BANK POLICY INSTITUTE

August 8, 2022

Via Electronic Submission

Daniel J. Harty, Director
Office of Capital Markets
United States Department of the Treasury
1500 Pennsylvania Avenue, NW
Washington, D.C. 20220

Re: "Ensuring Responsible Development of Digital Assets; Request for Comment" (87 Fed. Reg. 40881 (July 8, 2022))

Ladies and Gentlemen:

The Bank Policy Institute[1] appreciates the opportunity to comment on the Department of Treasury's Request for Comment on "Ensuring Responsible Development of Digital Assets" in connection with Executive Order 14067, "Ensuring Responsible Development of Digital Assets."[2] According to the Fact Sheet accompanying the Executive Order, digital assets, including cryptocurrencies, exceeded a $3 trillion market cap last November, although published reports indicate that recent turmoil in those markets has reduced that number by as much as two-thirds. In addition, some surveys indicated that around 16 percent of adult Americans – approximately 40 million people – have invested in, traded, or used cryptocurrencies. In light of the growth of digital assets over the past few years and the risks that are presented by digital assets and related activities that are not yet subject to a comprehensive regulatory framework, BPI supports the goal of the Executive Order to promote a coordinated, "whole of government" approach to fostering responsible innovation and the following specific policy objectives for digital assets articulated in the Executive Order:

[1] BPI 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 United States. Collectively, they employ almost 2 million Americans, make nearly half of the nation's bank-originated small business loans and are an engine for financial innovation and economic growth.

[2] 87 Fed. Reg. 14143 (March 14, 2022). The Executive Order 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 that are used to make payments or investments, or to transmit or exchange funds or the equivalent thereof, that are issued or represented in digital form through the use of distributed ledger technology. 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."

(a) protection of consumers, investors, and businesses in the United States;
(b) protection of United States and global financial stability and the mitigation of systemic risk;
(c) mitigation of illicit finance and national security risks posed by misuse of digital assets;
(d) reinforcement of U.S. leadership in the global financial system and in technological and economic competitiveness, including through the responsible development of payment innovations and digital assets;
(e) promotion of access to safe and affordable financial services; and
(f) support of technological advances that promote responsible development and use of digital assets.

Section 5(b)(i) of the Executive Order directs the Secretary of the Treasury, in consultation with the Secretary of Labor and the heads of other relevant agencies, to report to the President on the "implications of development and adoption of digital assets and changes in financial market and payment infrastructures for United States consumers, investors, businesses, and for equitable economic growth. The report must address the conditions that would drive mass adoption of different types of digital assets and the risks and opportunities such growth might present to United States consumers, investors, and businesses, including a focus on how technological innovation may impact these efforts and with an eye toward those most vulnerable to disparate impacts."[3] We appreciate the Treasury Department's solicitation of input and recommendations as it considers the implications of development and adoption of digital assets.

BPI supports innovation but believes it must be conducted in a manner consistent with the safety and soundness of the financial system, national security, and robust consumer and investor protection. Digital assets have the potential to provide benefits to consumers and businesses and to the financial system. However, uncertainties remain about the potential risks presented by digital assets. For this reason, a careful, data-driven, and whole-of-government approach for evaluating the potential benefits and risks of, and establishing a regulatory framework to address the risks presented by, digital assets, is prudent.

In the RFC, Treasury encourages commenters "to address any or all of the following questions, or to provide any other comments relevant to the development of the report . . . on the implications of developments and adoption of digital assets and changes in financial market and payment infrastructures for United States consumers, investors, businesses, and for equitable economic growth as directed by Section 5(b)(i) of the Executive Order." BPI has written extensively on a number of the topics raised by the questions.[4] We provide below references and citations to our prior work as relevant to the particular question.

However, we first emphasize, as we have articulated previously, high level principles that should guide digital asset regulation.

---

[3] As provided in the Executive Order, the term "mass adoption" is defined as a scenario where digital assets are accepted and used by the U.S. public on a large scale. For example, mass adoption of digital assets as a payment method would translate to use and acceptance of cryptocurrencies as a common and regular payment method for goods and services.

[4] *See*, *e.g.*, the Bank Policy Institute's work on central bank digital currency and stablecoins, available at https://bpi.com/category/digital-assets/central-bank-digital-currency/.

First, a coordinated, government-wide approach to establishing a comprehensive framework for regulating digital assets and related activities will help to ensure that the United States remains a global leader in innovation while also ensuring that consumers, the financial system, and national security are protected. Regulators should first create clear definitions of digital assets that capture the different risks they pose. Today, digital assets that are associated with different risk levels are broadly categorized (e.g., stablecoins).A fractured approach to this evaluation is likely to result in the failure to establish an appropriate, comprehensive regulatory framework for digital assets and related activities, ultimately harming customers and investors and potentially undermining United States national security and competitiveness in these markets.

The risks of an uncoordinated approach to the regulation of digital assets and related activities are real, as illustrated with respect to the activity of safeguarding cryptoassets. Banks have a long history of providing, and are well-suited to provide, safeguarding services. However, although the banking regulators last year promised additional clarity on the authority of banks to engage in certain crypto activities, including certain crypto custody activities, and related risk management expectations, that guidance has yet to be provided. Thus, banks continue to evaluate options to enter this business but have yet to do so at scale. Meanwhile, in March, the SEC issued Staff Accounting Bulletin No. 121, which would require an entity – presumably including a banking organization – 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.[5] This treatment of cryptoassets deviates from existing accounting treatment of safeguarded assets held in a custodial capacity, which does not result in assets or liabilities reported on the custodian's balance sheet because the custodian has no property right in the asset and no liability in the event of deterioration of the value of the asset or otherwise in respect of the cryptoasset. Furthermore, if SAB 121 is interpreted to require the inclusion of custodied cryptoassets on a banking organization's balance sheet, the knock-on effects under the prudential regulatory framework would be so significant that banking organizations effectively would be precluded from providing such services to clients.

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. BPI supports the need to mitigate these risks in the interest of investor protection. However, we note that, in the case of banking organizations, these risks are comprehensively addressed by the legal, regulatory and supervisory frameworks applicable to those organizations.[6]

[5] SEC Staff Accounting Bulletin No. 121 (March 31, 2022), available at: SEC.gov | Staff Accounting Bulletin No. 121. "Cryptoasset" is very broadly defined in the SAB to include digital assets issued and/or transferred using distributed ledger or blockchain technology using cryptographic techniques. SAB 121 discusses an entity whose activities include both operating a crypto-asset platform that allows its users to transact in cryptoassets and providing a service where it will safeguard the platform users' cryptoassets, including maintaining the cryptographic key information necessary to access crypto-assets. We understand, however, that SEC Staff has indicated that it interprets SAB 121 as applying to all instances involving the safeguarding of cryptoassets, regardless of whether the entity also operates a trading platform.

[6] There is no indication that the SEC staff took into account the fundamental dichotomy between banking and nonbanking organizations. Nor is there any indication that the SEC staff considered the preclusive effect of SAB 121 on banking organizations in relation to nonbanking organizations. Accordingly, it appears unlikely that the SEC gave appropriate consideration to whether banks should be excluded from the accounting treatment in the SAB or

The lack of communication and coordination among the agencies as well as the lack of consultation on this standard has resulted in the SEC perhaps not fully appreciating how these risks are handled differently by different market participants and therefore has resulted in banks' having to pause efforts underway to enter this business as they await further clarity from the agencies about the applicability of SAB 121 and the risk management expectations of their supervisors. Indeed, Federal Reserve Chair Jerome Powell noted at a Congressional hearing recently that: "Custody assets are off balance sheet, have always been . . . The SEC made a different decision as it relates to digital assets for reasons it explained, and now we have to consider those."[7] Investors and customers will be worse off without the participation of regulated banking organizations in this market, as customers and the market would benefit from the entry into the crypto custody market of highly regulated banks with sophisticated risk management capabilities.

Consistent with the goal of promoting responsible innovation via a "whole of government" approach as articulated in the Executive Order, the relevant agencies should jointly evaluate the comprehensive legal, regulatory and supervisory frameworks applicable to banking organizations that address the risks identified by the SEC and determine that banks should be excluded from the accounting treatment in the SAB, thereby enabling them to provide custody services for cryptoassets.[8] Moreover, future regulatory efforts should involve consultation among responsible agencies to identify this type of conflict with the stated goals of the Executive Order.

Second, and relatedly, BPI has previously identified the need for the relevant agencies to further clarify the ability of banks to engage in digital asset related activities and the risk management expectations related to those activities to foster responsible innovation, including with respect to providing custody services for cryptoassets, as referenced previously.[9] The OCC, through Interpretive Letter 1179, requires a banking organization to receive supervisory nonobjection regarding risk management systems and controls before conducting certain crypto-asset custody and other crypto-

---

the question of the impact on investor protection if it were not feasible, solely because of SAB 121, for banks to provide custody services for cryptoassets.

[7] Jesse Hamilton, "US Fed Evaluating SEC's Position on Digital Assets Custody, Powell Says," CoinDesk (June 22, 2022), available at: US Fed Evaluating SEC's Position on Digital Assets Custody, Powell Says (coindesk.com)

[8] *See* comment letter re: SAB 121 to the Office of the Chief Accountant of the Securities and Exchange Commission, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Federal Reserve Board, and the Department of the Treasury, June 23, 2022, ABA, BPI, and SIFMA, available at: https://bpi.com/bpi-aba-and-sifma-comment-on-staff-accounting-bulletin-no-121/.

[9] *See* comment letter re: Request for Information and Comment on Digital Assets (RIN 3064–ZA25), Bank Policy Institute and Consumer Bankers Association, July 16, 2021, available at: Microsoft Word - BPI Comment Letter - FDIC RFI on Digital Assets (FINAL - signed).

related activities.[10] The FDIC imposes a similar requirement.[11] The federal banking agencies jointly advised in November 2021 that throughout 2022 they would "provide greater clarity on whether certain activities related to crypto-assets conducted by banking organizations are legally permissible, and expectations for safety and soundness, consumer protection, and compliance with existing laws and regulations related to: crypto-asset safekeeping and traditional custody services; ancillary custody services; facilitation of customer purchases and sales of crypto-assets; loans collateralized by crypto-assets; Issuance and distribution of stablecoins; and activities involving the holding of crypto-assets on balance sheet."[12] The agencies have not yet provided additional clarity on these topics.

Banks have traditionally been at the forefront of technological innovation, and as more use cases emerge for digital assets, BPI's members are evaluating where and how these innovations can be applied in their own businesses to best serve the needs of customers (or potential customers). Both the public and the financial system would benefit from banks' involvement in digital assets. Banks are subject to comprehensive and robust risk management, supervision and examination processes, are subject to consumer protection laws and regulations, maintain strong capital buffers, carry deposit insurance, have well-developed anti-money laundering programs[13] including robust know-your-customer practices, and have substantial experience with incorporating new technologies into the financial system. Banks have the resources, talent and expertise to implement robust compliance programs, which are especially important with respect to digital assets, which present novel illicit finance risks.

Failure to provide clarity regarding the expectations for banks engaging in digital assets related activities is hindering the ability of banks to engage in responsible innovation in this space, thereby requiring consumers to look solely to unregulated or lightly regulated non-bank financial service providers and limited-purpose, uninsured banking institutions for digital asset products and services, instead of banks.[14] Disparate regulation ultimately harms consumers and the financial system. Non-

---

[10] 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), available at: Interpretive Letter 1179 (occ.gov); *see also* OCC Interpretive Letter No. 1170, Re: Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers (July 22, 2020), available at: Interpretive Letter 1170, Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers (occ.gov).

[11] *See* FDIC, FIL-16-2022, Notification of Engaging in Crypto-Related Activities (April 7, 2022), available at: FDIC: FIL-16-2022: Notification of Engaging in Crypto-Related Activities.

[12] Joint Statement on Crypto-Asset Policy Sprint Initiative and Next Steps (November 23, 2021), available at: Joint Statement on Crypto-Asset Policy Sprint Initiative and Next Steps (federalreserve.gov).

[13] For the purposes of this letter, references to AML practices are inclusive of bank compliance with economic sanctions programs administered by the Office of Foreign Assets Control ("OFAC").

[14] Non-bank financial service providers and limited-purpose banking institutions have been early providers of digital asset products and services. Many products and services offered by limited-purpose banking institutions resemble traditional bank products and activities, including custodial services, payment services and activity akin to deposit-taking. States have established regulatory frameworks supporting non-bank financial services providers' offering of these products. For example, the New York State Department of Financial Services ("NYDFS") has been issuing licenses related to virtual currency business activities, known as BitLicenses, since 2015 pursuant to its virtual currency regulations under the New York Financial Services Law. The NYDFS has also granted limited-purpose trust company charters under the New York Banking Law, giving such entities state authority to act as

banks and limited-purpose banking institutions offering digital asset products and services are generally not subject to comprehensive and robust supervision and examination or consumer protection regimes, may have thin capital requirements and may not have sufficient resources to cover operational and other losses.[15] Further, some non-banks offer digital asset products that bear similarities to bank products—like interest bearing accounts—even though such products lack FDIC insurance.[16] Indeed, the Federal Reserve and the FDIC recently issued a issued a joint letter demanding that the crypto lender firm Voyager Digital cease and desist from making false and misleading statements regarding its FDIC deposit insurance status.[17] Voyager had misled its customers into thinking their money invested with Voyager was FDIC insured, and therefore much safer than it was. It remains to be seen how much Voyager's customers will be able to recoup of their investments and cash held with the company.[18] The FDIC subsequently issued an advisory reminding insured banks "that they need to be aware of how FDIC insurance operates and need to assess, manage, and control risks arising from third-party relationships, including those with crypto companies."[19]

Finally, the requirements and expectations regarding digital assets-related activities should not be lower for financial institutions that operate outside the bank regulatory perimeter.[20] Policymakers should develop an appropriate regulatory framework for nonbank entities engaged in digital assets-related activities to ensure that those activities are subject to equivalent requirements and risk management expectations as would be expected of banking entities engaged in the same activities presenting the same risks. As noted, banks maintain strong capital buffers and are subject to numerous prudential and safety and soundness requirements. To the extent that nonbanks present similar risks

---

qualified custodians and exchanges for digital assets. Similarly, in 2019, the State of Wyoming created Special Purpose Depository Institution ("SPDI") charters, Wyo. Stat. § 13-12-101, *et seq.*, authorizing the chartering of institutions focused on digital assets.

[15] *See, e.g.*, BPI, *Beware the Kraken* (Oct. 21, 2020), https://bpi.com/beware-the-kraken/; BPI, *Why a Wyoming Charter is No Hail Mary for the Anti-Fractional Banking Team* (Nov. 9, 2020), https://bpi.com/why-a-wyoming-charter-is-no-hail-mary-for-the-anti-fractional-banking-team/.

[16] Consumers may view such products as equally safe as traditional, FDIC-insured bank deposit accounts. One exchange advertises one such account to customers who are "looking for a dollar-based experience that's more like an interest-bearing savings account . . . ." *See* Coinbase, *How to earn crypto rewards*, https://www.coinbase.com/learn/tips-and-tutorials/how-to-earn-crypto-rewards; Gemini, *What is Gemini Earn?*, https://support.gemini.com/hc/en-us/articles/360055836212-What-is-Gemini-Earn-.

[17] FDIC and Federal Reserve Joint Letter Regarding Potential Violations of Section 18(a)(4) of the Federal Deposit Insurance Act (July 28, 2022), available at: Joint Letter Regarding Potential Violations of Section 18(a)(4) of the Federal Deposit Insurance Act (federalreserve.gov).

[18] Yueqi Yang, "Bankrupt Crypto Broker Voyager Plans to Resume Cash Withdrawals" (August 5, 2022), available at: https://www.bloomberg.com/news/articles/2022-08-05/bankrupt-crypto-broker-voyager-plans-to-resume-cash-withdrawals.

[19] FDIC Advisory to FDIC-Insured Institutions Regarding Deposit Insurance and Dealings with Crypto Companies (July 29, 2022), available at: Advisory to FDIC-Insured Institutions Regarding FDIC Deposit Insurance and Dealings with Crypto Companies.

[20] *See* letter to the Department of Commerce re: Request for Comment on Developing a Framework on Competitiveness of Digital Asset Technologies (July 5, 2022), BPI, available at: DepartmentofCommerce-DigitalAssets-RFI-BPIResponse-2022.07.05.pdf.

that those requirements are intended to address, nonbanks should be subject to equivalent requirements and oversight.

In addition, it is important that consumers are protected regardless of whether they obtain digital asset related products or services from a regulated banking entity or a fintech. However, nonbanks in the digital asset ecosystem are not subject to regular, direct supervision for their compliance with consumer protection requirements, in contrast to federally regulated banks. Indeed, some tech companies "make technical, and questionable, arguments that their products or services fall outside the existing regulatory framework."[21] Further, "the enforcement authority for applicable consumer protection requirements on fintech activities is scattered among various federal and state regulators."[22] In addition, the diffuse organizational structure of many tech companies raises questions about who is responsible for consumer compliance and the mechanisms in place to ensure that those protections are implemented. Indeed, in the context of several cryptoasset companies, the ownership and executive management are murky, which is, of course, directly contrary to the regulatory requirements for insured banks. Banks, in contrast, have significant experience and expertise in implementing consumer protection safeguards. In addition, banks are subject to regular consumer compliance examinations by the federal banking agencies. To protect consumers, all participants in digital asset ecosystem should be subject to the same requirements and oversight for their privacy and security practices.[23]

Additionally, policymakers should ensure that data protection and cybersecurity requirements and expectations are consistently applied to all entities engaging in digital assets-related activities. BPI has long warned of the dangers of the uneven expectations and requirements regarding consumer data protections and cybersecurity controls for banks versus nonbank fintechs.[24] Banks have developed

---

[21] *See* Acting Comptroller Michael J. Hsu, Remarks before the American Fintech Council Fintech Policy Summit 2021, "Leveling Up Banking and Finance" (November 3, 2021) at 7, *available at*: Acting Comptroller Michael J. Hsu Remarks before the American Fintech Council Fintech Policy Summit 2021 Leveling Up Banking and Finance (occ.gov).

[22] *Id*.

[23] *See* comment letter re: National Institute of Standards and Technology – Draft Report 8389 Cybersecurity Considerations for Open Banking Technology and Emerging Standards, Bank Policy Institute, SIFMA and American Bankers Association, March 3, 2022, available at https://bpi.com/wp-content/uploads/2022/03/BPI-Comment-Letter-NIST-Open-Banking-Report.pdf. *See also* comment letter re: Notice and Request for Comment Regarding the CFPB's Inquiry Into Big Tech Payment Platforms, Consumer Financial Protection Bureau, BPI, Nov. 10, 2021, available at BPI-CommentCFPBBigTechInquiry-12-10-21final.forsubmission-CFPB-2021–0017.pdf. *See also* letter re: Updated Proposed Guidelines for Evaluating Account and Services Requests, Board of Governors of the Federal Reserve System, BPI, ABA, CBA, TCH, ICBA, and MBCA, April 22, 2022, available at https://bpi.com/wp-content/uploads/2022/04/BPI-Joint-Trades-Comment-Letter-to-Federal-Reserve-re-Fed-Accounts-Supplemental-Proposal-2022.04.21.pdf. *See also* comment letter re: Request for Information and Comment on Digital Assets (RIN 3064–ZA25), Bank Policy Institute and Consumer Bankers Association, July 16, 2021, available at: Microsoft Word - BPI Comment Letter - FDIC RFI on Digital Assets (FINAL - signed).

[24] *See* comment letter re: National Institute of Standards and Technology – Draft Report 8389 Cybersecurity Considerations for Open Banking Technology and Emerging Standards, Bank Policy Institute, SIFMA and American Bankers Association, March 3, 2022, available at https://bpi.com/wp-content/uploads/2022/03/BPI-Comment-Letter-NIST-Open-Banking-Report.pdf. *See also* BPI Statement Before House Task Force on Financial Technology on Consumer Consumers Access to Personal Financial Data, Sept. 21, 2021, available at https://bpi.com/bpi-

sophisticated systems to protect consumer data and to detect, prevent, and respond to cyber threats. These activities are subject to extensive regulatory oversight to ensure such protections are in place and can include financial penalties or restrictions on activities for failure to comply. In particular, banks are subject to the Gramm-Leach-Bliley Act and its implementing regulations that require maintaining consumer data privacy, extensive guidelines from the Federal Financial Institutions Examination Council Information Technology handbooks,[25] and the federal banking agencies' third-party risk management guidelines.[26] As noted, banks, contrasted with nonbanks, are subject to regular examination for compliance with these requirements.

Further, as noted, banks are required to implement robust anti-money laundering and countering the financing of terrorism programs as well as comprehensive sanctions compliance programs. While federal AML law requires all money services businesses to register with the U.S. Secretary of the Treasury, bringing them within the purview of the Financial Crimes Enforcement Network, to the extent that nonbank fintechs engage in the same activity with the same illicit finance risk characteristics as banks, the relevant regulators should work together to ensure that these tech companies are subject to the same expectations as banks are to combat financial crime.[27]

---

statement-before-house-task-force-on-financial-technology-on-consumer-consumers-access-to-personal-financial-data/. *See also* comment letter re: Re: Advance Notice of Proposed Rulemaking on Consumer Access to Financial Records (Docket No. CFPB-2020-0034), Bank Policy Institute, Feb. 4, 2021, available at https://bpi.com/wp-content/uploads/2021/02/BPI-Comment-Letter-Responding-to-CFPB-1033-ANPR-2021.02.04.pdf. *See also* comment letter re: Notice and Request for Comment Regarding the CFPB's Inquiry Into Big Tech Payment Platforms, Consumer Financial Protection Bureau, BPI, Nov. 10, 2021, available at BPI-CommentCFPBBigTechInquiry-12-10-21final.forsubmission-CFPB-2021–0017.pdf; *See also* Comment Letter Re: Request for Information and Comment on Digital Assets (RIN 3064–ZA25), Bank Policy Institute and Consumer Bankers Association, July 16, 2021, available at: Microsoft Word - BPI Comment Letter - FDIC RFI on Digital Assets (FINAL - signed.

[25] FFIEC IT handbooks are used in the supervision of financial institutions and cover topics such as information security, management, technology architecture and operations, and retail payment systems.

[26] The federal banking agencies also have issued "Third Party Risk Management Guidelines" that outline the expectations for banks to manage the risks of counterparties with whom they have business relationships. The agencies recently proposed amendments to this guidance and requested comment on the extent to which banking organization may have "business arrangements" and third-party relationships with data aggregators, and therefore should manage these relationships consistent with the third-party risk management guidance." BPI submitted a comment on the proposed amendments to the TPRM Guidance and stated that data aggregators — including both those that engage in unilateral "screen-scraping" and those with which a banking organization may have a contract or other data sharing relationship — can pose meaningful risks to banking organizations and their customers but that the TPRM practices and expectations described in the Proposed Guidance would not be appropriate for either type of activity for several reasons. However, the ultimate expectations of the regulators in this regard remain unclear at this point. *See* BPI's comment letter in response to the "Proposed Interagency Guidance on Third-Party Relationships," available at: Microsoft Word - BPI Comment Letter - Interagency Guidance on Third Party Relationships (Docket ID(7661407.20).docx.

[27] *See* Letter to Financial Crimes Enforcement Network, from Bank Policy Institute re: Request for Information and Comment Regarding Review of Bank Secrecy Act Regulations and Guidance (Feb. 14, 2022) (pgs. 30-32), *available at* https://bpi.com/wp-content/uploads/2022/02/BPI-Comments-on-FinCEN-Review-of-Bank-Secrecy-Act-Regulations-and-Guidance.pdf.

Finally, some entities engaged in digital assets activities that do not have deposit insurance and that are not regulated by a federal bank regulator at all levels of the organization have sought access to Federal Reserve master accounts. There are many benefits that a master account provides: the ability to place deposits directly with the Fed that act as a mechanism through which the Fed conducts monetary policy; being able to clear and settle private transactions without concern about liquidity and credit risk; access to the Fed's discount window for emergency borrowing; access to the nation's payments rails; and a suite of other services. These features are core elements of the nation's financial and monetary system, and therefore demand the highest protection against risk. Insured banks provide that protection, but the nonbank entities engaged in digital assets activities described above do not. Account access should be limited to institutions subject to a comprehensive federal regulatory and supervisory regime that matches the existing regimes for insured banks and their bank holding company parents and affiliates. Not limiting account access would pose significant risk to the country's payments and financial systems.

Moreover, there would be particular risks associated with granting certain nonbank stablecoin issuers unfettered access to Federal Reserve master accounts. For example, a nonbank-issued stablecoin backed fully by deposits at the Federal Reserve 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, causing them to cut credit lines and pull back from lending precisely at the time when those functions are needed most by the real economy. Thus, master account access should be limited to institutions subject to a comprehensive federal regulatory and supervisory regime akin to that which banks and their holding companies and affiliates are subject.

We provide specific responses to certain questions below.

(A) Adoption to Date and Mass Adoption

(1) What explains the level of current adoption of digital assets? Please identify key trends and reasons why digital assets have gained popularity and increased adoption in recent years. In your responses, please address the following:

b. What businesses are adopting digital assets and for what purposes?

BPI has explained previously how banks are evaluating where and how digital assets and other innovations can be applied in their own businesses to best serve the needs of customers (or potential customers) and why the public and the financial system would benefit from banks' involvement in digital assets.[28] However, as we have noted in the past and discussed above, the federal banking agencies must further clarify the ability of banks to engage in digital assets-related activities and the risk

[28] *See* letter to the FDIC re: Request for Information and Comment on Digital Assets (RIN 3064–ZA25), Bank Policy Institute and Consumer Bankers Association (July 16, 2021), available at: Microsoft Word - BPI Comment Letter - FDIC RFI on Digital Assets (FINAL - signed); Letter re: SAB 121 to the Office of the Chief Accountant of the Securities and Exchange Commission, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Federal Reserve Board, and the Department of the Treasury (June 23, 2022) ABA, BPI, and SIFMA, available at: https://bpi.com/bpi-aba-and-sifma-comment-on-staff-accounting-bulletin-no-121/; Letter to the Department of Commerce re: Request for Comment on Developing a Framework on Competitiveness of Digital Asset Technologies (July 5, 2022), BPI, available at: DepartmentofCommerce-DigitalAssets-RFI-BPIResponse-2022.07.05.pdf.

management expectations related to those activities to foster responsible innovation.[29] Furthermore, a coordinated, whole of government approach to the regulation of digital assets and related activities is critical. The risks of an uncoordinated approach are real, as illustrated with respect to the activity of safeguarding cryptoassets, as discussed above.[30]

(B) Opportunities for Consumers, Investors, and Businesses
(3) What are the main opportunities for consumers, investors, and businesses from digital assets? For all opportunities described, please provide data and specific use cases to date (if any). In your responses, please consider:

c. Potential for improved access to and greater ease of use of financial products

BPI has written extensively about the possible risks and benefits that certain types of digital assets may present. In particular, BPI believes that a United States retail CBDC is unlikely to provide the benefits its proponents cite. Furthermore, it would undermine the commercial banking system in the United States by severely constricting the availability of credit to the economy in a highly procyclical way, thereby ultimately harming not just banks, particularly the smallest banks, but consumers and financial stability.[31] In addition, most, if not all, of the potential benefits of a CBDC can likely be achieved through alternative, less harmful means.

For example, proponents often assert that a CBDC could improve financial inclusion. However, we are unaware of any substantiated use case for CBDC that would benefit low- and moderate-income people. For example, the FDIC survey of the unbanked highlights the main reasons why unbanked individuals remain unbanked.[32] Most simply have no money to deposit. Many have concerns about

[29] The OCC, through Interpretive Letter 1179, requires a banking organization to receive supervisory nonobjection regarding risk management systems and controls before conducting crypto-asset custody activities. 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); *see also* OCC Interpretive Letter No. 1170, Re: Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers (July 22, 2020). The FDIC imposes similar requirements. *See* FDIC, FIL-16-2022, Notification of Engaging in Crypto-Related Activities (April 7, 2022). The federal banking agencies jointly advised in November 2021 that throughout 2022 they would "provide greater clarity on whether certain activities related to crypto-assets conducted by banking organizations are legally permissible, and expectations for safety and soundness, consumer protection, and compliance with existing laws and regulations related to: crypto-asset safekeeping and traditional custody services; ancillary custody services; facilitation of customer purchases and sales of crypto-assets; loans collateralized by crypto-assets; Issuance and distribution of stablecoins; and activities involving the holding of crypto-assets on balance sheet." Joint Statement on Crypto-Asset Policy Sprint Initiative and Next Steps (November 23, 2021), available at: Joint Statement on Crypto-Asset Policy Sprint Initiative and Next Steps (federalreserve.gov). The agencies have not yet provided additional clarity on these topics.

[30] *See* comment letter re: SAB 121 to the Office of the Chief Accountant of the Securities and Exchange Commission, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Federal Reserve Board, and the Department of the Treasury, June 23, 2022, ABA, BPI, and SIFMA, available at: https://bpi.com/bpi-aba-and-sifma-comment-on-staff-accounting-bulletin-no-121/.

[31] *See* the Bank Policy Institute's work on central bank digital currency, available at https://bpi.com/category/digital-assets/central-bank-digital-currency/.

[32] How America Banks: Household Use of Banking and Financial Services 2019 FDIC Survey; available at: https://www.fdic.gov/analysis/household-survey/index.html.

minimum balance requirements or fees; others are concerned about privacy. None of these concerns would be addressed by a CBDC.[33] Moreover, private-sector developments are helping to bring previously unbanked or underbanked individuals into the financial system—for example, through the introduction of no or very low-cost bank accounts, such as "Bank On" transaction accounts.[34] Our research has shown that the take-up rate for Bank On accounts is greatest in areas with high concentrations of lower-income and minority households, demonstrating that these bank accounts are successfully addressing customer demand for these types of accounts and making banking more inclusive and accessible.[35]

f. Potential for improved cross-border payments and trade finance

CBDC

Similarly, although proponents of a CBDC often assert that a CBDC could increase the speed and lower the cost of payments, including cross-border payments, whether this could be achieved in practice is a complex question that many central banks and international bodies are just beginning to study.[36] Furthermore, there are other methods underway of improving payments – both domestically and

---

[33] *See* Gregory Baer, BPI Staff Working Paper, "Central Bank Digital Currencies: Costs, Benefits and Major Implications for the U.S. Economic System" (April 7, 2021), 16-17, available at: Central-Bank-Digital-Currencies-Costs-Benefits-and-Major-Implications-for-the-U.S.-Economic-System.pdf (bpi.com); *See* letter to the Board of Governors of the Federal Reserve System re: "Money and Payments: The U.S. Dollar in the Age of Digital Transformation" (May 20, 2022), available at: BPI-Files-Comments-in-Response-to-Federal-Reserve-CBDC-Discussion-Paper.pdf; *see* letter to the Department of Commerce re: Request for Comment on Developing a Framework on Competitiveness of Digital Asset Technologies (July 5, 2022), BPI, available at: DepartmentofCommerce-DigitalAssets-RFI-BPIResponse-2022.07.05.pdf.

[34] For more information about Bank On, see https://joinbankon.org/. Bank On accounts are certified by the Cities for Financial Empowerment Fund, a non-profit organization, and this type of account comes with a minimum balance requirement of only $25 and monthly fees of $5 or less; account opening is free, as is in-market ATM usage, and there are no overdraft charges. *See* Bank On National Account Standards 2021-2022, available at: https://2wvkof1mfraz2etgea1p8kiy-wpengine.netdna-ssl.com/wp-content/uploads/2020/10/Bank-On-National-Account-Standards-2021-2022.pdf. Bank On certified accounts are now offered by over 110 banks and credit unions at more than 39,000 branches nationwide, and over 3.8 million accounts were open and active in 2020 at just 17 institutions that reported data, and growth increased in 2021. *See* Written Testimony Submitted to the U.S. House Committee on Financial Services, House Subcommittee on Consumer Protection and Financial Institutions. Hearing on "Banking the Unbanked: Exploring Private and Public Efforts to Expand Access to the Financial System," (July 21, 2021), Submitted by David Rothstein, Senior Principal, Cities for Financial Empowerment Fund, available at: hhrg-117-ba15-wstate-rothsteind-20210721.pdf (house.gov); Accounts – BankOn (joinbankon.org); *See also* The Bank On National Data Hub: Findings from 2020, available at: bankonreport_2020findings.pdf (stlouisfed.org).

[35] *See* Calem, Paul, *"Bank On" Transaction Accounts: Making Traditional Banking More Inclusive* (April 13, 2021), available at: https://bpi.com/wp-content/uploads/2021/04/Bank-On-Transactions-Accounts-Making-Traditional-Banking-More-Inclusive.pdf.

[36] *See* Gregory Baer, BPI Staff Working Paper, "Central Bank Digital Currencies: Costs, Benefits and Major Implications for the U.S. Economic System" (April 7, 2021), 16-17, available at: Central-Bank-Digital-Currencies-Costs-Benefits-and-Major-Implications-for-the-U.S.-Economic-System.pdf (bpi.com); *See* letter to the Board of Governors of the Federal Reserve System re: "Money and Payments: The U.S. Dollar in the Age of Digital Transformation" (May 20, 2022), available at: BPI-Files-Comments-in-Response-to-Federal-Reserve-CBDC-Discussion-Paper.pdf; *see* letter to the Department of Commerce re: Request for Comment on Developing a Framework on Competitiveness of Digital Asset Technologies (July 5, 2022), BPI, available at: DepartmentofCommerce-DigitalAssets-RFI-BPIResponse-2022.07.05.pdf.

internationally – that could achieve that goal without a CBDC.[37] We discuss further below the uncertainty regarding the potential for a CBDC or a payment stablecoin to increase the speed or lower the costs of payments. At a minimum, further research is required before drawing any conclusions about the potential benefits of a CBDC in enhancing payments' efficiency or lowering costs.

Stablecoins

As with CBDC, some proponents of stablecoins have asserted that they could improve the speed and reduce the cost of cross border payments, including cross-border payments**.** There are three general types of stablecoins currently. The first type – the so-called "unstable stablecoin" – is backed by assets like corporate debt and asset-backed securities and is thus similar to a prime money market fund.[38] These stablecoins pose systemic risk, as they are susceptible to runs, and their interlinkage with crypto markets heightens that risk. The second type are "algorithmic" stablecoins, which pose similar run risk.[39] These risks must be addressed through better regulation and disclosure, as well as

---

[37] In the United States, there are other innovations underway that are improving and will continue to improve the domestic payments system. For example, The Clearing House runs its real-time payments system, the RTP network, which enables instantaneous settlement and availability. The Clearing House, "First New Core Payments System in the U.S. in More than 40 Years Initiates First Live Payments" (Nov. 14, 2017) (available at: https://www.theclearinghouse.org/payment-systems/articles/2017/11/20171114-rtp-first-new-core-payments-system). In addition, the Federal Reserve itself is developing a real-time payments system, FedNow, that is scheduled to begin operating in 2023. *See* The Federal Reserve FRBServices.org, "About the FedNow[SM] Service" (2022) (available at: https://www.frbservices.org/financial-services/fednow/about.html). In addition, the FSB has highlighted as a key priority the improvement of cross-border payments and established a roadmap achieve this goal. The G20 countries agreed in 2020 to a multiyear roadmap to identify and deploy improvements to cross-border payments. *See* Financial Stability Board, Enhancing Cross-border Payments: Stage 3 Roadmap (October 13, 2020), available at: Enhancing Cross-border Payments: Stage 3 roadmap (fsb.org). Furthermore, EBA CLEARING, SWIFT and The Clearing House have announced that they plan to launch a pilot service for immediate cross-border (IXB) payments by the end of this year. *See* John Adams, "Banks gearing up to test real-time payments across borders," *American Banker*, (May 2, 2022), available at: https://www.americanbanker.com/payments/news/banks-gearing-up-to-test-real-time-payments-across-borders; *See also* "EBA Clearing, SWIFT, and The Clearing House to deliver pilot service for immediate cross-border payments" (April 28, 2022), available at: EBA CLEARING, SWIFT and The Clearing House to deliver pilot service for immediate cross-border payments (prnewswire.com). In addition, Citi has posited that one possible way to realize the potential benefits of tokenization within the existing financial system would be to tokenize commercial bank, central bank, and electronic money on the same chain. *See* Citi, "The Regulated Internet of Value," available at: 2031240-Regulated-Internet-Value.pdf (citibank.com); *see also* Citi, "The Regulated Internet of Value, Executive Summary," available at: 2031240-Regulated-Internet-Value.pdf (citibank.com). In 2019, J.P. Morgan announced plans to launch JPM Coin, "a permissioned system that serves as a payment rail and deposit account ledger, that allows participating J.P. Morgan clients to transfer US Dollars held on deposit with J.P. Morgan within the system, facilitating the movement of liquidity funding and payments in right time," available at: Coin Systems | Onyx by J.P.Morgan (jpmorgan.com).

[38] Baer, Greg, "Making Stablecoins Stable: Is the Cure Worse than the Disease?", Bank Policy Institute (Sept. 27, 2021), available at: https://bpi.com/making-stablecoins-stable-is-the-cure-worse-than-the-disease/.

[39] These stablecoins generally "use an algorithm or smart contract to manage the supply of tokens and guide their value to some reference asset." Congressional Research Service, Insight, "Algorithmic Stablecoins and the TerraUSD Crash," (May 16, 2022), available at: IN11928 (congress.gov). These stablecoins also present run risk, and indeed, earlier this month, an algorithmic stablecoin lost its dollar peg, triggering a run on crypto, erasing over $400 billion in crypto market capitalization. Chow, Andrew R. "The Real Reasons Behind the Crypto Crash, and

enforcement of existing laws.[40] The calls by some policymakers for stablecoin regulation have escalated further in the wake of the recent run triggered by the failure of TerraUSD, an algorithmic stablecoin, to maintain its dollar peg.[41]

The third type, the so-called "stable stablecoin," would be backed solely by cash, government securities, or repos backed by government securities, which would make it safer than the other two types. Some have proposed that these more "stable" stablecoins could serve as a payments mechanism.[42] If a "stable" stablecoin – one backed by government securities and short-term Treasuries – were to grow at sufficient scale, it could pose similar concerns as a retail CBDC: namely that investors would run *to*, not *from*, it, particularly in times of financial instability.

As BPI has previously suggested, a stablecoin that was designed to, and would in actuality, exist in a state of equilibrium with bank deposits (which would be impossible for a CBDC) could avoid undermining the banking system while still offering convenience to customers.[43] Banks could issue stablecoins *pari passu* with bank deposits. Indeed, a recent Federal Reserve research paper concluded that under a framework in which stablecoins were backed by commercial bank deposits that were used for fractional reserve banking, bank intermediation would not be disrupted, so long as "the treatment of stablecoin deposits [were] the same as non-stablecoin deposits in terms of the required reserve ratio,

---

What We Can Learn from Terra's Fall," Time, (May 17, 2022), available at: What Terra's Crash Means For Crypto and Beyond | Time.

[40] *See, e.g.*, The President's Working Group on Financial Markets (PWG), the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, "Report on Stablecoins," (Nov. 1, 2021), available at: Report on Stablecoins (treasury.gov); White House, "Executive Order on Ensuring Responsible Development of Digital Assets" (March 9, 2022)j; and Remarks from Secretary of the Treasury Janet L. Yellen on Digital Assets, U.S. Department of the Treasury (April 7, 2022), available at: Remarks from Secretary of the Treasury Janet L. Yellen on Digital Assets | U.S. Department of the Treasury.

[41] Chris Matthews, "Terra crash sharpens Washington's attention on crypto regulations," MarketWatch, (Updated May 18, 2022), available at: Terra crash sharpens Washington's attention on crypto regulations - MarketWatch.

[42] It was concern over possible widespread use of these types of private sector digital currencies – particularly Facebook's Libra stablecoin proposal – that served as a catalyst for increased research around a possible CBDC.*See* Speech by Governor Lael Brainard, "Private Money and Central Bank Money as Payments Go Digital: an Update on CBDCs" to the Consensus by CoinDesk 2021 Conference (May 24, 2021) (available at: https://www.federalreserve.gov/newsevents/speech/brainard20210524a.htm) (noting that the growing role of digital private money is one reason that the Federal Reserve is "sharpening" its focus on CBDC and that a CBDC may increase payment system resilience "relative to a payments system where private money is prominent."). Policymakers were concerned about the potential for Facebook to use its Libra stablecoin to move finance outside of the banking system, disintermediating the dollar. However, Facebook has abandoned its stablecoin project and sold its stablecoin subsidiary, now named Diem. Sam Sutton and Victoria Guida, "Facebook's crypto project sold after political backlash," Politico, (Jan. 31, 2022), available at: Facebook's crypto project sold after political backlash - POLITICO.

[43] *See* Baer (2022). ("There does seem to be one way for stablecoins to avoid undermining the fractional reserve system while still offering convenience to customers, and that is for them to reach a state of equilibrium with bank deposits. (With a CBDC, equilibrium is impossible).").

liquidity coverage and other regulatory and self-imposed risk limits."[44] In order for there to be true equivalency, the stablecoin deposits would need to be insured and subject to similar treatment as other deposits in terms of insurance premiums.[45]

A stablecoin that was issued by banks *pari passu* with bank deposits would exist in a state of equilibrium with bank deposits. This type of stablecoin would avoid undermining the banking system while still offering convenience to customers because under economic stress, there would be no incentive for customers to run from stablecoins to bank deposits, or vice versa, because they would be backed by the same assets.

Furthermore, this design would seem to align with the public sector's expectations for appropriate regulation of stablecoins. The President's Working Group on Financial Markets recommended that only insured depository institutions be permitted to issue stablecoins.[46]

However, under the banner of competitive equity, some crypto firms have not only sought a special nonbank charter to issue stablecoins backed by Treasuries and Treasury repos, but also sought a requirement that any bank issuing a stablecoin do so through a separate subsidiary that holds only those same assets. This would not result in parity because a bank would have to hold capital against those assets (and be subject to the entire regulatory regime applicable to all of its assets), which means banks would be economically disadvantaged in issuing stablecoins as compared to nonbanks, which could foreclose banks from issuing stablecoins altogether. And, any stablecoin issued by a bank with these reserving requirements would then no longer fund lending and economic growth but rather would result in that bank buying Treasury securities. The current ability of insured banks to issue stablecoins should not be revoked or undermined.

As with a CBDC, whether a stablecoin could improve the speed and lower the cost of payments is unclear, and there are other methods underway of improving payments – both domestically and internationally – that could achieve that goal without a CBDC or payment stablecoin.

In the United States, there are innovations underway that are improving and will continue to improve the domestic payments system. For example, The Clearing House runs its real-time payments system, the RTP network, which enables instantaneous settlement and availability.[47] The value limit for

---

[44] Liao, Gordon Y. and John Caramichael (2022). "Stablecoins: Growth Potential and Impact on Banking," International Finance Discussion Papers 1334, 13-14, Washington: Board of Governors of the Federal Reserve System, available at: https://doi.org/10.17016/IFDP.2022.1334.

[45] *Id*. at note 30. The authors noted that "It is conceivable that deposits associated with stablecoin issuance are categorized as either transactional or brokered deposits. The former type has a lower assumed "run rate" in assessments of liquidity coverage. To achieve full equivalence to retail deposits, stablecoins would also require FDIC insurance."

[46] *See* The President's Working Group on Financial Markets (PWG), the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, "Report on Stablecoins," (Nov. 1, 2021), available at: Report on Stablecoins (treasury.gov).

[47] The Clearing House, "First New Core Payments System in the U.S. in more than 40 Years Initiates First Live Payments" (Nov. 14, 2017) (available at: https://www.theclearinghouse.org/payment-systems/articles/2017/11/20171114-rtp-first-new-core-payments-system).

transactions on the RTP network will soon be increasing to $1 million.[48] Other private sector innovation has exploded in the payments space, including the bank-led development of Early Warning Services' Zelle service for domestic P2P payments and other P2P services offered by fintechs, such as Venmo.[49] The automated clearing house system also has made same-day payments available and recently increased the value limit for same-day payments to $1 million.[50] In addition, the Federal Reserve itself is developing a real-time payments system, FedNow, that is scheduled to begin operating in 2023.[51]

There are several reasons why a CBDC and a payment stablecoin may be unlikely to increase the speed or lower the costs of cross-border transactions, including remittances. First, the AML/CFT compliance issues that contribute to current friction in the cross-border payment system would have to be addressed, but those issues are not related to the underlying technology and could be addressed now under the current system. Neither a CBDC nor a stablecoin (or the technology underpinning a stablecoin) in and of itself would address the frictions caused by AML/CFT compliance obligations. Central banks could agree to exempt transfers of CBDCs or stablecoins from all the regulatory and compliance requirements that currently complicate them – like going through the same AML/CFT and sanctions processes that banks do currently, including a full Know Your Customer process – but they could take the same action under the current payments regime and for important reasons have decided not to do so. Thus, participating institutions will need to conduct the appropriate AML and sanctions due diligence to facilitate transactions, adding additional friction to this multi-leg process. This includes compliance with the "Travel Rule," which requires financial institutions, including nonbank financial institutions, engaged in transmittal of funds (whether in fiat or crypto) to transmit transactions and customer details to the next financial institution in the chain of payment in order to aid law enforcement agencies by maintaining an information trail of transaction originators and beneficiaries – something that a handful of crypto firms have only recently unveiled a compliance solution for.[52]

In addition, to use CBDCs or stablecoins on a cross-border basis, the sender likely would need to convert local fiat currency into a CBDC or stablecoin, which likely would have a fee associated with that conversion. Assuming the recipient desires their own fiat currency, the recipient would then need to exchange the CBDC or stablecoin for the sender's currency and then convert that currency to the recipient's local currency. These transactions similarly would incur fees and likely involve F/X spreads. It is possible the recipient could exchange the sender's home country CBDC or stablecoin for the recipient's home country CBDC (or a stablecoin pegged to the home country's currency), although any possibility of that capability appears to be years away. Furthermore, that transaction likely would incur

---

[48] The Clearing House, "TCH to Raise RTP® Network Transaction Limit to $1 Million" (Apr. 6, 2022) (available at: https://www.theclearinghouse.org/payment-systems/articles/2022/04/tch_raise_rtp_network_transaction_limit_1million_04-06-2022).

[49] Fraud on P2P Payment Apps Like Zelle and Venmo: A Primer - Bank Policy Institute (bpi.com).

[50] *See* Nacha, "Same Day ACH $1 million increase" (2022) (available at: https://www.nacha.org/resource-landing/same-day-ach-resource-center) (noting the history of same-day-funds-availability initiatives using ACH).

[51] *See* The Federal Reserve FRBServices.org, "About the FedNow[SM] Service" (2022) (available at: https://www.frbservices.org/financial-services/fednow/about.html).

[52] *See* Keely, Aislinn, "Coalition of U.S. crypto firms unveils travel rule compliance platform, TRUST," February 16, 2022, available at https://www.theblockcrypto.com/post/134408/coalition-of-us-crypto-firms-unveils-travel-rule-compliance-platform-trust.

costs that would have to be borne by at least some parties in the chain, including, at a minimum, costs related to F/X spreads.[53]

Banks have not begun to issue retail payment stablecoins at a large scale because, as we understand from BPI members' payments experts, there has not been significant customer demand for a retail payment stablecoin. Banks' customers appear satisfied using RTP/real-time payment or ACH transfers,[54] and consumers continue to use Zelle, Venmo, debit cards, and credit cards.[55]

(C) General Risks in Digital Assets Financial Markets
(4) Please identify and describe any risks arising from current market conditions in digital assets and any potential mitigating factors. Identify any such responses that directly relate to:

c. Technological risks, including attacks, bugs, and network congestion

As recognized by the IMF, cyber risk is a major category of risk associated with DeFi platforms.[56] The IMF noted that cyberattacks "increased substantially in mid-2021 and remain elevated. The attacks are associated mostly with compromised wallet keys, vulnerabilities in computer code, and scams by developers."[57] For example, in August 2021, the stablecoin issuer Coinbase experienced a surge in consumer complaints related to insufficient account security that led to hacks and other related

[53] For a discussion about the on-and-off ramp costs with respect to stablecoins (which present similar costs as CBDCs), *see* "Should Western Union Worry About Stablecoins?" JP Koning, CoinDesk Insights, Jan 3, 2022, available at [Should Western Union Worry About Stablecoins? (coindesk.com)](). *See* generally, "Central bank digital currencies for cross-border payments," BIS Report to the G20 (July 2021), available at https://www.bis.org/publ/othp38.pdf. The BIS Report concluded that significant work remains to be done to determine whether CBDCs could reduce the current frictions in cross-border retail (or wholesale) payments, noting that "enhancements in other areas of the cross-border payments programme, such as aligning regulatory, supervisory and oversight frameworks for cross-border payments, Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) consistency, Payment versus Payment (PvP) adoption and payment system access will be critical for cross-border CBDC use." BIS Report at 1.

[54] The modern ACH Network experienced significant growth in 2021, with 29.1 billion payments valued at $72.6 trillion, and same day ACH payment volume grew nearly 74%. *See* NACHA, "ACH Network Sees 29.1 Billion Payments in 2021, Led by Major Gains in B2B and Same Day ACH.", February 3, 2022, available at: https://www.nacha.org/news/ach-network-sees-291-billion-payments-2021-led-major-gains-b2b-and-same-day-ach.

[55] The Clearing House's RTP network use has seen a seven-fold increase in volume since the first quarter of 2020 and in the fourth quarter of 2021 processed 37.8 million transactions. *See* TCH, "Real-Time Payments for All Financial Institutions.", available at: https://www.theclearinghouse.org/payment-systems/rtp. Mastercard reported a gross dollar volume increase of 25% year-over-year on branded cards and Visa reported a 17% increase in processed transactions year-over-year in 2020. *See* Mastercard Inc. (2021) Form 10-K, available at: https://s25.q4cdn.com/479285134/files/doc_financials/2021/q4/MA.12.31.2021-10-K-as-filed-Exhibits.pdf & Visa Inc. (2021) Form 10-K, available at: https://d18rn0p25nwr6d.cloudfront.net/CIK-0001403161/c2498d48-acd0-4f4d-8a36-9a10034f3060.pdf.

[56] IMF, Global Financial Stability Report, Chapter 3, "The Rapid Growth of Fintech: Vulnerabilities and Challenges for Financial Stability" (April 2022), at 79, available at: Global Financial Stability Report | April 2022 (imf.org).

[57] *Id*.

customer service complaints.[58] More recently, hackers stole more than $650 million in ether and stablecoins from Axie Infinity and more than $180 million in stablecoins from Beanstalk Farms.[59]

In addition, a recent report commissioned by the Defense Advanced Research Projects Agency highlighted certain vulnerabilities in blockchain technologies.[60] For example, the report found that certain people and companies have concentrated power over blockchain networks, contrary to the generally held view that blockchain networks are decentralized in nature. The report also cited as a vulnerability the fact that 60 percent of all bitcoin traffic runs over three internet service providers, which could make blockchain networks vulnerable to degradation or disruption. The report also highlighted weaknesses in the bitcoin network, finding that 21 percent of nodes are running an out-of-date version of the core bitcoin client, which has known vulnerabilities.

e. Settlement and custody

See our discussion above regarding SEC Staff Accounting Bulletin No. 121 and the need for the banking agencies and the SEC to jointly evaluate the comprehensive legal, regulatory and supervisory frameworks applicable to banking organizations that address the risks identified by the SEC and determine that banks should be excluded from the accounting treatment in the SAB, thereby enabling banks to provide custody services for cryptoassets.

(D) Risks to Consumers, Investors, and Businesses

(5) Please identify and describe potential risks to consumers, investors, and businesses that may arise through engagement with digital assets. Identify any such responses that directly relate to:

a. Frauds and scams

In many cases, cryptocurrency offers the potential advantage of anonymity while also making it easy for criminals to verify — using publicly available blockchain data — that a payment has been completed. Ransomware is only one type of illicit finance risk associated, in whole or in large part, with the increased use of cryptocurrencies and other emerging payment methods. While U.S.-based cryptocurrency firms are subject to AML requirements, many operators are located outside U.S. jurisdiction and solicit payments through foreign firms whose host country does not enforce the same rigorous AML expectations. We recommend that FinCEN take the following additional actions to clarify the regulatory requirements and expectations that apply to transactions involving these payment methods. If implemented, these recommendations would provide significant clarity regarding the application of the BSA to cryptocurrencies.

---

[58] Scott Zamost, Eamon Javers, Jennifer Schlesinger, Stephen Council, and Angélica Serrano-Román, "Coinbase slammed for what users say is terrible customer service after hackers drain their accounts," CNBC (Aug. 24, 2021), available at: Coinbase slammed for terrible customer service after hackers drain user accounts (cnbc.com).

[59] Benjamin Pimentel and the Fintech Team, "Crypto has weak spots. Hackers are pouncing," Protocol, (April 19, 2022), available at: A MESSAGE FROM PwC - Protocol.

[60] Trail of Bits, "Are Blockchains Decentralized? Unintended Centralities in Distributed Ledgers" (June 2022), available at: https://assets-global.website-files.com/5fd11235b3950c2c1a3b6df4/62af6c641a672b3329b9a480_Unintended_Centralities_in_Distributed_Ledgers.pdf.

- **Scope of regulation.** FinCEN should consider whether existing BSA regulatory requirements are sufficiently broad in their application to participants in cryptocurrency markets and whether there are additional participants in these markets that should expressly be subject to AML requirements. This may include, for example, intermediaries that provide ransom-related services, but take the view that they are not required to register with FinCEN as a money services business under the "integral exemption" for persons that only "[a]ccept[] and transmit[] funds only integral to the sale of goods or the provision of services, other than money transmission services, by the person who is accepting and transmitting the funds."[61] Ultimately, FinCEN should ensure that AML program requirements are consistent for all cryptocurrency market participants that engage in the same activity with the same illicit finance risk characteristics, regardless of a particular participant's status as a bank, money services business, or other type of financial institution.
- **Oversight.** FinCEN should, in coordination with other relevant authorities, increase oversight of AML regulatory standards for all participants in cryptocurrency markets subject to those standards. Certain participants are subject to the BSA, but are not complying in whole or in part with their BSA obligations.
- **Rulemaking regarding cryptocurrency wallets**. FinCEN should proceed with the rulemaking initiated in December 2020 that would impose obligations on banks and money services businesses to conduct reporting, recordkeeping, and customer verification on certain cryptocurrency transactions involving an unhosted wallet or otherwise covered wallet (e.g., a wallet held at an institution not subject to BSA/AML regulation and/or located in certain foreign jurisdictions identified by FinCEN).[62]
- **Travel Rule compliance.** The "Travel Rule" generally requires financial institutions, including certain cryptocurrency market participants, engaged in transmittals of funds involving $3,000 or more to transmit certain transaction and customer details to the next institution in the chain of payment. We appreciate FinCEN and the Federal Reserve's 2020 Notice of Proposed Rulemaking that would address, among other things, the application of recordkeeping requirements and the Travel Rule to cryptocurrencies, and we recommend that FinCEN engage with cryptocurrency market participants regarding, and encourage solutions that facilitate, Travel Rule compliance. A complete information trail regarding transaction originators and beneficiaries may be available only if those participants, and not solely banks, comply.

d. Losses from the failure/insolvency of wallets, custodians, or other intermediaries.

As discussed previously, the legal, regulatory, and technological risks presented to investors and consumers by entities safeguarding their cryptoassets are comprehensively addressed by the legal, regulatory and supervisory frameworks applicable to banking organizations.[63] These same protections are not present with respect to nonbank entities safeguarding cryptoassets.

---

[61] 31 C.F.R. § 1010.100(ff)(5)(ii)(F).

[62] Financial Crimes Enforcement Network, Requirements for Certain Transactions involving Convertible Virtual Currency or Digital Assets, Notice of Proposed Rulemaking, 85 Fed. Reg. 83840 (Dec. 23, 2020).

[63] *See* comment letter re: SAB 121 to the Office of the Chief Accountant of the Securities and Exchange Commission, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Federal Reserve Board, and the Department of the Treasury, June 23, 2022, ABA, BPI, and SIFMA, available at: https://bpi.com/bpi-aba-and-sifma-comment-on-staff-accounting-bulletin-no-121/.

g. Disclosures of other relevant terms

BPI has previously expressed concerns about the insufficient, and in some cases misleading, disclosures provided by certain nonbank entities providing digital assets related products and services, particularly, stablecoin issuers.[64] As noted above, so-called "unstable stablecoins" that are issued with backing from assets that include commercial paper—and in some cases receivables, including loans to crypto affiliates—present several risks to consumers and the financial system. First, some stablecoin issuers have failed, with consumers losing all their money because the underlying asset declined in value or, in some cases, because the money was simply stolen through hacking or defalcation.[65] Second, because stablecoins are often regulated only at the state level as money service businesses, there is generally no requirement that they disclose what is backing the stablecoins.[66] However, certain nonbank stablecoin issuers have marketed their stablecoins as being backed by "reserves," which, in banking parlance, connotes very safe and liquid assets.[67] However, in reality, these stablecoins are backed at least in part by commercial paper – essentially loans.[68] In other cases, as described further below, certain crypto-related products have been marketed by comparison to savings accounts. Thus, consumers have been deceived about the safety of these products.[69]

---

[64] *See* Bill Nelson, Paige Pidano Paridon, American Banker, BankThink: "Stablecoins are backed by 'reserves'? Give us a break" (Dec. 10, 2021), available at: Stablecoins are backed by 'reserves'? Give us a break. | American Banker.

[65] *See*, *e.g.*, Richi Jennings, "SafeDollar Stablecoin not Safe nor Stable: Hack Sends Value to ZERO," Security Boulevard (June 29, 2021), available at: SafeDollar Stablecoin not Safe nor Stable: Hack Sends Value to ZERO - Security Boulevard; Ryan Browne, "The world's biggest stablecoin has dropped below its $1 peg," CNBC (May 12, 2022), available at: Tether (USDT) stablecoin drops below $1 peg (cnbc.com); "The Biggest Threat to Trust in Cryptocurrency: Rug Pulls Put 2021 Cryptocurrency Scam Revenue Close to All-time Highs," (Dec. 16, 2021) (Chainanalysis report found that over $7.7 billion was stolen in cryptocurrency scams worldwide in 2021), available at: Crypto Scams: 2021 Rug Pulls Put Revenues Near All-Time High (chainalysis.com).

[66] *See* Awrey, Dan, Bad Money (February 5, 2020). 106:1 Cornell Law Review 1 (2020); Cornell Legal Studies Research Paper No. 20-38, Available at: SSRN: https://ssrn.com/abstract=3532681 or http://dx.doi.org/10.2139/ssrn.3532681.

[67] *See*, *e.g.,* Hubbard, R. Glenn, Money, the Financial System, and the Economy, Addison-Wesley Publishing Company, Inc. June 1994, p. 306 ("Reserves consist of vault cash and banks' deposits with the Federal Reserve System" and "Because of their liquidity, bank holdings of U.S. government securities are sometimes called secondary reserves."), Mishkin, Fredric S., The Economics of Money, Banking, and Financial Markets, Eleventh Edition, Pearson Education, 2016, p. 698 ("Reserves. Banks' holding of deposits in accounts with the Fed plus currency that is physically held by banks (vault cash)"), and European Central Bank, Minimum Reserves, available at: https://www.ecb.europa.eu/mopo/implement/mr/html/index.en.html ("The ECB requires credit institutions established in the euro area to hold deposits on accounts with their national central bank. These are called "minimum" or "required" reserves (MRR)."). In addition, reserves can include pass-through deposits at another institution that keeps the funds on deposit at the Federal Reserve.

[68] *See* Bill Nelson, Paige Pidano Paridon, American Banker, BankThink: "Stablecoins are backed by 'reserves'? Give us a break" (Dec. 10, 2021), available at: Stablecoins are backed by 'reserves'? Give us a break. | American Banker.

[69] *See* CFTC Orders Tether and Bitfinex to Pay Fines Totaling $42.5 Million | CFTC ("The Tether order finds that since its launch in 2014, Tether has represented that the tether token is a stablecoin . . . [but] that from at least June 1, 2016 to February 25, 2019, Tether misrepresented to customers and the market that Tether maintained sufficient U.S. dollar reserves to back every USDT in circulation with the "equivalent amount of corresponding fiat

Third, if the backing of these stablecoins were called into question, a run could be triggered whereby consumers seek to redeem their stablecoins all at once.[70] Financial stability risk could arise if the failure of a major stablecoin issuer prompted a run on other stablecoins, with those stablecoins forced to liquidate the assets backing those coins. As the President's Working Group, the President, the Secretary of the Treasury, and many other government officials have outlined, the risks of these instruments must be addressed by appropriate regulation, and we expect that regulation to address the significant run risk posed by these stablecoins will be forthcoming.[71] Indeed, algorithmic stablecoins also present run risk, which was illustrated earlier this year when an algorithmic stablecoin lost its dollar peg.[72] That event has prompted renewed calls for stablecoin regulation among policymakers.[73]

As noted above, nonbank entities providing digital asset related products and services may not adequately disclose risks to investors and consumers regarding those products and services. For example, so-called interest-bearing accounts for crypto asset holdings are marketed as being safe while promising returns significantly higher than high-yield bank savings accounts. Through these accounts, investors typically lend crypto assets to a cryptocurrency issuer in exchange for the company's promise to provide a variable monthly interest payment. Consumers, however, may not be aware that these accounts are not FDIC-insured and thus not as safe as bank deposits. Indeed, the SEC fined the crypto exchange BlockFi $100 million for its crypto lending product that offered variable monthly returns because the SEC found the product was a security that had not been properly registered as a security.[74] The SEC also found that BlockFi made a false and misleading statement for more than two years on its website concerning the level of risk in its loan portfolio and lending activity. In connection with the

---

currency" held by Tether and "safely deposited" in Tether's bank accounts. In fact Tether reserves were not "fully-backed" the majority of the time.").

[70] The President's Working Group on Financial Markets (PWG), the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, Report on Stablecoins (Nov. 1, 2021), available at: Report on Stablecoins (treasury.gov). The PWG report highlighted that "[t]he mere prospect of a stablecoin not performing as expected could result in a "run" on that stablecoin – i.e., a self-reinforcing cycle of redemptions and fire sales of reserve assets. Fire sales of reserve assets could disrupt critical funding markets, depending on the type and volume of reserve assets involved. Runs could spread contagiously from one stablecoin to another, or to other types of financial institutions that are believed to have a similar risk profile. Risks to the broader financial system could rapidly increase as well, especially in the absence of prudential standards."

[71] *See*, e.g., PWG Report on Stablecoins, Executive Order on Ensuring Responsible Development of Digital Assets (March 9, 2022), available at: Executive Order on Ensuring Responsible Development of Digital Assets | The White House, and Remarks from Secretary of the Treasury Janet L. Yellen on Digital Assets at American University's Kogod School of Business Center for Innovation (April 7, 2022), available at: Remarks from Secretary of the Treasury Janet L. Yellen on Digital Assets | U.S. Department of the Treasury.

[72] Alexander Osipovich and Caitlin Ostroff, "Crash of TerraUSD Shakes Crypto. 'There Was a Run on the Bank,'" (May 12, 2022), available at: Crash of TerraUSD Shakes Crypto. 'There Was a Run on the Bank.' - WSJ; Chow, Andrew R. "The Real Reasons Behind the Crypto Crash, and What We Can Learn from Terra's Fall," Time, (May 17, 2022), available at: What Terra's Crash Means For Crypto and Beyond | Time.

[73] Chris Matthews, "Terra crash sharpens Washington's attention on crypto regulations," MarketWatch, (Updated May 18, 2022), available at: Terra crash sharpens Washington's attention on crypto regulations - MarketWatch.

[74] SEC Press Release: "BlockFi Agrees to Pay $100 Million in Penalties and Pursue Registration of its Crypto Lending Product" (Feb. 14, 2022), available at: SEC.gov | BlockFi Agrees to Pay $100 Million in Penalties and Pursue Registration of its Crypto Lending Product.

announcement of this enforcement action, the SEC issued an Investor Bulletin on Crypto Asset Interest-bearing Accounts, warning investors that interest-bearing accounts for crypto asset holdings "may sound similar to interest-bearing accounts with a bank or credit union, but investors need to be aware that these crypto asset-related accounts are not as safe as bank or credit union deposits."[75]

More recently, Celsius, a crypto lender, and its affiliated companies filed for bankruptcy on July 13, 2022, one month after pausing all withdrawals, swaps, and transfers between accounts. Celsius had "held itself out as a safe alternative to traditional banks and promised users high interest rates. Customers could use their credit cards or bank accounts to buy crypto assets. To entice customers to stake their cryptocurrency with Celsius, the company promised returns of up to 20% on deposits, including 8.8% on stablecoins like Tether's USDT," and some Celsius customers have said that Celsius told customers repeatedly that Celsius was "safer than a bank . . .with better returns."[76] In addition, as noted above, Voyager, another crypto lending platform, suspended all trading, deposits, withdrawals, and rewards on July 1, 2022 and filed for bankruptcy on July 5, 2022. Voyager had misled its customers into thinking their money invested with Voyager was FDIC insured, and therefore much safer than it was. It remains to be seen how much of their investments and cash Voyager's and Celsius's customers will be able to recoup.

(E) Impact on the Most Vulnerable
(6) According to the FDIC's 2019 "How America Banks" survey, approximately 94.6 percent (124 million) of U.S. households had at least one bank or credit union account in 2019, while 5.4 percent (7.1 million) of households did not. And roughly 25 percent of U.S. households have a checking or savings account while also using alternative financial services.

Can digital assets play a role in increasing these and other underserved Americans' access to safe, affordable, and reliable financial services, and if so, how?

a. **In your responses, please describe specific ways in which digital assets can benefit the underserved and the most vulnerable vis-a`-vis traditional financial products and services. Address factors such as identify verification process, costs, speed, ease of use, and access.**

As noted in response to questions above, we are unaware of any substantiated use case for any particular digital asset, including a CBDC or a stablecoin, that would benefit low- and moderate-income people. Indeed, as BPI has previously noted, "[c]ryptocurrencies often are touted as a catalyst for financial inclusion, both for expanding investment opportunities to a broader spectrum of the population and potentially for delivering banking services to segments of the population that would otherwise be unbanked. However, such financial inclusion benefits of cryptocurrencies remain largely hypothetical; for instance, to date there is no evidence that cryptocurrency or DeFi platform use has benefitted the unbanked population in the U.S."[77]

[75] SEC Investor Bulletin: Crypto Asset Interest-bearing Accounts (Feb. 14, 2022), available at: Investor Bulletin: Crypto Asset Interest-bearing Accounts | Investor.gov.

[76] Hailey Lennon, "Bankrupt Crypto Lender Celsius Could Leave Customers Last In Line To Get Paid" (Aug. 1, 2022), available at: Bankrupt Crypto Lender Celsius Could Leave Customers Last In Line To Get Paid (forbes.com).

[77] Paul Calem, BPI, "Lax Supervision of FinTechs Harms Consumers" (May 10, 2022), available at: Lax Supervision of FinTechs Harms Consumers - Bank Policy Institute (bpi.com).

Further, as BPI has previously highlighted, crypto asset prices are highly volatile, making the holding of these assets very risky.[78] As noted, this was most recently illustrated by the bankruptcy filings by cryptoasset broker Voyager Digital, hedge fund Three Arrows Capital and lending firm Celsius Network.

> "Retail investors, particularly those who are younger or lower income, may not adequately assess or weigh this risk and its personal finance implications prior to investing or trading in crypto assets. Retail deposit accounts on DeFi platforms also expose consumers to substantial risk, and this risk may be less transparent than the volatility risk of cryptocurrencies. As described in the IMF report, "the liquidity of DeFi platforms could become insufficient during periods of market stress ... A more extreme outcome would be equivalent to a bank run—when participants rush to withdraw liquidity from the platform." Furthermore, the non-transparent nature of this risk is exacerbated by the platforms' use of misleading terminology and marketing. A previous BPI blog post, Nelson (2021), emphasizes the non-transparent nature and potentially illiquid nature of "stablecoin" deposits. Issuers of stablecoins, a privately issued, digital coinage, have claimed misleadingly that the coins are backed "one-for-one" by "safe assets" they term "reserves." However, as explained in that post, these "reserves" (which include commercial paper and bank certificates of deposit) are subject to substantially greater liquidity risk compared to what constitute reserves at traditional banks (risk-free cash or deposits at the Federal Reserve, or their close substitute, Treasury bills).[79]

Identity Verification

Financial services companies that offer services similar to banks, but are not subject to bank BSA regulations, may pursue innovative ways of efficiently, securely, and effectively identifying their customers. For example, these non-bank providers may obtain only the final four digits of an SSN from the customer and obtain the remainder from other trusted and secure sources. By virtue of the Customer Identification Program Rule, banks are not afforded the same flexibility.

We recommend that FinCEN, working with other relevant federal agencies, revise the CIP Rule to reflect a more flexible approach that is capable of accommodating the rapidly changing landscape of financial services and innovations in technology.

Modifications to the CIP Rule should, for example, permit institutions to: (1) obtain secure customer information from third-party trusted and secure sources (and not solely from the customer) for a broad set of account openings, with institutions empowered to determine the customer types for which reliance on such third-party information is reasonable; (2) verify identities through technologies that may not fit neatly into a documentary versus non-documentary dichotomy (e.g., video technology that reduces forgery and impersonation risks); and (3) adopt digital identification systems as they become available. The importance of these modifications is demonstrated by recent efforts, which we applaud, to improve digital verification and identification, such as the recently announced FDIC and FinCEN digital identity Tech Sprint and the Social Security Administration's Consent Based Social Security Number Verification Service.

---

[78] Id. (internal citations omitted).

[79] *Id*. (internal citations omitted).

* * * * *

We appreciate the opportunity to comment on the Department of Treasury's request for comment. If you have any questions, please contact the undersigned by phone at (703) 887-5229 or by email at paige.paridon@bpi.com.

Respectfully submitted,

Paige P. Paridon

Paige Pidano Paridon
Senior Vice President,
Senior Associate General Counsel
Bank Policy Institute

cc: Natalia Li, Deputy Director, Office of Financial Institutions
United States Department of the Treasury

Amanda Shulak, Attorney-Advisor, Office of General Counsel
United States Department of the Treasury