March 3, 2023

Via electronic mail to DARD-FTAC-RFI@nitrd.gov

Rachel Wallace, Deputy General Counsel
Office of Science and Technology Policy

Re: Comments on Request for Information; Digital Assets Research and Development

Ladies and Gentlemen:

The Bank Policy Institute[1] and the American Bankers Association appreciate the opportunity to comment on the White House Office of Science and Technology Policy's request for public comments to help identify priorities for research and development related to digital assets[2] issued in connection with Executive Order 14067, "Ensuring Responsible Development of Digital Assets."[3] The trades support the goal of the Executive Order to promote a coordinated, "whole of government" approach to fostering responsible innovation, which will help ensure that the United States remains a global leader in innovation while also ensuring that consumers, the financial system, and national security are protected. We recommend that the public and private sectors continue to collaborate on how to further responsible innovation in the United States, including through continued research and open dialogue.

The trades support responsible innovation conducted in a manner consistent with the safety and soundness of the financial system, anti–money-laundering ("AML") and countering-the-financing-of-terrorism ("CFT") standards, and robust consumer and investor protections. Digital assets and related activities have grown rapidly in recent years and have the potential to provide benefits to consumers and businesses and the financial system. As with any new technology, there are associated risks that must be carefully studied, mitigated, and managed through proper controls, regulation, and oversight.

Today, digital assets, though they may carry varying levels of risk, are often nevertheless broadly categorized.[4] Defining important terms and developing a comprehensive and harmonized lexicon for the

---

[1] See Appendix for association descriptions.

[2] 88 Fed. Reg. 5043 (Jan. 26, 2023).

[3] 87 Fed. Reg. 14143 (March 14, 2022).

[4] For example, the RFI provides that the term "digital assets" refers to all CBDCs, regardless of the technology used, and to other representations of value, financial assets and instruments, or claims are issued or represented in digital form and that are used to make payments or investments, or to transmit or exchange funds or the equivalent thereof. For example, digital assets include cryptocurrencies, stablecoins, and CBDCs. Regardless of the label used, a digital asset may be, among other things, a security, a commodity, a derivative, or other financial product. Digital assets may be exchanged across digital asset trading platforms, including centralized and decentralized finance platforms, or through peer-to-peer technologies. For the purposes of this RFI, "digital assets" is also inclusive of its underlying technologies (e.g., DLT).

various types of digital and crypto assets and entities active within the digital-asset ecosystem, and supporting infrastructures, will help authorities more effectively target the unique risks that each present. Authorities must distinguish among digital assets, cryptocurrencies, and tokenized assets, as well as the underlying distributed ledger technology ("DLT") and blockchain infrastructure, which may differ in use across functions and activities, when they apply existing (or develop new) regulatory frameworks for them. For example, the volatility and related risks often cited in connection with "digital assets" or "crypto assets" refers to risks presented by non-bank issued cryptocurrencies and stablecoins (e.g., bitcoin and Tether)[5], which operate on wholly different infrastructures and mechanisms of operation, but are comparatively different when using a distributed ledger network for use-cases other than cryptocurrencies.[6] Traditional banking products and activities utilizing DLT, blockchain, or other novel technologies provided by federally insured or regulated banks or subsidiaries of bank and financial holding companies do not present the risks presented by non-bank crypto-asset service providers and non-bank issued cryptocurrencies or related activities because banks appropriately manage their risks and are subject to a comprehensive regulatory framework and consolidated supervision, audits and examinations. Policymakers should research and study how to develop a comprehensive framework to apply appropriate standards and oversight to address the risks presented by nonbanks engaging in cryptoasset-related activities, such as issuance and trading of cryptocurrencies, to preserve financial stability and protect consumers, investors, and businesses.

Banks stand ready to innovate in this space, but the banking regulators do not appear to have appropriately distinguished between traditional bank activities using DLT or blockchain, such as tokenizing existing bank liabilities (deposits) or securities, and non-bank issued cryptocurrencies, which present very different risks given the inherent design of the various activities. Under the existing regulatory framework and effective robust risk management function of banks, traditional banking activities using new technology are well-managed by banks with well-established controls for product development, and banks can manage the risks of traditional banking activities using DLT or blockchain. Any contrary view is hindering the establishment of a reliable and clear regulatory environment, limiting the ability of banks to engage in responsible innovation that could potentially benefit consumers and investors, create marketplace efficiencies, and strengthen the resilience of the financial system.

The RFI asks several questions about topics on which BPI and ABA have written extensively, including CBDCs.[7] Below, we provide references and citations to our prior work on this topic and others, as relevant to the particular question, in light of the limitation on comment length.

1. Goals, sectors, or applications that could be improved with digital assets and related technologies.

---

[5] Examples are non-exhaustive.

[6] *See, e.g.,* Blockchain application within a multi-sensor satellite architecture, NTRS – Nasa Technical Reports Server, NASA (link) (discussing potential application of blockchain usage with constellation and swarm satellite architectures); *see also* Biology-Inspired Distributed Consensus in Massively Deployed Sensor Networks, NTRS – Nasa Technical Reports Server, NASA (link) (abstract discussing "fully distributed consensus can be attained in a scalable fashion in massively deployed sensor networks where individual motes operate based on local information, making local decisions that are aggregated across the network to achieve globally-meaningful effects)."

[7] As we have previously detailed, an intermediated, account-based CBDC could pose serious risks to the U.S. economy and financial system that would not be outweighed by the purported benefits. *See*, *e.g.*, the Bank Policy Institute's work on central bank digital currency and stablecoins (link), and ABA's work on CBDCs (link).

Using new technologies, banks have made significant progress in developing products and services that could benefit consumers and the financial system, consistent with the banks' safe and sound operation.[8] For example, banks have come to recognize that DLT is a secure method of recordkeeping that may have the potential to drive efficiencies, decrease transaction times, and reduce systemic risk. Banks' blockchain-based deposit accounts[9] have been used to clear and settle repo trades and conduct inter-affiliate, intra-company transfers.[10] Blockchain technology has also been used to facilitate information sharing across financial institutions where such information is required to clear or validate payments.[11]

Banks are also planning to use tokenized deposits to facilitate traditional trading and market activity, including spot transactions, lending, and collateral management. Blockchain-based deposits enable "advanced programmability features, the ability to exchange funds with other digital assets atomically, and the transfer of commercial bank money on shared or universal ledgers where enhanced transparency of transactions and 24/7 transfer availability are possible".[12] Today, digital assets, though they may carry varying levels of risk, are often nevertheless broadly categorized into a single group.[13] Policymakers should research and define important terms and develop a comprehensive and harmonized lexicon for the various types of digital and crypto assets and entities active within the

---

[8] Examples of banks' innovation include the Regulated Liability Network proof of concept to tokenize commercial bank, central bank, and electronic money on the same chain, which offers the promise of delivering a next-generation digital money format based on national currency units (*e.g.*, denominated in U.S. dollars). *See* Press Release, Members of the U.S. Banking Community Launch Proof of Concept for a Regulated Digital Asset Settlement Platform (Nov. 15, 2022) (link). As another example, Partior, a shared-ledger multicurrency clearing platform, was launched as a technology company by JPMorgan, DBS, and Temasek in 2021. *See* Press Release, JPMorgan Chase & Co., DBS, J.P. Morgan and Temasek to Establish Platform to Transform Interbank Value Movements in a New Digital Era (Apr. 28, 2021) (link). Partior is designed to perform atomic clearing and settlement on a 24x7 basis among participating institutions using blockchain and smart-contract technology. *See* "Partior Aims to Become the World's Ledger for Banks", DigFin (May 15, 2022) (link); "The Global Ambitions of Partior, the JP Morgan, DBS Blockchain Payment System", Ledger Insights (Nov. 16, 2022) (link).

[9] Banks are authorized to issue tokenized deposits, establish blockchain-based deposit accounts, and issue stablecoins, as governed under existing federal banking agency regulations and managed via banks' risk management systems. *See, e.g.*, Office of the Comptroller of the Currency, *OCC Chief Counsel's Interpretation on National Bank and Federal Savings Association Authority to Use Independent Node Verification Networks and Stablecoins for Payment Activities*, Interpretive Letter No. 1174 (Jan. 4, 2020) (link). *See also* TCH, Bank Issuance of Stablecoins and Related Services: Legal Authority and Policy Considerations (Nov. 2022) (link) (provided by Sullivan & Cromwell LLP at TCH's request).

[10] Blockchain deposits can exist in four forms: non-native deposit accounts, native deposit accounts, non-native token-based and native token-based. Tokenized deposits can be native or non-native. For purposes of this response, the term "tokenized deposit" refers to both native and non-native token-based blockchain deposits. *See* Oliver Wyman and Onyx by JPMC Report: "Deposit Tokens: A foundation for stable digital money," at 14 (Feb. 9, 2023) (link).

[11] For example, Liink by JP Morgan Onyx allows a bank sending a payment to pre-validate with the receiving bank that it is sending payment to a valid open account, avoiding prolonged payment processing and rejection for invalid accounts (link).

[12] *See* Oliver Wyman and Onyx by JPMC Report: "Deposit Tokens: A foundation for stable digital money," at 14 (Feb. 9, 2023) (link). For example, banks participated together in Partior and in the Monetary Authority of Singapore's project Guardian's "institutional DeFi" protocol (link).

digital-asset ecosystem, and supporting infrastructures, which will help authorities more effectively target the unique risks that each presents.

Traditional banking products and activities utilizing DLT, blockchain, or other novel technologies do not present the risks presented by nonbank-issued crypto assets. Policymakers should conduct research and understand the different risks posed by different categories of digital assets to identify the most effective ways to address risks within those categories.

Separately, there are different types of DLT/blockchain networks that vary in breadth of access and control. Public, permissionless blockchains allow anyone to access the network and engage with it, but within public blockchain infrastructures, permissions may be imposed on interactions with certain smart contracts deployed on the infrastructure, while within private, permissioned blockchains, access is limited to parties with appropriate entitlements. These types of networks present different levels of risk. The existing regulatory framework and banks' risk management practices enable banks to manage the risks presented by permissioned networks. Policymakers should consider further study of risk identification and management with respect to permissionless blockchains, which could potentially support the development of appropriate tools, such as digital identity or "verifiable credentials," that could make public blockchain more safe and secure so that banks and other commercial segments, as well as consumers, could potentially avail themselves of the benefits of such technology. Such benefits may include greater interoperability among bank systems, enhancement in information communication, and a reduction to barriers and costs in cross-border payments.[14]

Banks appropriately manage any technology-related risks in connection with standard internal recordkeeping functions and tokenizing traditional banking products. Banks use technology only if they determine the associated risks could be appropriately managed consistent with their risk appetites and risk management capabilities. Federally-insured banking organizations are subject to comprehensive regulation, supervision, and examination for compliance with prudential, consumer protection, and data privacy requirements, among others. Larger banking organizations have separate examinations of, among other areas, custody and technology.[15] Adherence to these standards is monitored by on- and offsite banking agency examiners. Banks' books and records systems are already subject to standards and oversight to address risks associated with these systems. Changing a bank's internal books and records design from a more traditional database design to a blockchain or DLT-based design does not change the underlying activity, nor introduce unknown parties, and should be evaluated under the

[14] For example, the Monetary authority of Singapore's Project Guardian will "develop and pilot use cases in four main areas," including exploring "the use of public blockchains to build open, interoperable networks that enable digital assets to be traded across platforms and liquidity pools. This includes interoperability with existing financial infrastructure" (link).

[15] This supervisory oversight includes the robust evaluation of information technology risk management, internal controls, and cybersecurity risk management. Banking organizations also must meet regulatory expectations with respect to other operational resiliency obligations and recovery and resolution planning mandates Banking organizations are subject to exams that evaluate how well management addresses risks related to the availability of critical financial products and services, including risks arising from cyber events. Management must also ensure the adoption of processes to oversee and implement resiliency, continuity, and response capabilities to safeguard employees, customers, and products and services. *See* Federal Financial Institutions Examination Council, FFIEC Information Technology Examination Handbook: Business Continuity Management (Nov. 2019) (link).

existing supervisory framework.[16] Banks are able to address operational risks associated with DLT and blockchain, thus avoiding the need for additional requirements, including capital requirements, to address operational risk from new technology. The regulators must appropriately identify and understand the risks of each type of network, controls and operating model to establish proper guardrails without adopting overly punitive measures that stifle responsible innovation. However, guidance issued by the regulators currently suggests that the regulators may view the risks presented by banks' use of DLT and blockchain as akin to those presented by nonbank-issued cryptoassets, which could slow the pace of banks' ability to engage in responsible innovation in this space.[17] In particular, guidance issued by the federal banking agencies requires banking organizations to provide advance notice, and if applicable, receive supervisory nonobjection based on an evaluation of the adequacy of risk management systems and controls before conducting certain traditional banking activities using DLT or blockchain, hindering responsible innovation."[18] Banks are consistently evaluating and managing the risk of incorporating new technologies and implementing solutions to mitigate evolving risks. Banks' management of dynamic cyber risks provides an example of how regulated financial institutions are able to evolve controls to mitigate new risks.

Policymakers, in particular, the federal banking agencies, should study how banks are able to appropriately manage the risks presented by permissioned DLT, blockchain, or other novel technologies in connection with traditional banking products such as deposits and securities, and for internal recordkeeping and eliminate the requirement that banks provide prior notice, or, in some cases, obtain prior approval, before engaging in those activities. Any concerns may be addressed through the normal supervisory process, as is the case with all of a banking organization's operations. Policymakers should study the impact of the banking regulators' conflation of the risks of different types of DLT/blockchain networks and digital asset products on the United States's competitive position in global financial markets, including potential implications if U.S. banks are unable to support digital clearing and settlement activities. For example, some firms have launched innovative banking and financial products

[16] The electronic book entries present in such a recordkeeping system serve the identical functional purpose as electronic book entries used to record assets in traditional electronic books and records systems. Accordingly, the use by a bank of blockchain or DLT for internal recordkeeping purposes and accompanying internal electronic book entries should not be subject to any additional regulation beyond the existing supervisory framework applicable to a bank's internal books and records systems or additional capital requirements.

[17] For example, the Federal Reserve's Policy Statement on Section 9(13) of the Federal Reserve Act, which discusses risks related to cryptoassets, states that "the term "crypto-assets" refers to digital assets issued using distributed ledger technology and cryptographic techniques (for example, bitcoin and ether), but does not include such assets to the extent they are more appropriately categorized within a recognized, traditional asset class." The Policy Statement then undermines this relative clarity by noting that "[t]o the extent transmission using distributed ledger technology and cryptographic techniques changes the risks of a traditional asset (for example, through issuance, storage, or transmission on an open, public, and/or decentralized network, or similar system), the Board reserves the right to treat it as a "crypto-asset" (link).

[18] *See* OCC Interpretive Letter No. 1179, Chief Counsel's Interpretation Clarifying: (1) Authority of a Bank to Engage in Certain Cryptocurrency Activities; and (2) Authority of the OCC to Charter a National Trust Bank (Nov. 18, 2021) (link); FDIC, FIL-16-2022, Notification of Engaging in Crypto-Related Activities (April 7, 2022) (link); Board of Governors of the Federal Reserve System, "Engagement in Crypto-Asset-Related Activities by Federal Reserve-Supervised Banking Organizations", SR 22-6 / CA 22-6 (Aug. 16, 2022) (link).

and services in other countries due to the uncertain regulatory environment in the United States for conducting such activities.[19]

Policymakers should also consider studying the impact of the banking regulators' limitations on banks' involvement in certain digital asset activities on consumers. The public and the financial system *benefit* from banks' involvement in the activities described in the Interpretive Letters. For example, with respect to custodying cryptoassets, banks have a long history of providing, and are well-suited to provide, safeguarding services. Thus, banks continue to evaluate whether to enter this business, and, for those who have already entered this business, they are precluded from doing so at scale.[20] If regulated banking organizations are effectively precluded from providing crypto-asset safeguarding services at scale, investors and customers, and ultimately the financial system, will be worse off; the market would then be limited to custody providers that do not afford their customers the legal and supervisory protections provided by federally-regulated banking organizations.

2. Goals, sectors, or applications where digital assets introduces risks or harms.

As we have described in the past, and as policymakers have recognized, crypto assets present unique risks.[21] As recommended previously, the only way to mitigate these risks is to adopt a comprehensive regulatory and supervisory framework at the national level that addresses each risk posed by crypto-asset companies, their subsidiaries, affiliates, and other related entities active in that ecosystem.[22] Policymakers should first study and develop an ontology to distinguish among crypto asset

---

[19] For example, HSBC recently launched the Orion platform, a bond tokenization initiative, in Luxembourg. The security would be both issued and registered under Luxembourg law (link).

[20] A related obstacle to banks' serving as custodians in the crypto marketplace is the SEC's Staff Accounting Bulletin No. 121, which would require an entity safeguarding a cryptoasset to present a liability (and recognize a corresponding asset) on its balance sheet equal to the fair value of the safeguarded cryptoasset. SEC Staff Accounting Bulletin No. 121 (March 31, 2022) (link). The SEC staff has indicated that SAB 121 is driven by investor protection concerns related to legal, technological, and regulatory risks arising from custodied assets; as we have previously explained, banking organizations comprehensively address these risks through the legal, regulatory and supervisory frameworks applicable to those organizations. The federal banking agencies and the SEC should jointly study these frameworks and determine that banks should be excluded from the accounting treatment in the SAB, thereby enabling them to provide custody services for cryptoassets at scale, which should include consideration of the SEC's recent proposal to expand the range of client assets that investment advisers must secure with "qualified custodians" such as banks or broker-dealers to include crypto assets and to enhance the protections afforded clients' custodied assets. *See* letter from ABA, BPI, and SIFMA re: SAB 121 to the Office of the Chief Accountant of the SEC, the OCC, the FDIC, the Federal Reserve Board, and the Department of the Treasury (June 23, 2022) (link); *see also* SEC proposed rule changes to enhance protections of customer assets managed by registered investment advisers (Feb. 15, 2023) (link).

[21] *See, e.g.*, Financial Stability Board, Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Consultative Document (Oct. 11, 2022) (link); Financial Stability Board, Review of the FSB High-Level Recommendations of the Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements: Consultative Report (Oct. 11, 2022) (link); *See* President's Working Group on Financial Markets, FDIC, & OCC, Report on Stablecoins (Nov. 2021) (link); [21] U.S. Department of the Treasury, Crypto-Assets: Implications for Consumers, Investors, and Businesses 51 (Sept. 2022) (link); Financial Stability Oversight Council, Report on Digital Asset Financial Stability Risks and Regulation (2022) (link). *See also* Letter from Paige Pidano Paridon, BPI, to Daniel J. Harty, Director, Office of Capital Markets, U.S. Department of the Treasury (Aug. 8, 2022) (link); Letter from Paige Pidano Paridon, BPI, and Robert H. Hunter, TCH, to The Financial Stability Board (Dec. 15, 2022) (link).

[22] *See* Letter from BPI and TCH to the FSB (Dec. 15, 2022).

types and the risks that are posed by each asset type to best determine what laws, regulations, and other requirements are most approiate to address those particular risks. For example, stablecoins may require prudential regulation, supervision, and examination while market-based regulation may be more appropriate for other types of crypto assets.

Crypto Assets

Policymakers should study the appropriate standards and oversight to address the risks presented by nonbank-issued crypto-assets and related activities to preserve financial stability and protect consumers, investors, and businesses worldwide. For example, policymakers should research the appropriate disclosures, and how the delivery of those disclosures would be most effective, of the activities (including rehypothecation) engaged in, risk management and corporate control functions to avoid fraud, affiliate transaction restrictions and other aspects of interconnectedness, and appropriate and effective BSA/AML requirements.

Stablecoins

It is important to define key terms and concepts related to "stablecoins." We use the term "stablecoin" to refer to nonbank-issued stablecoins and not to tokenized or blockchain-based bank deposits. In general, a stablecoin issuer commits to sell its stablecoin, and redeem it on demand, at the coin's par value and holds a designated pool of assets to "back" this commitment. The assets backing the stablecoin need to be available to, or prioritized for, the stablecoin holders who may want to redeem, and the assets cannot be subject to claims of others. The pool of assets should consist of safe, liquid assets, such as government securities (e.g., U.S. Treasury bills) and insured bank demand deposits, which could be used to meet many redemptions with high confidence. In practice, however, some of the assets currently held by some of the largest stablecoin issuers, which they refer to as their "reserves," are in fact less liquid and riskier assets, like commercial paper and corporate bonds, and can thus present run risk if the viability of the issuer is called into question. Stablecoin arrangements differ from existing payments systems, which have meaningful regulatory and supervisory frameworks that apply.[23]

Current laws and regulations provide a strong framework for imposing safety and soundness requirements on banks when using novel technologies, such as DLT, to engage in deposit taking and other financial services.[24] There is no federal legal framework governing the issuance of stablecoins by nonbanks, however. Should such a framework for nonbank issuers be developed, it should be designed to promote a safe, healthy, and competitive U.S. stablecoin system and should prioritize the safety, soundness, and resiliency of the stablecoin issuer; the protection of consumers; the preservation of U.S. financial stability; the prevention of financial crimes and illicit finance; and the assurance that stablecoin issuers can be resolved in a safe and orderly way if they become troubled and fail. For example, regulators should study, at a minimum, the appropriate requirements related to: capital; liquidity requirements; reporting and auditing requirements; limitations on permissible activities (including lending and rehypothecation); redemption; counterparty risk; technological standards; usage; anti-money laundering, countering the financing of terrorism, and economic sanctions obligations; operational resilience and cybersecurity; and data privacy and security. Given the significant risks that could arise should nonbank stablecoin issuers and uninsured and non–federally regulated banks be

[23] *See, e.g.,* Bank Service Company Act, 12 U.S.C. § 1861, *et. seq*. It should be further noted that supervisory oversight may also extend to such payment systems as a consequence of the regulatory approval national banks may need in order to invest in them. *See* 12 C.F.R. § 5.36.

[24] *See* note 8, *supra.*

granted access to central bank reserves, they should not be given such access given the lack of sufficient controls and governance.[25]

3. Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets.

As referenced previously, policymakers should research and establish a universal taxonomy for the digital asset ecosystem, standard setting rules for best practices, and the operational risk management and resiliency factors that make the banking industry able to adopt new DLT/blockchain technology consistent with banks' safe and sound operation. For example, banks can safely tokenize real-world assets that are already regulated and can be facilitated through transactions on the ledger. Policymakers also should investigate the potential implications and principles of interoperability between public and private blockchains. Additionally, policymakers should study other implications of using public blockchains, specifically regarding the underlying network governance, to help inform whether there may be potential for these networks to be used by banks.

Policymakers should also study how best to recognize and take actions to mitigate illicit finance risks associated with certain digital-asset transactions, which may include reduced transparency, disintermediation of financial institutions subject to AML and CFT obligations, increased complexity, and other risks.[26] The primary "illicit financing risks associated with virtual assets come from gaps in implementation of the international AML/CFT standards across countries; the use of anonymity-enhancing technologies; the lack of covered financial institutions as intermediaries—and thus the absence of AML/CFT controls—in some virtual asset transactions; and [virtual asset service providers ("VASPs")] that are non-compliant with AML/CFT and other regulatory obligations."[27] To mitigate these risks, policymakers should study how best to ensure that "international standards for the regulation and supervision of service providers associated with stablecoins and other digital assets [are] effectively implemented worldwide."[28] The Treasury Department should facilitate cross-border cooperation and other information sharing relating to the illicit finance risks of digital assets and digital-asset transactions. The requirements and expectations regarding AML and CFT activities should be consistent for all institutions that engage in equivalent activities with similar illicit finance risk characteristics, regardless of a particular entity's status as a bank, money services business, other type of institution, or the type of digital asset related activity.

---

[25] Some nonbank entities engaged in, or seeking to engage in, stablecoin issuance and entities with banking charters that do not have deposit insurance and are not subject to consolidated federal supervision have sought access to central bank reserves. Not limiting account access to appropriately regulated entities could pose significant risk to the U.S. financial system given the significant interconnections between the private sector and the central bank. Furthermore, if certain nonbank stablecoin issuers and other less-regulated entities were granted unfettered access to central bank reserves and they issued stablecoins backed fully by deposits at the central bank, those reserves could be perceived as the ultimate safe asset in times of economic or market stress and could lead to massive outflows of deposits in the banking system into that issuer's stablecoin, further exacerbating stress on the country's banks. There may be foreign policy effects that have not yet been entirely explored, and that should be researched further, should policymakers consider granting such entities access to the central bank.

[26] *See* U.S. Department of the Treasury, Action Plan to Address Illicit Financing Risks of Digital Assets (Sept. 16, 2022) (link); *see also* Letter from Gregg Rozansky, BPI, to Jon Fishman, Assistant Director, Office of Strategic Policy, Terrorist Financing, and Financial Crimes, U.S. Department of the Treasury (Nov. 3, 2022) (link).

[27] *See* Action Plan to Address Illicit Financing Risks of Digital Assets at 4.

[28] *Id.*

Additionally, policymakers should research how new technologies could support further compliance with AML/CFT/KYC requirements. For example, BPI has previously expressed support for proposed legislation that would establish a federal task force to identify a digital ID implementation strategy across federal, state, and local governments in a way that is user friendly and accessible and that enhances security and preserves privacy.[29] Research also should be considered regarding how programmable money/tokens could support AML/CFT/sanctions compliance because the asset itself could be programmed for compliance and thus, to interact with the token, an entity would have to meet the compliance conditions of its programmed rules.

Other important areas of research that should be pursued include how to enable more sophisticated encryption – such as post quantum safe encryption and privacy-preserving encryption – that would help strengthen the safety and privacy of all digital asset projects, whether public or private. Such research also would build on federal expertise and initiatives on encryption (e.g., National Institute of Science and Technology, National Security Agency) and links with academia (e.g., Defense Advanced Research Projects Agency). Furthermore, there is currently a void in private research on the topic, making public sector research, potentially jointly with the private sector, even more critical.

4. R&D that should be prioritized for digital assets.

The RFI appears focused on research related to a U.S. CBDC. As we have previously and extensively detailed, an intermediated, account-based CBDC could pose serious risks to the U.S. economy and financial system that would not be outweighed by the purported benefits. By attracting deposits away from banks, particularly during a period of economic stress, a CBDC likely would undermine the commercial banking system in the United States, and severely constrict the availability of credit to the economy in a highly procyclical way.[30]

Many of the potential benefits cited by proponents of a CBDC are uncertain, and, moreover, many are mutually exclusive and thus could not be realized simultaneously.[31] Some proponents of a U.S. CBDC claim that a CBDC would make domestic and cross-border payments systems more efficient. While perhaps relevant in some countries, this rationale for a CBDC seems increasingly inapt in the United States, where The Clearing House's RTP real-time payment system, operational since 2017, continues to grow in use, consumers happily pay each other with Zelle or Venmo, and PayPal and Square are used widely. In addition, the Federal Reserve is nearing launch of its FedNow, further adding to the availability of faster payments options. Any research into the potential value of a CBDC in the U.S. should consider the private and public sector solutions available or under development and their ability to achieve the same potential benefits without some of the potential drawbacks discussed above.

---

[29] *See* BPI Press Release, "BPI Supports Senate Effort to Achieve Digital ID Benefits" (Sept. 28, 2022) (link). *See also* Letter from BPI et al. to Speaker Pelosi, Republican Leader McCarthy, Majority Leader Schumer, & Republican Leader McConnell (Nov. 18, 2022) (link) (supporting passage of the Improving Digital identity Act of 2022).

[30] Through an intermediated, account-based model, consumers would hold their CBDC at an account at a bank or other intermediary, similar to the way a trust bank holds a security for a customer. Any transfer of a dollar deposit from a commercial bank or credit union to a CBDC is a dollar unavailable for lending to businesses or consumers.

[31] For example, one of the most frequently cited reasons in support of a CBDC is that it would increase financial inclusion, yet we are unaware of any substantiated use case for CBDC that would benefit low- and moderate-income people in the United States.

Inefficiencies in the current cross-border system are to some extent attributable to regulation for AML/CFT purposes, which a CBDC would not reduce. Policymakers should research other initiatives and means to modernize the payments system, including other efforts that are underway to improve cross-border payments outside of any potential CBDC issuance, including use of blockchain by the banking sector as a more effective rail for cross-border payments.[32] Improving the existing cross-border payments system is a key priority of the FSB, which has devoted and indicated it will continue to devote significant resources to this effort. The Clearing House, EBA CLEARING, and SWIFT have executed a proof of concept and announced plans to launch by the end of this year an immediate cross-border (IXB) payments system; it is being designed with the contribution of 24 financial institutions.[33] Several wholesale CBDC pilots are underway globally, but it is too early to draw conclusions as to whether a wholesale CBDC could improve cross-border payments. Thus, further research is required before determining whether a wholesale CBDC could enhance cross-border payments' efficiency.[34]

Policymakers should continue to invest in open-source research and projects underway from NIST, including research on technical standards and guidance on the use of blockchain technology,[35] cryptographic techniques, particularly regarding threshold schemes that may be used in the future, such as Multi-Party Threshold Cryptography,[36] standards and requirements, such as Security Requirements for Cryptographic Modules.[37] Policymakers also should pursue research regarding (i) specific cybersecurity standards or approaches for interacting with permissionless/pubic blockchains and provide further guidance regarding NIST's cybersecurity framework used by most banks (ii) inter-operability blockchain standards for banks.

5. Opportunities to advance responsible innovation in the broader digital assets ecosystem.

Policymakers should research how new technologies can facilitate the creation of verifiable credentials, which are digital identity tools, which may be used to ensure that transactions conducted using new technologies are only executed with verified counterparties. Researchers should also study how the banking sector can safely use private and/or permissioned chains in light of the highly supervised and controlled environments in which they operate. As part of this effort, policymakers should study examples of use cases of private permissioned networks and hybrid models to help determine how banks can leverage those models in the highly regulated and supervised environments in which they operate. Further research should be pursued on the use of permissioned smart contracts where business rules are self-executing on the network.

---

[32] As noted previously, Partior is designed to perform atomic clearing and settlement on a 24x7 basis among participating institutions using blockchain and smart-contract technology.

[33] *See* John Adams, "Banks gearing up to test real-time payments across borders," *American Banker*, (May 2, 2022) (link). *See also* "EBA Clearing, SWIFT, and The Clearing House to deliver pilot service for immediate cross-border payments" (April 28, 2022) (link).

[34] If the Federal Reserve wished to assist in these and other efforts to modernize payments, it could finalize plans announced in 2018 to convert Fedwire to a 24/365 system.

[35] *See* NIST "Blockchain." (link).

[36] *See* NIST "Information Technology, Laboratory, Computer Security Resource Center: Multi-Party Threshold Cryptography MPTC" (link).

[37] *See* NIST "Information Technology, Laboratory, Computer Security Resource Center: FIPS 140-2, Security Requirements for Cryptographic Modules (link).

* * * * *

We thank you for your consideration and review of these comments. If you have any questions or wish to discuss this letter, please do not hesitate to contact us using the contact information provided below.

Very truly yours,

/s/ Paige Pidano Paridon
Paige Pidano Paridon
Senior Vice President,
Senior Associate General Counsel
Bank Policy Institute
(703) 887-5229
paige.paridon@bpi.com

/s/ Brooke Ybarra
Brooke Ybarra
Senior Vice President
American Bankers Association
(202) 663-7642
bybarra@aba.com

Appendix – Descriptions of the Organizations

The Bank Policy Institute is a nonpartisan public policy, research, and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks, and the major foreign banks doing business in the U.S. Collectively, they employ almost two million Americans, make nearly half of the nation's bank-originated small business loans, and are an engine for financial innovation and economic growth.

The American Bankers Association is the voice of the nation's $23.6 trillion banking industry, which is composed of small, regional and large banks that together employ more than 2 million people, safeguard $19.2 trillion in deposits and extend $12.2 trillion in loans.