Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
Office of the Comptroller of the Currency

Crypto-Asset Safekeeping by Banking Organizations

The Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (Board), and Federal Deposit Insurance Corporation (FDIC) (collectively, the agencies) are issuing this statement for banking organizations[1] that provide or are considering providing safekeeping for crypto-assets.[2] For purposes of this statement, "safekeeping" is defined as the service of holding an asset on a customer's behalf.[3] The agencies recognize that crypto-asset custodians may provide other custody services[4] while safekeeping crypto-assets. This statement focuses on safekeeping. This statement discusses how existing laws, regulations, and risk-management principles[5] apply to this activity, and does not create any new supervisory expectations.

Banking organizations may provide safekeeping for crypto-assets in a fiduciary or a non-fiduciary capacity.[6] Banking organizations that provide crypto-asset safekeeping in a fiduciary capacity must comply with 12 CFR 9 or 150, as applicable, state laws and regulations, and any other applicable legal provisions, such as the instrument that created the fiduciary relationship. A banking organization providing safekeeping for crypto-assets in a fiduciary capacity—such as a trustee, an executor of a will, an administrator of an estate, or an investment advisor—has the authority to manage them in the same way banking organizations manage other assets they hold as fiduciaries.

---

[1] For the OCC, "banking organizations" includes national banks, Federal savings associations, and Federal branches and agencies of foreign banks. For the Board, "banking organizations" includes all U.S. bank holding companies, state member banks, Edge and agreement corporations, and uninsured state-licensed branches and agencies of foreign banks. For the FDIC, "banking organizations" includes all insured state nonmember banks, insured state-licensed branches of foreign banks, and insured state savings associations.

[2] For the purposes of this statement, a crypto-asset generally refers to any digital asset implemented using cryptographic techniques.

[3] By contrast, "custody" encompasses all the services a banking organization may provide in relation to assets held on a customer's behalf. See OCC Interpretive Letter 1170 (July 22, 2020) (IL 1170) and the "Custody Services" booklet of the *Comptroller's Handbook*.

[4] Id.

[5] See Interagency Guidelines Establishing Information Security Standards, 12 CFR 30 Appendix B, 12 CFR 208 Appendix D-2; 12 CFR 225 Appendix F ("Information Security Standards").

[6] Safekeeping services provided by a banking organization in a non-fiduciary capacity are established by the client contract. See the "Custody Services" booklet of the *Comptroller's Handbook*.

General Risk Management Considerations

Safekeeping for crypto-assets entails controlling the cryptographic keys associated with the crypto-asset in a manner that complies with applicable laws and regulations. As with all new products, services, and activities, banking organizations should consider potential risks prior to offering crypto-asset safekeeping.[7] An effective risk assessment would consider such things as the banking organization's (1) core financial risks given the strategic direction and business model; (2) ability to understand a complex, evolving, and potentially unfamiliar asset class, including by keeping abreast of industry leading practices;[8] (3) ability to ensure a strong control environment; and (4) contingency plans to address any unanticipated challenges in effectively providing services. Given the complexities of crypto-asset safekeeping, a banking organization's board, officers, and employees should have the requisite knowledge and understanding of crypto-asset safekeeping services to establish adequate operational capacity and appropriate controls to conduct the activity in a safe and sound manner and in compliance with applicable laws and regulations.

A banking organization that is contemplating providing safekeeping for crypto-assets should consider the evolving nature of the crypto-asset market, including the technology underlying the crypto-assets, and implement a risk governance framework that appropriately adapts to relevant risks. Providing crypto-asset safekeeping services may entail significant resources and attention, such as developing or procuring new technology, establishing a strong control environment, and ensuring staff have appropriate technical expertise. In addition, crypto-assets may experience price volatility, which could affect the demand for safekeeping services and the value of assets held. Furthermore, rapid evolution in the market could affect the technology used to provide safekeeping services.

Cryptographic Key Management

One of the primary risks of crypto-asset safekeeping is the possible compromise or loss of cryptographic keys or other sensitive information that could result in the loss of crypto-assets or the unauthorized transfer of the crypto-assets out of the banking organization's control.[9] In such cases, the banking organization faces the risk of being held liable for its customers' losses. Thus, effective safekeeping involves maintaining control of cryptographic keys and related sensitive information. In general, a banking organization assumes "control" for purposes of safekeeping a

---

[7] See OCC Bulletin 2017-43: "New, Modified, or Expanded Banking Products and Services: Risk Management Principles" (October 20, 2017).

[8] Banking organizations acting as fiduciaries are usually subject to heightened standards of care under applicable law in comparison to non-fiduciaries. Given the continued evolution of the crypto-asset sector, banking organizations managing crypto-assets as fiduciaries should keep abreast of leading practices to meet these heightened standards.

[9] Most crypto-assets are transferred through cryptographic key pairs made up of unique alphanumeric codes. Key pairs consist of a private key, which must be kept secret, and a public key, which may be shared in the context of a specific transaction. "Sensitive information" includes any information that could be used to transfer crypto-assets, including "seed phrases" used to regenerate keys and other backup material.

crypto-asset when it can reasonably demonstrate, consistent with the standard of care established by applicable law, that no other party—including the customer—has access to information sufficient to unilaterally transfer the crypto-asset out of the control of the banking organization. To establish initial control of a crypto-asset, a banking organization will usually require the asset to be transferred to the banking organization on the asset's underlying distributed ledger.[10] A banking organization would apply these same control standards to any sub-custodian used to perform crypto-asset safekeeping functions on the banking organization's behalf.[11]

Additional risk management issues related to cryptographic key management may include the secure generation of cryptographic keys[12] and contingency planning for lost or compromised keys. Effective risk management includes determining whether the banking organization's key management systems continue to be sufficient in light of technological developments,[13] resulting in the need for ongoing and dynamic product development and risk management programs. This may result in additional investment in technology to provide continued service.

Given the virtual nature of crypto-assets, and the potentially increased operational risks associated with crypto-asset safekeeping, a banking organization's cybersecurity environment should be a key focus of risk management.[14]

Additional Risk Management Considerations

Effective risk management also includes appropriate processes for determining the specific crypto-assets for which the banking organization will provide safekeeping,[15] especially as

[10] A banking organization that simply takes possession of existing cryptographic keys may not have control of the assets, since, for example, a customer may have retained copies of the keys or given them to others.

[11] See OCC Bulletin 2002–16, "Bank Use of Foreign-Based Third-Party Service Providers: Risk Management Guidance."

[12] A discussion of cryptographic key generation is beyond the scope of this document. Among other resources, the National Institute of Standards and Technology (NIST) has made recommendations on cryptographic key generation that may be an appropriate reference. Although keys may be generated by widely available cryptographic wallets, a banking organization may determine that such keys do not meet the requirements of its control environment.

[13] Cryptographic keys are often kept in "wallets," which exist in numerous forms and have various technical specifications. Generally, wallets exist on a continuum between "cold" wallets permanently disconnected from the internet and "hot" wallets that remain online at all times. As a general proposition, wallets that are more easily accessible may be less secure. See IL 1170. Not all wallets are compatible with all crypto-assets.

[14] OCC Bulletin 2023-22 "Cybersecurity Supervision Work Program," provides considerations aligned with existing supervisory guidance and the NIST Cybersecurity Framework.

[15] A banking organization should address the risks associated with a safekeeping account before acceptance. See, e.g., the OCC's "Custody Services" booklet of the *Comptroller's Handbook*. For fiduciary accounts administered by national banks and FSAs, these reviews are required by regulation. See 12 CFR 9.6(a); 12 CFR 150.200.

different types of crypto-assets may require different key management solutions.[16] Crypto-assets may feature software or hardware with which the banking organization may be inexperienced or that does not readily integrate with its current technology environment. Sound practices typically include performing a comprehensive analysis of each crypto-asset before safekeeping that crypto-asset, including for example, by identifying vulnerabilities and dependencies that could create material risks to the banking organization's safety and soundness. Effective risk management practices may also entail analyzing relevant technical, operational, strategic, market, legal, and compliance considerations relating to each crypto-asset and its underlying ledger as well as staying apprised of material developments specifically related to supported crypto-assets and their underlying ledgers.[17]

The provision of crypto-asset safekeeping entails the maintenance of an effective control environment, including appropriate risk management oversight and independent assurance conducted on a regular basis by individuals with the requisite expertise. Standard custodial risk management principles apply to the storage of cryptographic keys and sensitive information, but they may need to be tailored to the specific services provided.[18] Banking organizations should carefully consider the potential risks associated with the different types of account models (omnibus versus separate accounts) for safekeeping crypto-assets.[19]

Legal and Compliance Risk

Like all other banking activities, crypto-asset safekeeping relationships are subject to applicable Bank Secrecy Act/anti-money laundering (BSA/AML), countering the financing of terrorism (CFT), and Office of Foreign Assets Control (OFAC) requirements. [20] These laws and regulations require banking organizations to verify customer identity, perform due diligence to understand the nature and purpose of the customer relationship, perform ongoing monitoring to identify and report suspicious activity, block transactions in accordance with OFAC sanctions,

---

[16] Crypto-assets may have varying technical attributes, may exist on ledgers that are incompatible with each other, and may have been created through open-source or other less-formalized processes that would not require specific disclosures. Key management solutions refers to the tools, technologies, and systems used to implement a key management strategy.

[17] See, e.g., FFIEC Guidance on Risk Management of Free and Open Source Software (Oct. 21, 2004).

[18] 12 CFR 9 and 150 apply to the fiduciary activities of national banks and FSAs, respectively, including when they offer safekeeping in a fiduciary capacity.; For additional information, see IL 1170 and the "Custody Services" booklet of the *Comptroller's Handbook*.

[19] Omnibus accounts may permit greater efficiencies but could also create larger targets for theft. A banking organization using a separate account model might hold individual customer keys in separate, dedicated wallets, which could require the generation and management of a greater number of key pairs.

[20] Banking organizations must establish and maintain procedures reasonably designed to assure and monitor compliance with BSA regulatory requirements, which should be commensurate with the institution's size, complexity, and business activities. See, e.g., 12 CFR 21.21, 208.63.

and follow the "Travel Rule."[21] The design features of distributed ledger technology may present challenges for achieving or maintaining compliance with certain of these requirements[22] if compliance depends on review of the identifying information (for example, name and address) related to a transaction.[23] Before offering crypto-asset safekeeping, a banking organization should appropriately involve its BSA officer, board of directors (or designated committee), and senior management in assessing potential money laundering, terrorist financing, and other illicit financial activity risks.

Crypto-asset safekeeping may involve elevated levels of compliance and legal risks due to the evolving regulatory landscape. Banking organizations seeking to engage in these activities should ensure the activities are conducted consistent with all applicable laws and regulations.[24] A well-written customer agreement, outlining clearly defined duties and responsibilities of the parties, is an important tool to manage the risks of crypto-asset safekeeping and may be used to address issues specific to this service, such as on-chain governance and voting,[25] forks,[26] airdrops,[27] probabilistic settlement that may be characteristic of permissionless blockchains,[28] the method of holding the assets (cold/hot/hybrid storage), the use of a sub-custodian(s), and the use of smart contracts.[29]

Crypto-asset safekeeping activities present a risk that the customer could be misinformed of the banking organization's role in the arrangement. Banking organizations may be able to mitigate this risk by providing clear, accurate, and timely information to customers about their crypto-asset safekeeping activities, including the banking organization's role in any governance or other voting matter related to the crypto-asset. A banking organization providing crypto-asset

---

[21] 31 CFR 103.33(g).

[22] 31 CFR 1010.410.

[23] See the Financial Action Task Force (FATF) publication "Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs."

[24] See the "Corporate and Risk Governance" booklet of the *Comptroller's Handbook*.

[25] On-chain governance is an integrated voting system for managing and implementing changes to crypto-asset blockchains.

[26] A "fork" occurs when not all participants support a change to the rules governing a crypto-asset's ledger. This effectively causes the ledger to split in two, with one ledger following the new rules and one following the old rules.

[27] An "airdrop" is a distribution of crypto-assets to wallets, typically for no financial consideration.

[28] In permissionless blockchains, settlement can be probabilistic, meaning the probability of a transaction being revoked or reversed converges to zero but never fully reaches it as time progresses.

[29] Smart contracts are programs stored on a blockchain that are automatically executed when predetermined terms and conditions are met. If the crypto-assets under custody depend on smart contracts, a banking organization should exercise appropriate governance and oversight of these smart contracts throughout their life cycle.

safekeeping must follow applicable recordkeeping and reporting requirements. Evolving tax laws may also affect customer obligations in relation to crypto-asset safekeeping.

Third-Party Risk Management

In certain circumstances, a banking organization may choose to contract with one or more third-party sub-custodians or other service providers (e.g., technology providers, cash management) to provide safekeeping for crypto-assets.[30] A banking organization employing a sub-custodian for crypto-asset safekeeping should understand the benefits and risks associated with engaging sub-custodians, applicable laws and regulations, and relevant third-party risk management guidance.[31]

Third-party risk management processes should be commensurate with the risk posed by the activity performed. Subject to the terms and conditions in the customer agreement, a banking organization is responsible for the activities performed by the sub-custodian.[32] This responsibility includes decisions around selecting the crypto-assets for which custodial services will be provided, even if the sub-custodian assists in analyzing the crypto-assets and their underlying ledgers on the banking organization's behalf. Conducting due diligence before selection of a sub-custodian is an important part of sound risk management, and includes evaluating the effectiveness of the sub-custodian's cryptographic key-management solution, including polices, processes, and internal controls, as well as its adherence to standard safekeeping risk management practices.[33] Appropriate risk management may include analyzing the potential treatment of customer assets held at the sub-custodian in the event of insolvency or operational disruptions and evaluating the appropriateness of the sub-custodian's risk management and recordkeeping practices.[34]

A banking organization that opts to provide crypto-asset safekeeping directly without using a sub-custodian may still choose to use third parties in other ways, including through the use of

---

[30] These third parties, or sub-custodians, may provide services through various models, including API-based integrations or by white labeling their underlying platform to the client.

[31] See OCC Bulletin 2002–16.

[32] A banking organization could consider including in contracts with a sub-custodian the circumstances under which the banking organization will be notified of material events. In the context of safekeeping crypto-assets, this could include any potential compromise of cryptographic keys or sensitive information, any necessary use of backup information, or material transaction errors that cannot be reversed.

[33] These may include segregation of the sub-custodian's crypto-assets from those of the banking organization, dual control, separation of duties, and other appropriate technical or physical controls.

[34] For example, it would be inconsistent with appropriate risk management for a sub-custodian to commingle its own assets with assets being held on behalf of the banking organization, as this could risk the crypto-assets being treated as property of the sub-custodian in certain circumstances, such as bankruptcy. Similarly, if a sub-custodian fails to maintain proper recordkeeping or contingency planning, an operational disruption could prevent the banking organization's customers from being able to access their crypto-assets, potentially for an extended period of time or even permanently.

third-party technology. Effective risk management of third-party technology in this context will generally include weighing the risks of purchasing third-party software or hardware versus maintaining such software or hardware as a service.

Audit

Audit programs are essential to effective risk management and internal control systems. As such, a banking organization's audit program should provide appropriate coverage over the banking organization's crypto-asset safekeeping activities, including third-party risk management as applicable. A crypto-asset safekeeping audit should address the nuances of crypto-assets, including an assessment of cryptographic key generation, storage, and deletion; controls related to transfer and settlement of customer assets; and the sufficiency of relevant information technology systems.[35] Audits may assess management and staff expertise, including the ability to identify and control the unique risks associated with crypto-asset products and services, as well as the implementation of safekeeping controls. When audit expertise does not exist within the banking organization, management should engage appropriate external resources, with sufficient independence, to assess crypto-asset safekeeping operations.

[35] Insured depository institutions should have an internal audit system appropriate to the size of the institution and the nature and scope of the institution's activities. Among other things, the internal audit system should provide for adequate monitoring of the system of internal controls through an internal audit function. For an institution whose size, complexity or scope of operations does not warrant a full-scale internal audit function, a system of independent reviews of key internal controls may be used. See Interagency Guidelines Establishing Standards for Safety and Soundness § II.B, 12 CFR 30 Appendix A, 12 CFR 208 Appendix D-1.