Distributed Ledger Technology: A Case Study of The Regulatory Approach to Banks' Use of New Technology

Paige Paridon & Joshua Smith | Feb. 1, 2024

This post is the first of a series of two addressing the federal banking agencies' approach to bank adoption of certain emerging technologies. This 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. The second post will recommend ways to improve and enhance the current framework to enable banks to innovate more expeditiously while maintaining safe and sound operations.

Fundamental to the business of banking is the need to manage risk. Banks' long-term stability and trustworthiness, as well as regulation, supervision, market discipline and civil and criminal enforcement all incentivize strong risk management.

Of course, banks also seek to continuously improve, modernize and expand their offerings, including through innovation, to meet customer demand and compete in the continuously evolving marketplace. Therefore, banks must carefully assess and manage possible risks and benefits in all aspects of their businesses.

A present-day example of this balancing act is banks' innovation with distributed ledger technology (DLT), which has the potential to enhance banks' efficiency and security. With any new and emerging technology, it is of no surprise that risk management is a critical consideration for *both* banks and their regulators. The federal regulators have issued statements and taken certain actions intended to assist banks in identifying and mitigating the risks associated with DLT, which banks are able to manage through their existing risk management frameworks. However, while those statements and actions seek to provide guidance and clarity to banks on topics such as permissibility and supervisory expectations and processes, the opposite has resulted—banks are at times left with more questions than answers on substantive issues and must navigate an unnecessarily lengthy and opaque process before launching DLT-related products or services.

This post will discuss the federal regulators' current posture towards banks' use of DLT in more detail and explain why that posture is unwarranted.

DLT Generally

DLT is a buzzword one hears frequently when "crypto" is discussed, but what it is and its potential benefits are generally not well understood.[1] Fundamentally, DLT is simply a new way to record and maintain information without relying on a centralized system or party. It functions like a shared Excel spreadsheet. Network participants

[1] The World Bank has explained that "distributed ledgers use independent computers (or "nodes") to record, share and synchronize transactions in their respective electronic ledgers (instead of keeping data centralized as in a traditional ledger). World Bank Brief "Blockchain & Distributed Ledger Technology (DLT)" (April 12, 2018) (link).

all have access to the same shared ledger that reflects the current state of the world and agree on transactions in real time, which can reduce costs and the time associated with reconciling information between or among multiple entities' individual ledgers. Additionally, smart contracts, which are contracts with the terms of the agreement directly written into code, can self-execute on DLT. The technology thereby facilitates the simultaneous execution of the legs of a transaction among participants, reducing the time to complete transactions and counterparty risks from lags between instructions and settlement. Finally, DLT employs advanced cryptography to ensure secure, tamper-evident and immutable transaction recording, enhancing trust and security.

These are the broad contours of DLT and its benefits. At a high level, DLT can be subdivided into three primary types with differences in breadth of access and control. Private-permissioned DLT is not "decentralized" at all. Such networks are owned and operated by a central entity or group of entities that allow access only to parties with appropriate entitlements, and users' identities are known only to other users who are granted access. By contrast, public-permissionless DLT is fully decentralized and does not restrict access or privileges. Somewhere in between sits public-permissioned DLT, which mixes features of the other two types. For example, access to the network may be open, while at the same time, only certain users who authenticate might possess governance and administration rights.

With the adoption of this new technology, there have been several questions about the applicable legal frameworks for the assets that move on it. Current law and regulation apply to tokenized versions of real-world assets and liabilities that move on DLT, such as securities and fiat currency, to the same extent as they apply to their real-world counterparts today. Fundamentally, the use of blockchain itself does not change the underlying real-world instrument nor the legal framework around it. The OCC observes, "Over time, banks' financial intermediation activities have evolved and adapted in response to changing economic conditions and customer needs," and independent node verification networks such as DLT "represent new technological means of carrying out bank-permissible payment activities."[2] Tokenizing a deposit is simply a change of back-end infrastructure that can generally mirror the traditional asset to ensure legal clarity. In cases like these, the existing regulatory framework is sufficient to address this change.

DLT Use Cases

Banks have demonstrated over the past few years that they can effectively manage the risks presented by private-permissioned DLT. In close collaboration with the banking agencies, they have been experimenting with incorporating DLT in traditional banking products and services to make those products and services safer and more efficient.

For example, banks' DLT-based deposit accounts[3] have been used to clear and settle repo trades and conduct inter-affiliate, intra-company transfers.[4] Banks have used DLT to facilitate sharing payments-related information across financial institutions.[5] They have transferred programmable tokenized deposits to provide instant payments to service providers via smart contracts in the trade finance ecosystem. Banks have used DLT for secure and efficient recordkeeping and are currently exploring the use of tokens to transfer liquidity between a bank's

[2] Interpretive Letter 1174, OCC (Jan. 4, 2021), 3-4 (link).
[3] Banks are authorized to issue tokenized deposits, establish blockchain-based deposit accounts and issue stablecoins, as governed under existing federal banking agency regulations and managed via banks' risk management systems. *See, e.g.*, Office of the Comptroller of the Currency, *OCC Chief Counsel's Interpretation on National Bank and Federal Savings Association Authority to Use Independent Node Verification Networks and Stablecoins for Payment Activities*, Interpretive Letter No. 1174 (Jan. 4, 2020) (link). *See also TCH, Bank Issuance of Stablecoins and Related Services: Legal Authority and Policy Considerations* (Nov. 2022) (link) (provided by Sullivan & Cromwell LLP at TCH's request).
[4] Blockchain deposits can exist in four forms: non-native deposit accounts, native deposit accounts, non-native token-based and native token-based. Tokenized deposits can be native or non-native. For purposes of this response, the term "tokenized deposit" refers to both native and non-native token-based blockchain deposits. *See:* "Deposit Tokens: A foundation for stable digital money," OLIVER WYMAN AND ONYX BY JPMC, at 14 (Feb. 9, 2023) (link).
[5] For example, Liink by JP Morgan Onyx allows a bank sending a payment to pre-validate with the receiving bank that it is sending payment to a valid open account, avoiding prolonged payment processing and rejection for invalid accounts. *See Liink*, JP MORGAN (link).

branches on a 24/7 basis.[6] At some institutions, clients intentionally sign up for certain DLT services, though new DLT infrastructure can be naturally integrated without friction – the same way back-end systems are upgraded today without disruption to banks' customers.

Regulatory Treatment of Banks' Use of DLT

Banks have been consulting with the regulators and experimenting safely with permissioned DLT for several years, but the current expectation is that banks engage in extensive and time-consuming consultation with the regulators before deploying permissioned DLT and, in some cases, obtain a non-objection to proceed with the use of DLT.[7]

At best, this process can take many months to complete. At worst, banks may never receive a clear answer. While the agencies have made public statements supporting innovation, the current application of guidance creates barriers to bringing solutions to the market promptly and efficiently. The agencies have issued guidance on top of guidance, promising clarity and forward motion but ultimately falling short, as described further herein.

Consider, for example, that the OCC announced a joint agency "Digital Assets Initiative" in 2021, an update to an earlier iteration called the "Crypto Sprint." The aim was to provide guidance to banks on the use of new technologies and assets, including "understanding use cases and risks."[8] Around nine months after the "Digital Assets Initiative" was announced, the agencies informed the public that they would be providing greater clarity on the result of the initiative throughout 2022. It's almost 2024, and that clarity has yet to be provided. Instead, the agencies have issued numerous pieces of guidance articulating notice, consultation and non-objection requirements for banks before engaging in activities involving DLT, including permissioned DLT, rather than offering clear guidance and a streamlined and efficient process for evaluating banks' proposed use of permissioned DLT.

In addition, the agencies have established new offices and supervisory programs, ostensibly to help facilitate banking innovation related specifically to "crypto." However, it is hard to decipher any concrete examples of progress towards supporting more rapid innovation in this regard. For instance, in 2016, the Office for the Comptroller of the Currency created the Office of Innovation (which was transformed into the Office of Financial Technology in 2022). The OCC asserted the new office would enable the agency to "be more agile and to promote responsible innovation."[9] It only recently announced that it had installed an Acting Director after hiring a director now alleged to have falsified his credentials, and it is unclear how the office is promoting greater innovation among banks.[10]

Similarly, the FRB announced in August 2023 that it had established a "Novel Activity Supervision Program," 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

[6] *See Citi Develops New Digital Asset Capabilities for Institutional Clients*, CITI (Sept. 18, 2023) (link).
[7] *See, e.g., Interpretive Letter 1179*, OCC (Nov. 18, 2021) (link); *SR 22-6*, FRB (Aug. 16, 2022) (link); FIL-16-022, FDIC (April 7, 2022) (link); *Policy Statement on Section 9(13) of the Federal Reserve Act*, 88 FR 7848, FRB (Feb. 7, 2023) (link); *SR 23-8*, FRB (Aug. 8, 2023) (link). The regulators currently require banks to, at a minimum, engage in lengthy consultations with them before using DLT. In particular, the Board of Governors of the Federal Reserve System and the Office of the Comptroller of the Currency have issued guidance that can be construed as requiring banks to obtain supervisory non-objection before issuing deposits represented and recorded using DLT. The expectation for supervisory non-objection set forth in the OCC's Interp. Letter 1179 and the FRB's Policy Statement on Section 9(13) and SR 23-8 raises concern under the Administrative Procedure Act because it appears the OCC and FRB used guidance to create and impose legal obligations instead of the requisite notice-and-comment rulemaking. Even assuming a nonobjection is not ***technically required*** to issue deposit tokens, the overall process the regulators have established for banks to engage in so-called "crypto-related activities" – which includes the use of DLT for deposit tokens and other activities – is so convoluted and time-consuming that it is hindering banks' ability to use DLT.
[8] *Written Testimony of Michael Hsu Before the Senate Committee on Banking, Housing, and Urban Affairs*, OCC (Aug. 3, 2021) (link).
[9] *OCC Announces Office of Financial Technology,* OCC (Oct. 27, 2022) (link).
[10] *See, e.g.*, Penny Crosman, *Did the OCC hire a con artist to oversee fintech?*, AMERICAN BANKER (Nov. 25, 2023) (link).

other assets."[11] 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. The short description of the program does not indicate that permissioned DLT is out of scope of its review. Moreover, the issuance of dollar tokens is encompassed with this new program, which already must be issued on permissioned DLT under the regulators' existing guidance.

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 before moving forward with using DLT. At least on its face, this program does not appear intended to accelerate engagement between the private and public sectors to enable responsible and rapid innovation.

This regulatory quagmire that has left banks unable to widely deploy permissioned DLT that they can manage safely has not gone unrecognized. Just this past October, the Federal Deposit Insurance Corporation's Inspector General faulted the agency for failing to provide "effective guidance" to banks regarding the use of new technology and asset classes related to "crypto" and concluded that the agency had no clear process or timelines to provide supervisory feedback.[12]

Therefore, because of this uncertainty and the long engagement process the regulators require, banks have not yet launched this technology at scale, limiting the benefits it can provide.

This consultative process is unnecessarily lengthy and opaque. Clearer guidance and more efficient processes would help ensure that banks are able to deploy new and novel technology more efficiently and thereby help banks and their customers reap the benefits of new technology, whether DLT or otherwise.

Banks Can Manage the Risks of Permissioned DLT

The guidance issued by the banking agencies over the past few years attempts to articulate the extent to which banks can engage in so-called "crypto-related" activities, which (while not consistently or clearly defined, generally includes the use of DLT) highlights concerns about banks' ability to manage the risks related to it.[13]

The degree to which banks can or already mitigate such risks warrants closer examination. The most recent guidance, the FRB's SR 23-8, issued in August 2023, catalogs the risks banks must manage that seek to "engage in certain activities involving tokens denominated in national currencies and issued using distributed ledger technology or similar technologies to facilitate payments (dollar tokens)."[14] These risks include, but are not limited to, operational risks, cybersecurity risks, liquidity risks, illicit finance risks and consumer compliance risks.[15] SR 23-8

[11] *Novel Activities Supervision Program*, FRB (Oct. 4, 2023) (link).
[12] *See FDIC Strategies Related to Crypto-Asset Risks*, FDIC OFFICE OF INSPECTOR GENERAL (Oct. 2023) (link). The Report cites to the definition of "crypto-related activities" in FDIC FIL-16-2022, which provides that the term "crypto-related activities" includes "acting as crypto-asset custodians; maintaining stablecoin reserves; issuing crypto and other digital assets; acting as market makers or exchange or redemption agents; participating in blockchain- and distributed ledger-based settlement or payment systems, including performing node functions; as well as related activities such as finder activities and lending." The Report found that the FDIC had not established an expected timeframe for reviewing information and responding to the supervised institutions that received letters to "pause" their crypto-related activities or described what constituted the end of the review process. The OIG concluded that the FDIC's lack of clear procedures causes uncertainty for supervised institutions and recommended that the FDIC establish a plan with timeframes for assessing risks pertaining to crypto-related activities and update and clarify the supervisory feedback process related to its review of supervised institutions' crypto-related activities.
[13] *See Interpretive Letter 1170*, OCC (July 22, 2020) (link); *Interpretive Letter 1172*, OCC (Sept. 21, 2020) (link); *Interpretive Letter 1174*, OCC (Jan. 4, 2021) (link); *Interpretive Letter 1179* (Nov. 18, 2021), OCC (link). In these letters, the OCC explained that "cryptocurrencies are enabled by two technologies: cryptography and distributed ledger technology."
[14] *SR 23-8 / CA 23-5 Supervisory Nonobjection Process for State Member Banks Seeking to Engage in Certain Activities Involving Dollar Tokens*, FRB (Aug. 8, 2023) (link).
[15] These risks restate and build on those the agencies articulated previously in the January 2023 "Joint Statement on Crypto-Asset Risks to Banking Organizations." *See Joint Statement on Crypto-Asset Risks to Banking Organizations*, FRB, OCC, and FDIC (Jan. 3, 2023) (link).

requires a bank to demonstrate[16] that it has established appropriate practices to manage these risks, including having adequate systems in place to identify, measure, monitor and control the risks of the activities, and read in concert with the Fed's Policy Statement on Section 9(13) of the Federal Reserve Act, it mandates that the bank must receive supervisory non-objection before commencing those activities.

As a general note, banks operate in a highly regulated environment where *all* risks, including those related to technology, are regulated, supervised and well-managed. More specifically, banks using permissioned DLT networks are able to manage the risks raised in SR 23-8 in connection with using DLT, as described further below. As noted, banks have been consulting with the regulators for several years about using DLT, which banks have demonstrated they can manage safely. Therefore, establishing a clear, streamlined and efficient process through which banks may consult and deploy permissioned DLT is more than justified. Any supervisory concerns would, of course, be managed through consultation or in the ordinary course of the continuous supervision to which banks are subject.

SR 23-8 Discusses the Following Categories of Risk:

Operational risks, including those risks associated with the governance and oversight of the network; clarity of the roles, responsibilities and liabilities of parties involved; and the transaction validation process

A bank that operates and makes use of private-permissioned DLT directly controls the "governance and oversight of the network" and discretion to shape the "roles, responsibilities, and liabilities of parties involved." The bank owns the network. Access to it is restricted, and the identities of its users are known to the bank and other users. Additionally, permissioned DLT allows the organizer or administrator to establish legal obligations, platform agreements, rulebooks and operational procedures, clearly meeting the concern that the bank can effectively "establish roles, responsibilities, and liabilities." For example, to gain access to a bank's permissioned DLT network, a user would have to meet the bank's due diligence and compliance standards, such as the requirements of its Bank Secrecy Act and anti-money laundering program. Thus, the regulators' concern about the lack of governance mechanisms establishing oversight of the system is mitigated vis-a-vis permissioned DLT.

Additionally, banks must already meet regulatory expectations concerning other operational resiliency obligations and recovery and resolution planning mandates.[17] Adherence to these standards is monitored by the oversight and review of dedicated teams of on- and offsite examiners from the agencies.

Finally, banks have a proven track record of developing and operating governance for critical infrastructures. SWIFT, a critical infrastructure for cross-border payments, is a cooperative with internal governance driven by its financial institution members. As another example, the development and establishment of the RTP Network was driven by the banking industry through the collaborative efforts of The Clearing House's 25 owner banks.

Cybersecurity risks, including risks associated with the network on which the dollar token is transacted, the use of smart contracts, and any use of open source code.

Permissioned DLT makes managing cybersecurity risks more effective, given permissioned DLT's improved cryptography combined with its restricted access. Banks can appropriately manage any technology-related risks in connection with standard internal recordkeeping functions and tokenizing traditional banking products using DLT.

Banks are already subject to exams that evaluate how well they address risk related to the availability of critical financial products and services, including cyber events. Banks are required to adopt processes for management to

[16] As noted in note 7, mandating supervisory non-objection through guidance may be unlawful under the Administrative Procedure Act.
[17] 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).

oversee and implement resiliency, continuity and response capabilities to safeguard employees, customers, and products and services.[18] Larger banking organizations have separate examinations of the technology they employ.[19] On- and off-site banking agency examiners monitor adherence to these standards.

Liquidity risks, including the risk that the dollar token could experience substantial redemptions in a short period of time that would trigger rapid outflows of deposits.

Banks maintain strong capital and liquidity buffers and are subject to robust, comprehensive risk management, supervision and examination processes to ensure their safety and soundness. Managing liquidity risk is a fundamental aspect of banking operations. This is because banks predominantly operate by funding themselves with deposits that customers can withdraw at any time while simultaneously investing in assets like loans that are not as easily liquidated. Consequently, a critical part of any bank examination is thoroughly assessing how effectively a bank handles this particular risk. Part of this assessment includes ensuring that the bank has comprehensive and reliable strategies in place to address any adverse liquidity events that may arise.

Illicit finance risks, including risks relating to compliance with the Bank Secrecy Act and Office of Foreign Asset Control requirements, which include requiring banking organizations to verify the identity of a customer, perform due diligence to understand the nature and purpose of the customer relationship, and perform ongoing monitoring to identify and report suspicious activity.

Banks already have an affirmative responsibility to combat illicit finance and have well-developed AML/CFT programs,[20] including robust know-your-customer (KYC) practices. They are already required by the Bank Secrecy Act to implement a risk-based program to prevent money laundering and the financing of terrorism.

Permissioned DLT prepares them to meet these obligations. In fact, it *enhances* a bank's ability to comply because regulators receive better transaction data and insights due to blockchain's transparency and relative immutability as a recordkeeping technology. As noted, permissioned DLT restricts access to authorized users, can require authentication and reveals users on the network to the bank and other network users. Banks would meet their legal obligations by structuring DLT to comply with existing AML/KYC and sanctions regimes.

Consumer compliance risks, including risks related to identifying and ensuring compliance with any consumer protection statutes and regulations that apply to the specific dollar token activity.

Banks are subject to consumer protection laws and regulations and to direct oversight for compliance with those requirements. These include but are not limited to obligations to prevent fraud, provide accurate information, engage in fair lending practices, and protect consumers' privacy, overseen by federal banking regulators and agencies such as the CFPB.

[18] *See id.*

[19] This supervisory oversight includes the robust evaluation of information technology risk management, internal controls, and cybersecurity risk management. 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 id.*

[20] For the purposes of this letter, references to AML practices are generally meant to be inclusive of compliance with economic sanctions programs, though we occasionally refer explicitly to sanctions compliance for particular emphasis.

Conclusion: Looking Forward

The possible harm of banks experimenting with and ultimately using permissioned DLT within their already significantly regulated environment is low, while the expected benefits are significant. The adoption of blockchain technology should not be treated differently or more punitively than the adoption of any other technology. Banks are natural innovators and leverage the benefits of their existing supervisory framework to ensure scalability in a safe and sound manner.

Banks are adopting permissioned DLT to benefit customers and the financial system in terms of speed, reduced costs, cross-border efficiency, safer recordkeeping and more. Even though banks are able to manage the risks articulated by regulators, the agencies continue to require banks to, at a minimum, engage in extensive and drawn-out supervisory consultation before banks may use even permissioned DLT to provide banking products and services such as deposit tokens. This situation puts banks at a competitive disadvantage and their customers in a worse position. The agencies should work with banks to help move innovation forward safely, efficiently and effectively.

The second post in this series will recommend specific actions the regulators should take to improve the efficiency with which banks are able to launch technological innovations in a safe and sound manner and highlight a significant risk to the financial system if they don't.

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.