Deloitte.

Cryptocurrency custody

Insights and impact

Ten things to consider about OCC guidelines on digital asset custody

In its Interpretive Letter #1170 issued on July 22, 2020, the Office of the Comptroller of the Currency (OCC) issued a legal interpretation affirming that federally chartered banks and thrifts (collectively "national banks") may now provide cryptocustodial services for crypto assets. For national banks, and for state chartered banks in jurisdictions aligning with the OCC interpretation, this guidance holds out the promise of a great opportunity to generate new revenue streams, develop a new client base, cross-sell services to existing clients who want to enter the ecosystem of this new asset class, and disrupt the industry by developing new digital payment and asset protection solutions.

Given the OCC's greenlighting of cryptocustodial activities, banks should first consider how to develop a robust strategy that addresses several immediate questions, including:

1
Upon entering cryptocustodial activities, how will custody services align with the bank's long-term strategy? Through staking, crypto lending, other user fees?

2
How can banks differentiate their cryptocurrency custody services? For example, can they provide enhanced reliability through a FireBlocks solution?

3
Should banks view this new guidance as a first step toward a broader support of digital assets such as Central Bank Digital Currencies?

Teams that have the necessary OCC, Financial Industry Regulatory Authority (FINRA), Securities and Exchange Commission (SEC), US Treasury Department, and other deep regulatory experience are not only capable of helping to address these strategic business questions, but can also help guide banks in handling a host of technical questions. Consider the following:

4
Technical complexities.
Serving as a custodian of digital assets is unlike managing any other asset, including the fact that the bank does not physically possess the digital asset. It entails significant technical complexities, all in a world already marked by ever evolving regulatory and technical standards. Examples include enhanced global now your customer (KYC) rules and further clarity on when the SEC deems a digital asset to be a "security." That is why banks need to weigh whether providing custody of digital assets will be the first step in developing a new core competency in which to invest. If not, will they consider teaming with best of breed cryptocustodians to act on their behalf. (Note: The technical talent needed to custody digital assets is in short supply, particularly engineering resources with experience in cryptographic key management. Hence building a custody business for digital assets from scratch may prove impractical. Acquisition of, or partnering with, an existing digital asset custodian may be the only viable path to rapid deployment).

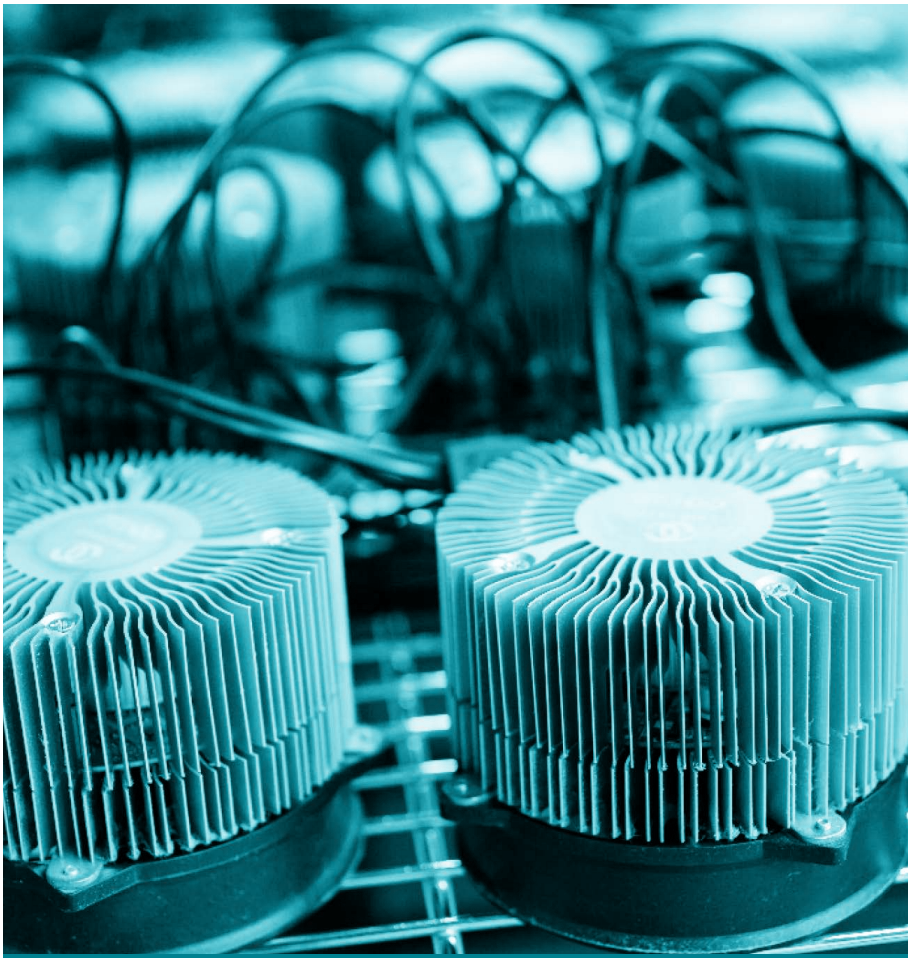
5
Risk assessment of new digital assets.
When deciding which digital assets to custody, banks need to assess the unique risks each digital asset carries. Those risks will help determine whether to offer custody only for certain asset types and how to structure that custody service and risk management program. It is the OCC's supervisory expectation that the bank maintain adequate systems to "identify, measure, monitor, and control the risks" of its custody. For companies licensed through the New York State Department of Financial Services, that agency is considering mandating a risk assessment as part of the onboarding of new digital assets. Digital asset custodians should institute and maintain a new asset listing and monitoring policy which includes, but is not limited to:

- Evaluation of the legal and regulatory risks of offering an asset in a selected jurisdiction (is the digital asset at risk of being classified as a security?)
- Ability to demonstrate custody and that the assets in fact exist and have a precise location. That will serve to align with and meet SEC and FINRA requirements. Note: Those requirements should be harmonized for banks that are also broker-dealers

- Risk evaluation of the protocol that supports the asset, including operational, cybersecurity, and market risk
- Auditability and availability of information created under this protocol
- Ongoing and periodic monitoring of assets held in custody to manage the risks associated with each asset, as they may evolve or change over time over time
- A process for delisting assets that have either ceased to be operative or that no longer meet designated risk management requirements

6

Enhanced anti-money laundering and know your client processes. Given the pseudonymous and potential cross-border nature of public ledgers, custodians of digital assets will need to establish an adequate, risk-focused anti-money laundering (AML) program, including sanctions compliance. Among these procedures, there should be a deeper knowledge of the bank's digital asset client base, including the identification of the source and lineage (historical origination) of their funds and appropriate monitoring of their transactions.



7

Controls and third-party assurance. Since the technology and systems required to custody digital assets are unique, so too will be their internal controls. In practical terms, banks will need to design custom internal controls that mitigate the unique technical risks of digital assets, particularly in areas such as cryptographic key management, segregation of duties, AML, compliance, and cybersecurity. If banks opt to have a third party perform custodian services, it will require obtaining formal third-party assurance from the custodian (typically in the form of a SOC 1 or SOC 2 report), which addresses the controls over the custody of digital assets. Understanding and maintaining an appropriate control structure is essential to:

- Being in and demonstrating compliance with Sarbanes-Oxley requirements for internal controls over financial reporting (as applicable)
- Monitoring and managing the bank's operational, vendor, and credit risk, as well the potential impact on a client's credit or margin in light of the totality of what a client has in that bank's custody

8

Regulatory environment.

The regulatory framework for digital assets continues to evolve quickly. That's why banks will need to have effective specialized regulatory and legal advice that will, among other things, position them to be ready to shift and adapt business operations quickly as regulations change. In addition, services offered to participants in the cryptoeconomy may cross the boundary from banking activities to securities activities, which are regulated by the SEC or FINRA. Those are just several of the dynamics that dictate why building a business in the cryptoeconomy, including acting as a digital asset custodian, requires a comprehensive regulatory strategy.

9

Internal and external audit.

Auditing in a distributed ledger environment carries unique risks that need to be addressed by both internal and external auditors, who understand and can respond to these unique risks. And maintaining adequate books and records for digital assets, from a regulatory and financial reporting perspective, may well entail additional considerations. Please consult the Deloitte perspectives in an internal auditors guide to auditing blockchain.

10

Tax.

With digital assets, there are additional, necessary tax considerations that could be the responsibility of the custodian of digital assets:

- Digital assets used in proof-of-stake protocols may lead to rewards that can be classified as "income." These rewards could then come into control of the custodian. This could trigger a potential requirement to report or withhold taxes, a need for tax basis tracking, and developing appropriate valuation methodologies for reporting on digital assets held in custody. Some staking processes may also produce income that is effectively connected with either the United States or other jurisdictions.
- Custodians who enable exchanges of digital assets may have reporting or withholding requirements based on their role and on the type of digital assets exchanged or sold.
- Digital representations of physical assets that are held or exchanged may require tax reporting or withholding of taxes in the jurisdiction of the custodian, the location of the physical asset, or the location of the buyer or seller. Banks need to think through these jurisdictions and the local requirements carefully.

The letter from the OCC is one of many recent inputs, from regulators in the United States and around the world, on digital assets—a clear sign that the industry is maturing. The caution flags raised in the OCC letter and as depicted above are complex. However, our experience in the digital asset industry for the past eight years across all aspects of the ecosystem, as well as interaction with a variety of regulators on the topics mentioned above, has demonstrated to us that these risks are manageable if addressed in a timely manner and with the appropriate level of expertise.

Authors

Tim Davis
Risk & Financial Advisory
Global Center of Excellence for Blockchain Assurance leader
Deloitte & Touche LLP
timdavis@deloitte.com

John Graetz
Risk & Financial Advisory
Principal
Deloitte & Touche LLP
jgraetz@deloitte.com

Brian P. Hansen
US Audit & Assurance
Blockchain & Digital Assets leader
Deloitte & Touche LLP
brianhansen@deloitte.com

Michael Marzelli
Audit & Assurance
Partner
Deloitte & Touche LLP
mmarzelli@deloitte.com

Rob Massey
Global & US Tax Blockchain & Digital Assets leader
Deloitte Tax LLP
rmassey@deloitte.com

Elana Mourtil
Managing Director
Deloitte Tax LLP
emourtil@deloitte.com

Amy Steele
Global and US Audit & Assurance methodology leader for Blockchain & Digital Assets
Deloitte & Touche LLP
asteele@deloitte.com

Richard Walker
US Financial Services Blockchain & Digital Assets leader
Deloitte Consulting LLP
richardwalker@deloitte.com

Robert Walley
Risk & Financial Advisory
Principal
Deloitte & Touche LLP
rwalley@deloitte.com

Deloitte.