

## MEMORANDUM

TO: North Dakota State-Chartered Banks

FROM: Department of Financial Institutions

SUBJECT: Guidance for Digital Assets/Virtual Currency

DATE: May 18, 2022

---

In response to many requests for information, the Department is providing this guidance to assist you when you consider providing digital asset and virtual currency services. This guidance is limited to address the most frequently asked questions we receive. This guidance is neither legal advice nor a comprehensive guide on all aspects of digital assets/virtual currencies<sup>1</sup>. The Department recognizes that this is a quickly evolving area and that Federal oversight, regulation, or additional guidance may be forthcoming<sup>2</sup>. Therefore, the Department may rescind or revise this guidance on short notice. The information herein is based on what is currently known and considered, and although the Department is aware of uncertainties involved, especially when it comes to Federal regulatory actions, the Department believes it is important to provide timely information to help state-chartered community banks meet customers' needs consistent with safe and sound principles. The Department does not encourage or discourage a bank's involvement in the virtual currency market, rather we are issuing this guidance to help ensure risks are considered and mitigated. This document contains the Department's current understanding of these risks. Any bank intending to engage in, or currently engaged in, activities involving or related to digital assets should consult its legal counsel and Federal regulator<sup>3</sup>. As with any activity, banks must have procedures in place to appropriately measure, monitor, control, and mitigate potential risks.

### **Definitions:**

**Blockchain (also known as distributed ledger) technology:** A distributed digital database shared among the nodes of a computer network. It is the underlying technology for cryptocurrency systems.

---

1 For a comprehensive overview of digital asset due diligence and risk management principles, refer to the [Wyoming Division of Banking's examination manual for Special Purpose Depository Institutions](#).

2 On March 9, 2022, President Biden issued an [Executive Order](#) directing federal agencies to coordinate efforts addressing the development of digital assets.

3 On April 7, 2022, the FDIC issued a [letter](#) requesting feedback on crypto-related activities.

Cryptocurrency: A type of virtual currency that utilizes cryptography to validate and secure transactions that are digitally recorded on a distributed ledger, such as a blockchain. There are thousands of cryptocurrencies in existence.

Cryptography: A system used for encryption/decryption of messages that cannot easily be deciphered by other users.

Cryptographic key: A particular unit of cryptocurrency is assigned to a party through the use of a set of unique cryptographic keys. These keys are typically stored in a digital wallet and the keys allow for the transfer of cryptocurrencies between two parties. If a party loses their key, access to the cryptocurrency is also lost.

Digital assets: An electronic record in which an individual has a right or interest. The term does not include an underlying asset or liability unless the asset or liability is itself an electronic record<sup>4</sup>. In this document it is referring to crypto assets.

Digital currency: A form of currency that is available only in digital or electronic form. All virtual currencies are digital currencies (the opposite is not true).

Fiat currency: Currency issued by a government such as the U.S. Dollar.

Stablecoins: A type of cryptocurrency that is backed by an asset, such as a fiat currency or a commodity.

Virtual currency: A digital or electronic representation of value that functions as a medium of exchange, a unit of account, and/or a store of value. Virtual currencies are neither issued nor guaranteed by any jurisdiction and do not have legal tender status in the U.S. Examples include Bitcoin, Ethereum, and Tether. A “convertible” virtual currency is a type of virtual currency which either has an equivalent value in real currency, or acts as a substitute for real currency.

### **General Authority:**

North Dakota state-chartered banks have long provided their customers with a variety of services. North Dakota Century Code § 6-03 covers the powers, management, and operation of banks, and although this section predates virtual currency considerations, the Department believes that authority for banks to provide many of the same services for virtual currencies already exists as they do for traditional assets. For example, as described below, North Dakota state-chartered banks may provide customers with virtual currency custody services, as long as the bank has adequate protocols in place to

---

<sup>4</sup> Definition in The Uniform Fiduciary Access to Digital Assets Act [North Dakota Century Code § 47-36](#).

effectively manage the risks and comply with applicable law. Thorough due diligence and considerations must be made when a bank decides on what services to offer. Custody of assets, for example, may require trust powers depending on activity. Also, considerations and required expertise may differ dependent on whether a bank engages directly with the virtual currency or through a third-party partnership. Consistent with the Office of the Comptroller of the Currency (OCC) requirements for national banks, the Department expects that a bank engaging in any activity must demonstrate “that it has controls in place to conduct the activity in a safe and sound manner”<sup>5</sup>.

### **Regulatory Expectations:**

Any time a bank is considering a new product or service, management should conduct thorough due diligence prior to implementation. A careful evaluation of the risks and necessary controls to sufficiently mitigate risk should be documented as part of the risk assessment process. The Board of Directors should ensure that appropriate policies and procedures are in place, as well as sufficient staffing and management expertise. Digital assets and virtual currencies are a newer and rapidly evolving area, and all risks may not be thoroughly understood. Prior to a bank engaging in this area, it is paramount that staff has sufficient expertise and knowledge and that appropriate risk controls are in place, which includes adequate insurance coverage.

Due to the technical nature of holding virtual currency, the bank may choose to establish a relationship with a service provider with expertise in handling virtual currency. Therefore, it is incumbent on the bank to maintain a strong service provider oversight program that addresses risk in the service provider relationship from the first steps of due diligence through a potential termination of the service provider relationship<sup>6</sup>. The bank also must be mindful that the service provider may also be subject to various state licensure requirements, and failure on the part of the servicer to meet their regulatory requirements may subject the bank to increased risk.

### **Reputational Risk Considerations:**

The bank’s customers have numerous ways of investing or transacting with virtual currencies directly with digital wallets outside of the traditional banking system. However, due to community banks’ reputation for being safe and stable, if a community bank offers

---

<sup>5</sup> The Office of the Comptroller of the Currency reiterated its expectations for national banks’ cryptocurrency activities in its [November 18, 2021, Interpretive Letter #1179](#).

<sup>6</sup> More information on outsourcing technology services can be found in the Federal Financial Institutions Examination Council’s [IT Examination Handbook for Outsourcing Technology Services](#). The FFIEC April 30, 2020, [Joint Statement on Risk Management for Cloud Computing Services](#) will also provide helpful guidance.

virtual currency access, either directly, via a partner, or part of its core banking platform, customers may be more inclined to engage in this activity with their bank rather than on their own. Although there has been tremendous growth in this market and the products are easily accessible, that does not mean that customers have a thorough understanding or knowledge of the products. The risks are prevalent and may not be thoroughly understood, and the bank must be transparent about the level of risks it may expose its customers to by facilitating access to these products. If the bank offers any investment products or other uninsured activities, the bank should ensure solid agreements with customers and proper disclosures are communicated. Due to the higher risk and volatility in these instruments, the bank should safeguard its reputation and consider its customer relationship if a customer's investment value suddenly goes down or the customer loses the investment. The bank must consider the role of simply facilitating transactions versus promoting an investment or providing investment advice.

#### **Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Considerations:**

Banks have the same compliance obligations for knowing its customers, monitoring transactions, and reporting for virtual currency transactions as they do for fiat currency. In the [FinCEN Advisory, FIN-2019-A003, May 9, 2019](#), FinCEN states that virtual currencies “may create illicit finance vulnerabilities due to the global nature, distributed structure, limited transparency, and speed of the most widely utilized virtual currency systems.” Since virtual currency transactions are anonymous/pseudonymous, the ability for a bank to monitor individual identities and transparency of transactions may require additional and different resources than what is currently deployed for fiat currency transaction monitoring. Similarly, Office of Foreign Assets Control (OFAC) compliance obligations also apply equally to transactions involving virtual currencies and those involving traditional fiat currencies. With virtual currencies' increasingly prominent role in the global economy, community banks will have an increased exposure to sanctions risks. OFAC issued its [compliance guidance](#) in October 2021 addressing these concerns. Banks need to provide sufficient resources in staffing and procedures to fully comply with these laws. Although a bank may outsource functions to third parties, this does not relinquish the bank's BSA/AML and OFAC risks, obligations, and liabilities. The responsibility ultimately remains with the bank to ensure transactions comply with the law.

#### **Virtual Currency as Deposits:**

Virtual currencies are not considered legal tender and can therefore not be taken as a deposit and placed on the bank's balance sheet as such. The bank may provide safekeeping and custody services as described below.

### **Virtual Currency as a Bank Investment:**

North Dakota Century Code § 6-03-47.2 does not allow for banks to invest bank funds in virtual currencies. In addition, with the fluctuations in value and speculative nature of this market, virtual currency investments pose heightened liquidity, asset quality, and earnings risks and are therefore not a prudent investment for banks.

### **Virtual Currency as Collateral:**

Although a bank can take virtual currency as collateral, there are numerous considerations to ensure the bank is fully protected against undue risk. First off, the loans themselves must be made with fiat currency and must be repayable in fiat currency, even if the underlying collateral is virtual currency. Additionally, as an example, when a bank makes a car loan, it will obtain and be in possession of the title to fully perfect the loan. To properly perfect a virtual currency loan, the bank will need possession or exclusive control over the private key. It is possible a bank could use a Uniform Commercial Code (UCC) filing; however, the bank must consider the likelihood of successfully obtaining the private key and thus the collateral from the borrower in the event of foreclosure. While a bank can theoretically obtain the private key through judgments from the courts, this is a new area of law, the collateral may be held in foreign jurisdictions, and this method of collecting will come with legal costs. The bank should know where the virtual currency is held and what measures are in place to safeguard the collateral. As with any loan, failure to fully perfect the collateral may result in examiners treating the loan as unsecured and the virtual currency collateral as an “abundance of caution”.

Another challenge using virtual currency as collateral is the volatility and quick changes in value. These loans could be treated similar to margin loans, requiring a periodic adjustment where the borrower adds collateral to ensure a specific loan-to-value limit is maintained. If the bank uses this approach, banks should give thorough consideration for the collateral margin, frequency and calculation of margin calls, and understand that the appropriate margin limitation may differ depending on the type of virtual currency.

Loan documentation and borrowing agreements may differ from traditional loan agreements due to the different nature of the collateral and where the collateral is kept. Also, in the event of foreclosure, the bank must consider how to take possession of the collateral, any system requirements for safeguarding, and fees for converting the collateral into fiat currency for loan repayment. A bank would need to liquidate any crypto collateral following a foreclosure timely to extinguish the debt and to realize any losses.

### **Virtual Currency as an Underwriting Consideration:**

A borrower's crypto activity can impact their overall financial condition. Whether a bank actively engages in providing crypto services or not, all lenders need to be aware of the impact crypto assets can have on borrower equity and cash flow, even if the loan products offered are traditional consumer, agricultural, or commercial loans. When evaluating a borrower's financial condition, be mindful of the impact changes in crypto prices can have when virtual currency makes up a large share of a customer's balance sheet. Crypto price changes and margin calls may have an impact on a borrower's cash flow position, even if the bank's specific loan is not for, or secured by, the crypto assets.

### **Virtual Currency Custody Services:**

The OCC has opined that providing cryptocurrency custody services is a modern form of the traditional bank activities of custody and safekeeping, and that providing these services is a permissible form of a traditional banking activity that banks are authorized to perform via electronic means<sup>7</sup>. Similarly, North Dakota state-chartered banks have long provided their customers with safekeeping and custody services for a variety of assets. These services play a crucial role in the business of banking as customers look to banks to offer secure and dependable storage. While custody and safekeeping of virtual currencies will necessarily differ from that associated with more traditional assets, the Department believes that the authority to provide these services with respect to virtual currencies already exists pursuant to North Dakota Century Code § 6-03. Therefore, North Dakota state-chartered banks may provide customers with virtual currency custody services, as long as the bank has adequate protocols in place to effectively manage the risks and comply with applicable law.

What virtual currency custody services a bank chooses to offer will depend on the bank's expertise, risk appetite, and business model. For instance, the bank may choose to allow the customer to retain direct control over their own virtual currency and merely store copies of the customer's private keys associated with that virtual currency. Alternatively, the bank may cause the customer to transfer their virtual currency directly to the control of the bank, creating new private keys that are then held by the bank on behalf of the customer. As with the method of custody services, several secure storage options are available to the bank, each of which has distinctive characteristics pertaining to level of security and accessibility. The bank will have to determine which storage option best fits the circumstances.

Custody services may be provided by a North Dakota state-chartered bank in either a fiduciary or non-fiduciary capacity. In providing such services in a non-fiduciary capacity,

---

<sup>7</sup> In July 2020, the OCC issued its [Interpretive Letter 1170, Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers](#).

the bank takes possession of the customer's asset for safekeeping while legal title to that asset remains with the customer. The extent of the bank's duties regarding the asset depends on the custodial agreement between the bank and the customer but generally, the bank owes its customer the duty to use proper care to keep the asset safely and to return it unharmed upon request. The owner of the virtual currency holds cryptographic keys associated with the specific unit of virtual currency in a digital wallet. The keys enable the rightful owner of the virtual currency to access and utilize it further. Therefore, safekeeping for a bank is most likely not a physical possession of the virtual currency itself, rather it is safekeeping for the cryptographic key that allows for control and transfer of the customer's virtual currency. The bank must carefully consider whether this is best done directly or via a third party.

A bank proposing to offer custody services for digital assets in a fiduciary capacity must possess trust powers, which requires an application to the State Banking Board in accordance with North Dakota Century Code § 6-05-01 prior to doing so. In its fiduciary capacity, the bank has the authority to manage virtual currency assets as it would any other type of asset held in such capacity<sup>8</sup>.

Regardless of approach for custody services, necessary controls must be in place prior to engaging in the activity. Comprehensive board-approved policies and procedures must be in place to properly safeguard the assets. The bank must consider technical controls such as access controls and authentication, and physical controls such as protection of hardware and data specific to the virtual currency held. The bank should also confirm the existence of adequate coverage with its insurance carrier, and consult with knowledgeable legal counsel to understand the legal liabilities and risks to the bank if something were to go wrong. If the bank is providing fiduciary services, even if not accepting virtual currencies directly as an asset to manage, the bank must consider the possibility of at some point having custody of virtual currency if it takes possession of an estate that includes virtual currency.

---

<sup>8</sup> The Uniform Fiduciary Access to Digital Assets Act is found in [North Dakota Century Code § 47-36](#).