CHAMBER OF DIGITAL COMMERCE

July 16, 2021

James P. Sheesley
Assistant Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street N.W., Washington, D.C. 20429.

Attention: Comments-RIN 3064-ZA25

Re: Request for Information and Comment on Digital Assets (RIN 3064-ZA25)

Dear Mr. Sheesley:

The Chamber of Digital Commerce (the "Chamber") welcomes the opportunity to comment on the Federal Deposit Insurance Corporation (the "FDIC") Request for Information and Comment on Digital Assets (the "DA Request")[1]. The Chamber strongly supports the FDIC's request for input on current and potential use cases involving insured depository institutions ("IDIs") and their affiliates and risk and compliance management in conducting activities with respect to digital assets.

The Chamber is the world's leading blockchain and distributed ledger technology ("DLT")[2] trade association. The Chamber was created, and has grown rapidly, because its members recognize that DLT offers immense possibilities in global, innovative economy for business, government, and consumers. The Chamber represents the world's leading companies in the DLT ecosystem, including financial institutions, as well as leading edge software companies, global IT consultancies, insurance companies, law firms, and investment firms. Our membership includes IDIs that are regulated and insured by the FDIC. Our mission in supporting this diverse and global membership is to promote the acceptance and use of digital assets and blockchain and distributed ledger technology through education, advocacy, and close and ongoing engagement with policymakers, regulatory agencies, and industry leaders.

[1] Federal Deposit Insurance Corporation, Request for Information and Comment on Digital Assets, RIN 3064-ZA25, https://www.fdic.gov/news/press-releases/2021/pr21046a.pdf.

[2] DLT, including blockchain technology, is a database technology. "Distributed ledgers" are ledgers that are shared across locations or among participants, and DLT is used to validate or authenticate data on a distributed ledger. A distributed ledger allows multiple participants to trust the data stored on it without the presence of a single, centralized ledger that could be a single point of operational failure. A "blockchain" is one type of distributed ledger with entries that must be validated or authenticated in a certain manner such that each new piece or collection of data (a "block") must be added to a chain of prior blocks and each block bears a relationship to the entire chain of blocks. This letter uses the terms "distributed ledger" and "DLT" unless specifically referring to blockchain technology.

To help ensure that the U.S. maintains its position as a hub for global finance and innovation leadership in DLT, the Chamber is at the forefront of encouraging regulators to adopt clear and flexible policy frameworks that promote responsible innovation for this technology. Regulatory and other obstacles that hinder DLT adoption pose risks to the United States ("U.S.") losing its leadership position as a global center for financial technology to other nations that, with government support, are making significant advances in promoting and adopting this technology. For example, Bermuda[3] and Singapore[4] released regulatory codes of practice with guidelines for custody of digital assets and access to traditional banking services. Without clear guidance and support, IDIs – and by extension their customers – may be reluctant to utilize this important tool that can help increase financial inclusion and promote market competition.

The FDIC's DA Request comes at a crucial juncture in the evolution of the domestic banking system. The U.S. has lost 70% of its domestic banks over the past four decades.[5] As President Biden's recent Executive Order on Competition notes, increasing concentration within banking threatens financial access and inclusion,[6] while at the same time technology costs increasingly drive further market concentration.[7] A clear, flexible, and cost-effective framework around technology such as DLT can help expand competition by giving IDIs the option of forming partnerships with technology providers, or building solutions in-house. Such a framework would allow IDIs of all sizes to offer the market-leading products necessary to retain and grow their customer base.

On the consumer side, while meaningful progress has been made in reducing the number of underbanked and unbanked households, 7.1 million U.S. households remain unbanked.[8] In a 2019 FDIC survey, 48.9% of unbanked households stated they did not have a bank account because they could not meet minimum balance requirements; 34% stated that bank account fees are too high; and 14.1% indicated that bank locations were inconvenient.[9] Technology such as DLT has the potential

[3] Bermuda Monetary Authority, Digital Asset Custody Code of Practice (May 2019), https://www.bma.bm/viewPDF/documents/2019-05-20-16-07-35-Digital-Asset-Custody-Code-of-Practice-2018.pdf.
[4] Singapore: Cryptocurrency Regulation In Singapore: Challenges And Opportunities Ahead (January 14, 2021), https://www.mondaq.com/fin-tech/1025630/cryptocurrency-regulation-in-singapore-challenges-and-opportunities-ahead-#_ftn39.
[5] "Over the past four decades, the United States has lost 70% of the banks it once had, with around 10,000 bank closures. Communities of color are disproportionately affected, with 25% of all rural closures in majority-minority census tracts." https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/09/fact-sheet-executive-order-on-promoting-competition-in-the-american-economy/.
[6] Id.
[7] https://www.wsj.com/articles/bb-t-suntrust-tie-up-brings-tech-arms-race-into-focus-11549575429. "Behind one of the biggest bank deals in a decade is a recognition that BB&T Corp. and SunTrust Banks Inc., both dominant banks in the South, would be more competitive with a bigger tech budget."
[8] https://www.fdic.gov/analysis/household-survey/2019execsum.pdf.
[9] Id.

to reduce the cost structure and increase the convenience of banking, thereby addressing primary reasons why households remain unbanked. In a study with Georgetown University's Center for Financial Markets and Policy, the Chamber found that financial institutions around the world are using DLT solutions to increase access to financial services, such as retail payments, by lowering costs and barriers to accessing the financial systems.[10] With policies that both encourage certainty and adoption, such solutions could be brought to bear in the U.S., as well.

As the FDIC begins its study of digital assets and DLT use cases for IDIs, the Chamber urges it to consider how it can maintain technology neutral regulation that does not unfairly disadvantage a new technology like DLT. In other words, risk and compliance management frameworks and any supervisory guidance with respect to IDI digital activities should embrace the principle of same activity, same risk, same regulation. Where new technology poses new or different risks, those risks, where appropriate, should be addressed through the FDIC's existing supervisory risk management framework. However, where new technology reduces risk, these reduced risks should also be recognized in the regulatory standards that apply to the activity.

The Chamber believes that risk and compliance management frameworks and any supervisory guidance with respect to IDI digital activities should embrace the principle of same activity, same risk, same regulation. It is important to understand new or different risks posed by a new technology, though such risks, wherever appropriate, should be addressed through the FDIC's existing supervisory risk management framework. But if innovative technology involves the same risks as or fewer risks than legacy systems, regulation should not be a disincentive to adopting the new technology. DLT has the ability to improve the delivery of existing banking products and services in a number of ways, such as through increased efficiency, cost-reduction, and information security. Where DLT reduces the risks to an IDI when engaging in an activity, these reduced risks should be recognized in the regulatory standards that apply to the activity.

Additionally, supervisory approaches should be consistent and coordinated across U.S. regulators and jurisdictions globally, including to avoid U.S. institutions being placed at a competitive disadvantage. A key promise of technology, including DLT, is the ability for entities to interact more quickly and efficiently across the world in a manner that supports trust among them. The FDIC should work with other U.S. and global regulators to support this collaboration, empower U.S. IDIs to provide digital

[10] Chamber of Digital Commerce, Blockchain and Financial Inclusion (March 2017), https://digitalchamber.org/assets/blockchain-and-financial-inclusion.pdf.

banking services across the globe, and provide regulatory certainty, where possible, with respect to DLT and other digital activities.[11]

As discussed above, DLT has the ability to improve the delivery of existing IDI products and services in a number of ways. Regulation should not be a disincentive to adopting new technology.

Attached are the specific responses to the questions in the DA Request that are relevant to the Chamber's Members. Thank you for your consideration. We are available to serve as a resource as the FDIC continues its evaluation of DLT and the growing involvement of IDIs in the DLT space.

Very truly yours,

Perianne Boring
Founder & President

[11] For instance, the Chamber strongly encourages the FDIC to work with other U.S. federal regulators, as well as U.S. state lawmakers and regulators and non-U.S. authorities, to develop a clear regulatory framework regarding payment and settlement for DLT systems.

Questions Regarding Current and Potential Use Cases

2. What, if any, activities or use cases related to digital assets are IDIs currently engaging in or considering? Please explain, including the nature and scope of the activity. More specifically: a. What, if any, types of specific products or services related to digital assets are IDIs currently offering or considering offering to consumers? b. To what extent are IDIs engaging in or considering engaging in activities or providing services related to digital assets that are custodial in nature, and what are the scope of those activities? To what extent are such IDIs engaging in or considering secondary lending? c. To what extent are IDIs engaging in or considering activities or providing services related to digital assets that have direct balance sheet impacts? d. To what extent are IDIs engaging in or considering activities related to digital assets for other purposes, such as to facilitate internal operations?

Financial services firms, including IDIs, currently engage in a variety of activities involving DLT and digital assets and are doing so consistent with existing law. The Basel Committee on Banking Supervision ("BCBS") released a discussion paper[12] in December 2019 listing digital asset-related activities in which banking organizations may engage currently or in the future. In that paper, BCBS developed the below illustrative list of potential bank activities, omitting activities outside the scope of permissible activities for banks (as opposed to those permissible for bank affiliates).

- Using crypto-assets for internal or inter-bank operational processes,
- Fiat currency lending to, or providing deposit or other banking services to, entities dealing directly with crypto-assets,
- Fiat currency lending and taking crypto-asset collateral,
- Fiat currency lending to individuals, corporates, or financial institutions to allow them to invest in crypto-assets,
- Taking deposits of crypto-assets or extending loans denominated in crypto-assets,
- Acting as a custodian or taking deposits from a reserve of non-crypto-assets that back crypto-assets,
- Issuing crypto-assets directly,
- Market-making in crypto-assets,
- Exchanging crypto-assets for fiat currency, and vice versa—either as a core business or as an incident to other permitted activities (including activities otherwise unrelated to crypto-assets),

[12] BCBS, Discussion Paper, Designing a Prudential Treatment for Crypto-Assets (Dec. 2019), https://www.bis.org/bcbs/publ/d490.pdf.

- Validating crypto-asset transactions, including blocks of transactions with respect to blockchain technologies—e.g., "mining" transactions through proof of stake or proof of work—and other crypto-asset transactions,[13]
- Owning crypto-assets directly, including to hedge other exposures to crypto-assets, and
- Owning products with underlying crypto-assets—e.g., entering into a derivative transaction or taking a long position on an exchange-traded fund that has invested in digital assets.

In connection with the issuance of digital assets, IDIs may, in particular, issue, custody or otherwise transact in stablecoins. The Financial Stability Board has identified a number of activities in a stablecoin arrangement that IDIs might engage in including: (i) establishing rules governing the stablecoin arrangement; (ii) issuing, creating and destroying stablecoins; (iii) managing reserve assets; (iv) providing custody/trust services for reserve assets; (v) operating the infrastructure; (vi) validating transactions; (vii) storing the private keys providing access to stablecoins (e.g., using a wallet); and (viii) exchanging, trading, reselling, and market making of stablecoins. [14]

3. In terms of the marketplace, where do IDIs see the greatest demand for digital asset-related services, and who are the largest drivers for such services?

Demand for digital asset related services to be provided by IDIs has been growing from both retail and institutional customers. Up 47% from June of 2020, [15] the increase in total worldwide bitcoin wallets highlights the growing demand from retail customers to utilize digital asset-related services. Retail customers, used to a traditional banking system and interested in digital assets, drive demand for IDIs to provide digital asset-related services as a one-stop-shop for fiat deposits and digital assets. Institutional customers are the other driver of demand for digital asset-related services as a result of a number of factors,[16] including: (i) a movement towards regulatory clarity from governments around the world; (ii) increased use by retail customers; and (iii) diversification for an investment portfolio as an alternative asset class.

Other federal financial regulators have recognized the potential benefits of DLT to advance consumer protection in the context of digital activities by financial service providers. For example, a distributed ledger may be used to provide to a client a tamper-resistant record of a transaction or other activity.

[13] This could involve a bank operating a "node" or server on a DLT network.
[14] Financial Stability Board, Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements, Final Report and High-Level Recommendations (Oct. 13, 2020). The Financial Stability Board defines a stablecoin "as a crypto-asset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets." *Id.*
[15] Statista, Number of Blockchain wallet users worldwide from November 2011 to July 11, 2021, (July 12, 2021), https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/.
[16] Blocksize Capital, Five reasons for growing institutional demand in digital assets (May 19, 2021), https://blocksize-capital.com/five-reasons-for-growing-institutional-demand-in-digital-asset/.

The Bureau of Consumer Financial Protection (the "CFPB") recognized that the adoption of innovative technology could positively benefit consumers, stating the CFPB "also believes that expanded adoption of SWIFT's gpi product or Ripple's suite of products could . . . allow banks and credit unions to know the exact final amount that recipients of remittance transfers will receive before they send the transfer."[17]

Questions Regarding Risk and Compliance Management

> *4. To what extent are IDIs' existing risk and compliance management frameworks designed to identify, measure, monitor, and control risks associated with the various digital asset use cases? Do some use cases more easily align with existing risk and compliance management frameworks compared to others? Do, or would, some use cases result in IDIs' developing entirely new or materially different risk and compliance management frameworks?*

Given that digital assets may exist only on blockchains, substantial risks relating to access and security accompany the use, storage, and transfer of digital assets. IDIs that seek to participate broadly in blockchain related activities may need to upgrade risk and compliance management skills with respect to customer identification to understand the digital asset ecosystem and enhance existing risk evaluating models to account for digital assets.

Approximately one-third of internet users typically use a Virtual Private Network ("VPN") with a wide range of tools readily available to anonymize identity online, including VPNs, proxies, Tor, Fake Location Apps, GPS anonymizers, emulators, rooted or jailbroken devices among others. The increasing ability for consumers to operate anonymously on the internet creates challenges to trust in online transactions, including:

- Facilitating uninterrupted online criminal activities and allowing customers to operate while evading detections by law enforcement;
- Masking real IP addresses and preventing device tracking, lowering the quality of data available for reporting and to ensure the integrity of transactions;
- Enabling users to bypass geographic restrictions and conduct transactions from high-risk or sanctioned regions; and
- Obfuscating reporting and oversight capabilities.

[17] CFPB, Remittance Transfers Under the Electronic Fund Transfer Act (Regulation E), 85 Fed Reg. 34,870, 34,880 (June 6, 2020), https://www.govinfo.gov/content/pkg/FR-2020-06-05/pdf/2020-10278.pdf.

Tools to anonymize location are frequently the first line of defense for an actor conducting nefarious activity online.

To address the risks posed by the proliferation of anonymizing/spoofing tools, IDIs have begun checking IP addresses against lists of VPNs, Tor exit points, and other non-trusted IP Addresses, blocking any matches. These risks and challenges are not unique to DLT and are currently identified, measured, monitored, and controlled by existing risk and compliance management frameworks.

Geolocation data collected from devices, such as GPS, WiFi Triangulation and GSM, enhances risk management and addresses certain risks posed by DLT transactions. Multi-sourced geolocation data gives far more accurate intelligence into a user's true location, while providing some protection against spoofing. Such accurate data strengthens an IDI's ability to create a secure digital identity, in addition to their ability to evaluate risk and detect suspicious and fraudulent behavior.

IDIs can address this risk by collecting the following geolocation data:

- the genuine, device-based geolocation data (WiFi triangulation, GPS, GSM) of the user at the point of transaction;
- the genuine IP address of the user, authenticated by viable anti-spoofing software in real-time to detect anonymizing tools; and
- a device identifier that captures a digital fingerprint of technology used to make a transaction.

By collecting multiple authentication factors, an authentication process becomes more robust and trustworthy. In addition, periodic geolocation authentication throughout the course of an online interaction can give a better understanding of consumer behavior, facilitating the monitoring of anomalous or suspicious behavior. For example, a user's latitude/longitude or IP-based location coordinates jumping a large distance in a short period of time can indicate account sharing or account takeover.

Therefore, geolocation authentication at varying stages during an online session, combined with the power of real-time and historical risk analytics enables suspicious activity to be detected and flagged. Such controls go a long way in detecting and deterring illicit actors at an earlier stage. With authentic geolocation data, IDI's would have far more robust and effective risk management processes, by enabling early detection of suspicious activities and a holistic overview of real-time and historic behavioral patterns.

> *5. What unique or particular risks are challenging to measure, monitor, and control for the various digital asset use cases? What unique controls or processes are or could be implemented to address such risks?*

Volatility Considerations

IDIs are familiar with assessing credit risk and will need to assess the strength and stability of various issuers of digital assets that may be circulating and used by IDI customers through the payments system or as investments. Currently some digital assets are highly volatile, much more so than currencies and IDIs may need upgraded monitoring and evaluation systems to effectively manage volatility risk.

DLT Reliability

The FDIC should consider if insurance for digital assets should cover the reliability of the DLT technology and what evaluations or certifications may need to be performed.

IDIs have traditionally offered consumers deposit products, such as checking, savings and money market deposit accounts, and certificates of deposit for which each depositor is insured by the FDIC up to at least $250,000. Deposits can occur via methods such as wire transfer and physical cash.

A deposit of digital assets occurs via transfer to an omnibus digital wallet address controlled by the IDI or to an address that is unique to the depositor and controlled by the IDI (solely or possibly through a multi-party signature scheme). FDIC insurance may cover the proper handling and protection of the related private keys (given accurate and complete internal record keeping at the IDI).

However, there will need to be clarification for what FDIC insurance actually covers as it relates to digital assets. The IDI may properly safeguard deposits of digital assets, but the reliability of the underlying blockchain for any digital asset can fail or be compromised – thus depositors may experience a loss of digital assets (i.e., the digital asset no longer exists) and look to the FDIC for coverage.

To validate, or authenticate, the existence of digital assets under ann IDI's custody is to identify that the claimed data record is consistent with the blockchain (or rule set) that has been selected and placing reliance upon such blockchain where they reside. FDIC (and other regulators) should consider the importance and role that reliance on blockchain data plays in determining insurance coverage.

Standard setting bodies are thinking about implications of blockchain reliability and the need for related evaluations. For example, the AICPA recently published the updated practice aid for financial

statement auditors, "Accounting for and auditing of digital assets."[18] This nonauthoritative guidance for CPAs and auditors states, "Reporting digital asset transactions involves the following processes, including . . . evaluating the reliability of blockchain data and methods used to extract blockchain data."[19]

As discussed in an article published by the World Economic Forum,[20] a reliable blockchain should have an effective design for its intended purpose and continue to operate as designed. The following elements of a blockchain can be considered as part of a risk assessment to conclude on its reliability and the existence of the associated digital asset:

1. *Deployment services* through which transactions are initiated and digital assets are observed
2. The *consensus protocol* that governs the agreement by the network for recording a digital asset's creation or transfer
3. *Network enablers* that maintain the distributed ledger
4. *Security* of the blockchain through cryptography
5. *Community of developers* that support the blockchain network

A digital asset may not exist if one or more of these elements indicates a risk to the reliability of the blockchain.

Customer Identity

Because certain permissioned blockchains preserve historical records of financial transactions and, when implemented with appropriate governance, do not suffer from data integrity issues, they provide unprecedented ability for IDIs and government agencies to track and trace transactions by token and wallet or account. Depending on the design of other non-blockchain distributed ledgers, DLT may also provide historical records. This ability to trace transactions back through time has helped law enforcement efforts to detect and prosecute criminals. Distributed ledgers can also strengthen (real time) auditability of financial transactions between counterparties and facilitate practical, technology-

[18] *Available at* https://www.aicpa.org/content/dam/aicpa/interestareas/informationtechnology/downloadabledocuments/2104-39790-da-pda-update-web.pdf.
[19] *Id.*
[20] World Economic Forum, Why the evolution of blockchain reliability is critical to protecting your digital assets (June 11, 2020), *available at* https://www.weforum.org/agenda/2020/06/evolution-of-blockchain-reliability-and-digital-asset-protection/.

enabled know-your-customer ("KYC") and customer due diligence ("CDD") efforts and transaction monitoring and tracking.

Beyond KYC, IDIs incur excess costs and customer frustration related to identity with respect to, among other things:

- obtaining customer PII and managing associated risks,
- duplicating identity verification for common customers, and
- applying varying data requirements across jurisdictions.

Innovations for identity have matured to move identity into the digital age – data security and protection/authentication protocols, open APIs, data exchange standards, open authentication protocols and technology such as biometrics, RFID, mobile devices, and the like. DLT thinkers have long considered digital identity as a powerful use case as DLT can be the system of record upon which digital identity innovations can rely. Any consideration of a regulatory framework for digital assets should address concepts of digital identity (i.e., centralized vs. self-sovereign) to streamline IDIs' processes and enable inclusion for the unbanked.

6. What unique benefits to operations do IDIs consider as they analyze various digital asset use cases?

Where IDIs use DLT to provide services, the technology provides clear benefits as compared to legacy technologies. These benefits may translate into applications that IDIs could provide as products or services more broadly including:

- *Programmable*: Many DLT applications are programmable, allowing IDIs and their clients to develop software "rules" that can automatically execute instructions to change the state of a distributed ledger at specified times or if specified conditions occur.
- *24x7*: DLT software can operate 24 hours a day, seven days a week—even outside of bank branch hours when legacy technology that requires greater human support is unavailable.
- *Straight-through processing*: Because participants can each maintain their own addresses or accounts on a distributed ledger, transactions (e.g., payments) and data can be processed straight-through between participants' accounts and networks, rather than through intermediaries, improving settlement certainty and decreasing processing times.
- *Increased resiliency*: Because distributed ledgers involve redundant copies being hosted across multiple systems, DLT may be more resilient to cyberattacks and system failures, and may experience less system downtime, than legacy systems operated by a centralized entity.

- *Enhanced transparency*: Blockchains (and, depending on their configuration, other distributed ledgers) provide tamper-resistant records of activities on the network, enhancing the transparency and auditability of those records and providing more reliable proof of regulatory compliance than legacy technology.
- *Reducing settlement risk*: DLT systems can be programmed to execute one leg of a transaction only if, and at the same time as, the other leg of the transaction settles. This feature can be used to provide real-time processing and settlement of crypto- asset transactions, including securities token transactions, reducing settlement risk.
- *Payment systems*: Digital assets should play an increasing role in the payments system and may reduce costs, ensure greater accuracy and speed in transmittals. Foreign remittances should benefit from the deployment of digital assets on a global scale.

Given these benefits and potential applications, banks should be permitted, and even encouraged where appropriate, to use DLT in connection with their permissible activities.

Questions Regarding Supervision and Activities

10. Are there any unique aspects of digital asset activities that the FDIC should take into account from a supervisory perspective?

It is imperative that the FDIC have a clear understanding of the different types of digital asset wallets that an IDI chooses to use to provide customer access to their digital assets. Every type of digital asset wallet falls into one of two categories: hot (custodial or hosted) or cold (non-custodial) wallets. There are significant differences and pros and cons between the two.

Hot wallets are connected to the internet and are easier to use for day-to-day digital asset transactions. Examples of hot wallets include exchange wallets (e.g. Coinbase), web-based wallets (e.g. MetaMask), desktop wallets (e.g. Electrum) and mobile wallets (e.g. Exodus).

While cold wallets are not connected to the internet (although the associated address balances are viewable on a public blockchain), the digital assets stored in them are harder to access and use. Examples of cold wallets include hardware wallets (e.g. Ledger Nano S) which are physical devices that can connect to a computer and mobile via USB ports or Bluetooth technology so one can perform send and receive functions of digital assets. Another type of cold wallet is a paper wallet (e.g. hand-written) and can be generated by WalletGenerator.net, for example.

For further security measures an IDI may look to implement the use of multisignature wallets (or multisig, for short), which are digital asset wallets that require two or more private keys to sign and

send a transaction. The storage method requires multiple cryptographic signatures (a private key's unique fingerprint) to access the wallet. Multisig wallets can be used via a combination of hot (desktop and mobile) and cold (hardware) wallets.

> *11. Are there any areas in which the FDIC should clarify or expand existing supervisory guidance to address digital asset activities?*

Regulatory expectations may be difficult to frame in advance of broad scale adoption of digital assets by IDIs, but clear guidance will enhance the ability of a wider range of IDIs to participate in the development of digital asset products and services. Supervisory guidance should empower and encourage banks to develop and use new technologies to serve customers' needs and enhance consumer protection. IDIs should have the ability to explore new interfaces, customer engagement methods models.

The Chamber believes that many applications of DLT can be analogized to existing activities—e.g., facilitating payments, custody, or wallet services for digital assets, or the use of digital assets as collateral. If DLT (or other technology) enables IDI to engage in a new activity, the supervisory guidance for such activity should be evaluated without the underlying technology being determinative.

The Chamber believes that the FDIC should consider two additional principles as guiding its approach to the supervision of digital bank activities. First, any confirmations or clarifications on bank digital activities provided by the FDIC should be accompanied by enhancements to its supervisory and examination approach. These enhancements should be designed to ensure that supervisory and examination staff have the information and skills they need to appropriately assess DLT and other digital activities of IDIs. For regulatory determinations to be effective, regulatory developments must be integrated into supervisory approaches, manuals, and systems. Supervisory tools, such as checklists and software, should permit supervisory personnel to categorize and confirm compliance of DLT and other digital activities on a basis that appropriately reflects the functions and risks of the specific technology. Given the rapid pace of development in the digital banking market, FDIC personnel at all levels may benefit from education and training regarding not only the potential risks of new technologies but also how those technologies operate—e.g., the technical processes by which DLT validates and authenticates data stored on the ledger.

> *12. In what ways, if any, does custody of digital assets differ from custody of traditional assets?*

Digital assets involve elaborate key protocols to maximize security in ways that depart widely from traditional custodied assets. A variety of tested and accepted methods exist to securely hold, account

for, and transfer traditional asset classes. Digital assets can be created with unique transfer protocols. While there are larger clearing organizations evolving to manage transfers and exchanges of digital assets, there are no accepted analogs to DTCC currently for digital assets.

In the digital asset space, custodians operate in a similar fashion to traditional financial markets in that their primary role remains the responsibility for, and the safekeeping of customer's digital assets. This is achieved through safe key management, which allows the digital assets to be cryptographically secured. However, unlike for traditional assets, an entity has custody of a digital asset simply by holding the private key on behalf of the asset holder, ensuring that it cannot be accessed by the asset holder or any other party without appropriate approval from the asset holder. Limiting access to private keys is paramount, particularly given that some transactions, depending on the type of DLT used, may be irreversible. Moreover, if a key is lost or stolen, depending on the nature of the digital asset, its recovery by the asset holder or its rightful owner may be difficult unless the digital asset is a representation of an actual asset e.g. a security token offering, where an actual asset may remain secure and a new token or digital asset can be issued. Digital asset custodians play a vital role in facilitating the safekeeping of customers assets by harnessing their market and technology expertise to minimize the risk of fraud, theft or loss of digital assets and ensuring market efficiency.

> *13. FDIC's Part 362 application procedures may apply to certain digital asset activities or investments. See 12 C.F.R. Part 362, subpart A. Is additional clarity needed? Would any changes to FDIC's regulations or the related application filing procedures be helpful in addressing uncertainty surrounding the permissibility of particular types of digital asset-related activity, in order to support IDIs considering or engaging in such activities?*

The FDIC may wish to consider establishing a center tasked with managing developments in digital assets for IDIs, along the lines of the SEC's FinHub. Because of the new and unique aspects of digital assets, specialized knowledge should be developed, and consistent advice and guidance issued as new products and services are introduced or requested by customers.

Questions Regarding Deposit Insurance and Resolution

> *14. Are there any steps the FDIC should consider to ensure customers can distinguish between uninsured digital asset products on the one hand, and insured deposits on the other?*

The Chamber believes that the following digital asset activities are part of or incidental to the business of banking and, therefore, permissible IDI activities: Deposit activities involving crypto-assets, including stablecoins; and dealing in crypto-assets, including stablecoins, to the extent a digital asset is functionally similar to a fiat asset. Each of these activities is similar to existing

activities that are commonly understood as core to the business of banking for fiat assets—accepting fiat deposits, holding fiat assets in custody on behalf of clients, and dealing in fiat currencies.

Nevertheless, we acknowledge that the application of the deposit insurance coverage rules for pass-through insurance is complicated for customers to understand. Accordingly, using legends and disclosures along the lines that uninsured IDIs or trust companies use to alert customers where they may be working with uninsured obligations should protect the public from surprises and put bank-related products in appropriate categories.

In general, the Chamber supports an approach to consumer protection that balances protecting consumers while supporting growth, jobs, and innovation. If a new or existing technology gives rise to consumer protection risks, these risks should be appropriately addressed in a technology-neutral manner with clear and objective consumer protection principles adaptable to digital activities as appropriate. For example, different consumer protection principles may apply if a bank sells a digital asset to a retail client versus if a bank provides traditional banking services, such as extending a dollar-denominated loan, to an institutional client that is engaged in digital asset business.

> *16. If the FDIC were to encounter any of the digital assets use cases in the resolution process or in a receivership capacity, what complexities might be encountered in valuing, marketing, transferring, operating, or resolving the digital asset activity? What actions should be considered to overcome the complexities?*

IDIs contemplating expanding into digital asset activities are often concerned with how such businesses will be evaluated by examiners and supervisors. To avoid this uncertainty, IDIs often seek to establish new independent subsidiaries or use other regulated avenues such as broker-dealers. The use of newly established affiliates can implicate state law money transfer laws and subject the company to a patchwork of supervision.

The AICPA report, referenced above, provides an understanding of the control environment the FDIC could implement for obtaining, maintaining, and transferring control of digital assets (i.e., access to private keys).

Additional Considerations

> *17. Comments are invited to address any other digital asset-related information stakeholders seek to bring to the FDIC's attention. Comments are also welcome about the digital asset-related activities of uninsured banks and nonbanks.*

We believe the FDIC should ensure that regulatory clarifications are accompanied by measures to ensure appropriate implementation in the supervisory and examination process. For a clarification to be truly effective, it must be not only reflected in regulations and guidance but also integrated into the activities and systems of supervisory personnel, supported by appropriate training and education. IDIs have robust and conservative governance regarding new activities (e.g., "new product review" processes). The mere sense that a supervisor is likely to be skeptical of an innovative product or service involving new technology may lead an IDI to forego developing or using the product or service. FDIC supervisory guidance should be revised to explicitly apply, where relevant, to digital activities so that supervisors can easily classify digital activities and document that new technologies comply with applicable rules. FDIC supervisors should also update their supervisory processes to recognize that distributed ledgers, including blockchains, can provide tamper-resistant records of certain required activities. If a rule requires an IDI to perform an activity and a distributed ledger records that the activity occurred at the time and in the manner required, supervisory staff should not seek further proof of the same activity when evaluating an IDI's compliance with the rule.

Now more than ever, the financial services industry and its clients are in need of more efficient digital services, including payment services. Consumers need access to low-cost and efficient payment and other digital banking services without entering a physical branch office. The COVID-19 pandemic has highlighted inefficiencies in the use, processing, and delivery of physical checks for payments, such as dividends or income distributions. We therefore support efforts by the FDIC and other U.S. and global regulators to reduce barriers to the deployment of digital payment services across the financial services industry.