



August 8, 2022

Natalia Li
Deputy Director
Office of Financial Institutions Policy
Department of the Treasury
1500 Pennsylvania Ave. NW
Washington, DC 20220

RE: Docket 2022-14588 Ensuring Responsible Development of Digital Assets

Dear Ms. Li:

Thank you for the opportunity to comment on these questions.

The National Community Reinvestment Coalition (NCRC) is an association of more than 600 community-based organizations that work to promote access to essential banking services, including credit and savings. Our members include community reinvestment organizations, community development corporations, local and state government agencies, faith-based institutions, community organizing, civil rights groups, and minority and women-owned business associations. They work to create and sustain affordable housing, job development, and vibrant communities for America's families.

Our comment consists of two parts: first, we outline some of our strategic priorities for the regulation of digital assets, and then second, we respond to some of the specific questions raised in the request for comment.

The questions raised by the lack of clear regulatory authority for some types of digital assets underscore the need for policy makers to take a “whole of government” approach. In some parts of this comment, we call for a policy change without calling for action by a specific agency or through new legislation because of the lack of a recognized authority in that sphere.

I. Policy makers must address regulatory gaps and clarify which agencies have authority over the different types of digital assets.

a) Asset tokens – which provide a claim against something of value, could be defined as investment contracts and regulated by the SEC.

b) Most exchange tokens will not meet the definition of a security, but without clarification, they may not meet the criteria to qualify for supervision by the CFTC. Regulators should clarify when the CFTC has jurisdiction over a digital asset that is not a security and is sold in the "cash market."

c) The SEC and the CFTC should work together to determine the opportunities and risks posed by "self-regulatory organizations" and "embedded regulation."

d) Uninsured deposits of digital assets that pay interest should be defined as securities offerings. Their issuers should be required to file a registration statement.

e) Issuers of uninsured interest-bearing digital asset depositories should be required to file a registration statement under Sections 5(a) and 5 (c) of the Securities Act of 1933.

f) A crypto trading platform (CTP) that offers trading of digital assets that are securities should be considered a securities exchange. It should have to register as one with the SEC.

g) Some CTPs act as investment companies. If the activities of a CTP meet the criteria, the SEC should supervise it as an investment company.

II. Regulators should determine how a stablecoin could be structured to reside inside the regulatory perimeter. Nonetheless, bank stablecoins must meet specific safety standards, have community reinvestment obligations, be subject to consolidated supervision, and holders of these accounts should benefit from Regulation E protections. There should be strict rules that support interoperability.

a. When a stablecoin can meet these standards for safety, it should be eligible to be held on deposit at insured depository institutions and be eligible for deposit insurance.

b. While there are many potential ways that a stablecoin could be folded into the formal banking system, most are suboptimal because they would pose risks to consumers and to systemic safety. A fully-insured closed-loop bank-issued interoperable stablecoin is a safe alternative.

c. Financial institutions that issue insured closed-loop stablecoin should have a community reinvestment obligation.

d. Regulators must adopt uniform standards for insured stablecoins and apply similar consumer protections to fiat and insured digital deposits.

e) Regulation E protections should be applied to insured stablecoin accounts held at insured depository institutions.

f) Stablecoin issuers should be required to make public reports on their diversity, equity, and inclusion programs.

III) Policy makers should address threats of cyber security, contagion, and systematic importance.

a) CTPs should be examined for cyber risks

b) Non-bank stablecoin issuers must be subject to heightened regulatory scrutiny.

c) Policy makers should be prepared to determine when a digital asset, particularly a stablecoin, has become "too big to fail."

DISCUSSION

I. Regulators must address regulatory gaps and clarify which agencies have authority over the different types of digital assets.

Policymakers must define what activities are consistent with what types of regulatory functions.

It will be easier to regulate digital assets if they can be defined within the categories of legacy assets so that regulators have clear and well-demarcated authority for their oversight of specific activities. However, appropriate analogs are not easily ascertained for all types of digital assets. Clarifying that an asset token is a security is somewhat straightforward under the *Howey* test. Other types of tokens may be more challenging to define.

Many regulators could claim supervisory authority – and the rivalries will be more significant without clearly stated and universally accepted definitions. The leading candidates are prudential regulators of banks, the Securities and Exchange Commission (SEC), and the Commodities and Futures Trading Corporation (CFTC). However, the two primary regulators will be the SEC and the CFTC.

To fully meet the challenges presented by the mass adoption of digital assets, policymakers must address jurisdiction issues. By splitting capital markets among the SEC and CFTC, policymakers have made the definition of digital assets much harder. This artificial division underscores the importance of the FSOC's role. If the FSOC can close regulatory gaps and synthesize activities, regulatory work will advance faster – to the benefit of everyone.

a) Asset tokens – which provide a claim against something of value, could be defined as investment contracts and regulated by the SEC.

The US Securities and Exchange Commission (SEC) has issued guidance that applies the “*Howey* test” framework in determining when a digital asset is an investment contract and whether the offering and sales of the digital asset represent a securities transaction.¹ We agree that the *Howey* test is a valuable instrument established by legal precedent to define when a digital asset is an investment. It would be consistent that when a digital asset is sold a) for money for a stake in a b) common enterprise to a person who c) expects profits d) based on the managerial efforts of others, then it meets the standard for the *Howey* test and can be considered a security.

b) Most exchange tokens will not meet the definition of a security, but without clarification, they may not meet the criteria to qualify for supervision by the CFTC. Regulators should clarify when the CFTC has jurisdiction over a digital asset that is not a security and is sold in the "cash market."

Many types of digital assets do not meet the definition of a security or a commodity. New legislation proposed to create new classes of “ancillary assets” that do not confer the profit-sharing opportunities of investment contracts or represent a derivative interest in an asset.²

If Congress does not proceed with a definition, including but not exclusively with the proposed “ancillary asset” definition, then regulators should clarify how they will regulate exchange tokens. These tokens do

¹ U.S. Securities and Exchange Commission. (n.d.). Framework for “Investment Contract” Analysis of Digital Assets. Retrieved August 4, 2022, from <https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets>

² Roy, A. (2022, July 8). Lummis-Gillibrand Crypto Bill: An Important Step In Bringing Regulatory Clarity To Bitcoin, Stablecoins, & Digital Assets. Forbes. <https://www.forbes.com/sites/theapothecary/2022/07/08/lummis-gillibrand-crypto-bill-an-important-step-in-bringing-regulatory-clarity-to-bitcoin-stablecoins--digital-assets/>

not constitute a claim on the token's issuer (versus an NFT). For example, the exchange token Bitcoin does not fit the *Howey* test as it does not represent a stake in an entity (prong a), and no entity is acting in a management role (prong c). Unfortunately, Bitcoin makes up almost half of all digital asset trades. If Bitcoin is not a security and thus not suitable for regulation by the SEC, then the most significant digital asset is unregulated.

Unfortunately, Bitcoin is not an exception. There is a sizeable regulatory gap: many digital assets are not securities but are also not derivatives of any other asset. The CFTC cannot regulate the "cash market" in the trading of goods. Unfortunately, most trading of digital assets is in the "cash market."

c) The SEC and the CFTC should work together to determine the opportunities and risks posed by "self-regulatory organizations" and "embedded regulation."

Decentralized autonomous exchanges (DAOs), self-regulatory organizations (SROs), and non-governmental, non-profit organizations claim to provide governance functions for individual tokens or marketplaces. They are analogous to traditional SROs that fulfill governance needs in established markets, such as the Financial Industry Regulatory Authority or the Chicago Board of Trade. They provide self-directed and industry-led coordination of rules and standards for market participants. However, SROs in the crypto context differ in significant ways. For example, DAOs and embedded regulation substitute code for human judgment.

To address the uncertainty surrounding the ability of DAOs and digital SROs to provide governance, the SEC and the CFTC should establish a working group to consider the opportunities and risks of these models.

A self-regulatory framework will not substitute for a formal regulatory regime. Standards without rules and enforcement are unlikely to produce a baseline level of consumer protection.

The Financial Stability Oversight Council should determine where there are opportunities to integrate the work of the CFTC and the SEC. Joint engagement could expedite regulation in this space. In the spirit of the "whole of government" approach called for by the Biden Administration, the organizations should commission a joint Task Force on digital assets and meet regularly.

d) Uninsured deposits of digital assets that pay interest should be defined as securities offerings. Their issuers should be required to file a registration statement.

Consumers are likely to view an uninsured stablecoin as an alternative to a money market mutual fund (MMMF) – neither is fully insured. Still, both usually pay a rate of interest above the prevailing rate paid on insured deposits. The SEC defines MMMFs as securities,³ but the framework for ongoing supervision is undefined.

Uninsured digital asset deposits that pay interest should be defined as securities. Uninsured interest-bearing digital deposits meet the definition of securities because investors use them with a reasonable expectation of profit and at some risk. If the deposits were insured, they would not meet the risk criterion. However, as currently offered, they bear risk.

³ U.S. Securities and Exchange Commission. (2022, February 14). *BlockFi Agrees to Pay \$100 Million in Penalties and Pursue Registration of its Crypto Lending Product*. <https://www.sec.gov/news/press-release/2022-26>

Under the *Howey* test, an investment contract is “a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party.”⁴

e) Issuers of uninsured interest-bearing digital asset depositories should be required to file a registration statement under Sections 5(a) and 5 (c) of the Securities Act of 1933.

This step would give investors more information about their funds' use. As a part of that statement, platforms that use deposits to make loans should have to disclose the lending and investment activities they will utilize to pay for the yield on deposit liabilities. Under this approach, regulators could supervise activities before consumer harm occurs. Investors would receive disclosures to understand the risks they are taking when they put funds in these accounts.

When defined as a security, an uninsured digital asset deposit will receive “like” treatment for the “like activity” of a money market mutual fund.

f) A crypto trading platform (CTP) that offers trading of digital assets that are securities should be considered a securities exchange. It should have to register as one with the SEC.

CTPs should register with the SEC as exchanges. By requiring that they register with the SEC, CTPs would have to comply with rules designed to ensure market integrity and protect investors.

Most CTPs that only sell digital assets have not registered with the SEC as exchanges. A pure CTP is not under an obligation to do so. For now, a handful of exchanges that have added digital asset trading to existing securities-trading platforms are already registered, leading to a bifurcated regulatory structure. Without intervention, the inconsistency will confuse consumers as to the protections from risk and level of transparency they can expect.

Regulators should consider how initial coin offerings (ICOs) could be subject to review as securities offerings. Currently, issuers who bring new investment offerings to public markets must submit an S-1 to the SEC. A similar approach would work. The status quo, where issuers publish a white paper, is insufficient to protect the public.

The introduction of a new token not defined as a security (an "ICO") is also an unregulated gap. Currently, issuers use white papers to describe the design and features of new tokens. Many white papers are focused on the code. No set of required content exists as is standard with SEC filings such as an S-1 (registration of securities). The SEC should create registration requirements for ICOs, establish standards for explaining why consumers should consider the ICO, and prevent conflicts of interest among management. The S-1 system provides these protections for traditional initial public offerings (IPOs) of stock. Similar benefits should be conferred to consumers considering an investment in a digital asset that is a security.

g) Some CTPs act as investment companies. If the activities of a CTP meet the criteria, the SEC should supervise it as an investment company.

An investment company is any issuer that “is engaged or proposes to engage in the business of investing, reinvesting, owning, holding, or trading in securities, and owns or proposes to acquire investment securities having a value exceeding 40 per centum of the value of such issuer’s total assets (exclusive of Government securities and cash items) on an unconsolidated basis.” One risk is that trading platforms

⁴ SEC v. W.J. Howey Co., 328 U.S. 293 (1946).

will co-mingle customer assets with their assets. Some CTPs do not separate customer funds from their funds. Some fail to record the ownership of a digital asset on the blockchain. Instead, they register the transaction on an internal ledger. These two factors speak to some of the potential for systematic fraud.

II. Regulators should determine how a stablecoin could be structured to reside inside the regulatory perimeter. Nonetheless, bank stablecoins must meet specific safety standards, have community reinvestment obligations, be subject to consolidated supervision, and holders of these accounts should benefit from Regulation E protections. There should be strict rules that support interoperability.

a. When a stablecoin can meet these standards for safety, it should be eligible to be held on deposit at insured depository institutions and be eligible for deposit insurance.

Many government agencies are considering where a stablecoin fits inside the banking regulatory perimeter. In 2020, the Office of the Comptroller of the Currency (OCC) clarified that all federally-chartered banks and thrifts could hold digital assets in custody.⁵ In January, the OCC issued an interpretive letter addressing how banks may use stablecoins and blockchain technology to facilitate payment activities and other "bank-permissible functions."⁶ In August 2021, the Chair of the Securities and Exchange Commission (SEC) proposed to define certain stablecoins and other cryptocurrencies as securities.⁷ Last month, the President's Working Group on Financial Markets said that stablecoins should be held by insured depository institutions (IDIs), and that stablecoin issuers should be generally regulated like banks but did not clarify if funds held by those IDIs would be insured.⁸

With very few exceptions, most stablecoins are unsafe and should remain outside the financial system. However, if strict rules were established for when a stablecoin could be issued by a bank, consumer and systemic concerns could be addressed.

The benefits of being inside the banking regulatory perimeter should not be lost when a consumer moves a fiat deposit at a bank into a stablecoin deposit inside a bank.

As a first principle, accounts must be safe and sound: a stablecoin fully backed by a mixture of cash, short-term Treasuries, and other risk-free assets could qualify for inclusion within the banking regulatory perimeter. Risky assets, such as corporate bonds, mortgage-backed securities, other cryptocurrencies, commodities, and securities should not be considered viable instruments for reserves.

b. While there are many potential ways that a stablecoin could be folded into the formal banking system, most are suboptimal because they would pose risks to consumers and to systemic safety. A fully-insured closed-loop bank-issued interoperable stablecoin is a safe alternative.

⁵ Office of the Comptroller of the Currency. "Federally Chartered Banks and Thrifts May Provide Custody Services for Crypto Assets." News Release 2020-98, July 22, 2020. <https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-98.html>.

⁶ Office of the Comptroller of the Currency. Interpretive Letter. "OCC Chief Counsel's Interpretation on National Bank and Federal Savings Association Authority to Use Independent Node Verification Networks and Stablecoins for Payment Activities." Interpretive Letter, January 4, 2021. <https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-2a.pdf>.

⁷ Gary Gensler. "Remarks Before the Aspen Security Forum," August 3, 2021. <https://www.sec.gov/news/public-statement/gensler-aspen-security-forum-2021-08-03>.

⁸ President's Working Group on Financial Markets, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency. "Report on Stablecoins." Washington, D.C.: U.S. Department of the Treasury, November 1, 2021. <https://home.treasury.gov/news/press-releases/jv0454>.

Currently, most stablecoins are issued by non-banks that operate without consolidated supervision, do not offer insurance, are not interoperable (without a “bridge” token) with other stablecoins, do not provide Regulation E protections, and do not have a community reinvestment obligation.

While an example does not yet exist, a stablecoin issued by an institution with an ILC charter is unacceptable as it would open up the possibility that a commercial firm could use the ILC loophole to create a proprietary currency.

A bank could create a non-bank subsidiary to issue an uninsured stablecoin. While that would permit for consolidated supervision, it would not improve consumer protections for accounts, would not trigger a community reinvestment obligation, and would reinforce the overall lack of interoperability that is a current market wide shortcoming.

The bank-issued insured closed-loop stablecoin structure is optimal because it provides the benefits of stablecoin technology while preserving the safety of bank regulation. It requires coordination among banks to create a uniform and interoperable stablecoin.

Deposit insurance would apply when a consumer converted insured fiat-based funds into a stablecoin at the same financial institution or to a bank within a formal consortium of partner financial institutions. The principle is that protections afforded to fiat deposits should not be lost when a consumer moves those funds into an adequately constructed stablecoin account at the same institution. To permit the transfer to trigger the loss of consumer protections is risky. Also, by maintaining deposits within the same institution, standards for examining capital reserves could remain consistent.

For illustrative purposes, consider the USDF Consortium. Last year, five FDIC-insured banks founded the USDF consortium, and several other banks have joined since then. They have created a tokenized digital asset redeemable at par at every member bank.⁹ It is “closed-loop” in the sense that the token only operates inside the consortium. A consumer can transfer a deposit from New York Community Bank into a USDF token but then exchange their USDF for fiat currency at Webster Bank. The governance of the token is “off-chain.” A benefit is that these banks have effectively created a real-time gross settlement system.

By bringing a stablecoin product inside the banking regulatory perimeter, the payments system could benefit from the unique aspects of digital dollars without sacrificing consumer protections or compromising the safety and soundness of the financial system.

c. Financial institutions that issue insured closed-loop stablecoin should have a community reinvestment obligation.

When community reinvestment obligations are determined by who regulates the supervised entity, it opens the door for evasions and may undermine the scope of community reinvestment activity. When regulations focus on activities rather than entities, the effect is to prevent evasions.

For example, although banks and mortgage companies originate mortgages, they do not have the same community reinvestment obligations. Non-bank mortgage companies have no community reinvestment obligations. Nonetheless, mortgage companies benefit from government support, such as selling their

⁹ Introducing the USDF Consortium. (2022, April). USDF Consortium. <https://www.usdfconsortium.com>

loans to government-sponsored entities (Freddie Mac, Fannie Mae) and originating loans with FHA insurance.

Currently, when consumers exchange fiat deposits for uninsured stablecoins, it can undermine the scope of community reinvestment activities. For example, when fiat dollars are exchanged for stablecoins and transferred to trust accounts, funds have moved outside the community reinvestment ecosystem. Suppose they are transferred to a different bank but still held in an insured account in another metropolitan statistical area. In that case, it severs the relationship between a depositor's community and the assessment area. Moving from a bank with a full-scope CRA examination to one with a lighter review is also a change for the worse. Paxos Trust, the issuer of three of the world's six largest stablecoins, takes fiat deposits and converts them to stablecoins. While it holds reserves on a 1-to-1 basis, only a tiny fraction of those remain as dollars held in FDIC-insured accounts. Paxos invests the great majority of reserved funds in Treasury notes and bonds,¹⁰ severing the relationship between taking deposits and community reinvestment obligations.

d. Regulators must adopt uniform standards for insured stablecoins and apply similar consumer protections to fiat and insured digital deposits.

There are drawbacks to regulatory inconsistencies. One factor that led Congress to create the Financial Stability Oversight Council (FSOC) in Dodd-Frank was the belief that fragmentation created opportunities for firms to seek opportunities to elude regulation. By its very nature, shadow banking provides services similar to those offered by fully-regulated financial institutions but in contexts that evade equivalent regulation. When Lehman Brothers' Reserve Primary money market fund "broke the buck" in 2008, it caused a cascading series of problems that triggered the financial crisis. Lightly regulated entities such as non-bank mortgage loans and derivatives markets – also examples of shadow banking – played their parts in creating the grounds for the crisis.

To support interoperability, no distinction should exist in the structure or use of insured stablecoins that different banks issue within a consortium. To prevent run risk, consumers must not perceive that one stablecoin is safer than another. As a result, bank-minted stablecoins must have consistent reserve requirements, observe the same rules for risk management, and share capital and liquidity requirements.

e) Regulation E protections should be applied to insured stablecoin accounts held at insured depository institutions.

The fact that a stablecoin payment can settle in real-time presents both opportunities and risks for consumers. Consumers and businesses need real-time gross settlement (RTGS) of funds. The United States payments system is a laggard in addressing these needs. Developed economies have had real-time payment systems for over a decade.¹¹ Lesser-developed economies such as India¹² and Brazil have introduced new real-time payments systems after only several years of preparation. In contrast, FedNow

¹⁰ Charles Cascarilla. (2020, June 30). "The Digitization of Money and Payments" Testimony of Charles Cascarilla, CEO and Co-Founder of Paxos. <https://www.banking.senate.gov/imo/media/doc/Cascarilla%20Testimony%2006-30-201.pdf>

¹¹ Deloitte. (2019). *Economic Impact of Real-Time Payments* [Research Report]. <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-economic-impact-of-real-time-payments-report-vocalink-mastercard-april-2019.pdf>

¹² PricewaterhouseCoopers. (2020, December). *The remarkable rise of UPI in 2020*. PwC. <https://www.pwc.in/consulting/financial-services/fintech/dp/the-remarkable-rise-of-upi-in-2020.html>

has not yet been implemented, even though the Federal Reserve originally convened the Faster Payments Task Force in 2015.¹³

Unfortunately, RTGS systems must reconcile their attractiveness to fraudulent actors and the frequency of misdirected payments. The United Kingdom publishes a bi-annual report on payments fraud. While faster payments were not a significant vector for sender-authorized fraud when initially introduced, they became the favorite mode for scams by 2020. The U.K. reported that 95 percent of sender-authorized fraud involves a faster payment.¹⁴

To the extent that stablecoins become a part of the formal payments system, they should receive similar treatment. If a stablecoin that is held at an insured depository is structured to provide deposit insurance to account holders, then electronic payments made from the account should have Reg E protections. To implement that, the blockchain on which the stablecoin operates may have to be coded to allow for reversal of transactions.

f) Stablecoin issuers should be required to make public reports on diversity, inclusion and equity programs.

The prudential regulator of a bank-issued insured stablecoin issuer should require those banks to provide reports on their diversity and inclusion programs. Reports should cover employee and contractor diversity and commitments to purchase services and goods from businesses owned by women and people of color. Additionally, non-bank stablecoin issuers should provide insight into the demographics of their account holders.

III) Policy makers should address threats of cyber security, contagion, and systematic importance.

a) CTPs should be examined for cyber risks

Under regular regulatory regimes, financial institutions must demonstrate that their information systems can withstand attacks from cyber criminals. No such provisions exist in the unregulated world of cryptocurrencies. Yet the rationale for such responsibility exists. The scope of the market, its lack of transparency, the fact that its domain is entirely digital, and its lack of place-based infrastructure make it incumbent that someone "minds the store." Fifty-one percent of attacks, the Mt. Gox theft, crypto lockers, and ransomware are examples of systemic vulnerabilities.

Even the claim that customer transactions are registered on a blockchain is suspect; a 2018 paper contends that many trading platforms limit their record-keeping of customer assets to internal books and never report trades to a distributed ledger.

A regulatory body should assume responsibility to protect asset holders – and potentially the entire crypto ecosystem – from cybercrime. CTPs hold customer identification data, bank routing and account numbers, require tax information to report gains and losses to the Internal Revenue Service, and keep records of transactions. These activities make them targets for cybercrime. Unless a regulatory structure can hold them accountable for cyber-fraud, CTPs will not make the investments needed to defend against cyber-attacks.

¹³ Federal Reserve System. (2015). *Strategies for Improving the U.S. Payments System* [Consultation Paper]. <https://fedpaymentsimprovement.org/wp-content/uploads/strategies-improving-us-payment-system.pdf>

¹⁴ UK Finance. (2021). *Fraud—The Facts 2021: The Definitive Overview of Payment Industry Fraud*. <https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf>

b) Non-bank stablecoin issuers must be subject to heightened regulatory scrutiny.

Although stablecoins purport to be redeemable at par to the fiat currency on which they are pegged, this is not always the case. Earlier this year, TerraUSD (UST) – at the time the largest algorithmic stablecoin – lost nearly all of its value. Values of other algorithmic stablecoins fell below par, underscoring the capacity for contagion in this space. Some non-bank stablecoin issuers have not provided honest disclosures of the credit quality of their reserves. Some non-bank stablecoin issuers publish audits of their reserves at regular cadences, but there are no strong rules in place to make this mandatory nor are there standards and licenses for the auditors. Non-bank stablecoin issuers register with the Financial Crimes Enforcement Network (FinCEN) but that is not the same as being regulated. In spite of the lack of consistent and strong supervision, more than \$150 billion in stablecoins are in circulation.

To maintain safeguards against systemic risk, private non-bank issuers of stablecoins must be held to capital, reserve, and liquidity requirements.

FSOC should state that the Federal Reserve has supervisory authority over non-bank issuers of stablecoins. As well, the Federal Reserve should have a macroprudential responsibility to ensure that contagion in non-bank issued stablecoin markets do not carry over to the banking sector.

To be able to accept U.S. fiat deposits, non-bank stablecoin issuers should be required to establish a subsidiary within the United States that is subject to Federal Reserve supervision.

Any third parties that provide services for a non-bank stablecoin issuer should submit to supervision.

Non-bank stablecoin issuers should not be permitted to use funds received from consumers to make loans. By prohibiting non-bank stablecoin issuers from making loans, the Federal Reserve would create a firewall between the demonstrated volatility of these assets and other market participants.

The Federal Reserve should require all non-bank stablecoin issuers to provide reports on their diversity and inclusion programs. Reports should cover employee and contractor diversity and commitments to purchase services and goods from businesses owned by women and people of color. Additionally, non-bank stablecoin issuers should provide insight into the demographics of their account holders.

c) Policy makers should be prepared to determine when a digital asset, particularly a stablecoin, has become “too big to fail.”

Currently, the weak level of regulation and intense use of stablecoins create concerns for systemic safety. Federal agencies do not review stablecoins for safety and soundness. Several states have established regimes to charter digital asset issuers, but the majority of attention from state and federal agencies has been limited to enforcement actions.

Even after the onset of the most recent “crypto winter,” the market cap of all stablecoins exceeded \$150 billion at the end of July 2022. While this sum is by itself not large enough to present systemic risk, digital asset markets have shown themselves to be extremely prone to contagion. Moreover, the danger is clearly real, as the value of two stablecoins currently constitute almost eighty percent of the overall value of all stablecoins.¹⁵

¹⁵ CoinMarketCap. (n.d.). *Top Stablecoin Tokens by Market Capitalization*. Retrieved November 5, 2021, from <https://coinmarketcap.com/view/stablecoin/>

Moreover, the volume of stablecoin trading as a share of overall market capitalizations falls far outside of most other asset markets. On average, stablecoin trading volumes represent almost half of total market capitalization. During 2021, daily trading volume in Tether (USDT) routinely exceed its market capitalization. During a span in November 2021, daily trading volume exceeded total market capitalization by a factor of fifteen.¹⁶

Additionally, while concentration in stablecoin markets is extreme, even a small stablecoin can create havoc. The recent fall in digital asset prices began when a small stablecoin imploded. The fact that a minor asset could provoke such a change should present a warning.

Given these contexts, regulators choose a standard for defining “too big to fail” and then determine what level of trading would constitute the need to label a stablecoin with such a designation. In response to recommendations made by the President’s Working Group,¹⁷ FSOC should consider when a non-bank stablecoin achieves a level of systematic importance that it could be considered a Financial Market Utility.

RESPONSES TO SELECTED FSOC QUESTIONS

(A) Adoption to Date and Mass Adoption

(1) What explains the level of current adoption of digital assets?

a. Who are the users, consumers, and investors that are adopting digital assets?

While "mass adoption" may not yet stand as an accurate description of consumer exposure, dollar-equivalent values held in stablecoin are extensive and exceeded \$150 billion at the end of June 2022. Together, two stablecoins backed on a 1-to-1 basis to fiat-denominated assets have a value above \$120 billion.¹⁸

b. What businesses are adopting digital assets and for what purposes?

A distributed ledger is an efficient way to store information. Private firms have created blockchain-enabled services that solve interesting “back-end” problems such as identity verification and loan servicing. There are services that, for the price of a token, can review transactions to root out actors responsible for fraudulent behavior.

c. What are the main use cases for digital assets for consumers, investors, and businesses?

Consumers may choose to hold a digital asset for one or several reasons. Those motives are essential when considering how a digital asset should be regulated.

The ability of digital assets to settle in real-time is an important attribute.

¹⁶ Tether volume per day 2020-2022. (n.d.). Statista Financial Instruments and Investments. Retrieved August 5, 2022, from <https://www.statista.com/statistics/1272865/tether-trade-volume/>

¹⁷ President’s Working Group on Financial Markets, Federal Deposit Insurance Corporation, & Office of the Comptroller of the Currency. (2021). Report on Stablecoins. US Department of the Treasury. <https://home.treasury.gov/news/press-releases/jy0454>

¹⁸ CoinMarketCap. (n.d.). *Top Stablecoin Tokens by Market Capitalization*. Retrieved November 5, 2021, from <https://coinmarketcap.com/view/stablecoin/>

The ability to offer value-added data creates opportunities to serve consumers and small businesses in ways that cannot occur now. Even an RTGS using ISO 20022 would not have the same capabilities as a stablecoin running smart contracts for specific use cases. For example, in the internet of things, the payment amount could be a function of a diagnosis made by a machine, leading to a need for an itemized invoice for a conditional sum.

NFTs will provide support for artists and other creators of intellectual property. Since the rise of the internet, content creators have been challenged to capture the value of their work. It used to be that artists sold “rights” to their work for specific geographies, for the size of the print, for color versus black-and-white, etc. That has been nearly impossible. As a second-best option, many creators have resorted to selling all rights to their work in a single contract. NFTs will restore power to creators. Foreign correspondents use bitcoin to settle their accounts with overseas editors because it would be impossible to receive funds in fiat currency in a timely manner – or at all – in some places.

d. What are the implications for equitable economic growth?

Evidence shows that underserved and first-time investors are disproportionately more likely to have held a digital asset. Unfortunately, the volatility of these assets means their rapid adoption as investment instruments may not be suitable for everyone. As an asset class, digital assets are hazardous.

The unfortunate problem is that sophisticated investors participating in these asset classes will do so as a part of a diversified investment strategy. In contrast, many novice investors will overconcentrate their holdings in these risky investments. Data shows that individuals who trade in digital assets are less likely than the population as a whole to own stocks.¹⁹

Moreover, to differing extents, securities laws protect investors when they purchase most traditional investments. The same standard is not valid with digital assets. While some are subject to some regulation, most are not. In some instances, regulators have used enforcement tools, but there are fewer examples where private actors are supervised and held to meet regulatory requirements. That set of distinctions has established a two-tiered set of investor protections.

(B) Opportunities for Consumers, Investors, and Businesses. (3) What are the main opportunities for consumers, investors, and businesses from digital assets? For all opportunities described, please provide data and specific use cases to date (if any). In your responses, please consider:

a. Creating of new types of financial products and contracts

Digital assets, when utilized inside "smart contracts," create possibilities for new kinds of transactions. For example, a smart contract permits the internet of things to embed payments inside its ecosystem.

The ability for digital assets to trade in micropayments sets up possibilities to help certain providers find cash flows to support their operations. For example, micro payments could support journalism.

The blockchain promises to improve systems for anti-money laundering (AML) and know-your-customer (KYC) compliance. A distributed ledger running on a blockchain, by its very nature, maintains a trail of transactions. When ransomware as a service (RaaS) company Dark Side compromised a Colonial Pipeline account in 2021, the FBI used a service to track down the hackers and were able to recover most of the

¹⁹ Terri Bradford. (2022). *The Cryptic Nature of Black Consumer Cryptocurrency Ownership* [Payment Systems Research Briefing]. Federal Reserve Bank of Kansas City. <https://www.kansascityfed.org/research/payments-system-research-briefings/the-cryptic-nature-of-black-consumer-cryptocurrency-ownership/>

bitcoin that Colonial originally paid.²⁰ The outcome contradicts some popular opinions about cryptocurrency's utility for money laundering. In this case, an AML solution that has proven valuable in tracking illicit finance on a blockchain involves using a service that operates on the blockchain.

b. Potential for improved access to and greater ease of use of financial products.

Blockchain services could improve the ability to source indicia needed to open accounts for thin-file or no-file households. For example, one service provider uses the Stellar network to capture and store personally-identifying documentation from information sources in foreign countries. The service can help financial institutions confidently approve bank account applications from consumers and small businesses in cases where traditional document collection would have been too cumbersome or potentially impossible. As a result, the technology allows more people to be brought into the formal financial system.²¹

c. Potential opportunities for building wealth.

In some cases, non-fungible tokens (NFTs) may be able to introduce opportunities for owners of intellectual property to capture the value of their work. The NFT is creating meaningful benefits for photographers, for example.

However, consumers who perceive cryptocurrency as a means to "catch up" may be among the most vulnerable investors and are disproportionately likely to have less wealth and are more likely to be persons of color. A 2021 survey found that 55 percent of crypto investors do not have a college degree, more than one-third earn less than \$60,000 per year, and only 2 percent refer to a broker or advisor as a source of information to support a crypto-related trade.²² According to a 2022 survey, Black investors are twice as likely as others to rank cryptocurrency as the "best investment choice overall," twice as likely to choose crypto for their first investment, almost twice as likely to view it as safe, more than twice as likely to believe it is government-regulated and less likely to think it is risky.²³ While white households are almost three times more likely to own stocks (directly) than black households, they are only two-thirds as likely to own cryptocurrency. Black households are more likely to own cryptocurrency than holding a stock or a mutual fund. Owners of cryptocurrency are more likely to use alternative financial services than are other portions of the US population. For example, they are twice as likely to have used a payday loan, 2.5 times more likely to have used a check cashing service, and three times more likely to have used an auto title loan.²⁴

Given how consumers have reacted to the price increases in cryptocurrency and the demonstrated volatility in its values, regulators should ensure that it works to support an ecosystem with strong consumer protections.

²⁰ Uberti, D. (2021, June 11). How the FBI Got Colonial Pipeline's Ransom Money Back. *Wall Street Journal*. <https://www.wsj.com/articles/how-the-fbi-got-colonial-pipeline-ransom-money-back-11623403981>

²¹ Finclusive. (n.d.). *Compliance Made Simple*. Retrieved August 2, 2022, from <https://finclusive.com/why-finclusive#Not-a-Risk>

²² NORC at the University of Chicago. (2021). More Than One in Ten Americans Surveyed Invest in Cryptocurrencies. University of Chicago. <https://www.norc.org/NewsEventsPublications/PressReleases/Pages/more-than-one-in-ten-americans-surveyed-invest-in-cryptocurrencies.aspx>

²³ Claire, S.-P. (2022). *Stock Market Investing Is—And Isn't—Black & White* (Personal Finance). Charles Schwab. <https://workplace.schwab.com/content/stock-market-investing-is-and-isnt-black-white>

²⁴ Principato, C., Jesse Wheeler, & Sonnet Frisbee. (2022). The Crypto Report: Our Analysts on the State of Cryptocurrency (p. 29). The Morning Consult.

Similarly, prudential regulators should ensure that when a bank or a consortium of banks issues an insured stablecoin, they incur a community reinvestment obligation.

(D) Risks to Consumers, Investors, and Businesses: (5) Please identify and describe potential risks to consumers, investors, and businesses that may arise through engagement with digital assets. Identify any such responses that directly relate to:

State of play: When the crypto trading platform Voyager Digital suspended trading on July 1, 2022, it revealed some problems in unregulated crypto markets.

A lack of safeguards to ensure safe and sound procedures and a failure to review how Voyager conveyed to consumers about the lack of safety of their deposits demonstrate the need for regulatory intervention.

First, Voyager was making loans against the crypto assets held by its customers. No regulatory body had the kind of power that could have ensured that it held back enough capital to protect against fluctuations in asset values. Moreover, Voyager was reckless in how it structured its loan portfolio. It extended 68 percent of its loans to a single entity. That borrower was a holder of digital assets – so it shared the same vulnerability as Voyager to fluctuation in values of digital assets. Additionally, Voyager made false and misleading claims about the protections given to consumers over the safety of their assets. At various times, Voyager claimed that it was FDIC-insured, that its customers would receive FDIC insured on all funds provided to Voyager, and that the FDIC would insure customers against the failure of Voyager itself.²⁵

Except for the most experienced (accredited) investors, few retail customers had the means to understand the risks they were taking when they deposited funds inside a Voyager account. Through its website, Voyager stated that "through our strategic relationships with our banking partners, all customers' USD held with Voyager is now FDIC insured. That means that in the rare event your USD funds are compromised due to the company or our banking partner's failure, you are guaranteed a full reimbursement (up to \$250,000)."²⁶ Dollars on deposit at Voyager were held at FDIC-insured Metropolitan Commercial Bank, but the entity indemnified against risk was not the depositor but Voyager. Depositor funds would only be insured if Metropolitan Commercial Bank went bankrupt – deposit insurance did not cover the soundness of Voyager.

Even consumers who could understand distinctions in stablecoin reserving policies might have been confused by the claims made by Voyager about the safety of funds. For example, while the U.S. Dollar Coin issued by OCC chartered Paxos National Trust is supposed to be fully redeemable at par at any time, USDC held inside a Voyager account did not have the same protections in the event of Voyager's demise. A significant contributor to that risk was that Voyager was extending credit on its bitcoin and stablecoin. These practices would have been prohibited if Voyager had been held to consolidated supervision.

Unfortunately, the risks taken by Voyager and the corresponding absence of supervision in this space will hurt many consumers. Its proposed plan for reorganization out of bankruptcy will not return those funds

²⁵ Board of Governors of the Federal Reserve & Federal Deposit Insurance Corporation. (2022, July 28). FDIC and Federal Reserve Board issue letter demanding Voyager Digital cease and desist from making false or misleading representations of deposit insurance status [Joint press release]. <https://www.federalreserve.gov/newsevents/pressreleases/bcreg20220728a.htm>

²⁶ Invest Voyager. (2019, December 18). *USD held with Voyager is now FDIC Insured*. <https://web.archive.org/web/20210218190959/https://www.investvoyager.com/blog/voyager-is-now-fdic-insured/>

in dollars. Instead, consumers will receive shares of cryptocurrency and crypto tokens, have a claim to a pro-rata portion of any recoveries from Three Arrows Capital, and equity in Voyager.²⁷

a) Consumers are also vulnerable to potential losses associated with interacting with counterparties directly

Digital assets exist in highly volatile and relatively closed ecosystems. Digital assets are not interoperable with fiat currencies, so any consumer that wants to close a position in a digital currency must convert into a stablecoin before moving into fiat. Many stablecoins are themselves backed by other forms of cryptocurrency. For these reasons, digital assets are subject to contagion. For example, the recent crypto winter started when the value of the TerraUSD stablecoin plummeted to ten cents on the dollar. Holders of TerraUSD were suddenly underwater on assets that they were led to believe would be stable. Soon after that, crypto hedge fund Three Arrows Capital (3AC) filed for bankruptcy, leading to crises at two CTPs.

Depending on the scale of the compromised assets, contagion could spread to fiat-denominated spheres. The same crypto winter has impacted Signature Bank. Signature operates the digital service Signet. The bank recently reported that its clients withdrew almost \$700 million in stablecoin deposits in the last quarter. The bank attributed that to the loss in value of crypto assets.

b) To protect consumers from the failure/insolvency of wallets, custodians, or other intermediaries and disclosures of other relevant terms, regulators should supervise custodians, wallet providers, CTPs, and different types of intermediaries to ensure their safety and soundness.

Some CTPs use the funds they receive from consumers to make loans. This practice differs from the activities at traditional retail brokerages, where lending is limited to margin lending to account holders.

The privileges taken by digital asset intermediaries break from the policies at other types of brokerages. There are inconsistencies between the light regulation of CTPs compared to other exchanges. Traditional retail brokerages submit to supervision from the Securities and Exchange Commission and the Financial Industry Regulatory Authority (FINRA). The SEC establishes standards for disclosures of risks, sets capital reserve rules, ensures against conflicts of interest by managers, and promotes "fair, orderly, and efficient markets." FINRA has rules designed to protect investors and ensure market integrity. Equivalent rules and standards do not cover CTPs.

c) To address false and deceptive claims, intermediaries should be held accountable by regulators, including not just the SEC but also the CFPB and FDIC when applicable, to make truthful claims about the security of funds.

Consumers cannot be expected to recognize false claims about the safety of funds. The FDIC and the CFPB should review claims that funds have FDIC insurance. The CFPB and the SEC should review claims that stablecoins are redeemable anytime.

²⁷ Voyager Capital. (2022, July 11). Update on Customer USD and Crypto. *NODE from Voyager*. <https://www.investvoyager.com/blog/update-on-customer-assets/>

d) Rules should be established to separate trading from custody.

In traditional securities trading contexts, laws require trading platforms to establish firewalls between trading and custody of client assets.²⁸ The rules protect consumers. Equivalent controls do not exist for CTPs. Additionally, rules do not ensure that platforms have funds on hand to redeem customer assets.

(6) a. In your responses, please describe specific ways in which digital assets can benefit the underserved and the most vulnerable vis-a`-vis traditional financial products and services. Address factors such as identity verification processes, costs, speed, ease of use, and access.

As currently structured, digital assets may not advance financial inclusion to a meaningful degree. Short of holding a digital asset in a private key, consumers must have a bank account to move funds into a crypto trading platform account. From the perspective of addressing the number of unbanked households, digital assets will not advance policy goals.

a. *Some processes could utilize the blockchain to address shortcomings in the authentication and identify verification procedures that financial institutions deploy when evaluating an account application.*

By one estimate, between 90 and 99 percent of account applications rejected on the grounds of concerns about KYC/AML are false positives²⁹ – implying that qualified applicants are being turned down because of flaws in screening techniques. Nonetheless, financial institutions defer to caution because reputational and financial risks are associated with money laundering and illicit finance.³⁰

However, blockchain systems can solve other problems related to financial inclusion. In its purest form, a blockchain is a ledger that can hold information and verify its authenticity. Because of their distributed nature, blockchains can collect and preserve data. Many people cannot access the financial system because they lack proper indicia. Immigrants are one example – while they may have identifying documentation, it may not be in a form that meets the criteria of know-your-customer (KYC) rules. Items such as foreign driver's licenses, tax returns, utility bills, and consular identifications could provide supporting information to qualify for a financial service. The blockchain is well-suited for this role. A blockchain can store all of the previously-mentioned examples. Moreover, it can maintain it in a re-usable format. Once collected, any financial institution with the right blockchain expertise could use it to identify an account applicant.

Regulators should determine the efficacy of on-blockchain applications to track illicit activity. As a part of that effort, they should review procedures for procuring technology. Some regulators contend that the slow pace of procurement hinders their ability to take advantage of supervisory technology. Conversely, whereas there are many fintech startups, virtually no private investment goes into seeking methods to use blockchain technology to aid with supervisory efforts.

b. *A tokenized digital asset would overcome the concerns about privacy that compel some consumers to remain unbanked.*

²⁸ Timothy G. Massad. (2019). *It's Time to Strengthen the Regulation of Crypto Assets* (Brookings Economic Studies). John F. Kennedy School of Government at Harvard University. <https://www.brookings.edu/wp-content/uploads/2019/03/Timothy-Massad-Its-Time-to-Strengthen-the-Regulation-of-Crypto-Assets-2.pdf>

²⁹ Howard Bush. (2018, September 11). Reduce false positives, become more efficient by automating anti-money laundering detection. *Microsoft Azure Artificial Intelligence*. <https://azure.microsoft.com/en-us/blog/reduce-false-positives-become-more-efficient-by-automating-anti-money-laundering-detection/>

³⁰ Sarah Rutherford. (2019, November 14). How to Reduce AML False Positives and False Negatives [FICO Blog]. *FICO Decisions Blog*. <https://www.fico.com/blogs/how-reduce-aml-false-positives-and-false-negatives>

Privacy concerns are one of the main concerns given by the unbanked as a reason not to have a bank account.

A digital asset account can be structured in two forms – as an account or only as a tokenized digital asset. In the former, creating an account and associating it with an individual person or business is necessary. In the latter, there is no account. It is a representation of a single unit of value. The blockchain records the chronological history of the unit of value but without associating it with an individual. The ability to spend is derived from a permissioned right. The asset-based construct would, by disassociating the holding of an asset from an identity, overcome some of the privacy concerns that make some individuals reticent to use a bank account.

Conclusion

Consumers are suffering harm now and will continue to do so without intervention. The lack of uniform regulation and instances where entities are operating with little or no regulation create risks to consumers. Notably, digital assets have been adopted by populations that include those traditionally underserved by the financial system at concerning rates, leading to the possibility that volatility will further exacerbate economic inequality. The FSOC must work across agencies to address the gaps in protection.

Please contact Adam Rust (arust@ncrc.org) or me if you have additional questions.

Sincerely,

A handwritten signature in black ink that reads "Jesse Van Tol". The signature is written in a cursive, flowing style.

Jesse Van Tol
Chief Executive Officer
National Community Reinvestment Coalition
jvantol@ncrc.org