a range of projects using underlying blockchain technology to improve upon existing industry functions and processes. The focus is not to create new blockchain based assets, but to make processes around existing assets faster, more secure, and more efficient, or to take advantage of the way blockchain records provide immutability and greater transparency in data.

These applications include using blockchain based settlement models to allow for faster, more efficient, or more customized settlement of existing "traditional" securities on an optional basis.[3] Similarly, firms are exploring how smart contracts could automate existing industry processes, such as payment or delivery of securities or funds, allowing for faster transactions, increased confidence, and greater customization. Other projects explore the potential for blockchain based records to provide an authoritative record of information, showing not just current prices or ownership structures, but also historical developments. Blockchain based "oracles" can be designed to provide common understanding of critical information within a single firm or across a range of participants in a market, or investors in a common asset or investment vehicle. For example, certain forms of privately held companies feature evolving ownership structures and corresponding valuation levels, which could be tracked using blockchain systems.

B) Issuance of Natively Digital Securities

Another area of interest for SIFMA members is the issuance of natively digital securities, which are issued and tracked on blockchain infrastructure. These have been referred to using a range of different terms, including "security tokens" and "digital asset securities," and, as discussed below, share some similarities with "tokenized securities" (that is securities that are issued traditionally but represented on a blockchain for books and recordkeeping purposes).

[3] While market participants are exploring the potential for blockchain based settlement models to allow for faster settlement options, the industry is preparing to shorten the settlement cycle for equities and certain other securities to one business day after the trade is executed (T+1), which is expected to be complete in 2024. Moving the settlement cycle broadly to something faster than T+0 (whether same day settlement on an end of day basis (T+) settlement) or "atomic settlement" is challenging.

Natively digital securities offer potential advantages to market participants and can enable a range of innovations in how securities are issued, traded, settled, and serviced. Natively digital securities can be more easily marketed and can also be easier to structure and issue. This can allow for greater customization, potentially allowing asset types which were previously cost inefficient to be offered to investors with the protections provided by securities laws and regulations.

Blockchain based trading and settlement can also offer greater speed and efficiency, although it would need to be supported by a robust set of settlement tools on the blockchain network and an on-blockchain network payment option, whether that be tokenized cash, a settlement token or equivalent, or a CBDC. These considerations also apply to already existing assets that are tokenized, as discussed below.

Natively digital securities can also embed the calculations for the security (such as coupon payments) in the asset itself, providing greater efficiency in asset servicing and greater customization to fit either investor demands or the unique features of the economic asset underlying the security. For example, green bond payments could have functionality that embeds the ability to track climate developments within the security when it is issued, providing greater transparency to investors.

C) Tokenization of Previously Issued Securities

In addition to issuing securities natively on a blockchain, firms are also exploring the opportunities offered by tokenizing securities which were already issued "traditionally" using existing industry infrastructure. Under this process, a security holder can create a representation of the security on a blockchain network through the process of tokenization, so that the representation of the rights to the security can be tracked, traded, and cleared and settled using DLT infrastructure. This process can be managed by a custodian, who ensures that the underlying security is secure and immobilized, using existing industry operations and in compliance with well-established regulations.

Tokenization of existing securities can offer a range of benefits, some of which overlap with natively digital securities. Tokenization in traditionally opaque markets can improve efficiency and market quality, such as by providing additional liquidity, exposure to broader groups of investors, or more efficient settlement and asset servicing. Tokenization can also offer flexibility in its functionality in areas where existing industry infrastructure cannot, such as highly customized settlement instructions or securities lending or repo transactions on shorter time periods than are currently available. Additionally, tokenized securities can address challenges around cross-border asset transfers.

D) Tokenization of Non-Security Assets

Non-security assets can also be represented on a DLT network via tokenization, offering a range of benefits to market participants, infrastructure operators, and end investors.

One key example is commercialized bank deposits, which can function as tokenized fiat currency that can serve as a vehicle for handling the payment leg of securities settlement on-chain, allowing for the entirety of a transaction or trade (*i.e.,* through settlement and payment) to be carried out on a DLT network, facilitating greater efficiency and potentially faster settlement models. Alternatively, they can be used to support settlement tokens which can be used within a given infrastructure venue. The Bank for International Settlements has recently highlighted to potential for such tokenized deposits to become interoperable with central bank money in

commercial payment systems.[4] Examples of such tokenized deposits include products already in operation, such as Onyx, and the Regulated Liability Network, which is in proof of concept.[5] This function has some overlap with the potential role for a CBDC, which may be, at best, duplicative, as discussed below.

E) Cross Border Transfers

Firms are also using blockchain to support innovation in cross border payments. Beyond discussions of how digital assets might potentially facilitate cross-border payments, there are a range of use cases and potential benefits for handling fiat currencies in cross border transactions via DLT infrastructure. These include faster payments and greater security and auditability of transaction histories, as well as potentially lower costs, broader access, and more robust controls for anti-money laundering ("AML") / know-your-customer ("KYC") programs.[6]

3. Understanding Technology Differences and their Risk Implications

Just as it is critical for policymakers to understand and define the differences between digital asset types and to ensure that policy and regulatory frameworks reflect those differences, it is equally important to differentiate among different configurations of the underlying technology infrastructure that enables digital asset products and services. Discussions of DLT or blockchain infrastructure often conflate all types of network configurations and obscure the very real differences between them – differences that have major impacts on risk, users, and how technology innovation can be integrated within existing regulatory frameworks.

The type of digital ledger architecture employed has important implications across a range of issues of concern to policymakers, including anonymity, efficiency of transaction processing, and asset security. Focusing on the risks associated with certain types of common ledger configurations may obscure the fact that other technology arrangements can be designed to align with the goals and requirements of existing regulatory frameworks. For example, policymakers should not conflate the experiences of markets and infrastructure developed for pseudonymous bearer assets (such as Bitcoin) with regulated entities engaging in traditional capital markets activities, and DLT infrastructure more broadly.

At a high level, the key features of DLT networks can be differentiated along two axes – the accessibility of the network (whether it is restricted only to certain users or is publicly available)

---

[4] "Innovation and the future of the monetary system," Keynote speech by Agustín Carstens, General Manager of the BIS, at the Monetary Authority of Singapore (MAS), Singapore, 22 February 2023.https://www.bis.org/speeches/sp230222.htm

[5] As proposed, the tokenized commercial bank deposits under the Regulated Liability Network (RLN) proposal could be readily exchanged with existing account-based forms. A description of the RLN proposal can be found at Regulated Liability Network. Policymakers should explore if and how these alternative technology configurations could meet the objectives of a CBDC, such as the instant movement of value 24/7 either domestically or internationally, integrated into other digitized processes, and serve as "programmable money" insofar as payments can be automated or made conditional on events.

[6] For example, in 2021, Wells Fargo and HSBC entered into a bilateral agreement to settle FX transactions through a blockchain-based solution designed to, among other things, reduce settlement risk in certain foreign exchange transactions, further details available at: *"*Wells Fargo and HSBC establish Bilateral Agreement to Settle FX Transactions Through a Blockchain-based Solution*".*

and the control of privileges for users of the network (*i.e.*, authentication of who can carry out specific actions, such as writing changes to the ledger). This schema results in three main types of distributed ledgers:

- ***Private Permissioned:*** Closed-loop, private networks, which restrict access to predetermined users only.
- ***Public Permissioned*****:** These applications are built on a public network foundation but with the addition of use controls on top of the underlying network to create what are effectively closed networks (which vary by design), given selective restriction of access through authentication for governance, administration, or other privileges.
- ***Public Permissionless*****:** Open, public networks that do not restrict access for privileges. While they present several risk issues, these networks are among the largest operating today and present a track record of resilience, supported by a large community of users.

The chart below summaries some of the key distinguishing features of these network types[7]:

	Private Permissioned	**Public Permissioned**	**Public Permissionless**
Governance	Centralized	Centralized protocol for the application (as opposed to the broader network)	Decentralized
Accessibility to Users	Closed	Closed (for the relevant application)	Open
Control over Privileges	Can be defined as required	Users authenticated for specific roles	All users can perform all roles
Identification	All users known	All users known (for the relevant app.)	Pseudonymous
User Base	Very limited (by design)	Limited (for the relevant application)	Broad

Understanding and clearly defining these differences is critical, so that oversight and regulation can focus on best managing the risks associated with each activity. Without understanding these structural differences in how DLT networks manage risk, policymakers may assume incorrectly that anything touching DLT introduces novel risk and so requires novel regulatory treatment, such as that articulated in SEC Staff Accounting Bulletin 121[8] or in the imposition of capital surcharges for banks engaging in any form of DLT activity.

In general, regulated financial institutions are working with DLT configurations that are built on embedded control frameworks – whether those controls involve access to the network, permission structures, or both. These frameworks need to be distinguished from the technology configurations adopted by certain other crypto assets, which have emphasized pseudonymity and distributed networks, creating additional risks not present in certain types of distributed

[7] The summary above introduces at a high level the risk management controls associated with each type of technology configuration. SIFMA would be happy to discuss in greater depth the risk management controls associated with each network type and how they are consistent with the oversight and risk management requirements of regulated financial institutions.

[8] Securities and Exchange Commission Staff Accounting Bulletin No. 121, March 31, 2022, available at: https://www.sec.gov/oca/staff-accounting-bulletin-121

ledger configurations. For example, policymakers have raised concerns about certain features of the Bitcoin network – that system looks the way it does because of specific design choices made by its users. In contrast, regulated financial institutions are making choices based on their own requirements, including safety and soundness concerns as well as consumer protection, which result in a very different set of controls and operating models.

It is critical not to assume that any one type of network is necessarily more risky than other types. The key is understanding applicable risk management features and how they align with the goals of the product they are supporting, other organizational controls that may be in place, and any regulatory requirements. For example, if a permissionless network has certain attributes (*e.g.,* significant volume and dispersion of nodes), its immutability and threat resistance can be significantly lower than a permissioned network with a single party controlling the network. As a result, the Bitcoin network itself – while it has many features that are concerning for financial regulators – has proved to be very resistant to direct hacks.

4. Regulated Financial Institutions Working with DLT Can Build on Existing Risk Management Programs

Beyond the controls inherent in the blockchain network itself, DLT applications in the capital markets leverage controls from regulated financial institutions' existing technology and operational risk management programs. These well-developed and mature programs provide a framework for financial institutions to assess and identify which technology configurations present the least risk for potential applications and then layer additional controls on top of those offered by the DLT platform itself. This process of managing risks when deploying new DLT infrastructure is like the processes that financial institutions have historically used to manage prior waves of technology innovation and address risks.

As discussed above, the rubric of "digital assets" covers a broad range of diverse products, supported by technology configurations with fundamental differences in the tools they offer to manage multiple types of risk. Analysis of risk in DLT applications and products must not be generalized but focus on specific applications and shaped by risk through a combination of 1) the digital asset type, 2) its implementation model and underlying technology, and 3) its place in the securities lifecycle.

When SIFMA focuses on the regulated products and use cases described above (such as infrastructure applications, digital securities issuance and asset tokenization), we believe that they represent traditional financial products and activities and can therefore be governed effectively under existing risk frameworks. The existing, well-developed and broadly understood regulatory frameworks at both the federal and state level that apply to regulated entities provides a robust foundation for the risk management and customer protection in digital asset markets. These frameworks should be supported by appropriate modifications that reflect the unique features of blockchain technology to ensure that activities with similar risk profiles are regulated similarly.

As regulated firms look to apply DLT to regulated products and activities, they are guided by these regulatory frameworks, covering everything from entity disclosures and reporting requirements, compliance and risk management rules, requirements for the separation of different functions and activities, trading and market rules, and protection and segregation of client assets. These regulatory frameworks place investor protection at the forefront, alongside other key regulatory objectives such as market integrity and risk management. While some

regulatory modernization might be necessary to account for the unique features of DLT, these frameworks provide a robust baseline of customer protection and risk management.[9]

For example, many have pointed to illicit finance concerns as a key risk associated with expansion of digital asset markets. Regulated financial institutions, however, have a long history of developing and honing Bank Secrecy Act ("BSA") and Combating the Financing of Terrorism ("CFT") compliance programs, including AML and KYC procedures, and illicit financing controls. They have a well-established track record of managing a wide variety of existing and emerging illicit financing risks and they are uniquely positioned to apply that deep expertise to digital assets. Similarly, mature regulatory frameworks governing illicit financing risks can be applied to digital asset technologies, albeit with possible modifications that reflect the underlying technology's unique characteristics.[10]

As policymakers assess the risk impact of DLT, it is important to remember that existing systems also pose risks. Over time, those risks have been understood and managed, and financial institutions have continued to evolve controls to address them. For example, over the past decade, the financial services industry has recognized the threat from cyberattacks and evolved its controls to meet the cyber threat and secure its expanding digital operations.

Given this experience and the focus of regulated institutions on deploying risk mitigants from the outset of any new technology development, SIFMA members and the financial infrastructure providers they work with are well equipped to apply existing risk management structures to manage DLT as they have withc other new technologies. SIFMA appreciates the concern of policymakers to ensure that future financial innovation based on DLT meets the same standards of security, reliability and client protection as existing technology. The securities industry agrees that addressing these concerns is foundational to our work with blockchain applications.

Given the existing technology and operational risk frameworks that regulated firms already have in place, combined with the protections inherent in appropriate technology configurations and the protections provided by existing product and entity level regulations, there is no reason to impose additional restrictions on the application of DLT by such firms. In particular, imposition on banks of any form of infrastructure risk capital surcharge for simply using DLT is both unnecessary and a major impediment to responsible blockchain innovation.[11] Allowing regulated financial institutions to apply DLT to regulated products and activities policymakers provides low-risk opportunities for regulators understand the benefits of digital assets

[9] For a further discussion of the role of existing regulations in providing oversight to emerging digital asset markets and activities, please refer to SIFMA's January 2023 blog post "Addressing Regulatory Gaps in the Digital Asset Ecosystem," available at: https://www.sifma.org/resources/news/addressing-regulatory-gaps-in-the-digital-asset-ecosystem/

[10] For a further discussion of the application of illicit financing regulations to digital assets and opportunities for regulatory modernization, please see SIFMA's response to the Treasury Department's September 20, 2022 Request for Comment ("RFC") on "Ensuring Responsible Development of Digital Assets" as it pertains to illicit finance and national security risks, November 2022, available at https://www.sifma.org/wp-content/uploads/2022/11/SIFMA-Treasury-Illict-Finance-RFC-11-03-2022.pdf

[11] SIFMA discussed these issues in greater depth in our joint trades' response to the second consultation issued by the BCBS on the prudential treatment of crypto assets Global Financial Markets Association ("GFMA"), Institute of International Finance ("IIF"), International Swaps and Derivatives Association ("ISDA"), Financial Services Forum, Futures Industry Association ("FIA"), Bank Policy Institute, International Capital Market Association ("ICMA"), and International Securities Lending Association ("ISLA"), "Comments in Response to the Second Consultation on the Prudential Treatment of Cryptoasset Exposures." Available at: Joint Trades Comment Letter - Second Consultation on Prudential Treatment of Cryptoasset Exposures (sifma.org).

innovation, with innovation occurring in a controlled environment with well-established regulatory and risk management guardrails in place.

As discussed above, different technology configurations and infrastructure types have their own inherent strengths. This difference needs to be considered as policymakers assess how the broader risk management frameworks in place at regulated financial institutions integrate with new DLT platforms. For example, applications that use public blockchains which are open source, and are supported by many users who are working on the technology itself and vetting its code, while private ledgers offer control over choosing who participants are and how they interact, and rely on the individual users to vet all coding and functionality.

Policymakers should also consider broader technology and governance developments that can support risk management for DLT infrastructure. As discussed later, standards development and modernization, an area where the support of the Federal government is particularly valuable, is vital. The development of systems for verifiable credentials can address the risks of certain network types. Similarly, frameworks for the governance and management of public vs private information *(i.e.,* zero knowledge proofs) and how and what is disclosed on chain can draw from existing reporting and SEC disclosure frameworks, which provide models for appropriate sharing of information.

5. Regulatory Modernization

As noted above, SIFMA believes that existing and well understood regulatory frameworks can be applied, with appropriate modifications to reflect the distinct features of blockchain technology, to the types of digital assets and activities discussed in this letter. SIFMA welcomes the efforts of the Administration, (including the President's Executive Order on Digital Assets[12] and subsequent reports[13]) as well as Members of Congress and regulatory agencies to address gaps in the regulatory framework governing digital asset products and activities. It is crucial that policymakers act in a thoughtful but expeditious manner to clarify which existing rules or guidance apply to various types of digital assets and activities, define asset classes clearly, and identify rules that should be updated in order to foster responsible innovation by regulated financial institutions.

It is vital that robust investor protections should be at the forefront of all regulatory modernization efforts in order to build confidence in these new products and technologies. Any framework should also adopt a technology neutral approached based on "same risk, same

[12] Exec. Order No. 14067, 87 Fed. Reg. 40881 (July 8, 2022); White House, Fact Sheet: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets (2022).

[13] U.S. Department of Treasury, Report on The Future of Money and Payments (2022); U.S. Department of Treasury, Report Crypto-Assets: Implications for Consumers, Investors, and Businesses (2022); U.S. Department of Treasury, Action Plan to Address Illicit Financing Risks of Digital Assets (2022); Press Release, Janet Yellen, Sec'y, U.S. Department of Treasury, on the Release of Reports on Digital Assets (Sept. 16, 2022); U.S. Department of Justice, Office of the Attorney General, The Role Of Law Enforcement In Detecting, Investigating, and Prosecuting Criminal Activity Related To Digital Assets (2022); Press Release, U.S. Department of Justice, Justice Department Announces Report on Digital Assets and Launches Nationwide Network (Sept. 16, 2022); U.S. Department of Commerce, Responsible Advancement of U.S. Competitiveness in Digital Assets (2022); Press Release, Statement from Gina M. Raimondo, Sec'y, U.S. Department of Commerce, Responsible Advancement of U.S. Competitiveness in Digital Assets Report Release (Sept. 16, 2022); Financial Stability Oversight Council (FSOC), Report on Digital Asset Financial Stability Risks and Regulation (Oct. 3, 2022).

activity, same regulatory outcome" principle, acknowledging that there are important differences between types of digital asset products, applications and activities that do not allow for a "one-size-fits-all" approach to regulation. It is also important that in any regulatory modernization effort that regulators recognize the differences between blockchain-native assets and the use of blockchain technology to facilitate traditional asset transactions given the significantly different risk profiles inherent of each activity.[14] Finally, to the extent possible, U.S. policymakers should also work towards regulatory interoperability between jurisdictions, to support the cross-border role of many digital asset market participants and support the competitiveness of U.S. capital markets and firms.

6. Updating Standards

SIFMA welcomes the OSTP's interest in supporting development of industry standards. The Federal government can play a critical role in responsible digital asset innovation by supporting the modernization of existing technology and operational standards to accommodate DLT. Standards provide common practices that firms can apply to demonstrate that they are understanding and managing risk appropriately. Updated standards are particularly valuable in providing common industry approaches to understanding and managing risk that can allow users of DLT to demonstrate that they are using this technology in ways that meet the expectations of their clients, counterparties, and regulators.

SIFMA encourages NIST to continue its investment in open-source research and initiatives focused on producing technical standards and guidance. In particular, SIFMA members look forward to building on standards under development such as:

- The use of blockchain technology (Blockchain | NIST);
- Cryptographic techniques particularly around threshold schemes that firms may use in the future such as multiparty computation (Multi-Party Threshold Cryptography | CSRC (nist.gov)); and
- Updating standards and certifications (such as FIPS 140-2, Security Requirements for Cryptographic Modules | CSRC (nist.gov) – FIPs) to include considerations for blockchain technology. [15]

SIFMA also encourages NIST and other standard setters to explore how specific cybersecurity standards or approaches could guide interactions with public permissionless blockchains (such as more guidance for the application of these technology configurations under NIST's

[14] These points were discussed in more detail in SIFMA, Prioritizing Investor Protection and Existing Regulatory Frameworks in Digital Asset Legislation, Letter to Senate Banking Committee, Senate Agriculture Committee, House Financial Services Committee, and House Agriculture Committee (Oct. 11, 2022). See also Peter Ryan, "U.S. Digital Assets Policy Should Prioritize Investor Protection and Build Upon Our Robust Regulatory Frameworks," SIFMA Blog, November 16, 2022, available at: US Digital Assets Policy Should Prioritize Investor Protection and Build Upon Our Robust Regulatory Frameworks - SIFMA - US Digital Assets Policy Should Prioritize Investor Protection and Build Upon Our Robust Regulatory Frameworks - SIFMA.

[15] National Institute for Standards and Technology (NIST) Blockchain Projects, available at: https://www.nist.gov/blockchain; NIST Multi-Party Threshold Cryptography Project, available at: https://csrc.nist.gov/Projects/threshold-cryptography; NIST Security Requirements for Cryptographic Modules Project, available at: https://csrc.nist.gov/publications/detail/fips/140/2/final

cybersecurity framework, which is used by most financial institutions).[16] Additionally, research and development into interoperability of blockchain standards for banks as well as smart contract standards are valuable.

Beyond technical standards, accounting and valuation standards will likely need to be updated to account for unique features of new digital asset types and operating models. Finally, work on all standards development will be most effective if those efforts are coordinated internationally, both through engagement with international processes such as the International Organization for Standardization ("ISO") as well through bilateral and multilateral cooperation with other major jurisdictions.

7. CBDCs

SIFMA appreciates the RFI's questions on mechanics and design considerations for a potential U.S. CBDC. Before undertaking what would be "a highly significant innovation in American money," policymakers should be clear on why a U.S. CBDC is needed and what problems it would address. Once that is established, it is important to agree on a clear understanding of the many design considerations that would shape its impact and operations. These analyses should include, but would not be limited to, an evaluation of the effects of different types of CBDC systems on financial stability and the implementation of monetary policy; key short-term funding markets; existing payments systems, with which any CBDC would need to be interoperable; consumer privacy; as well as AML and sanctions regimes.

Given that much more study needs to be undertaken to properly understand these benefits and costs, SIFMA does not take a position in this letter on the desirability of adopting a U.S. CBDC, although SIFMA does believe that *if* policymakers were to move forward with adoption at some future point, after the appropriate steps above were completed, the primary focus should be on wCBDC. SIFMA encourages the OSTP to review the SIFMA comment letter in response to the Federal Reserve Board discussion paper "Money and Payments: The U.S. Dollar in the Age of Digital Transformation."[17]

SIFMA also encourages policymakers to explore a careful review of whether the goals of a wCBDC might best be accomplished through regulated commercial models which are already available or under development and proving effective. Analysis should cover a broad range of models which could meet the objectives that policymakers seek to achieve through a potential digital dollar. For example, these could include various systems of private tokens, tokenized cash, bank-minted tokenized deposits referencing fiat currency on blockchain, or the Regulated Liability Network (RLN) proposal to tokenize central bank, commercial bank, and electronic money on the same chain to deliver a next generation digital money format based on national currency units.[18] . SIFMA's response to the Treasury Department's Request for Comment on

[16] National Institute for Standards and Technology (NIST) Cybersecurity Framework, available at: https://www.nist.gov/cyberframework

[17] SIFMA response to the Federal Reserve Board of Governors discussion paper entitled "The U.S. Dollar in the Age of Digital Transformation," May 2022, available at: https://www.sifma.org/resources/submissions/cbdc-discussion-paper-response/

[18] For example, as proposed, these "RLN tokens" could be readily exchanged with existing account-based forms. Policymakers should explore if and how these alternative technology configurations could meet the objectives of a CBDC, such as the instant movement of value 24/7 either domestically or internationally, integrated into other

"Ensuring Responsible Development of Digital Assets provides a more extended discussion of the potential role of private sector alternatives to a CBDC.[19]

8. Public-Private Partnerships

As the OSTP looks to move forward with its research agenda for the responsible development of digital assets, SIFMA strongly recommends the formation of a public-private working group/task force to help drive analysis and accelerate the policy changes that are needed for broader adoption and responsible innovation. We believe there is great value in the public sector working with the private sector users of blockchain technology, to understand the use cases and technology configurations which are most relevant and the design considerations and regulatory challenges that shape financial institutions' work. Including representatives of regulated financial institutions in any public-private working group would be particularly valuable given SIFMA's members' perspective as responsible users of the technology who are trying to innovate within a controlled and regulated environment.

digitized processes, and serve as "programmable money" insofar as payments can be automated or made conditional on events.[18]

[19] SIFMA response to Treasury Department's Request for Comment ("RFC") on "Ensuring Responsible Development of Digital Assets," August 2022, available at: https://www.sifma.org/wp-content/uploads/2022/08/Ensuring-Responsible-Development-of-Digital-Assets.pdf