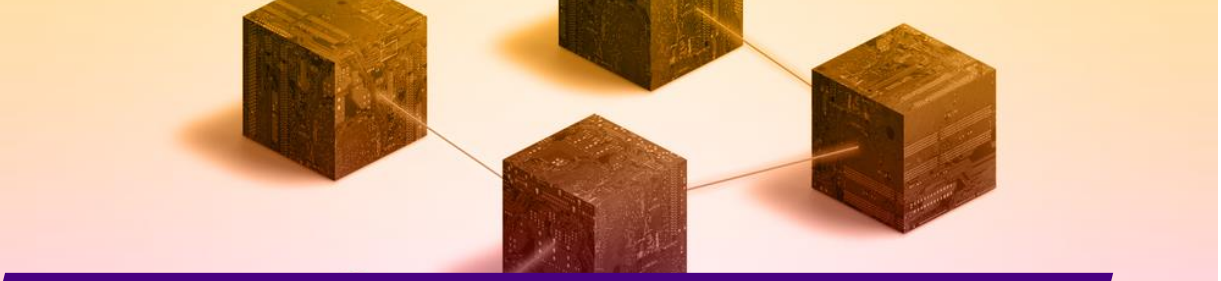

Distributed Ledger Technology: Enhancing the Current Regulatory Approach

Paige Paridon & Joshua Smith | Feb. 9, 2024

This post is the second of a series of two addressing the federal banking agencies' approach to bank adoption of emerging technologies. The first post describes the federal banking agencies' current supervisory approach to banks' use of DLT and other digital asset activities and the implications of that approach. This post recommends ways to improve and enhance the current framework to enable banks to innovate more expeditiously while maintaining safe and sound operations.

The first post in this series discussed the inordinately time-consuming and opaque process of consultation, prior notice and supervisory non-objection that the banking agencies impose on banks seeking to engage in (the misleadingly named) "crypto-related activities," including the use of distributed ledger technology (DLT). That post detailed some of the benefits of allowing banks to use DLT, including use cases that have already benefited customers, such as using DLT-based deposit accounts to clear and settle repo trades. Banks' use of DLT can improve the efficiency and security of recordkeeping and transactions, benefiting customers and the safety and soundness of banks.

This post will argue that while the banking agencies may be overestimating the risk of adopting new technology like DLT, it is imperative that the banking regulators not underestimate the risk to banks from failing to adopt new technologies, such as beginning to experiment with technology to combat the harms that quantum computing may render. Combined with the regulatory procedural morass surrounding bank innovation, this underestimation of the threat of banks' failure to adopt new technologies may raise serious risks for banks, consumers and the financial system more generally if the regulators do not streamline the experimentation and consultation process for bank innovation soon.

The banking agencies have made several statements indicating they are supportive of banks' ability to innovate.[1] But, as discussed in more detail in the last blog, many of their initiatives in this regard have not produced the clear guidance they promised, such as the "Digital Assets Initiative" (generally referred to as the "Crypto Sprint"), which failed to deliver guidance on any of the six identified "crypto-related activities."[2] Furthermore, other initiatives appear to have generated *more* complications, such as the Federal Reserve's Novel Activities Supervision Program, which adds even more staff but no clear, streamlined process, to review banks' plans to engage in certain "novel

[1] For example, in October 2022, the OCC announced that it was establishing the Office of Financial Technology to enable the OCC to "be more agile and to promote responsible innovation, consistent with our mission." OCC Announces Office of Financial Technology, OCC (Oct. 27, 2022) (link). As another example, in March of this year, Federal Reserve Governor Michelle Bowman acknowledged that innovation "has long been a high priority for banks" and that new "technologies have created significant opportunities for banks to become more efficient and competitive and to provide improved products and services for customers." She went on to warn that regulators' "lack of transparency, and the corresponding limits on bank innovation, has adverse consequences for consumers, businesses, and communities" and "it should be a regulatory priority to ensure our approach continues to support innovation that is conducted in a safe and sound manner and is consistent with applicable laws, including consumer protection." Governor Michelle Bowman, *The Innovation Imperative: Modernizing Traditional Banking*, FRB (Mar. 14, 2023) (link).

[2] *Written Testimony of Michael Hsu Before the Senate Committee on Banking, Housing, and Urban Affairs*, OCC (Aug. 3, 2021) (link).

activities,"[3] which includes activities related to DLT and crypto assets. These additional layers have also failed to address risks right around the corner. For instance, the Novel Activities Supervision Program does not contemplate or cover bank experimentation with defensive quantum computing even though adversarial nation-states or cyber criminals could deploy this new technology against U.S. banking organizations and their customers.

This post will recommend a better way forward to help achieve the regulators' stated goal of fostering safe yet rapid innovation by banks. Specifically, the regulators should

i. Rebalance their risk assessment of bank adoption of novel technology;
ii. Streamline the process for lower-risk activities where banks have already demonstrated they can operate safely and soundly;
iii. Enhance agency expertise in novel technology; and
iv. Engage in public-private partnerships with banks to encourage safe innovation.

Overestimation of Risks Plagues the Current Regulatory Approach to Innovation

With any new technology, novel, incremental and unique risks associated with that technology must be considered. Both regulators and regulated entities need time for this consideration. Both regulators and regulated entities need a well-considered approach to risk.

One driver behind the current regulatory morass regarding banks' ability to innovate using DLT, in particular, is an *overestimation* of the risks of a bank adopting this technology. As we explained in the first blog, because *permissionless* DLT is the foundation for popular cryptocurrencies, such as Bitcoin and Ethereum, it has become more broadly associated – and inappropriately conflated – with the crypto ecosystem and its unique attendant risks. However, a bank transitioning to using *permissioned* DLT to represent real-world funds is no different from a bank transitioning from paper-based banking to mobile banking that employs binary code. The value remains all in the *real world;* the underlying instruments and legal framework are *unchanged*; the mechanics of its *representation and method of movement* are what change. Regulators should not deny or impede the expected benefits of banks' use of this technology. Once a bank has demonstrated that it can manage a technology successfully, there should be a streamlined and expedited process to consult with the regulators and launch the technology.

As articulated in the first blog in this series, banks *must* be able to launch the use of relatively new yet tested technology after demonstrating the ability to use it safely without having to navigate a months- or *years*-long regulatory engagement process beforehand. Indeed, there should be an expedited process or "swim lane" for the technological applications that are similar or consistent with prior applications that have not threatened safety or soundness, such as private-permissioned DLT. Of course, this critique should not be mistaken for a wholesale criticism of the regulators appropriately scrutinizing banks' use of new technology. Banks appreciate regulators' responsibility to ensure the financial system is not threatened by poor implementation of novel technology. A longer experimentation and consultation process would, of course, be more appropriate for banks' use of technologies with which banks are just beginning to experiment, and the regulators have not distinguished between those technologies and those that banks have demonstrated an ability to manage safely. For example,

[3] *Novel Activities Supervision Program,* FRB (Oct. 4, 2023) (link). Announced in August 2023, the program is intended to "enhance the supervision of novel activities conducted by banking organizations," including "the exploration or use of DLT for various use cases such as issuance of dollar tokens and tokenization of securities or other assets." Specialized supervisory staff will be added to the existing supervisory and exam staff at organizations engaged in "novel" activities who already facilitate the lengthy consultative process banks currently must undergo before using permissioned DLT. Thus, the creation of this new supervisory program seems likely to ***further slow the process*** by which banks can deploy new technology, as they will have to engage with even more supervisors and exam staff and answer more questions than they do currently.

the Novel Activities Supervisory Program does not delineate whether different types of use cases will be treated differently – such as adjacent use cases and entirely new technologies.

When banks have demonstrated the ability to manage the risks, the process of launching a new application of that technology should be straightforward, with clear, reasonably short timelines for regulatory consultation.

Underestimation of Risks Presents Dangers, Too

On the other hand, another driver behind regulatory slow walking in certain instances may be an *underappreciation* of the risks of a bank *failing* to adopt a new technology. Technological adaptation is about far more than marginal improvement. When banks are able to innovate nimbly, they can offer customers products and services that less well-regulated nonbanks may offer, benefiting those customers, as banks are subject to comprehensive regulation and supervision. Banking innovation also helps U.S. banks remain competitive on a global scale. In addition, at times innovation is in the service of preparing defenses against the risk of significant harm. The OCC has identified a bank's *failure* to innovate as a critical strategic risk that could threaten a bank's operational resilience.[4] The potential future threat from quantum computing underscores the importance of banks being permitted to explore and prepare for new technologies as a means of developing countermeasures against future risks.

Quantum computing has the potential to decrypt banks' encrypted information. Adversarial nation-states or criminal actors with quantum computing capabilities could unravel the cryptography that currently protects critical information at banks. Much of the information that a bank encrypts has a significance that is hard to overstate: personal transaction history, information provided to law enforcement about possible criminal activity and security protocols to protect the theft of client funds, to name just a few.[5]
In one sense, the threat of quantum computing has already manifested, as hostile actors are stealing encrypted data today and planning to decrypt it after they have developed quantum capabilities.

The Federal Reserve has acknowledged the long-term significance of quantum computing, noting its potential to "render current encryption standards used by financial institutions obsolete."[6] This recognition underlines the importance of preparedness in the banking sector. The Financial Services Information Sharing and Analysis Center, a nonprofit industry organization dedicated to cybersecurity and the financial system's global resilience, has also taken note. Quantum computing "in the wrong hands would significantly compromise the privacy and security of the digital communications on which the world, and the financial system, increasingly relies on."[7] The Bank of International Settlements announced a project in January 2024 to "prepare central banks and the global financial system for a transition towards quantum-resistant encryption," noting that quantum computers could "potentially expos[e] all financial transactions and much of our existing stored financial data to attack."[8]

While we understand that the banking agencies have informally indicated that they plan to start discussing quantum-related risks and mitigation measures this year with firms, currently, there seems to be an absence of a defined regulatory process for banks to engage in preparatory experiments and develop defensive strategies

[4] *See Semiannual Risk Perspective Spring 2019*, OCC, 12 (link) ("Banks that do not assess business relevancy and impacts from technological advancement or innovation, or are slow adopters to industry changes, may be exposed to increasing strategic risk."). The most recent OCC Semiannual Risk Perspective similarly highlighted that "Prolonged use of . . . older or legacy systems could increase the likelihood of operational outages, introduce security vulnerabilities, create system maintenance challenges, and create other concerns that could reduce operational resilience." *See Semiannual Risk Perspective Spring 2023*, OCC, 19 (link).
[5] BPI's technology arm, BITS, has proactively developed a Quantum Risk Calculator. This forward-looking tool is intended to assist in future planning by determining potential timelines and strategies for banks to effectively address and mitigate quantum risks, a crucial step in long-term regulatory-required data storage and security planning. *See Quantum Risk Calculator*, BANK POLICY INSTITUTE BITS (link).
[6] *Report to Congress: Cybersecurity and Financial System Resilience Report*, FRB (Aug. 2023) (link).
[7] *Preparing for a Post-Quantum World by Managing Cryptographic Risk*, FS-ISAC (Mar. 2023), 3 (link). This report offers an extensive overview of the challenges and risks, along with a framework for financial institutions to prepare for a post-quantum future, and is a valuable resource for understanding the landscape and planning ahead.
[8] *Project Leap: quantum-proofing the financial system*, BANK OF INTERNATIONAL SETTLEMENTS (Jan. 10, 2024) (link).

against future threats from quantum computing. Establishing a fast-track process would benefit future readiness, resilience and the safe adoption of emerging technologies. It is important for regulators to support bank efforts to develop defensive countermeasures against hostile foreign actors or sophisticated cyber-criminals. A fast-track option when a technology relates to a bank's preparedness against critical threats would benefit the security and resilience of banks, their customers and the broader financial sector.

If appearances are correct, and the regulators have not communicated a clear plan to foster banks' experimentation with new technology in this regard, and this experimentation becomes subject to the same slow and opaque process as banks' use of permissioned DLT, there could be damaging effects on the security of the financial system. While this experimentation would, of course, proceed on a different path from technologies such as permissioned DLT, which banks have demonstrated they are able to manage, the need for clarity about how banks can explore cutting-edge innovation is no less salient.

We make the following recommendations for improvements to the regulatory approach to facilitating experimentation by banks in cutting-edge technologies.

The Banking Regulators Must Enhance Their Expertise and the Speed with Which They Collaborate with Industry to Advance Banks' Use of Novel Technologies Safely and Expeditiously

First, to help the regulators anticipate and understand new technologies that may benefit banks and the financial system, as well as technological threats that banks will need to guard against, the banking regulators must expand the technical knowledge of their supervisory staff and increase access to technology experts from outside the regulatory agencies. Innovation will continue to drive change in the financial services sector, requiring the agencies to have sufficient access to technical expertise that can help examiners quickly understand and assess banks' proposals to use new technology and help facilitate banks' safe use of such technology. For example, the banking agencies must employ experts who can quickly understand banks' plans to experiment with open/quasi-open DLT, quantum computing and other emerging technologies, and engage in robust and*,* most critically*, appropriately expeditious* consultations regarding that experimentation.

Banks already follow the guidance of Acting Comptroller of the Currency Michael Hsu, who stated that innovation in the regulated banking sector should proceed as follows:

1. "innovate in stages";
2. "build the brakes while building the engine" (in other words, involve risk and compliance professionals in the development of potential uses of the technology); and
3. "engage regulators early and often."[9]

The acting Comptroller, in those same remarks, acknowledged that regulators must be "***responsive, knowledgeable, and agile***" in responding to banking efforts to innovate.[10] As discussed in the prior post, the banks have abided by the words of the Acting Comptroller, and in turn, the regulators should reciprocate as he articulated. The Acting Comptroller is not alone in noting the importance of innovation. The Vice Chair for Supervision of the Federal Reserve, Michael Barr, has observed that "innovation never stops" and the Federal Reserve is "committed to supporting responsible innovation."[11]

[9] Acting Comptroller of the Currency Michael J. Hsu, *Tokenization and AI in Banking: How Risk and Compliance Can Facilitate Responsible Innovation*, REMARKS TO THE AMERICAN BANKERS ASSOCIATION RISK AND COMPLIANCE CONFERENCE (June 16, 2023), 12 (link).
[10] *Id*. at 13.
[11] Vice Chair for Supervision Michael S. Barr, *The Federal Reserve's Role in Supporting Responsible Innovation*, REMARKS AT THE FEDERAL RESERVE BANK OF PHILADELPHIA SEVENTH ANNUAL FINTECH CONFERENCE, (September 8, 2023) (link).

To meet this commitment, the regulators should retain additional knowledgeable technology and other subject matter experts and provide clear timelines for technology and risk management reviews so that banks and the public sector can work together to advance innovation in the regulated banking system expeditiously.

Public-Private Partnerships are a Safe and Effective Method for Banks to Experiment with Cutting-Edge, Untested Technology

As noted, banks have demonstrated that they are able to use permissioned DLT safely and, therefore, should be able to use it generally after a routine and expeditious consultation process. For other untested technologies, public-private partnerships can help advance progress on experimentation with these technologies in the regulated banking sector. For example, the Financial Services Information Sharing and Analysis Center,[12] the Financial Services Sector Coordinating Council (FSSCC)[13] and its government equivalent, the Financial and Banking Information Infrastructure Committee (FBIIC)[14] serve as exemplary models of public-private partnerships in cybersecurity, demonstrating the immense value of collaboration between government agencies and private sector entities in enhancing national security and resilience against cyber threats. This ongoing engagement showcases a proactive approach by industry stakeholders and government partners to align with emerging standards and contribute to the development of robust, quantum-resilient frameworks.

Additionally, several executive orders[15] and a national security memorandum on quantum computing[16] underscore the importance of, and urgent need for, public-private collaboration to prepare for future threats from quantum technology. The National Institute of Standards and Technology (NIST) and the National Security Agency have been leading collaborative efforts to develop technical standards and mitigation measures to support readiness and the transition to Post-Quantum Cryptography (PQC). These partnerships facilitate the sharing of critical information, expertise and resources, ultimately strengthening the collective defense against cyberattacks and promoting a safer online environment.[17]

Such partnerships can also help drive technological innovation, particularly when it is in its nascent stages. The banking agencies should engage with the private sector more frequently and extensively in various ways to facilitate banks' experimentation and adoption of novel technologies and the speed with which banks can innovate responsibly. This engagement will also help to establish clear expectations and parameters around banks' use of new technologies. For example, the agencies should work with the private sector to continue to develop proof-of-concept projects, pilot programs and other public-private exploratory test cases.

One prime example here is quantum computing. As noted, the agencies have informally indicated that they plan to start discussing quantum related risks and mitigation measures this year with firms. This would be a positive development to the extent that the regulators intend to advance an open and collaborative discussion with banks to support the safe and sound development of quantum computing capabilities and to articulate a defined regulatory process for banks to develop and deploy defensive strategies against future threats from quantum

[12] The Financial Services Information Sharing and Analysis Center is a member-driven, not-for-profit organization that advances cybersecurity and resilience in the global financial system, protecting financial institutions and the individuals they serve. (link)
[13] The FSSCC is an industry-led, nonprofit organization whose mission is to bring together members from financial services, trade associations and other industry leaders to assist the sector's response to natural disasters, threats from terrorists and cybersecurity issues of all types. (link)
[14] The FBIIC is chartered under the President's Working Group on Financial Markets and is charged with improving coordination and communications among financial regulators, promoting public-private partnerships and enhancing the resiliency of the financial sector. *See Financial and Banking Information Infrastructure Committee* (link).
[15] *See, e.g., Executive Order on Enhancing the National Quantum Initiative Advisory Committee*, THE WHITE HOUSE (May 4, 2022) (link)
[16] *See National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*, THE WHITE HOUSE (May 4, 2022) (link).
[17] International partnerships across governments and public sector entities are also critical. For example, the G7 Cyber Expert group is a "multi-year working group that coordinates cybersecurity policy and strategy across the eight G7 jurisdictions" that is co-chaired by the U.S. Treasury. *See G7 Cyber Expert Group*, U.S. DEPT. OF TREASURY (link). The initiative educates and informs regulators about quantum-related developments. *See 'Systems need to monitor AI deployment in financial sector and identify emerging Risks'*, ET CISO.in (Dec. 23, 2023) (link) (noting the G7 Cyber Expert Group leads an "international effort […] coordinate cybersecurity policy and strategy across the eight G7 jurisdictions.")

computing.[18] These capabilities *will enter and affect the financial system*. Regulatory action can support their defensive introduction by banks before introduction by bad actors. Of course, where the stakes are high and banks urgently need to deploy new technology, such as to protect their data, the longer process of consultation and experimentation via pilot programs may prove too time-consuming. Therefore, banks should be able to accelerate innovation and deployment of innovative technology where warranted.

Another example where further public-private engagement should continue to move forward is in ***expanding*** banks' use of permissioned DLT to public/decentralized DLT. While some banks have reached a point where they can safely use private-permissioned DLT to engage in permissible activities and should no longer be forced to consult with the regulators before its deployment in typical use cases, there are novel use cases that require further consideration. Banks and regulators can leverage the lessons learned from safely using permissioned DLT to begin to study and pilot discrete novel use cases of quasi-open and open DLT. The regulators have engaged in some pilot projects to explore the potential of new technologies in the financial sector. For example, the Federal Reserve Banks of Boston and New York have developed proof of concept projects and pilot programs that use new technology in controlled settings, such as Project Hamilton, Project Cedar and the Regulated Liability Network.[19] BPI members have participated in the RLN and Project Guardian, among others.[20]

A good project for public-private collaboration is to explore the issuance of deposit tokens that rely on open/quasi-open DLT. Deposit tokens that could function in an open/quasi-open system would offer the benefits of DLT within the safety of the regulatory perimeter. Using deposit tokens as a payment mechanism and store of value as "regular" deposits are used today could enable significant efficiencies, cost savings and enhanced security in traditional banking products and services. Banks could use deposit tokens to facilitate traditional trading and market activity, including spot transactions, lending and collateral management. Still, regulators have slowed

[18] The FSSCC has engaged with NIST on post-quantum preparedness and long supported NIST's efforts in developing quantum-resistant cryptographic algorithms. *See, e.g., NIST releases encryption tools to combat quantum computing threats*, ABA BANKING JOURNAL (July 8, 2022) (link). More generally, NIST, the National Security Agency and the U.S. Treasury have been actively engaged in collaborative efforts to support readiness and a transition to PQC. *See National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems,* THE WHITE HOUSE (May 4, 2022) (link) (signed by NIST, NSA, and Treasury alongside other relevant agencies); *see also Post-Quantum Cryptography*, NIST (link); Lisbeth Perez, *NSA Plans for Full Post-Quantum Cryptography by 2035*, MERITALK (Sep. 15, 2022) (link).

[19] "Project Hamilton" is a joint research effort between the Federal Reserve Bank of Boston and the Massachusetts Institute of Technology into the technical feasibility of a potential CBDC. *See Boston Fed, MIT complete research project into feasibility of a central bank digital currency*, FEDERAL RESERVE BANK OF BOSTON (Dec. 22, 2022) (link). The New York Fed's "Project Cedar" is "a multiphase research effort to develop a technical framework for a theoretical wholesale central bank digital currency in the Federal Reserve context." *New York Fed Announces Phase I Results of the New York Innovation Center's Project Cedar*," FEDERAL RESERVE BANK OF NEW YORK (Nov. 4, 2022) (link). The Regulated Liability Network proof of concept would tokenize commercial bank, central bank and electronic money on the same chain, which offers the promise of delivering a next-generation digital money format based on national currency units (*e.g.*, denominated in U.S. dollars). *See Members of the U.S. Banking Community Launch Proof of Concept for a Regulated Digital Asset Settlement Platform,* BUSINESS WIRE (Nov. 15, 2022) (link).

[20] The Monetary Authority of Singapore launched Project Guardian in 2022 as "a collaborative initiative with policymakers and the financial industry that seeks to test the feasibility of applications in asset tokenisation and DeFi while managing risks to financial stability and integrity." *Project Guardian*, MONETARY AUTHORITY OF SINGAPORE (Oct. 19, 2022) (link). Project Guardian "aims to advance the development of efficient and safe financial networks," and several pilots in different disciplines have been launched, including those that "support the following objectives: [i]mprov[ing] understanding of the opportunities and risks of digital assets and assess[ing] longer-term transformational impact; [e]nabl[ing] interoperability across different platforms, use cases, and amongst participating entities; [d]efin[ing] standards and best practices for risk management and operational execution." *Project Guardian,* Monetary Authority of Singapore and Bank of International Settlements (June 2023) (link); *see also* Claire Huang, *MAS-led Project Guardian adds five more pilots in asset tokenization*, THE STRAITS TIMES (Nov. 15, 2023) (link) (discussing new Project Guardian pilot initiatives including "using blockchain to price and execute bilateral digital asset trades" or "trying out a cross-border foreign exchange payment product to enable secure payment across networks of different origins"). Multiple BPI member banks are participants in Project Guardian, including JPMorgan Chase, Citi, HSBC, UBS, Bank of New York Mellon and UBS. Additionally, as noted above, the Federal Reserve did announce in August 2023 that it had established a Novel Activities Supervision Program to enhance the supervision of novel activities conducted by banking organizations supervised by the Federal Reserve and will focus on, among other things, *projects that use DLT with the potential for significant impact on the financial system, including t*he exploration or use of DLT for various use cases such as issuance of dollar tokens and tokenization of securities or other assets. The Fed stated that the Program will be advised by a range of multidisciplinary leaders from around the Federal Reserve System and will engage broadly with external experts from academia and the banking, finance and technology industries and that the Program will also inform the development of supervisory approaches and guidance for banking organizations engaging in novel activities. The Fed and other agencies should collaborate with multidisciplinary leaders and experts on these topics to help accelerate banks' exploration of the use of DLT and other novel technologies and not merely to develop supervisory programs. *See SR 23-7: Creation of Novel Activities Supervision Program*, FRB (August 8, 2023) (link).

banks' ability to further experiment with this product and expand the scope and scale of its use. Based on incremental research and experimentation, the regulators and other government bodies could work towards banks' broader use of deposit tokens on more open networks.

The public and private sectors could work together to achieve incremental milestones towards banks' ability to potentially use more open DLT. One first step could be working towards establishing standards for verifiable credentials, which are digital identity tools that may be used to ensure that transactions conducted using open/quasi-open DLT are only executed with verified counterparties. Another step towards broader use could be public-private collaboration to study the potential for universal messaging standards using open blockchain, which could be led by the White House Office of Science and Technology Policy, the National Institute of Standards and Technology or another government entity, in collaboration with the banking regulators.

Banks Are Well-Suited to Partner with the Public Sector to Innovate

Banks are ideal entities to partner with the public sector to test, experiment and ultimately launch new technologies for numerous reasons.

Federally insured banking organizations are subject to comprehensive regulation, supervision, and examination for compliance with prudential, consumer protection, data security and data privacy requirements, among others. Larger banking organizations have separate examinations of, among other areas, custody and technology.[21] Banking organizations must follow the same due diligence, risk review and risk management processes when engaging in all activities. They must establish, maintain and enforce policies and procedures that assess technological, legal and regulatory risks before engaging in any new activities, including using new technologies for banking activities.

The prudential oversight of banking organizations ensures that all activities and operations are conducted safely and soundly through proper assessment and management of risk. Regulatory oversight is conducted through a comprehensive and frequent examination process. Larger banking organizations have special, separate examinations of, among other areas: technology, which includes the robust evaluation and management of IT risk; the implementation of proper internal controls; the adequate assessment of potential legal risk; the operation of comprehensive cybersecurity programs; and the identification and mitigation of potential conflicts of interest. Banking organizations also must meet regulatory expectations with respect to other operational resiliency obligations, recovery and resolution planning mandates[22] and anti-money laundering and financial crimes regulation.[23] This comprehensive regulatory risk management framework distinguishes banking organizations from nonbanks, protects clients and promotes safety and soundness regardless of the activity in which a banking organization is engaged.

Other protections and contingency sources include large and diversified balance sheets backing deposit tokens, access to central bank contingency funding (e.g., discount window funding in the U.S., standing facilities in the Eurozone), and deposit insurance schemes for deposits below certain thresholds (where applicable). Banks are required to meet these minimum liquidity, capital and risk management requirements at all times — their

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

[22] Banking organizations are subject to exams that evaluate how well management addresses risk related to the availability of critical financial products and services, including cyber events, and require adoption of processes for management to oversee and implement resiliency, continuity and response capabilities to safeguard employees, customers and products and services. *See id.*

[23] *See, e.g.*, *BSA/AML Examination Manual*, FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL (link).

activities are monitored regularly by supervisors with strict implications in case of a breach.

Banks have the resources, talent and expertise to implement robust compliance programs to manage the risks presented by specific products and services involving novel technologies, such as quantum computing and DLT. Banks are also experienced in developing and implementing novel technologies. Moreover, the public and the financial system would benefit from banks' innovative products and services, as banks would provide these within the regulatory perimeter in which they operate.

Conclusion

A cumbersome regulatory approach to bank adoption of novel technology is not warranted. Currently, the regulators continue to overestimate the risks of banks' use of certain technology, particularly the use of permissioned DLT, that banks have demonstrated they can manage safely and soundly. They also may be underestimating the threat to banks and the broader financial system of ***not innovating***, such as the movement of cutting-edge products and services out of the regulated financial system where risks may accrue outside the view of regulators. One extreme example is the threat of hostile foreign adversaries or criminal actors with impending quantum computing capabilities. An overly convoluted and drawn-out process will put sensitive financial and other information at risk of being compromised by adversaries or criminals with quantum computing capabilities. The regulators must begin accelerating the adoption of public-private experimentation and collaboration to explore and adopt novel technologies and clearly communicate this process to banks. While in some cases, pilot programs may be appropriate to explore certain new technologies, these programs can take time to develop and run. Therefore, these programs must begin development now when time is of the essence. Indeed, in some cases, pilot programs may be too time-consuming, and other, more expeditious collaboration should be pursued.

We suggest three critical changes to the regulatory process. As we articulated in the first blog in this series, banks must be able to deploy technology that they have managed safely and soundly without engaging in a months-or-years-long consultative process. The regulators should develop a clear, streamlined process with specific timelines for review and consultation when banks have demonstrated their ability to manage a technology.

Second, the banking regulators must enhance their expertise to help increase the speed with which they collaborate with industry to advance banks' use of novel technologies safely and expeditiously.

Finally, for new and cutting-edge technology or novel use cases, the regulators should expand their use of public-private partnerships through proof-of-concept projects and pilot programs to develop and refine applications within the regulatory perimeter and clearly articulate these plans and programs. This approach builds on successful precedent and would ensure banks may experiment while maintaining safe and sound operations. Furthermore, it will help enable banks ultimately to use technology to enhance their efficiency, security, safety and soundness, which will benefit consumers and the financial system more broadly.

Disclaimer: The views expressed do not necessarily reflect those of the Bank Policy Institute's member banks, and are not intended to be, and should not be construed as, legal advice of any kind.