

July 16, 2021

James P. Sheesley
Assistant Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street N.W.
Washington, D.C. 20429

Submitted electronically on July 16, 2021 via email correspondence to: Comments@fdic.gov

Re: Request for Information and Comment on Digital Assets (RIN 3064-ZA25)

Assistant Executive Secretary Sheesley:

We appreciate the opportunity to offer comments to the Federal Deposit Insurance Corporation (FDIC) regarding insured depository institutions' (IDIs') current and potential activities related to digital assets. We thank the FDIC for this public consultation and hereby provide input from Chainalysis based on our industry and technical experience as a blockchain analysis company. Chainalysis provides data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and cybersecurity companies in over 60 countries. Our blockchain analysis tools allow for investigation, compliance, and risk management, and have been used to solve some of the world's most high-profile cyber criminal cases and grow consumer access to cryptocurrency safely.

Outlined below please find Chainalysis' responses to select questions in the request, informed by our extensive experience working with industry members, financial institutions, cryptocurrency exchanges, law enforcement, and regulatory agencies.

2. What, if any, activities or use cases related to digital assets are IDIs currently engaging in or considering?

Chainalysis has had conversations with a number of different IDIs who are interested in entering the digital asset space. With cryptocurrency increasingly mainstream, IDIs no longer view it as a passing fad or tool for criminals. Instead, they're trying to incorporate it into their larger strategies, recognizing the ways it can help their customers while driving revenue.

IDIs vary in their current comfort levels with digital assets and the degree to which they've incorporated them into their future plans, ranging from allowing retail banking customers to send funds to cryptocurrency businesses to even issuing their own tokens. Many IDIs still view cryptocurrencies as a special asset class, rather than a mainstream asset class. They are working to understand how to apply their anti-money laundering/countering the financing of terrorism (AML/CFT) frameworks to cryptocurrencies, as well as which regulations apply to cryptocurrencies and how. One common refrain is that financial institutions are not always certain what the current US regulatory framework allows them to do, and many would like additional clarity from regulators on this front.

Despite these uncertainties, financial institutions are taking seriously what they see as a clear demand for cryptocurrencies among their customers. Bitcoin especially has become a big enough asset for financial institutions to consider. Chainalysis data shows that there has been an increase in holders of large amounts (1,000 or more bitcoin each) of bitcoin that rarely spend

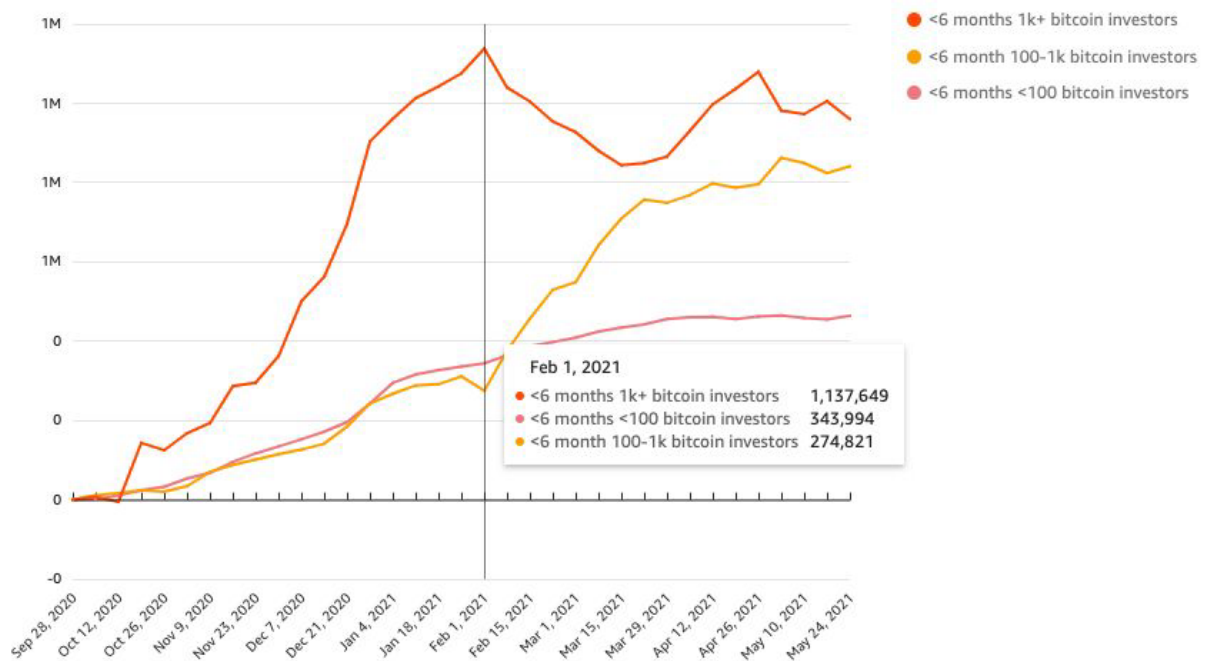
their bitcoin. As the chart below demonstrates, these investors have increased their holdings by 800,000 bitcoin from mid-March through to the end of 2020.

Change in bitcoin held since 2017-01-01 by type of holder



In February 2021, Chainalysis data illustrated a steep increase in investor wallets under six months old holding more than 1,000 bitcoin, indicating a trend in first-time buyers with deep pockets. The chart below illustrates this. The data largely fits the narrative we’ve heard over the last year: Investors, especially those from mainstream financial institutions, have embraced bitcoin specifically, and cryptocurrencies generally, as a long-term investment, with many positioning the asset as a hedge against inflation and other economic trends they find worrisome. That’s why we see such a high percentage of bitcoin being held for long periods of time compared to other cryptocurrencies.

Change in bitcoin held since 2020-09-28 by investors holding for less than six months



IDIs want to be able to offer their customers the products and services that they are interested in, including digital assets. For these IDIs, the key is determining the right types of products and services to build out at each step as they increase their knowledge base and technical capabilities. The inherent transparency of cryptocurrency makes this process easier -- with the right tools, financial institutions can aggregate the transaction data recorded on public blockchains, observe how funds flow between different types of wallets and services, and use that data to inform decisions about which types of cryptocurrency services make the most sense for their customers. They can leverage similar blockchain analysis tools in their AML/CFT compliance efforts, identifying transactions between their customers and illicit services or sanctioned entities.

4. To what extent are IDIs' existing risk and compliance management frameworks designed to identify, measure, monitor, and control risks associated with the various digital asset use cases? Do some use cases more easily align with existing risk and compliance management frameworks compared to others? Do, or would, some use cases result in IDIs' developing entirely new or materially different risk and compliance management frameworks?

IDIs will be required to update their existing Bank Secrecy Act (BSA) and AML programs and policies, including their BSA/AML risk assessments, as well as their compliance programs, to address digital assets. IDIs can continue to utilize legacy banking systems to complete customer identification programs (CIP), Know Your Customer (KYC), and sanctions obligations. These existing policies and procedures are a good starting point to address the specific risks associated with various digital asset use cases. However, as with any new product, digital assets carry unique risks that will need to be identified and mitigated. Specifically, transaction monitoring of digital assets differs from traditional fiat transaction monitoring. Without proper controls in place, IDIs may be interacting with risky counterparties and facing regulatory action.

IDIs must use blockchain analysis tools to ensure compliance in regards to transaction monitoring of digital asset offerings. Blockchain analysis helps people interpret public

blockchain ledgers and understand which real-world entities are transacting with each other. For example, using blockchain analysis, Chainalysis can show that a given transaction took place between two different cryptocurrency exchanges, or between a cryptocurrency exchange and an illicit entity, such as a sanctioned individual or organization. Using this technology, you can gain transparency into blockchain activity in ways that aren't possible in traditional finance. Likewise, with transaction monitoring, cryptocurrency exchanges and financial institutions can flag high-risk activity and fulfil their regulatory obligations to report them.

6. What unique benefits to operations do IDIs consider as they analyze various digital asset use cases?

Like other businesses, IDIs must adapt and innovate to remain successful. Digital assets present a new line of business that can help them to do this, expanding their business and remaining forward-looking in this ever-digitizing world. This will allow them to serve more customers and provide them with a more diversified array of products, increasing their profitability.

Beyond bringing in new lines of business for IDIs, digital assets also offer a number of unique benefits over traditional financial assets. For example, they operate on distributed ledger technology that functions 24 hours a day, seven days a week, meaning that data can be processed continuously, rather than on a bank or its intermediaries' operating schedules. They are resilient to cyber attacks because distributed ledger technology involves many different copies of a ledger being hosted on multiple systems, thus building in redundancy that provides an improved level of security against attacks. Finally, they provide transparency, as they are built on immutable ledgers, which enable the use of blockchain analysis for efficient audits and investigations. These benefits may make digital assets an attractive option for IDIs as they consider the various digital asset use cases available to them.

8. Please identify any potential benefits, and any unique risks, of particular digital asset product offerings or services to IDI customers.

While digital assets have historically been associated with their illicit use, for example being used on Darknet markets or in ransomware payments, according to Chainalysis data, in 2020, the criminal share of all cryptocurrency activity was just 0.34%, or \$10.0 billion in transaction volume. We should note that as we identify more cryptocurrency addresses associated with illicit activity over time, we expect this estimate to increase. Still, it remains a small part of the overall cryptocurrency economy, and it is comparatively smaller to the amount of illicit funds involved in traditional finance. This means the vast majority of cryptocurrency transactions are legitimate. Furthermore, blockchain analysis platforms will allow IDIs to conduct transaction monitoring on digital assets. In fact, risk assessment in cryptocurrency is actually easier than in most other industries due to the inherent transparency of most blockchain-based assets. Unlike with fiat currency, most cryptocurrency transactions are recorded on a public ledger. That means that with the right tools, IDIs can monitor cryptocurrency businesses' transactions and accurately size their exposure to illicit activity, ensuring every client they take on fits into their desired risk profile.

Using blockchain analysis tools and cryptocurrency transaction monitoring software, IDIs can see the flow of cryptocurrency to pinpoint the source or destination of the funds. These tools can be integrated into existing frameworks, and IDIs can customize them to align with their compliance and risk policies. IDIs can automatically detect and receive alerts to patterns of potential high-risk activity, from addresses included as identifiers by the Office of Foreign

Asset Control (OFAC) on sanctions lists and darknet markets, to scams and anomalous transactions. This technology is already proven - it is employed by hundreds of cryptocurrency businesses and financial institutions in their AML/CFT compliance programs.

Some risks that are particular to digital assets include potential weaknesses associated with decentralized finance (DeFi). This includes poor security controls that can leave protocols vulnerable to hacking. According to some estimates, DeFi hacks resulted in \$100 million in stolen funds. Many DeFi protocols are undergoing smart contract security audits in order to address this concern, but this does continue to pose a risk in this space.

Another unique challenge associated with digital assets is related to their storage. Digital assets can be stored in “hot” or “cold” storage wallets. Hot wallets are connected to the internet, and include hosted or custodial wallets on cryptocurrency exchanges, desktop wallets, and mobile wallets. Cold wallets are not connected to the internet - these are often physical devices that can connect to computers or hand-written paper wallets. IDIs will need to become familiar with the different types of wallets, their advantages and disadvantages, as well as the various security measures they should consider implementing, such as multi-signature wallets, which require multiple private keys to send a transaction.

10. Are there any unique aspects of digital asset activities that the FDIC should take into account from a supervisory perspective?

FDIC should ensure that IDIs are updating their compliance program and policies to adequately account for the specific risks associated with digital assets, specifically related to blockchain analysis. For example, at the state-level a number of regulators require that their regulated entities must implement a form of blockchain analysis to ensure that sufficient transaction monitoring is occurring on digital assets. FDIC should take this into account when contemplating additional supervisory guidance to address digital asset activities. Blockchain analysis tools also provide unique insight for supervisory entities, as they can conduct supervisory oversight activities without having to request information from their supervisees. Using blockchain analysis, supervisory entities can review transactions related to their supervisees and determine which may not be meeting their regulatory obligations and therefore need to be prioritized for additional review.

* * * * *

Thank you for your kind attention to these issues. We look forward to serving as a resource to the FDIC as it evaluates digital assets in this space. Please do not hesitate to contact us with any questions you may have.

Sincerely,

Jonathan Levin
Co-Founder and Chief Strategy Officer
Chainalysis, Inc.