

VaultLink, Inc.
200 W Jackson Blvd #1250
Chicago, IL 60606
(833) 858-5465

September 30, 2022

**VaultLink’s Submission to the Basel Committee on Banking Supervision (BCBS):
Second Consultation on the Prudential Treatment of Cryptoasset Exposures¹**

VaultLink welcomes this opportunity extended by the Bank for International Settlements (BIS) to offer comments on the Basel Committee on Banking Supervision’s (BCBS, or the “Committee”) second consultative document regarding prudential treatment of cryptoasset exposures.

The evolution of value-transfer systems is migrating towards a digital infrastructure prioritizing convenience, transparency, immutability, and traceability. Distributed ledger technology (“DLT”) and blockchain technology are enduring innovations that may positively transform financial systems, accelerate business processes, and facilitate daily life activities for all members of society. These efficiencies should be embraced as long as their associated risks and vulnerabilities are appropriately addressed. Cryptoassets built on blockchain technology represent a new form of highly transferable bearer assets. If cryptoassets remain largely outside the regulatory perimeter, they remain susceptible to misuse as effective tools for money laundering, terrorism financing, and sanctions evasion. A digital ecosystem should not increase risks to nations, societies, monetary systems, or individuals.

Cryptoassets are more powerful and convenient than traditional fiat currencies for facilitating illicit activities—due to the velocity, magnitude, and portability by which value can be transferred without oversight. Large quantities of physical cash cannot be accepted into the banking system without being documented and reported to the appropriate regulatory bodies. This standard control mechanism must also apply to cryptoassets, whereby initial provenance is verified before being deposited at a bank. All transfers and movements of cryptoassets should be identified and monitored in real-time. For example, cryptoassets can be placed onto a USB drive and physically handed to another person to easily circumvent money transmitter and funds transfer² controls. In this regard, even central bank digital currencies (CBDCs) and stablecoins can be misused if the transfer of value is insufficiently regulated.

¹ Basel Committee on Banking Supervision (BCBS) Consultative Document, “Second Consultation on the Prudential Treatment of Cryptoasset Exposures”. June 2022. (<https://www.bis.org/bcbs/publ/d533.htm>)

² 31 C.F.R. § 1010.410(f). (<https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1010/subpart-D/section-1010.410>)

The international banking system already maintains the capability and capacity to ensure cryptoassets are fully compliant with existing local regulatory standards and the global regulatory framework set forth by the Financial Action Task Force (FATF).³ Banking systems should be recognized as appropriate environments for cryptoassets due to their sound control mechanisms for identifying and reporting suspicious activities.

Cryptoassets' origins and sources must be vetted before entering the banking system, and then fully adhere to all banking regulations. This policy position is consistent with the Committee's mandate⁴; and fulfills the general principles of "same risk, same activity, same treatment" and "minimum standards."⁵

The current viewpoint that custody of a cryptoasset equates to exposure is incorrect. The conversation should focus on properly bringing cryptoassets into the regulated environment for custody and servicing rather than calculating reserve requirements for at-risk scenarios on-balance sheet.

A Framework for Regulating Cryptoassets and Protecting Global Banking Systems:

While cryptoassets have permeated most elements of the global economy, their overall utilization is still in the nascent stages of development and acceptance. Regulatory clarity continues to be a critical barrier to optimizing the full potential of this powerful new asset class.

Traditional fiat currencies are durable, portable, divisible, uniform, and controllable in supply. As the primary source of reserves in the global financial system, they are the foundation of liquidity for transactions and are explicitly utilized to facilitate lending activities. Fiat currencies' wide acceptance and usage over a long period of time instills a basic level of stability—enabling them to reside on banks' balance sheets as bank-owned assets, or as liabilities in the form of customer deposits.

Conversely, cryptoassets are typically transacted in significant value outside traditional financial systems' regulatory perimeter. As a relatively immature asset class, cryptoassets can exhibit high price volatility and instability. Banks should insulate their balance sheets from adverse impacts to capital and liquidity metrics by avoiding direct ownership of, or lending against, cryptoassets. Banks should instead simply expand into this new asset class by providing their core competencies of custody, asset-servicing, and escrow. The objective is to foster a regulated environment appropriately surveilling and overseeing illicit cryptoasset activity risks and not to dissuade well-regulated banks from providing cryptoasset services.

Similar to how banks enable storage of physical assets in safe deposit boxes or vaults off-balance sheet, private keys associated with cryptoassets should be held in cold storage by the custodian for the benefit

³ Financial Action Task Force (FATF), "Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers". October 2021.

(<https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>)

⁴ Basel Committee Charter. Updated 5 June 2018. (<https://www.bis.org/bcbs/charter.htm>)

⁵ Basel Committee on Banking Supervision (BCBS) Consultative Document, "Prudential Treatment of Cryptoasset Exposures". June 2021. (<https://www.bis.org/bcbs/publ/d519.htm>)

of bank customers. Until some form of regulatory insurance is provided by governments, additional protection, such as private asset insurance, should also be strongly considered to guard against theft or other cybercrime activities. The asset-to-insurance coverage should be the focus to protect consumers.

The need for a calculation to hold capital reserves against cryptoassets is wholly unnecessary and misguided if banks' cryptoasset-related services are limited to custody and staking. Unregulated cryptoasset activities will continue in inadequate or unregulated environments. Capital reserve requirements create unnecessary hurdles for banks desiring to provide off-balance sheet cryptoasset services.

The regulatory oversight authority applied to traditional custodial banking activities should simply extend to cryptoassets. If the status quo of insufficient regulation continues, non-bank entities and bad actors will continue to exploit existing vulnerabilities created through inconsistent, self-regulated governance. The use of cryptoassets to circumvent traditional funds transfer and monetary transmission controls will continue to increase as more participants enter the marketplace. Regulatory arbitrage opportunities must be significantly reduced by clearly defining the role of banks as the most well-positioned global entities to safely and soundly offer cryptoasset services to consumers.

Approving banks to be the appropriate entities for offering cryptoasset services to customers is in the best interest of consumer protection and ensures financial system stability. Banks are the most secure, practical, and scrutinized environment for offering cryptoasset services in a regulatory-compliant manner because of the following characteristics on which their foundations are established:

- Banking regulations are interconnected across global financial systems
- Banks consider consumer protection paramount in establishing trust
- Banks are held to the highest governance and risk management standards
- Core banking services, such as asset custody, servicing, and escrow, are agnostic to customer asset types (such as cash, securities, real estate, and cryptoassets) as long as proper technology requirements are in place
- Banks' recordkeeping and reporting obligations are pillars of their ongoing transaction monitoring requirements
- Banks have fiduciary responsibilities to their customers
- Banks are required to identify, monitor, and report suspicious activities
- Banks have a regulatory foundation rooted in their "culture of compliance"

Similar to other countries, the United States currently regulates bearer assets, such as traditional fiat currencies, through its Bank Secrecy Act (BSA). The BSA is technology-neutral and follows a risk-based approach. All BSA-regulated entities ("covered entities") in the U.S. financial system are obligated to implement an anti-money laundering (AML) program, which must include a customer identification program (CIP). Covered entities must identify and validate beneficial owners, perform customer due

diligence (CDD), and demonstrate full compliance with “Know Your Customer” (KYC) requirements.⁶ Cryptoassets should likewise be thoroughly vetted before being brought inside the “walled-off garden” of the banking system and then continuously monitored afterward.

Banks should employ several risk controls to properly intake the bearer cryptoassets, including

1. Cryptoasset Risk Committees (CARCs)
2. Blockchain Transaction Analysis (BTA)
3. Cryptoasset to Insurance Ratio Coverage
4. Cryptoasset Education and a “Culture of Compliance”

1. Cryptoasset Risk Committees (CARCs):

Each bank providing cryptoasset services should add to their risk committee specific and specialized crypto expertise and form a Cryptoasset Risk Committee (CARC) responsible for overseeing all risks associated with offering cryptoasset services. The CARC should be appointed by the Board of Directors of a bank to assist the risk group in fulfilling its responsibilities by providing oversight of a bank’s policies and management activities relating to the identification, assessment, measurement, and management of a bank’s risks related to offering cryptoasset services. In addition, the CARC should be charged with the following:

- Assessing the eligibility of cryptoassets to be considered for custody services
- Assessing the adequacy of and ensuring compliance with a bank’s overall compliance and risk policies
- Maintaining an active list of supported cryptoassets which is reviewed on an ongoing basis by the CARC and other stakeholders of a bank

Assessment factors may include asset quality, liquidity, total market capitalization, protocol strength, regulatory classification, creation/issuance methodology, governance, usage, or technological design.

2. Blockchain Transaction Analysis (BTA):

The transparency of blockchain technology and the ability to analyze the history of all transactions since inception enables a high level of regulatory oversight to identify illicit activities in real-time. A rigorous process described as “Blockchain Transaction Analysis (BTA)” enables covered entities to uphold regulatory obligations by conducting automated and forensic analyses on the universe of all blockchain transactions and assets. BTA can assess the provenance of cryptoassets and their transactional risk cohort activities. A comprehensive BTA process identifies the source of assets and examines wallet associations for interactions with illicit activities such as terrorist financing, human trafficking, sanction evasion, ransomware, and child abuse material. Groups of wallets with similar behavioral associations can be monitored in real-time and clustered to ensure the integrity and safety of assets being transmitted. The concept of KYC can thus be extended to “Know Your Digital Asset” (KYDA) and “Know Your Digital Asset Transaction” (KYDAT) to increase regulatory efficacy.

⁶ 31 C.F.R. § 1010.410(f).

Banks can use BTA to apply KYC, KYDA, and KYDAT during the initial vetting, approval, and onboarding process to establish a more detailed profile of a customer. After examining all cryptoassets and the history of all associated transactions, banks can determine whether potential customers and their corresponding wallets and activities meet regulatory standards. Comprehensive risk profiles can be created by assigning customized risk scoring metrics to the activities associated with specific bank customers and their transactions. This rigorous level of due diligence serves as the baseline for detecting suspicious or unusual activity. Those customers who are approved for onboarding must then be continually monitored to mitigate risks of future illicit activities. Banks can use BTA to conduct real-time, 24/7 surveillance for suspicious activities through block-by-block monitoring of how customers transact and transfer their cryptoassets.

The analysis of blockchain data elevates a bank's ability to develop more granular insight into a customer's behavior which strengthens the overall security of the monetary system. Given every transaction that has ever occurred is recorded and immutable, blockchain technology is a powerful tool for banks to combat money laundering and other illicit financing activities.

Figure 1: Using Blockchain Transaction Analysis (BTA) to Vet and Onboard Potential Customers

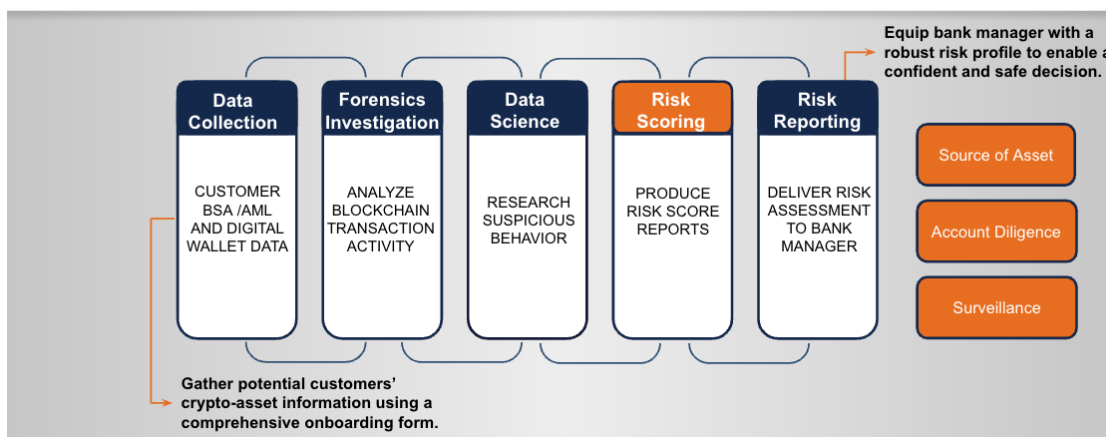
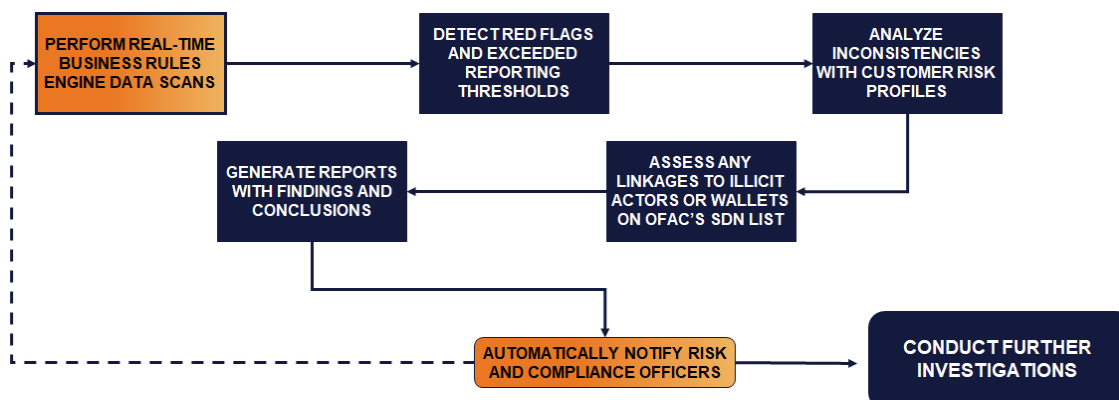


Figure 2: How Blockchain Transaction Analysis (BTA) Continuously Monitors for Suspicious or Unusual Activities, Significant Funds Transfers, and Associations with Illicit Entities



Once inside the banking system, consumer protections must be prioritized so cryptoassets are monitored, insured, and placed into segregated accounts protecting them from creditors in the event of custodian bankruptcy. A resilient operational infrastructure would be needed to create risk profiles, identify suspicious behaviors and irregular activities, approve the onboarding and custody of new types of cryptoassets, educate and certify cryptoasset handlers, implement robust network security and encryption, ensure hardened physical security and storage of cryptoasset wallets, and comply with recordkeeping and reporting requirements.

Custodians must also implement protections that limit cryptoassets' exposure to liability in the event of custodian bankruptcy. Such protections to shield cryptoassets can be incorporated through internal and external safeguards. For example, segregating customers' cryptoassets from general omnibus accounts and ensuring a proper wallet technology stack protect customers in the event of bankruptcy. External safeguards include ensuring cryptoassets remain off-balance sheet for customer protection, and conducting appropriate due diligence if engaging third-party vendors given the current lack of crypto expertise inside the banking system.

3. Cryptoasset to Insurance Ratio Coverage:

Priority and emphasis must also be given to consumer protections. Cryptoasset holders may desire to secure their holdings in digital cold storage within the banking system, similar to how customers seek to hold valuable physical assets inside safety deposit boxes. Technological and contractual protections should safeguard consumers' cryptoassets, so they are not tied to a bank's general accounts. A secure technology stack will ensure security procedures are in place to protect customers' cryptoassets and private keys in all aspects of permission-based protocols. Customers can also mitigate risks of their cryptoassets being compromised or stolen by purchasing private insurance. This practice is conceptually similar to the guidance provided by the United States Federal Deposit Insurance Corporation (FDIC), which recommends bank customers consult their homeowner's or renter's policy provider if they seek insurance coverage on physical assets held in safe deposit boxes.⁷

4. Cryptoasset Education and a "Culture of Compliance":

To promote a "culture of compliance," banks should offer a robust education program that provides foundational knowledge of cryptoassets and blockchain technology. Formal coursework, audio and visual content, informational presentations, and industry articles will all provide a thorough comprehension of the cryptoasset services banks are choosing to provide to their customers. Banks should implement a certification program and bi-annual requirements for employees to demonstrate an understanding of key concepts, methodologies, and risks.

⁷ Federal Deposit Insurance Corporation (FDIC), "FDIC Consumer News - Winter 2018". Updated 29 March 2018. (<https://www.fdic.gov/consumers/consumer/news/cnwin18/fivethings.html>)

Summary:

As emphasized earlier, the conversation should focus on how to properly bring cryptoassets into the regulated environment for custody and servicing, rather than on calculating reserve requirements for on-balance sheet at-risk scenarios.

Bringing cryptoassets into the banking system will enable the digital world to be fully compliant with already established laws, regulations, risk-based approaches, and best practices. Regulatory guidance should explicitly approve the mature and well-established banking system as the appropriate environment for offering and engaging in cryptoasset services. Doing so will preserve cryptoassets' inherent purpose and ease of use while ensuring they are in compliance with all existing AML/KYC standards to which banks are rigorously held.

The core banking pillars of compliance, governance, and risk management should be applied to cryptoassets. This framework is consistent with the guidance and approaches set forth by global regulatory bodies and will promote stability in the servicing of cryptoassets. Highly-regulated banking systems provide the safest and most scrutinized environment for cryptoasset service delivery through third-party providers equipped with technical knowledge and regulatory expertise.

Regulating cryptoassets inside banks will preserve financial stability without compromising innovation. In turn, the safety and security of the present global financial system will be ensured for all participants in the future digital environment.

VaultLink appreciates the opportunity to offer insight on the prudential treatment of cryptoasset exposure and is available to answer questions on the aspects highlighted.

Warm Regards,



James Slazas
Chief Executive Officer
VaultLink, Inc.

Government-Relations@Vault.Link