



Interpretive Letter #1170
July 2020

July 22, 2020

Re: Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers

Dear [],

I. Introduction and Summary Conclusion

This letter responds to your request regarding the authority of a national bank to provide cryptocurrency custody services for customers. For the reasons discussed below, we conclude a national bank may provide these cryptocurrency custody services on behalf of customers, including by holding the unique cryptographic keys associated with cryptocurrency.¹ This letter also reaffirms the OCC's position that national banks may provide permissible banking services to any lawful business they choose, including cryptocurrency businesses, so long as they effectively manage the risks and comply with applicable law.²

II. Background

Cryptocurrencies—also known as “digital currencies” or “virtual currencies”—are designed to work as a medium of exchange and are created and stored electronically.³ Depending on the type of cryptocurrency, it may have characteristics of either fiat money or money backed by some underlying asset(s) or claim(s). Fiat money refers to instruments that do not have intrinsic value but that individuals and institutions are willing to use for purposes of purchase and investment because they are issued by a government. Government-issued currencies, including the U.S. dollar following abandonment of the gold standard, are traditional fiat money. Some types of cryptocurrencies may have similar characteristics as fiat money

¹ As discussed further below, this conclusion also applies to Federal savings associations (FSAs).

² Banks determine the levels and types of risks that they will assume. Banks that operate in compliance with applicable law, properly manage customer relationships and effectively mitigate risks by implementing controls commensurate with those risks are neither prohibited nor discouraged from providing banking services. As the federal banking agencies have previously stated, banks are encouraged to manage customer relationships and mitigate risks based on customer relationships rather than declining to provide banking services to entire categories of customers. See Joint Statement on Risk-Focused Bank Secrecy Act/Anti-Money Laundering Supervision, at 2 (July 22, 2019), available at <https://www.occ.gov/news-issuances/news-releases/2019/nr-ia-2019-81a.pdf>.

³ The term “cryptocurrency” as used in this letter also encompasses digital assets that are not broadly used as currencies.

because they are not backed by any other assets. Other types of money may be backed by assets (such as a commodity). The U.S. dollar was a type of asset-backed money prior to abandonment of the gold standard. Some types of cryptocurrencies may have similar characteristics to this type of money. For example, stablecoin is a type of cryptocurrency that is backed by an asset, such as a fiat currency or a commodity.

While cryptocurrency shares certain characteristics of these traditional types of money, the exchange mechanism is novel. The exchange mechanism for most cryptocurrencies is based on two separate underlying technologies. The first is advanced cryptography, which is used to protect information related to the cryptocurrency. Cryptography allows the creation of digital code that generally cannot be altered without the permission of the creator.

The second type of technology underlying cryptocurrencies' exchange mechanism is known as "distributed ledger technology," and consists of a shared electronic database where copies of the same information are stored on multiple computers. This shared database functions as both a mechanism to prevent tampering and as a way to add new information to the database. Information will not be added to the distributed ledger until consensus is reached that the information is valid. Furthermore, attempts to change the information on one computer will not impact the information on the other computers. Some distributed ledgers are known as "blockchains" because the transactions stored on the ledger are sequentially grouped together in blocks, thus creating a chronological record of all transactions to that point.⁴

Cryptocurrencies do not exist in any physical form. They exist only on the distributed ledger on which they are recorded. A particular unit of cryptocurrency is assigned to a party through the use of a set of unique cryptographic keys. Those keys allow that party to transfer the cryptocurrency to another party.⁵ If those keys are lost, a party will generally be unable to access its cryptocurrency. Furthermore, if a third party gains access to those keys, that third party can use the keys to transfer the cryptocurrency to themselves.

The first widely-adopted cryptocurrency, Bitcoin, was introduced in 2008.⁶ Since the creation of Bitcoin, hundreds of additional virtual currencies have been created, all of which have different characteristics and potential uses. Some cryptocurrencies may have characteristics of currency or cash, including as a medium of exchange, but with a new exchange mechanism

⁴ See, e.g., How does Bitcoin work?, bitcoin.org (last visited July 20, 2020), <https://bitcoin.org/en/how-it-works> (describing Bitcoin's shared public ledger as a blockchain).

⁵ See, e.g., FAQs, How does Bitcoin work?, bitcoin.org (last visited July 20, 2020), <https://bitcoin.org/en/faq#how-does-bitcoin-work> (from a user perspective, Bitcoin is nothing more than an application that provides a digital wallet); How does Bitcoin work?, bitcoin.org (last visited July 20, 2020), <https://bitcoin.org/en/how-it-works> (describing use of keys to sign transactions); How do Bitcoin Transactions Work?, Coindesk.com (last visited July 20, 2020), <https://www.coindesk.com/information/how-do-bitcoin-transactions-work/>.

⁶ See Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, available at <https://bitcoin.org/bitcoin.pdf> (Bitcoin Whitepaper).

(i.e., electronic transfer without an intermediary). This letter expresses no opinion on whether cryptocurrencies may be exchange for purposes of 12 U.S.C. 24(Seventh).

Cryptocurrencies have been used for a variety of payment and investment activities. Bitcoin remains the most widely used and valuable cryptocurrency, with a current market capitalization approximately \$170 billion.⁷ Bitcoin is now accepted as payment by thousands of merchants worldwide; customers may even purchase Bitcoin for cash at various retail locations.⁸ Contracts on Bitcoin futures have been established and options on Bitcoin futures are now trading.⁹ The SEC recently approved a Bitcoin futures fund.¹⁰ Although transactions in cryptocurrencies can occur directly between parties via decentralized, peer-to-peer cryptocurrency transactions, many cryptocurrencies may also be traded through centralized, online cryptocurrency exchanges where parties trade one cryptocurrency for another or trade for fiat currencies such as the U.S. dollar through a financial intermediary.¹¹ Some centralized cryptocurrency exchanges have obtained state banking licenses as trust banks.¹²

⁷ See Top 100 Cryptocurrencies by Market Capitalization, Coinmarketcap.com, (last visited July 20, 2020), <https://coinmarketcap.com/>.

⁸ See Maddie Shepherd, How Many Businesses Accept Bitcoin? (last visited July 20, 2020), <https://www.fundera.com/resources/how-many-businesses-accept-bitcoin> (reporting that nearly 15,174 merchants worldwide accept bitcoin as of December 31, 2019). See also Turner Wright, LibertyX Allows BTC Purchases in Cash at 7-Eleven, CVS, and Rite Aid, Cointelegraph.com (June 23, 2020), <https://cointelegraph.com/news/libertyx-allows-btc-purchases-in-cash-at-7-eleven-cvs-and-rite-aid>.

⁹ See CME Group, Bitcoin futures and options on futures (last visited July 20, 2020), <https://www.cmegroup.com/trading/bitcoin-futures.html>.

¹⁰ In December of 2019, the SEC approved an investment fund that invests in bitcoin futures contracts. See Kevin Helms, SEC Approves Bitcoin Futures Fund, Bitcoin.com (Dec. 7, 2019), <https://news.bitcoin.com/sec-approves-bitcoin-futures-fund/>.

¹¹ See Top Cryptocurrency Spot Exchanges, Coinmarketcap.com (last visited July 20, 2020), <https://coinmarketcap.com/rankings/exchanges/> (listing over 300 separate cryptocurrency exchanges). “Decentralized” in this context refers to the lack of a third-party intermediary; instead, buyers and sellers exchange cryptocurrency directly. “Centralized” refers to a third-party intermediary (such as a banking organization) that facilitates trades between buyers and sellers. See Dylan Dedi, Centralized Cryptocurrency Exchanges, Explained, Cointelegraph.com (March 10, 2018), <https://cointelegraph.com/explained/centralized-cryptocurrency-exchanges-explained>.

¹² See, e.g., New York Department of Financial Services, Financial Services Superintendent Linda A. Lacewell Announces Grant of DFS Trust Charter to Enable Fidelity to Engage in New York’s Growing Virtual Currency Marketplace (Nov. 19, 2019), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1911191; New York Department of Financial Services, NYDFS Grants Charter to “Gemini” Bitcoin Exchange founded by Cameron and Tyler Winklevoss (Oct. 5, 2015), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1510051.

As of June 2020, a majority of states have adopted laws and regulations pertaining to cryptocurrencies.¹³ Recent survey evidence suggests that almost 40 million Americans own cryptocurrencies.¹⁴ Institutional investors also have invested in cryptocurrencies.¹⁵

III. The Proposed Activities

The bank has proposed to offer cryptocurrency custody services to its customers as part of its existing custody business. We understand that there is a growing demand for safe places, such as banks,¹⁶ to hold unique cryptographic keys associated with cryptocurrencies on behalf of customers and to provide related custody services.¹⁷ These services are in demand for several reasons. First, because the underlying keys to a unit of cryptocurrency are essentially irreplaceable if lost, owners may lose access to their cryptocurrencies as a result of misplacing their keys, resulting in significant losses of value.¹⁸ Second, banks may offer more secure

¹³ Numerous states have adopted or proposed legislation that relates to cryptocurrency, usually exempting digital currencies from money transmitter licensing requirements and securities laws or recognizing that records secured through blockchain technology have the same legal status as written records. See Dale Werts, *Blockchain & Cryptocurrency: State Law Roundup 2019* (July 18, 2019), <https://www.jdsupra.com/legalnews/blockchain-cryptocurrency-state-law-59816/>.

¹⁴ See Helen Partz, *11% of Americans Own Bitcoin, Major Awareness Increased Since 2017*, Yahoo! Finance (Apr. 30, 2019), <https://finance.yahoo.com/news/11-americans-own-bitcoin-major-164400483.html>.

¹⁵ See, e.g., Olga Kharif, *Fidelity Says a Third of Big Institutions Own Crypto Assets* (June 9, 2020), BNN Bloomberg, <https://www.bnnbloomberg.ca/fidelity-says-a-third-of-big-institutions-own-crypto-assets-1.1447708> (reporting that, according to a survey by Fidelity Investments, 36 percent of institutional investors in the U.S. and Europe report holding crypto assets); Luke W. Vrotsos and Cindy H. Zhang, *Harvard Invests Millions in New Cryptocurrency*, *The Harvard Crimson*, April 12, 2019, available at <https://www.thecrimson.com/article/2019/4/12/hmc-crypto-investment/>; Jonathan Watkins, *The Institutional Crypto Backers: How Endowments are Allocating to Cryptocurrency Investments* (Apr. 2019), available at <https://www.globalcustodian.com/wp-content/uploads/2019/04/The-institutional-crypto-backers-How-endowments-are-allocating-to-cryptocurrency-investments.pdf>.

¹⁶ States are beginning to recognize the growing demand for safe locations to hold cryptocurrencies. At least one state has passed legislation and promulgated regulations allowing state-chartered banks to opt-in to providing custody services for digital assets. See, e.g., Wyo. Admin. Code 021.0002.19. These regulations were promulgated pursuant to Wyoming Statute (“W.S.”) 34-29-104, Digital asset custodial services. Under W.S. 34-29-104, banks that elect to provide digital asset custodial services must comply with all provision of W.S. 34-29-104 and the new regulations (known as the enhanced digital custody opt-in regime). The states of Hawaii and Rhode Island have also recently proposed legislation on digital asset custody. See Hawaii SB2594 (introduced Jan. 17, 2020), available at https://www.capitol.hawaii.gov/measure_indiv.aspx?billtype=SB&billnumber=2594&year=2020; Rhode Island HB7989, available at <https://legiscan.com/RI/bill/H7989/2020> (introduced Mar. 11, 2020).

¹⁷ See, e.g., Melanie Kramer, *Will Cryptocurrency Custody Services Fuel Institutional Demand?*, Bitcoinist.com (July 22, 2018), <https://bitcoinist.com/crypto-custody-services-fuel-institutional-demand/> (describing how institutional investors may feel more comfortable maintaining cryptocurrencies in the custody of banks than exchanges).

¹⁸ One empirical analysis of the bitcoin blockchain calculated that roughly 20% of all currently outstanding bitcoin have been lost. See Jeff John Roberts and Nicolas Rapp, *Nearly 4 Million Bitcoins Lost Forever, New Study Says*, *Fortune* (Nov. 25, 2017), available at <http://fortune.com/2017/11/25/lost-bitcoins/>; see also, Alison Sider and Stephanie Young, *Good News! You Are a Bitcoin Millionaire. Bad News! You Forgot Your Password*, *The Wall Street Journal* (Dec. 19, 2017), available at <https://www.wsj.com/articles/good-news-you-are-a-bitcoin-millionaire->

storage services compared to existing options.¹⁹ Third, some investment advisers may wish to manage cryptocurrencies on behalf of customers and may wish to utilize national banks as custodians for the managed assets.

Providing custody for cryptocurrencies would differ in several respects from other custody activities. Cryptocurrencies are generally held in “wallets,” which are programs that store the cryptographic keys associated with a particular unit of digital currency. Because digital currencies exist only on the blockchain or distributed ledger on which they are stored, there is no physical possession of the instrument. Instead, the right to a particular unit of digital currency is transferred from party to party by the use of unique cryptographic keys. Therefore, a bank “holding” digital currencies on behalf of a customer is actually taking possession of the cryptographic access keys to that unit of cryptocurrency. Those keys are held in a “wallet” that protects the keys from discovery by a third party.²⁰ Keys can be stored in “hot” wallets or “cold” wallets. Hot wallets are connected to the internet, which makes them convenient to access but more susceptible to hacking. Cold wallets are physical devices that are completely offline (for example, paper or hardware wallets that can be stored in a physical vault). Currently, cold storage is considered the most secure method of storing cryptographic keys.²¹

The OCC recognizes that, as the financial markets become increasingly technological, there will likely be increasing need for banks and other service providers to leverage new technology and innovative ways to provide traditional services on behalf of customers. By providing such services, banks can continue to fulfill the financial intermediation function they have historically played in providing payment, loan and deposit services. Through intermediated exchanges of payments, banks facilitate the flow of funds within our economy and serve important financial risk management and other financial needs of bank customers.²²

[bad-news-you-forgot-your-password-1513701480](#) (reporting numerous examples of individuals losing access to significant value in bitcoin as a result of lost passwords).

¹⁹ Some cryptocurrency exchanges that store access to cryptocurrency on behalf of customers have proven vulnerable to hacking and theft. See Steven Russolillo and Eun-Young Jeong, [Cryptocurrency Exchanges Are Getting Hacked Because It's Easy](#), The Wall Street Journal (July 16, 2018), available at <https://www.wsj.com/articles/why-cryptocurrency-exchange-hacks-keep-happening-1531656000> (detailing light security and regulatory gaps at some cryptocurrency exchanges).

²⁰ See, e.g., Aziz, [Guide to Cryptocurrency Wallets: Why Do You Need Wallets?](#) (last visited July 20, 2020) <https://masterthecrypto.com/guide-to-cryptocurrency-wallets/> (holding cryptocurrency at an exchange means having the exchange host the wallet).

²¹ See, e.g., [Hot wallet vs cold wallet in cryptocurrency storage](#), Coin Insider, <https://www.coininsider.com/hot-vs-cold-wallets-cryptocurrency/> (last visited July 16, 2020).

²² See, e.g., OCC Interpretive Letter No. 1110 (Jan. 30, 2009); OCC Interpretive Letter No. 1101 (July 7, 2008); OCC Interpretive Letter No. 1079 (April 19, 2007).

IV. Discussion

National banks have long provided safekeeping and custody services for a wide variety of customer assets, including both physical objects and electronic assets. These functions of national banks are well established and extensively recognized as permissible activities for national banks.²³ The OCC concludes, for the reasons discussed below, that providing cryptocurrency custody services, including holding the unique cryptographic keys associated with cryptocurrency, is a modern form of these traditional bank activities.

Safekeeping services are among the most fundamental and basic services provided by banks.²⁴ Bank customers traditionally used special deposit and safe deposit boxes for the storage and safekeeping of a variety of physical objects, such as valuable papers, rare coins, and jewelry.²⁵ As the banking industry entered the digital age, the OCC recognized the permissibility of electronic safekeeping activities. Specifically, the OCC has concluded that a national bank may escrow encryption keys used in connection with digital certificates,²⁶ finding that the key escrow service is a functional equivalent to physical safekeeping, except it uses electronic technology suitable to the digital nature of the item to be kept safe. The OCC has also concluded that a national bank may provide secure web-based document storage, retrieval and collaboration of documents and files containing personal information or valuable confidential trade or business information because these services are the electronic expression of traditional safekeeping services provided by banks.²⁷ The OCC codified these interpretive rulings in 12 CFR Part 7.²⁸

Traditional bank custodians frequently offer a range of services in addition to simple safekeeping of assets. For example, a custodian providing core domestic custody services for

²³ See OCC Conditional Approval 479 (July 27, 2001) (Conditional Approval 479). “Safekeeping” implies the basic service of a bank holding on to an asset for a customer (e.g., gold or securities). “Custody” is a broader term that may involve all aspects of bank services performed for customers in relation to items they are holding for them (i.e., processing, settlement, fund administration). Historically, banks only offered safekeeping services, which then evolved into banks providing custodial services to their customers. See Comptroller’s Handbooks on Custody Services (Jan. 2002) (Custody Handbook).

²⁴ Colorado Nat. Bank of Denver v. Bedford, 310 U.S. 41, 50 (1940) (finding that providing safe deposit boxes is “such a generally adopted method of safeguarding valuables [that it] must be considered a banking function authorized by Congress” under the National Bank Act). The safekeeping of valuable personal property is a traditional function that banks have performed since the earliest times. “Originally the business of banking consisted only in receiving deposits, such as bullion, plate and the like for safe-keeping until the depositor should see fit to draw it out for use. . . .” Oulton v. German Savings and Loan Soc’y, 84 U.S. 109, 118 (1872); see also Bank of California v. City of Portland, 157 Ore. 203, 69 P.2d 273 (1937).

²⁵ See Conditional Approval 479; Comptroller’s Handbook on Custody Services (Custody Handbook) (Jan. 2002) at page 15 (jewelry listed as one of the miscellaneous assets that banks hold via on-premises custody).

²⁶ See OCC Conditional Approval 267 (Jan. 12, 1998) (Conditional Approval 267).

²⁷ See Conditional Approval 479.

²⁸ See 12 CFR §§ 7.5002(a)(4) and 7.5005(a).

securities typically settles trades, invests cash balances as directed, collects income, processes corporate actions, prices securities positions, and provides recordkeeping and reporting services.²⁹ It is well-established that national banks may provide custody services to their customers in **either a fiduciary or non-fiduciary capacity**. 12 U.S.C. 92a expressly authorizes the OCC to grant fiduciary powers to national banks.³⁰ National banks may also provide non-fiduciary custody services to their customers.³¹ The OCC has determined national banks may act as non-fiduciary custodians pursuant to the business of banking and their incidental powers.³² OCC guidance has recognized that banks may hold a wide variety of assets as custodians, including assets that are unique and hard to value.³³ These custody activities often include assets that transfer electronically.³⁴ The OCC generally has not prohibited banks from providing custody services for any particular type of asset, as long as the bank has the capability to hold the asset and the assets are not illegal in the jurisdiction where they will be held.³⁵

Providing custody services for cryptocurrency falls within these longstanding authorities to engage in safekeeping and custody activities. As discussed below, this is a permissible form of a traditional banking activity that national banks are authorized to perform via electronic

²⁹ See Custody Handbook at 2.

³⁰ “The Comptroller of the Currency shall be authorized and empowered to grant by special permit to national banks applying therefor, when not in contravention of State or local law, the right to act as trustee, executor, administrator, registrar of stocks and bonds, guardian of estates, assignee, receiver, or in any other fiduciary capacity in which State banks, trust companies, or other corporations which come into competition with national banks are permitted to act under the laws of the State in which the national bank is located.” 12 U.S.C. 92a(a). 12 CFR Part 9 implements 12 U.S.C. 92a. The fiduciary capacities defined under Part 9 are “trustee, executor, administrator, registrar of stocks and bonds, transfer agent, guardian, assignee, receiver, or custodian under a uniform gifts to minors act; investment adviser, if the bank receives a fee for its investment advice; any capacity in which the bank possesses investment discretion on behalf of another; or any other similar capacity that the OCC authorizes pursuant to 12 USC 92a.” See 12 CFR 9.2(e).

³¹ National banks do not need the trust or fiduciary powers found in sections 92a to offer these custodial services. Thus, no trust powers are necessary in order to conduct these activities. See Conditional Approval 267.

³² See, e.g., Conditional Approval 267 (agency services such as custody that do not involve fiduciary powers are performed by banks as part of their incidental powers); OCC Interpretive Letter 1078 (April 19, 2007) (authority of national banks to engage in custody activities derives from general business of banking, and from incidental powers language in 12 U.S.C. § 24(Seventh)).

³³ See, generally, Comptroller’s Handbook, Unique and Hard-to-Value Assets (August 2012) (providing guidance on bank management of unique assets and listing examples of such assets, including real estate, closely held businesses, mineral interests, loans and notes, life insurance, tangible assets, and collectibles). See also Comptroller’s Handbooks on Custody Services (Jan. 2002) (Custody Handbook), Asset Management (Dec. 2000), Asset Management Operations and Controls (Jan. 2011), Retirement Plan Products and Services (Feb. 2014), Conflicts of Interest (Jan. 2015); OCC Bulletin 2013–29, “Third-Party Relationships—Risk Management Guidance” (Oct. 30, 2013).

³⁴ See Custody Handbook at 19, 70 (describing book-entry securities as securities that transfer electronically and stating that banks should assess their technological readiness to maintain a competitive position).

³⁵ See Custody Handbook at 7.

means.³⁶ Providing such services is permissible in both non-fiduciary and fiduciary capacities. A bank that provides custody for cryptocurrency in a non-fiduciary capacity would essentially provide safekeeping for the cryptographic key that allows for control and transfer of the customer's cryptocurrency. In most, if not all, circumstances, providing custody for cryptocurrency will not entail any physical possession of the cryptocurrency. Rather, a bank "holding" digital currencies on behalf of a customer is actually taking possession of the cryptographic access keys to that unit of cryptocurrency.³⁷ As described above, the OCC has found that the authority to provide safekeeping services extends to digital activities and, specifically, that national banks may escrow encryption keys used in connection with digital certificates because a key escrow service is a functional equivalent to physical safekeeping. Holding the cryptographic access key to a unit of cryptocurrency is an electronic corollary of these traditional safekeeping activities. The OCC's regulations in Subpart E of Part 7 explicitly authorize national banks to perform, provide or deliver through electronic means and facilities any activities that they are otherwise authorized to perform.³⁸ Because national banks are authorized to perform safekeeping and custody services for physical assets, national banks are likewise permitted to provide those same services via electronic means (*i.e.*, custody of cryptocurrency).³⁹

³⁶ 12 CFR 7.5002(a) provides that a national bank may perform, provide, or deliver through electronic means and facilities any activity, function, product, or service that it is otherwise authorized to perform, provide, or deliver. This regulatory provision is based on the longstanding "transparency doctrine," under which the OCC looks through the means by which a product is delivered and focuses instead on the authority of the national bank to offer the underlying product or service. *See* 67 FR 34992, 34996 (May 17, 2002). *See also* OCC Conditional Approval 369 (Feb. 25, 2000) (national bank may host a virtual mall consisting of a web page with links to third-party merchants arranged according to product or service offered); OCC Conditional Approval 304 (Mar. 5, 1999) (electronic bill presentment is part of the business of banking); Conditional Approval 267 (a national bank may store electronic encryption keys as an expression of the established safekeeping function of banks); OCC Conditional Approval 220 (Dec. 2, 1996) (the creation, sale, and redemption of electronic stored value in exchange for dollars is part of the business of banking because it is the electronic equivalent of issuing circulating notes or other paper-based payment devices like travelers checks).

³⁷ Banks may offer different methods of providing cryptocurrency custody services, depending on their expertise, risk appetite, and business models. Some banks may offer to store copies of their customers' private keys while permitting the customer to retain their own copy. Such services may be more akin to traditional safekeeping and would permit the customer to retain direct control over their own cryptocurrencies. Other banks may permit customers to transfer their cryptocurrencies directly to control of the bank, thereby generating new private keys which would be held by the institution on behalf of the customer. Such services may be more akin to traditional custody services, but as with traditional custody, would not permit the customer to maintain direct control of the cryptocurrency. Banks may also offer other custody models that may be appropriate. Banks acting as fiduciaries for cryptocurrency should consider how to ensure their custody models comply with requirements of 12 CFR 9.13 and 12 CFR 150.230-250.

³⁸ *See* 12 CFR 7.5002(a).

³⁹ The services national banks may provide in relation to the cryptocurrency they are custodying may include services such as facilitating the customer's cryptocurrency and fiat currency exchange transactions, transaction settlement, trade execution, recording keeping, valuation, tax services, reporting, or other appropriate services. A bank acting as custodian may engage a sub-custodian for cryptocurrency it holds on behalf of customers and should develop processes to ensure that the sub-custodian's operations have proper internal controls to protect the customer's cryptocurrency. *See, e.g.*, Custody Handbook at 15-16. As set forth below, banks should develop and implement new activities in accordance with OCC guidance.

To the extent that a national bank with trust powers conducts cryptocurrency custody activities in a **fiduciary capacity**, such activities would be permissible if conducted in compliance with **12 CFR Part 9, applicable state law**, and any other applicable law, such as the instrument that created the fiduciary relationship. A **national bank holding cryptocurrencies in a fiduciary capacity**—such as a trustee, an executor of a will, an administrator of an estate, a receiver, or as an investment advisor—would have the authority to manage them in the same way banks can manage other assets they hold as fiduciaries.⁴⁰

These conclusions apply equally to **federal savings associations (FSAs)**. Like national banks, FSAs may provide custody services in either a fiduciary or non-fiduciary capacity. The OCC may grant fiduciary powers to an FSA under 12 U.S.C. 1464(n).⁴¹ These fiduciary activities of an FSA must be conducted in compliance with 12 CFR Part 150. In addition, FSAs have authority to act as a non-fiduciary custodian under 12 U.S.C. 1464.⁴² Similar to national banks, FSAs are authorized to “use, or participate with others to use, electronic means or facilities to perform any function, or provide any product or service, as part of an authorized activity.”⁴³ Accordingly, for the same reasons described above with respect to national banks, providing custody services for cryptocurrency falls within an FSA’s established authority to provide custody services.

A national bank or FSA engaging in new activities should develop and implement those activities consistent with sound risk management practices and align them with the bank’s overall business plans and strategies as set forth in OCC guidance.⁴⁴ There may be services that banks may provide in connection with cryptocurrencies that are unique to cryptocurrency.⁴⁵ As with all other activities performed by national banks and FSAs, a national bank or FSA that provides cryptocurrency custody services must conduct these activities in a safe and sound

⁴⁰ National banks 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 cryptocurrency sector, banks managing cryptocurrency as fiduciaries should ensure they keep abreast of best practices to ensure they continue to meet these heightened standards.

⁴¹ 12 U.S.C. 1464(n)(1) states, “The Comptroller may grant by special permit to a Federal savings association applying therefor the right to act as trustee, executor, administrator, guardian, or in any other fiduciary capacity in which State banks, trust companies, or other corporations which compete with Federal savings associations are permitted to act under the laws of the State in which the Federal savings association is located.”

⁴² See Testimony of John Bowman, Chief Counsel, Office of Thrift Supervision, before the Senate Committee on Banking, Housing, and Urban Affairs (June 22, 2004) (HOLA allows thrifts to provide trust and custody services on the same basis as national banks).

⁴³ See 12 CFR 155.200(a).

⁴⁴ See OCC Bulletin 2017-43, “New, Modified, or Expanded Bank Products and Services: Risk Management Principles” (Oct. 20, 2017).

⁴⁵ Custody agreements are an important risk management tool and should clearly establish the custodian’s duties and responsibilities. See Custody Handbook at 8. The handling, treatment, and servicing of cryptocurrencies held in custody may raise unique issues that should be addressed in the agreement, such as (for example) the treatment of “forks” or splits in the code underlying the cryptocurrency being held.

manner, including having adequate systems in place to identify, measure, monitor, and control the risks of its custody services. Such systems should include policies, procedures, internal controls, and management information systems governing custody services. Effective internal controls include safeguarding assets under custody, producing reliable financial reports, and complying with laws and regulations. The OCC has previously described that custody activities should include dual controls, segregation of duties and accounting controls.⁴⁶ A custodian's accounting records and internal controls should ensure that assets of each custody account are kept separate from the assets of the custodian and maintained under joint control to ensure that that an asset is not lost, destroyed or misappropriated by internal or external parties. Other considerations include settlement of transactions, physical access controls, and security servicing. Such controls may need to be tailored in the context of digital custody. Specialized audit procedures may be necessary to ensure the bank's controls are effective for digital custody activities. For example, procedures for verifying that a bank maintains access controls for a cryptographic key will differ from the procedures used for physical assets. Banks seeking to engage in these activities should also conduct legal analysis to ensure the activities are conducted consistent with all applicable laws.

Consistent with OCC regulations and guidance on custody activities, the risks associated with an individual account should be addressed prior to acceptance.⁴⁷ A custodian's acceptance process should provide an adequate review of the customer's needs and wants, as well as the operational needs of the account. During the acceptance process, the custodian should also assess whether the contemplated duties are within its capabilities and are consistent with all applicable law. Understanding the risks of cryptocurrency, the due diligence process should include a review for compliance with anti-money laundering rules. Banks should also have effective information security infrastructure and controls in place to mitigate hacking, theft, and fraud. Banks should also be aware that different cryptocurrencies may have different technical characteristics and may therefore require risk management procedures specific to that particular currency. Different cryptocurrencies may also be subject to different OCC regulations and guidance outside of the custody context, as well as non-OCC regulations.⁴⁸ A national bank should consult with OCC supervisors as appropriate prior to engaging in cryptocurrency custody activities. The OCC will review these activities as part of its ordinary supervisory processes.

I trust this is responsive to your inquiry.

⁴⁶ See Custody Handbook at 6-8. Banks with fiduciary powers that hold assets as fiduciaries are subject to the requirements of 12 CFR Part 9 (for national banks) and Part 150 (for FSAs). These regulations include specific provisions governing the custody of fiduciary assets. See 12 CFR 9.13 (national banks); 12 CFR 150.230-250 (FSAs).

⁴⁷ See 12 CFR 9.6(a) (requiring bank fiduciaries to perform a pre-acceptance review before accepting a fiduciary account to determine whether the bank can properly administer it); Custody Handbook at 7-8.

⁴⁸ For example, cryptocurrencies that are considered "securities" for purposes of the Federal securities laws may be subject to the OCC's regulations on recordkeeping and confirmation requirements for securities transactions, 12 CFR Part 12, as well as the Federal securities laws administered by the SEC.

Sincerely,

/s/

Jonathan V. Gould

Senior Deputy Comptroller & Chief Counsel