Crypto Council for Innovation

December 15, 2022

Secretariat to the Financial Stability Board
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland
fsb@fsb.org

Re: Consultations on the International Regulation of Crypto-Asset Activities: a Proposed Framework - questions for consultation (Oct. 11, 2022)

Dear FSB Secretariat:

The Crypto Council for Innovation ("CCI") submits this letter in response to the FSB's questions of October 11, 2022, for consultation on a set of recommendations and questions regarding the international regulation of crypto-asset activities ("Request").[1]

CCI appreciates the opportunity to share its information, expertise, and views on these vital issues with the FSB. Digital assets represent one of the most significant innovations in finance—and beyond—in many years, with the potential to alter ownership structures, commercial applications, cross-border payments, transaction processing and settlement, access to capital, investment opportunities, and much more. These developments contribute to equitable growth and financial inclusion, as well as investor and consumer choice and security.

Accordingly, the regulation of digital assets is a critical topic facing policymakers. In CCI's view, an appropriate regulatory framework for digital assets and activities will further rather than hinder the development and use of crypto. Balanced risk management is an integral component of effective technology innovation. This requires understanding and carefully considering the technologies and associated business models and use cases—both how they echo traditional financial structures and how they bring distinct benefits and risks.

In this submission, we elaborate on a series of foundational principles for a crypto regulatory framework called the *CCI Global Regulatory Blueprint* (see Exhibit 1). We propose the CCI Global Regulatory Blueprint to help guide policymakers as they consider the building blocks necessary for constructing a legal and regulatory framework that supports the growth of a robust and resilient Web3 economy. CCI views the Global Regulatory Blueprint as a living document of policy principles that address technical standards, illicit finance and national

[1] https://www.fsb.org/wp-content/uploads/P111022-2.pdf.

security, risk-management of centralized exchanges, consumer and investor protection; digital money, DeFi, digital identity, private commercial law, bankruptcy, accounting, tax and energy.

The development of a flourishing Web3 and digital ecosystem ultimately relies upon not only a foundation of optimistic innovators but also on laws, regulations and policies that guide policymakers, investors, and businesses to facilitate long term value. While the principles we lay out are by no means exhaustive, they nevertheless provide a valuable starting point when formulating more granular rules, design choices, economic incentive structures, and governance structures in the future. We look forward to continuing to work with the FSB as it develops its framework.

ABOUT CCI

CCI is an alliance of crypto industry leaders with a mission to communicate the benefits of crypto and demonstrate its transformational promise. CCI members include some of the leading global companies and investors operating in the crypto industry, including Andreessen Horowitz, Block (formerly Square), Coinbase, Electric Capital, Fidelity Digital Assets, Gemini, Paradigm, and Ribbit Capital. CCI members span the crypto ecosystem and share the goal of encouraging the responsible global regulation of crypto to unlock economic potential, improve lives, foster financial inclusion, protect national security, and disrupt illicit activity. CCI and its members stand ready and willing to work with the Financial Stability Board members to accomplish these goals and ensure that the most transformative innovations of this generation and the next are anchored in the United States.

DISCUSSION

I. Technological Innovation Improves Access, Efficiency, and Equity for Digital Consumers

Technological innovation enhances people's lives in meaningful ways. In the financial sector, policy should focus on consumer benefits, including empowering individuals to make informed financial decisions, ensuring competitive and open markets for products and services, increasing efficiency and reducing costs, minimizing abuse, and expanding access and opportunities for those who have been underserved by traditional financial providers. In short, technological innovation should be harnessed to improve access, efficiency, and equity for digital consumers.

Digital assets have already proved capable of furthering these goals. Digital assets often serve as a medium of exchange that is faster, more secure, and less expensive than traditional mediums. Digital assets, which can be accessed and used by anyone with a smartphone are also more widely available than traditional banking and investment mechanisms, which require bank or brokerage accounts and extensive documentation.

Substantial percentages of adults around the world today lack access to basic banking and financial opportunities. A recent World Bank report found that 1.4 billion people worldwide are unbanked (i.e., no access to a bank account).[2] Although lack of access is more significant in developing countries, it is also common in advanced economies. Almost one in five U.S. adults is at least partially constrained in their ability to use traditional financial services: about 5% are unbanked and another roughly 13% are underbanked (i.e., insufficient access to a bank account to meet financial needs).[3] Most adults who are unbanked or underbanked represent communities that have historically been the victim of discriminatory or exclusionary financial practices, including low education, low income, and people of color. With lower barriers to entry and without historically exclusionary or abusive practices and stigmas, digital assets offer people from historically excluded or unbanked and underbanked communities new access to secure, low-cost, and effective financial services—and members of those communities have already shown a strong interest in and adoption of digital assets.

Further, in many places in the world, especially where people are living under authoritarian regimes or suffer from hyperinflation or strife, crypto can provide a lifeline to store value out of the reach of corrupt or poorly run governments. For example, in 2020 digital assets provided one of the few means by which the U.S. government was able to deliver assistance to desperate people in Venezuela.[4] Similarly, the Ukrainian government has been able to receive and use digital assets quickly to buy essential items for the war effort.

Continued collaboration between governments and industry can further develop mechanisms to realize the full benefits of digital assets for all.

See also Exhibit 2 (Letter from CCI to Natalia Li, U.S. Department of Treasury, *re: Ensuring Responsible Development of Digital Assets*, at 9-13 (Aug. 8, 2022)); Exhibit 3 (Letter from CCI to Ali Khawar, U.S. Employee Benefits Security Administration, *re: Compliance Assistance Release No. 2022-01, 401(k) Plan Investments in "Cryptocurrencies,"* at 11-12 (June 14, 2022)).

II. Technical Standards Should Promote Openness, Interoperability, and Composability to Support the Evolution to Web3

Web3, which builds on decentralization, blockchain, and tokens and other digital assets, is the next stage in the evolution of the internet. Web3 can foster new creative and economic opportunities and systems for creators, investors, and consumers. The technological revolution arising out of the invention of the internet was based on the internet's ability to move information

---

[2] https://thedocs.worldbank.org/en/doc/25dde6ca97fde9ec442dcf896cbb7195-0050062022/original/Findex-2021-Executive-Summary.pdf.
[3] Board of Governors of the Federal Reserve System, Economic Well-Being of U.S. Households in 2020 (May 2021), https://www.federalreserve.gov/publications/2021-economic-well-being-of-us-households-in-2020-banking-and-credit.htm. *See also* Silvia Foster-Frau, *Locked Out of Traditional Financial Industry, More People of Color are Turning to Cryptocurrency*, Washington Post (Dec. 1, 2021), https://www.washingtonpost.com/national/locked-out-of-traditional-financial-industry-more-people-of-color-are-turning-to-cryptocurrency/2021/12/01/a21df3fa-37fe-11ec-9bc4-86107e7b0ab1_story.html.
[4] Nikhilesh De, *US Government Enlists USDC for 'Global Foreign Policy Objective' in Venezuela: Circle CEO*, CoinDesk (Nov. 20, 2020), https://www.coindesk.com/markets/2020/11/20/us-government-enlists-usdc-for-global-foreign-policy-objective-in-venezuela-circle-ceo/.

at the speed of light. Web3 now makes it possible to move value at the speed of light, and the consequences are similarly profound.

Web3's success depends on having standards that promote openness, interoperability, and composability. Open source code allows anyone to examine and verify the technical underpinnings of service provision, which furthers the integrity of the code and the system. Open APIs also facilitate interoperability—the reliable exchange of information between nodes in a system. And composability ensures that system components can be evaluated independently and recombined in myriad ways with other components to meet evolving user needs. Together, these features enable effective and trustworthy products and services.

In contrast, market asymmetries and monopolies arise when there are closed technical standards. The associated costs and friction can lead to suboptimal products for consumers and deprive creators of control over their work and data.

See also Exhibit 2 (Letter from CCI to Natalia Li, U.S. Department of Treasury, *re: Ensuring Responsible Development of Digital Assets*, at 6-10 (Aug. 8, 2022)).

III. Privacy, Anti-Money Laundering, and National Security

A. There Should Be Cross-Border Cooperation and Precise Know-Your-Customer and Anti-Money Laundering Regulations That Identify and Stop Illicit Activities

Having a clear and consistent global regulatory framework to strengthen financial integrity and combat money laundering and terrorist financing is critical to the maturation of the digital asset sector. Such a framework should be supported by proactive collaboration and real-time information sharing between the public and private sectors to mitigate the risk of money laundering, terrorist financing, and other illicit activity. Policymakers around the world should engage in regular cross-border cooperation and coordination.

The consultative approach of the Financial Action Task Force ("FATF") to developing initial guidance on anti-money laundering ("AML") and combating the financing of terrorism ("CFT") in the digital asset sector is important and encouraging. As the sector continues to innovate, FATF should continue to consult with the private sector and its members should engage in hands-on experimentation with the technology to ensure that they understand the full capabilities of the technology. And just as FATF has gained input from digital asset firms during its private sector consultations, local regulators should similarly engage the digital asset industry as they implement FATF's virtual asset guidance.

The United States provides an early example of successful public-private development of AML/CFT rules and practices. Many cryptocurrency businesses are covered by the U.S. Bank Secrecy Act, which requires implementation of various AML programs; such companies, mindful of close regulatory supervision, have drawn from the AML programs of traditional

financial institutions while developing additional elements reflective of the unique circumstances of crypto. Additionally, the U.S. Financial Crimes Enforcement Network ("FinCEN") has worked closely with crypto companies to leverage its advanced information and threat-detection capabilities.

Know-Your-Customer ("KYC") rules should be fit-for-purpose, using the technical capabilities of blockchain technology. KYC processes that collect the minimum amount of identifiable user data should be encouraged, as should experimentation with technologies and processes via exceptive relief and regulatory sandboxes. That can facilitate the development of crypto-native tools that leverage blockchain technology and transparency to effectively combat illicit finance.

See also Exhibit 4 (Letter from CCI to Jon Fishman, U.S. Office of Terrorist Financing and Financial Crimes, *re: Responsible Development of Digital Assets*, at 3-7, 10-12 (Nov. 3, 2022)); Exhibit 5 (Letter from CCI to Himamauli Das, U.S. FinCEN, *re: Response to FinCEN's Request for Information on the Modernization of U.S. AML/CFT Regulatory Regime*, at 2-20 (Feb. 13, 2022)); Exhibit 2 (Letter from CCI to Natalia Li, U.S. Department of Treasury, *re: Ensuring Responsible Development of Digital Assets*, at 17-20, 29-30 (Aug. 8, 2022)).

B. There Should Be Privacy-Preserving Technologies That Respect National Security Interests

Privacy is a fundamental human right and social good. Privacy-preserving technology allows data computation and targeted analysis while remaining encrypted to those performing the computation and malicious actors who might seek to steal or corrupt that information. Zero-knowledge rollups and configurable privacy blockchains are emerging forms of privacy-preserving technologies that balance individuals' privacy interests with broader public policy and societal requirements, such as effective compliance, transparency, and safety.

Governments should adopt laws and policies that allow for the development and use of privacy-preserving technologies, while also enabling compliance. For example, regulators could establish processes to evaluate the way novel mechanisms can be used to create and maintain digital identity records, including the adoption of digital identity verification techniques that can use a combination of decentralized blockchain-based technologies and secure "off-chain" data repositories. Regulators could also encourage zero-knowledge proof technologies, which allow users to interact with systems without revealing specific personal identifying information.

Concurrently, governments should respect personal privacy themselves by accessing or using data on individuals only when doing so is necessary to further a specific, narrowly tailored, and legitimate governmental objective.

See also Exhibit 5 (Letter from CCI to Himamauli Das, U.S. FinCEN, *re: Response to FinCEN's Request for Information on the Modernization of U.S. AML/CFT Regulatory Regime*, at 8-9, 17-18 (Feb. 13, 2022).

IV. Risk-Management of Centralized Exchanges

This section focuses on risk management standards for centralized exchanges. CCI is preparing a paper on best practices in risk management of centralized exchanges, which is forthcoming next month. In addition, we acknowledge that more study of DeFi is needed before we can suggest policy solutions. For more on DeFi, please see Section VII.

A. Centralized Exchanges Should Have a Pathway to Registration and Be Regulated Prudently

Centralized exchanges should have a pathway to regulatory registration and be subject to appropriately tailored regulations. The regulations should be calibrated to the risks associated with the functions and activities performed by a centralized exchange. In all cases, centralized exchanges should adhere to reasonable standards of operational and financial resilience, including risk management controls and systems that enable the exchange to identify, measure, monitor, and control the risks of its activities.

B. Consumers Should Be Informed via Audits and Disclosures

Transparency is necessary for exchange users to feel confident in their crypto-assets and the exchange. Exchanges should provide clear disclosures to customers as to the terms and conditions of their accounts. Issuers should improve their disclosures to help their users to make informed decisions about their investments based on their individual preferences.

Disclosures and other user-facing documents should clearly explain the terms, conditions, and risks associated with an entity, a product or service, and an asset. These materials should establish that: (i) withdrawal and transfer rights to user assets remains at all times with the user; (ii) an exchange can never sell, transfer, assign, lend, rehypothecate, pledge, or otherwise use or encumber user assets, except at the clear direction of the user; and (iii) the terms and conditions of any custodial arrangement, as well as associated risks.

Exchanges, custodians, and other third-party service providers should be subject to annual third-party public audits.

See also Exhibit 4 (Letter from CCI to Jon Fishman, U.S. Office of Terrorist Financing and Financial Crimes, *re: Responsible Development of Digital Assets*, at 5 (Nov. 3, 2022)); Exhibit 6 (Letter from CCI to Sen. Andrew Bragg, *re: The Digital Assets (Market Regulation) Bill 2022*, at 5-6 (Oct. 31, 2022)); Exhibit 2 (Letter from CCI to Natalia Li, U.S. Department of Treasury, *re: Ensuring Responsible Development of Digital Assets*, at 15-16 (Aug. 8, 2022)).

C. Centralized Crypto Exchanges Must Limit Risks That Affect Users

It is essential that centralized crypto exchanges maintain the trust of their users by protecting their assets and providing knowledge about how the platform's handles user assets. Accordingly, customer property must be segregated from non-customer property; such segregation can be achieved through the exchange's books and records.

Centralized exchanges should also maintain written policies to handle customer complaints. Appropriate training and processes should be in place to address complaints and escalate them, as needed, to senior management. Centralized exchanges should maintain customer service support available during normal business hours. Additionally, centralized exchanges should adapt their FAQs to account for customer complaints that occur with a large number of customers.

D. Operational Compliance Structures and Procedures Should Be Established for Operational Resilience on Centralized Exchanges

Centralized exchanges should establish effective frameworks for risk management, including for operational and compliance risk, and operational resilience.

Effective operational risk management is necessary for centralized exchanges to ensure operational resilience. As part of operational risk management, centralized exchanges should implement robust cybersecurity frameworks, which may include risk assessments; controls to identify, monitor, and mitigate risks; oversight of third-party and vendor relationships; employee training; secure identity management and access systems; and failover capabilities. In addition, insider risks should be mitigated through whistleblower protections, and malfeasance by managers and other employees should result in industry suspension or bans. Company directors should be held to the highest duty of loyalty.

E. Regulators Should Set Rules via ex Ante Regulations Rather Than ex Post Enforcement

Regulatory and supervisory expectations should be clearly established through ex ante rules for technologists and innovators. Developing rules ex post, through prosecution and government enforcement actions, creates uncertainty, which inhibits often-beneficial innovation.

See also Exhibit 2 (Letter from CCI to Natalia Li, U.S. Department of Treasury, *re: Ensuring Responsible Development of Digital Assets*, at 24 (Aug. 8, 2022)).

V. Consumer and Investor Protection

A. There Should Be a Comprehensive Consumer-Protection Framework Wherein Individuals Have a Right to Control Their Digital Assets

Property rights are fundamental in the physical world, and they should have the same status in the digital world as well. Consumers should be able to maintain control of their digital assets, including the right to transfer, give, host, and display their assets. Earlier internet platforms typically provided only some of these rights, but the successful implementation of a Web3 ecosystem can provide this entire bundle of rights to empower consumers in new ways.

The meaningful protection of these rights depends on many of the protections and practices described above: there must be disclosure requirements for asset sellers, safeguards against risks, clear governance, and operational resilience processes. These regimes should be accessible and comprehensible by the average customer without the need for a lawyer to interpret complex terms and conditions.

See also Exhibit 6 (Letter from CCI to Sen. Andrew Bragg, *re: The Digital Assets (Market Regulation) Bill 2022*, at 5-6 (Oct. 31, 2022)).

B. The Promise of Crypto Warrants Making Digital Assets Widely Available to Retail Consumers

Crypto's great promise warrants regulatory sensitivity to protect consumers without unduly deterring the expanded use of digital assets and services. Accordingly, regulators should prioritize educational tools and disclosure duties over overly prescriptive and restrictive rules which present barriers to retail consumers. However, regulators should prohibit predatory and other bad-faith practices such as targeted advertising based on debt-levels, race, or other vulnerable circumstances.

See also Exhibit 6 (Letter from CCI to Sen. Andrew Bragg, *re: The Digital Assets (Market Regulation) Bill 2022*, at 3-5 (Oct. 31, 2022)).

VI. Global Stablecoins

A. There Should Be Fiat-Backed Payment Tokens That Are Treated as Cash-Equivalents for Legal and Accounting Purposes

Payment tokens, including stablecoins, power the digital assets ecosystem. Fiat-backed stablecoins issued by centralized issuers should be backed by fiat currency 1:1, secure, audited, and subject to sufficient risk management practices. Such fiat-backed payment tokens should be backed only by segregated cash, bank deposits, or high-quality liquid assets ("HQLA"), such as short-term U.S. Treasuries or other internationally liquid denominated

government debt instruments (Euro, GBP, CHF, JPY). Issuers should also be required to publish quarterly third-party attestations and an annual third-party audit.

Accordingly, regulations and accounting rules should treat fiat-backed tokens as cash-equivalent and avoid double-counting and capital charges. Correspondingly, such payment tokens should be subject to appropriate taxation policies. And private commercial law should prohibit secured interests in such payment tokens.

See also Exhibit 6 (Letter from CCI to Sen. Andrew Bragg, *re: The Digital Assets (Market Regulation) Bill 2022*, at 6-7 (Oct. 31, 2022)); Exhibit 2 (Letter from CCI to Natalia Li, U.S. Department of Treasury, *re: Ensuring Responsible Development of Digital Assets*, at 27-28 (Aug. 8, 2022)).

B. Consumers and Investors Should Have the Right to Redemption

Consumers should be able to redeem stablecoins without fear of excessive delay, decline in value, or systemic risk. Under all circumstances, consumers should be able to redeem stablecoins for fiat currency or other equivalent pegged value within three business days from the day the transfer request is received. Redemption conditions, such as redemption fees and minimum redemption amount, must not be more onerous than existing conditions on withdrawals from traditional commercial bank accounts.

C. Stablecoin Issuers That Use Customer Funds for a Lending Business Should Be Subject to Appropriately Tailored Rules

Policymakers should not make artificial distinctions between who may issue stablecoins or how they reduce fluctuations in their value. Rather, they should follow the principles of tailoring and non-exclusion when designing any regulatory controls for stablecoins. The government should not limit the ability to issue stablecoins to banks or, as has been suggested more recently, affiliates of banks; it should allow responsible bank and non-bank entities alike to issue stablecoins.

Stablecoins that are backed 1:1 by cash or cash equivalents unbundle payments from the business of banking, which involves maturity and liquidity transformation. Accordingly, issuers of such payment tokens should not be required to have a banking license or bank affiliation. In contrast, issuers of any type of stablecoins that are not backed 1:1 by cash and cash equivalents and instead use customer funds for lending have not unbundled payments from maturity and liquidity transformation. Such stablecoins should be subject to more stringent rules.

See also Exhibit 2 (Letter from CCI to Natalia Li, U.S. Department of Treasury, *re: Ensuring Responsible Development of Digital Assets*, at 25-27 (Aug. 8, 2022)).

D. A Ban on Algorithmically-Valued Stablecoins is Not Necessary as a Stabilization Mechanism

The FSB's recommendation for stablecoin — that reserves should be "at least equal" to the amount of an issuer's outstanding stablecoins, consist only of "conservative" assets, "and not derive its value from algorithms" — would result in negative and unintended consequences for the blockchain ecosystem. The FSB recommendation exempts entities subject to prudential regulations, but the majority of stablecoin issuers do not fall within that category. Thus, a framework based on this recommendation would effectively ban algorithmic stablecoins — the best of which operate through over-collateralization by exogenous collateral.

We respectfully note that the FSB's concern may be largely misplaced because it focuses on algorithms as a source of instability, rather than the real problem — under-collateralization. Nearly one year into the current market volatility, the vast majority of algorithmic stablecoin projects have performed remarkably well, and the exceptional few that did not were significantly under-collateralized and had relied on collateral created by the issuers themselves.

A ban will unnecessarily treat all algorithmic stablecoins alike, when they are actually very different. The systemic risk posed by stablecoins is more a product of the design of their collateralization than their use of algorithms. Existing regulations could have been utilized to prevent much of the recent systemic harm, and new precise regulation could eliminate the risk of such systemic harm being repeated without hindering innovation. A ban of all algorithmic stablecoins is an overly blunt tool for the problem at hand. No one country would be able to remove all algorithmic stablecoins from its respective market, and consequently, a ban is likely to encourage regulatory arbitrage, putting users at an even greater risk of harm. [5]

The FSB should recommend a regulatory framework for algorithmic stablecoins that recognizes the important role of algorithms and digital assets. Regulation should prevent stablecoin issuers from taking on unreasonable amounts of risk, and lawmakers can protect users without such broad bans by enacting narrowly tailored collateralization requirements that allow for the development of safe software code. Algorithms are not only important to stablecoin development, they are also key to other aspects of the blockchain ecosystem, including DeFi, web3, and other digital asset markets. A blanket ban of algorithmic stablecoins could be viewed as an attack on these mechanisms, which could inadvertently hinder a wide array of web3 innovation.

[5] A blanket ban on stablecoins may also result in other unintended consequences, such as disrupting financial markets and causing significant user losses. A ban would be reckless and ultimately counterproductive from both an investor protection and software development perspective, potentially resulting in billions of dollars of losses for users policymakers are trying to protect.

VII. Decentralization

A. Policies and Regulations Should Recognize the Unique Features and Contributions of Decentralized Finance

Decentralized finance ("DeFi") is an emerging area of blockchain-enabled financial services and instruments, including brokerage, banking, and exchange, that do not involve the use of intermediaries. Financial intermediaries often introduce inefficiency through higher costs or slower execution. By eliminating intermediaries, DeFi holds the potential to level the playing field for many financial actors who have traditionally been disadvantaged, such as lower-income and unbanked/underbanked individuals and small businesses.

To realize these DeFi benefits, an appropriately tailored regulatory framework for DeFi is necessary and should involve the regulation of the centralized/business-owned applications, or onboarding access points to protocols, not the protocols or software themselves. In a decentralized system, no one particular entity controls the protocol, and a protocol cannot incorporate subjective determinations that traditional finance regulations sometimes require. Unlike the protocol layer, businesses and developers of DeFi applications do not have the same constraints with respect to subjective determinations. They can comply with different jurisdictional regulations and design flexible access points that minimize legal and regulatory risks.

Adoption of a regulatory framework that captures the software infrastructure that fuels the web3 ecosystem, rather than the applications which operate as access points, could jeopardize the benefits of DeFi for millions of people, and push lending protocol developers to jurisdictions with particularly loose regulatory frameworks. Similarly, in the context of BSA applicability, FinCEN has correctly recognized that suppliers of tools (communications, hardware, or software such as protocols) that may be utilized in money transmission, like anonymizing software, are engaged in trade and not money transmission. If regulators were to impose subjective and globally conflicting regulations on DeFi protocols, decentralization would be untenable, undermining the very properties that make DeFi protocols, and the web3 business models they support, functional and useful in the first place. Thus, regulators must account for decentralization when crafting policies and rules; frameworks for centralized platforms and instruments are unsuitable for decentralized ones.

Governments should take time to carefully study DeFi before making policy frameworks for this quickly-developing space. Governments may consider aspects such as progressive decentralization, varying governance and economic models, and the unique risks and benefits associated with operating financial services in this manner. For example, regulators should carefully consider the practice of progressive decentralization (a process whereby a blockchain-enabled application shifts gradually from centralized to decentralized, aka transmogrification), the diversity of governance and economic models supported by DeFi, and the distinct risks and benefits of DeFi.

There is a spectrum of varying levels of decentralization ranging from fully decentralized to strong centralized elements. For example decentralization might be evaluated according to the following multi-pronged test: Has the protocol been deployed beyond the developer team's unilateral control?; Is the protocol deployed on a blockchain with a high number of unaffiliated validator nodes?; Is the governance model of the protocol controlled by hundreds of unaffiliated participants or by only a few participants?; Are users' funds or assets held by a single party or custodian or in user's own wallets or bank accounts?

B. Decentralized, Self-Managed Identity is Critical to the Digital Economy

As discussed above, promoting privacy-preserving technology is vital. Emerging decentralization technologies facilitate privacy and control by enabling self-management of digital identity. Self-managed identity in turn enables users to participate in decentralized financial activity and, more broadly, to reap many benefits of online activities without the restrictions, intrusions, and privacy risks posed by intermediaries—which often face strong incentives to harvest, sell, or exploit individuals' personally identifiable data.

Regulators should prioritize appropriate frameworks to ensure access to, respect for, and the integrity of self-managed digital identity. Individuals should be compelled to share identifiable information only to the extent necessary to perform desired tasks and transactions.

Exhibit 5 (Letter from CCI to Himamauli Das, U.S. FinCEN, *re: Response to FinCEN's Request for Information on the Modernization of U.S. AML/CFT Regulatory Regime*, at 3 (Feb. 13, 2022)).

VIII. Insolvency Rules Should Put Crypto Consumers First as Technologies Evolve

Distinct features of digital assets necessitate insolvency rules for digital assets that are distinct from the insolvency rules for cash, securities, commodities, and associated accounts. Within the broader class of crypto, however, insolvency rules should be drawn flexibly to cover different crypto platforms, both as they exist today and as they might evolve, to provide continued predictability and integrity to investors and customers alike. And as with traditional bankruptcy rules, crypto-oriented bankruptcy rules should reflect investor and customer interests, not internal organization, technology, or business models except to the extent needed to promote investor and customer interests.

Still, within this framework, bankruptcy rules for crypto should protect customer interests while minimally impeding counterparty transactional flexibility. Bankruptcy rules should honor commercially agreed terms for digital assets. Those terms should define the specifics of the relationship between entities that transact with crypto and those customers. Customers should be provided with default customer protections, but customers should have the ability to opt out of this default relationship and its protections. Default customer protections should include: (i) mandated segregation of customers' digital assets from proprietary custodian assets, which can

be achieved through the custodian's books and records; (ii) prohibitions on encumbrances on the digital assets, other than as directed by and for the benefit of the customer; and (iii) fast and easy netting of customer positions and transferring of net custodied digital assets.

See Exhibit 7 (CCI, *Principles for Insolvency-Related Legislation and Regulation* (Dec. 15, 2022)).

IX. Private Commercial Law Should Provide Certainty for Market Participants

Private commercial law should provide clarity for market participants that engage in the acquisition or disposition of digital assets. The legal characterization and treatment of digital asset transactions should provide parties with confidence over key transactional issues, such as property rights, settlement finality, how to legally protect oneself from adverse claims in digital asset sales, or how to perfect and enforce security interests in digital assets against third parties, where applicable.

In common law countries, private commercial laws govern private transactions. For example, the U.S. has the Uniform Commercial Code, which was recently revised to take into account digital assets and is in the process of being adopted by the 50 states. In the UK, the UK Law Commission has proposed a new asset class: "data objects". Private commercial law around the globe should be flexible enough to cover the many different types of digital assets: ranging from digital money to digital securities to digital art along with new types of assets.

The legal recognition of property rights over digital assets should not hinge on impractical transfer mechanics or complex categorical definitions, as this can lead to uncertainty over the legal validity of transfers. Moreover, a successful crypto ecosystem cannot operate without digital money free of security interests. To the extent possible, perfecting a security interest in a digital asset should parallel the process of perfecting a security interest in the digital asset's analogous, physical counterpart. Private law should outline straightforward procedures that good faith purchasers can undertake to ensure the acquisition of digital assets free from any prior security interests.

X. Tax Regimes Should Avoid Over-reporting Errors for Taxpayers

Fair and sensible tax frameworks should account for the varied and constantly evolving nature of digital assets and blockchain technologies. Accordingly, blanket categorizations of certain digital assets as always taxable or nontaxable should be avoided as this can lead to serial underreporting or overreporting of a taxpayer's liability, inundating reporting agencies with ultimately unhelpful information. Taxpayers should be provided with clear guidance with regards to what types of crypto transfers and activities are taxable.

While governments should pursue goals of gathering complete and accurate tax reporting information, modifications of tax forms and reporting requirements should not cause taxpayers to mistakenly assume nontaxable transactions are taxable. Over-reporting can lead to erroneous estimates of one's tax liability, which can result in a taxpayer disposing of a digital asset before they would have done otherwise. Compliance with regulations and reporting should not be overly onerous or stymie participation in DeFi governance and Web3 innovation.

XI. Accounting Rules Should Recognize the Different Types of Crypto and be Globally Consistent

We support globally consistent treatment of digital assets under US GAAP and IFRS rules. In the US, many companies holding digital assets report digital assets as indefinite-lived intangible assets, like intellectual property. This treatment may be appropriate for some digital assets, but it is less appropriate for digital fiat, such as 1:1 fiat-backed stablecoins and CBDCs, and digital assets that are traded on platforms.

In October 2022, FASB met to discuss reporting of digital assets on a fair value basis and is planning to issue a crypto proposal for public comment. Meanwhile, earlier in the year, the US Securities & Exchange Commission issued Securities Accounting Bulletin 121,[6] opining that companies should account for custodial services of crypto assets as liabilities and corresponding assets on their balance sheets at fair value, which would pose challenges for custodians.

Accounting rules should take into account potential implications with regulations, such as Basel capital requirements and SEC reporting requirements under Section 13(a) and 15(b) of the Securities Exchange Act of 1934 and the registration requirements under Securities Act of 1933. For example, if digital money were treated as an intangible asset, then banks would have to hold capital against equivalents to cash.

XII. CCI Champions Crypto as a Bridge to Renewables and a More Sustainable Future.

While we recognize this principle is not directly relevant to financial regulation, we wish to mention our key principle on energy issues. Concerns about crypto's energy consumption often lack context or comparison to other industries and do not take into account the social value crypto offers nor take into account the commitment to clean energy by a number of the crypto industry. New developments in blockchain technology aim to reduce its energy impact and proactive and collaborative policy design can continue this trend.

In fact, there are significant energy infrastructure challenges today across the global economy, including around energy transfer and storage, as well as wasted and harmful

[6] https://www.sec.gov/oca/staff-accounting-bulletin-121

byproducts. Crypto data centers have unique properties that are already making them a valuable partner in the transition to a zero-carbon future. This includes their utilization in demand response programs, the use of stranded zero-carbon energy sources, and creating a market for under-valued renewables, among other approaches.

Furthermore, blockchain technology can bring transparency and accountability to previously opaque and inaccessible climate-related markets. Governments should leverage blockchain technology and crypto to unlock novel sustainability solutions and create new market incentives for zero-carbon energy sources. This includes the creation of new financial instruments and mechanisms that support the transition to a zero-carbon economy, as well as the use of blockchain-based platforms for tracking and verifying environmental impacts.

CONCLUSION

The last decade has witnessed unprecedented dynamism in the ways financial products and services are delivered, largely as a result of the development of blockchain technology. As FSB examines these developments and crafts a regulatory framework for crypto-related activities, it faces an opportunity to similarly reimagine how financial activities occur and are governed. On every aspect of crypto-related financial activity, traditional regulatory approaches hold some instructive value but cannot be directly applied; the distinct features, benefits, and risks of crypto-related activities compel a novel, textured regulatory approach. We hope the preceding discussion of principles helps guide the FSB effectively on its endeavor, and we look forward to continuing to collaborate with the FSB.

Respectfully submitted,

/s/ Sheila Warren

Chief Executive Officer
Crypto Council for Innovation

Exhibits:

1. CCI, *Global Regulatory Blueprint,* (Dec. 15, 2022).
2. Letter from CCI to Natalia Li, U.S. Department of Treasury, *re: Ensuring Responsible Development of Digital Assets*, (Aug. 8, 2022).

3. Letter from CCI to Ali Khawar, U.S. Employee Benefits Security Administration, *re: Compliance Assistance Release No. 2022-01, 401(k) Plan Investments in "Cryptocurrencies,"* (June 14, 2022).

4. Letter from CCI to Jon Fishman, U.S. Office of Terrorist Financing and Financial Crimes, *re: Responsible Development of Digital Assets*, (Nov. 3, 2022).

5. Letter from CCI to Himamauli Das, U.S. FinCEN, *re: Response to FinCEN's Request for Information on the Modernization of U.S. AML/CFT Regulatory Regime*, (Feb. 13, 2022).

6. Letter from CCI to Sen. Andrew Bragg, *re: The Digital Assets (Market Regulation) Bill 2022*, (Oct. 31, 2022).

7. CCI, *Universal Principles for Insolvency-Related Legislation and Regulation* (Dec. 15, 2022).

Crypto Council for Innovation

GLOBAL REGULATORY BLUEPRINT

CCI's mission is to ensure policies and regulations support the growth of a resilient and sustainable global digital economy. CCI believes the following global regulatory blueprint will assist, accelerate, and promote this mission.

Legal and regulatory frameworks should be bespoke, proportionate, and appropriately calibrated. Regulatory policies in this nascent but quickly evolving part of the financial services sector should be developed through transparent and open dialogues with industry, wider societal stakeholders, and the public. International frameworks should also seek to minimize asymmetrical policy development globally. Adopting this approach creates the building blocks of a successful, globally interoperable digital economy of the future, leveraging the innovative, technological foundations upon which the digital assets ecosystem is based.

Policy and regulation should recognize the nuance within the digital assets space—including, but not limited to, design choices, governance mechanisms, and economic incentive structures. They should also support Web3's growth in a diverse range of applications and use cases, including, but not limited to: decentralized finance (DeFi), decentralized identity, non-fungible tokens (NFTs), and decentralized autonomous organizations (DAOs).

Financial Inclusion

1. **CCI believes that technological innovation can improve access, efficiency, and equity for the average digital consumer.**

Technological innovation should be focused on meeting the needs of customers. Ensuring that financial inclusion is at the core of any framework is essential to achieving this goal. Heightened financial inclusion will create new opportunities for historically excluded communities, empower individuals to make informed financial decisions, enhance fundamental rights, and foster a competitive and open market for financial products and services, delivering efficiency and cost savings for end users. Governments and industry can work together to develop solutions that take full advantage of digital assets, both domestically and internationally.

Digital assets and blockchain technology can enable more inclusive and transparent allocation of financial resources. For example, crypto assets and blockchain-based platforms can enable the creation of new financial instruments and mechanisms that allow for the more efficient and equitable distribution of capital and resources, providing opportunities for individuals and communities that are traditionally excluded from the financial system, such as those without access to traditional banking services or credit.

Technology and Industry Standards

2. **CCI champions interoperable and open standards that facilitate permissionless and composable systems.**

Web3 is the idea of a ground-breaking new internet ecosystem powered by blockchain and digital assets and owned by contributors and users. Web3's success is contingent on the free exchange of information and composability.

Interoperability, open standards, and composability are key to disintermediating financial services. Open-source code allows anyone to examine and verify the technical underpinnings of service provision. This code can also be used to form the building blocks of new services, facilitating more competitive markets. Additionally, open APIs allow for information exchange across services. Composability refers to the idea that any application on a network can frictionlessly interact with any other application.

Bringing data together via open-source code, open APIs, and interoperable standards can add value to customers through specialized services provision or by creating new products and services altogether.

Market asymmetries and monopolies arise when there are closed technical standards, which can lead to additional costs and suboptimal products for consumers.

Privacy, AML, and National Security

3. **CCI advocates precise Know Your Customer and Anti-Money Laundering (AML) regulations that identify and mitigate illicit activities and for international cooperation that prevents regulatory arbitrage.**

The digital asset industry around the world needs clear AML regulations in order for the sector to grow in a way that mitigates illicit finance and bolsters international financial integrity. The Financial Action Task Force (FATF) has helped this aim immensely through its formal AML/CFT guidance on virtual assets. As regulators confront newer innovations in the crypto space, FATF should continue to consult with the private sector and its members should engage in hands-on experimentation with the technology to ensure that they understand the full capabilities of the technology. And just as FATF has gained input from digital asset firms during its private sector consultations, local regulators should similarly engage the digital asset industry as they implement FATF's virtual asset guidance.

Proactive collaboration and real-time information sharing between the public and private sector is crucial to mitigate the risk of money laundering, terrorist financing, or other criminal or illicit activity. Policymakers around the world should engage in regular cross-border cooperation to share AML/CFT best practices and lessons learned. The alternative poses the risk of creating a fractured and unevenly regulated digital assets market, which can ultimately create more danger for countries' national security.

Know Your Customer rules should be fit-for-purpose, utilizing the unique technical capabilities of blockchain technology. Experimentation should be encouraged via exceptive relief and

regulatory sandboxes, as doing so can facilitate the development of crypto-native tools that leverage blockchain technology and transparency to create a compliant ecosystem that effectively combats illicit finance.

4. **CCI supports the development of privacy-preserving technologies that respect national security interests.**

Privacy is a fundamental human right, and governments should only access or utilize data on individuals when doing so is necessary to further a specific and narrowly-tailored objective. Privacy-preserving technology allows data computation and targeted analysis while remaining encrypted to those performing the computation and adversaries who might seek to steal that information.

Zero-knowledge rollups and configurable privacy blockchains are examples of innovative technologies that are being developed to enhance privacy in the digital world. These technologies are designed to strike a balance between the need for individual privacy and broader public policy and societal requirements such as effective compliance, transparency, and safety.

Risk Management

5. **CCI believes centralized exchanges must be regulated prudently and have operational compliance structures that create operational resilience**

Centralized exchanges should have a pathway to regulatory registration and be subject to appropriately tailored regulations. The regulations should be calibrated to the risks associated with the functions and activities performed by a centralized exchange. In all cases, centralized exchanges should adhere to reasonable standards of operational and financial resilience, including risk management controls and systems that enable the exchange to identify, measure, monitor, and control the risks of its activities.

It is essential that centralized crypto exchanges maintain the trust of their users, above all by protecting users' assets. Accordingly, customer property must be segregated from non-customer property; such segregation can be achieved through the exchange's books and records.

Effective operational risk management is necessary for centralized exchanges to ensure operational resilience. As part of operational risk management, centralized exchanges should implement robust cybersecurity frameworks, which may include risk assessments; controls to identify, monitor, and mitigate risks; oversight of third-party and vendor relationships; employee training; secure identity management and access systems; and failover capabilities. In addition, insider risks should be mitigated through whistleblower protections, and malfeasance by managers and other employees should result in industry suspension or bans. Company directors should be held to the highest duty of loyalty.

6. **CCI believes consumers should be informed via audits and disclosures**

To ensure full confidence in user rights and claims, exchanges should provide clear disclosures to customers as to the terms and conditions of their accounts. Issuers should improve their disclosures to help their users make informed decisions about their investments based on their individual preferences.

Disclosures and other user-facing documents should clearly explain the terms, conditions, and risks associated with an entity, a product or service, and an asset. These materials should establish that: (i) withdrawal and transfer rights to user assets remains at all times with the user; (ii) an exchange can never sell, transfer, assign, lend, rehypothecate, pledge, or otherwise use or encumber user assets, except at the clear direction of the user; and (iii) the terms and conditions of any custodial arrangement, as well as associated risks.

Moreover, exchanges, custodians, and other third-party service providers should be subject to annual third-party public audits.

Consumers and Investor Protection

7. **CCI agrees that we should work towards a comprehensive consumer protection framework wherein individuals have a right to control their digital assets.**

The possession of property rights are a fundamental right in the physical world, and they should be protected in the digital world as well. Consumers should be able to maintain control of their digital assets, which includes the right to transfer, gift, self-host, and display their assets. Status quo internet platforms have only provided some of these rights, but the successful implementation of a Web 3.0 ecosystem can provide this entire bundle of rights to empower consumers in a new way.

The right to control one's digital assets necessitates that sellers of these assets provide proper disclosures, appropriate safeguards and protections, and a clear governance and operational resilience process for when something goes wrong. Disclosures should allow individuals to make informed decisions. Regimes should be accessible and parsable by the average customer without the need for a lawyer to interpret complex terms and conditions.

8. **CCI believes in the promise of crypto and making crypto assets available to retail consumers.**

An internationally consistent regulatory framework should facilitate making crypto mainstream. In order for consumers to use crypto, retail consumers should have access to fiat-backed payment stablecoins.

Retail consumers also should have inclusive access to retail trading of crypto-assets and related structured products. Governments should prioritize anti-money laundering and consumer protection without going to the extent of entirely banning access to this asset class to the retail segment. A concerted effort from the industry and policymakers should be focused on education enablement and risk assessment to ensure individuals are well-informed before they engage in investing in digital assets and to embrace self-hosted wallets. Predatory and other

bad-faith practices such as targeted advertising based on debt-levels, race, or other sensitive categories should be prohibited.

Payment Tokens, Stablecoins, and CBDCs

9. **CCI advocates for fiat-backed payment tokens being treated as cash-equivalent under laws, regulations, and accounting.**

Payment tokens issued by centralized issuers, including stablecoins, power the digital assets ecosystem and should be backed 1:1, secure, audited and have sufficient risk management practices. Fiat-backed payment stablecoins should be backed only by segregated cash, bank deposits and HQLA, such as short-term US Treasuries or other internationally liquid denominated government debt instruments (EUR, GBP, CHF, JPY).

Stablecoin issuers should provide daily proof of reserves along with real-time reporting of the tokens across blockchains. Issuers should publish quarterly third-party attestations and an annual third-party audit.

Private commercial law should prohibit secured interests in fiat-backed payment tokens. Regulations and accounting rules should treat them as cash-equivalent and avoid double-counting and capital charges. This also includes establishing appropriate taxation policies.

Separately, a regulatory framework for algorithmic stablecoins should recognize the role of algorithms and digital assets and how they operate through over-collateralization by exogenous collateral.

10. **CCI supports consumers and investors having the right to redemption.**

Consumers should be able to redeem stablecoins without the fear of excessive delay, decline in value, or systemic risk. Under all circumstances, consumers should be able to redeem stablecoins for fiat currency within three business days from the day the transfer request is received. Redemption conditions such as redemption fees and minimum redemption amount must not be more onerous than status quo conditions on withdrawals from traditional commercial bank accounts.

11. **CCI believes any centralized stablecoin issuer that uses customer funds for a lending business should be subject to bank-like rules.**

Stablecoins of centralized issuers that are backed 1:1 by cash and cash equivalents unbundle payments from the business of banking, which involves maturity and liquidity transformation. Stablecoins of centralized issuers that are not backed 1:1 by cash and cash equivalents and instead use customer funds for lending have therefore not unbundled payments from maturity and liquidity transformation. Such issuers, therefore, should be subject to more stringent rules.

12. **CCI supports a clear pathway in bankruptcy that puts consumers first.**

Insolvency rules should be crafted flexibly to cover different crypto platforms, both as they exist today and as they might evolve, to provide continued predictability and integrity to investors and customers alike. Additionally, bankruptcy rules should protect customer interests while minimally impeding on counterparty transactional flexibility.

Bankruptcy rules should honor commercially agreed terms for digital assets. The terms should define a custodial relationship for digital assets held for customers. This custodial relationship should be the default relationship that customers can opt out of, if they are aware of the risks of doing so. Other default customer protection should include: (i) mandated segregation of customers' digital assets from proprietary custodian assets; (ii) prohibitions on encumbrances on the digital assets, other than as directed by and for the benefit of the customer; and (iii) fast and easy netting of customer positions and transferring of net custodied digital assets.

Decentralized Finance

13. CCI supports policy and regulatory proposals that recognize the unique features and contributions of decentralized finance (DeFi).

Decentralized finance (DeFi) is a general term for an emerging area of blockchain-enabled financial services. This includes the offering of financial services and instruments without the use of intermediaries such as brokerages, banks, or centralized exchanges.

By removing expensive, inefficient and slow intermediaries that can affect lower income individuals the most, DeFi provides greater access to financial services for those who otherwise would remain underbanked, decreases fees, and improves efficiency for consumers, especially small business owners. DeFi protocols on the blockchain should aim to reach to achieve decentralization by evaluating the following:

Superimposing regulatory frameworks for centralized financial players may be untenable for decentralized finance players. Governments should take time to carefully study DeFi before making policy frameworks for this quickly-developing space. This may consider aspects such as progressive decentralization, varying governance and economic models, and the unique risks and benefits associated with operating financial services in this manner.[1]

Decentralized Identity (aka Self-Managed Identity)

14. CCI supports truly decentralized applications on blockchain that provide the opportunity for self-managed identity as a critical building block of the digital economy.

Governments should prioritize the creation and adoption of appropriate frameworks for self-managed digital identity, which will be one of the key building blocks for a Web3 digital economy. Self-managed digital identity refers to a model whereby individuals have more autonomy over and control over their digital identities. Initial on-ramps which leverage

[1] For example decentralization might be evaluated according to the following: 1) Has the protocol been deployed beyond the developer team's unilateral control?; 2) Is the protocol deployed on a blockchain with sufficient validator nodes through a decentralized consensus mechanism?; 3) Is the governance model of the protocol controlled by hundreds of unaffiliated participants or by only a few participants?; 4) Are assets managed in user controlled non custodial wallets or centrally managed by the platform?

centralized infrastructure or third parties should use a KYC process that collects the minimum amount of identifiable data necessary to verify a user's identity.

Decentralized applications can provide tools to enable individuals the ability to reap the benefits of the internet without the need of a third-party intermediary harvesting, selling, or transferring an individual's identifiable data. An individual should only be compelled to share identifiable information when it is deemed a necessary precondition for access, and digital identity verifiers should enable people to share the least amount of data possible to minimize the sharing of unnecessary personally identifiable information.

Private Commercial Law

15. Private Commercial Law should provide legal certainty and efficiency.

Private commercial law should provide clarity for market participants engaging in the acquisition or disposition of digital assets. The legal characterization and treatment of digital asset transactions should provide parties with confidence over key transactional issues, such as property rights, settlement finality, how to legally protect oneself from adverse claims in digital asset sales, or how to perfect and enforce security interests in digital assets against third parties.

The legal recognition of property rights over digital assets should not hinge on impractical transfer mechanics or complex categorical definitions, as this can lead to uncertainty over the legal validity of transfers. Moreover, a successful crypto ecosystem cannot operate without digital money free of security interests.To the extent possible, perfecting a security interest in a digital asset should parallel the process of perfecting a security interest in the digital asset's analogous physical counterpart. Private law should outline straightforward procedures that good faith purchasers can undertake to ensure the acquisition of digital assets free from any prior security interests.

Tax

16. Tax Regimes should avoid over-reporting that cause taxpayers to mistakenly assume nontaxable transactions are taxable

Fair and sensible tax frameworks should account for the varied and constantly evolving nature of digital assets and blockchain technologies. Accordingly, blanket categorizations of certain digital assets as always taxable or nontaxable should be avoided as this can lead to serial underreporting or overreporting of a taxpayer's liability, inundating reporting agencies with ultimately unhelpful information. Taxpayers should be provided with clear guidance with regards to what types of crypto transfers and activities are taxable.

While governments should pursue goals of gathering complete and accurate tax reporting information, modifications of tax forms and reporting requirements should not cause taxpayers to mistakenly assume nontaxable transactions are taxable. Over-reporting can lead to erroneous estimates of one's tax liability, which can result in a taxpayer disposing of a digital asset before they would have done otherwise. Compliance with regulations and reporting should not be overly onerous or stymie participation in DeFi governance and Web3 innovation.

Accounting

17. Accounting rules should be globally consistent and recognize the different types of crypto accounts and interactions with regulatory rules that rely on reporting.

CCI supports globally consistent treatment of digital assets under US GAAP and IFRS rules. In the US, many companies holding digital assets report them as indefinite-lived intangible assets, like intellectual property. This treatment may be appropriate for some digital assets, but it is less appropriate for digital fiat, such as 1:1 fiat-backed stablecoins and CBDCs, and digital assets that are traded on platforms.

In October 2022, FASB met to discuss reporting crypto assets on a fair value basis and is working toward the development of a crypto proposal that will be issued for public comment. Earlier in the year, US Securities & Exchange Commission issued Securities Accounting Bulletin 121,[2] opining that many crypto assets should be treated as liabilities. Accounting rules should take into account potential implications with regulations, such as Basel capital requirements and SEC reporting requirements under Section 13(a) and 15(b) of the Securities Exchange Act of 1934 and the registration requirements under Securities Act of 1933.

Energy

18. CCI champions crypto as a bridge to renewables and a more sustainable future.

Concerns about crypto's energy often lack context or comparison to other industries and do not consider the social value that crypto offers. New developments in blockchain technology aim to reduce its energy impact and proactive and collaborative policy design can continue this trend.

There are significant energy infrastructure challenges today across the global economy, including around energy transfer and storage, as well as wasted and harmful byproducts. Crypto data centers have unique properties that are already making them a valuable partner in the transition to a zero-carbon future. This includes through demand response programs, utilization of stranded zero-carbon energy sources, and creating a market for under-valued renewables, among other approaches.

Moreover, blockchain technology can be used as a tool to bring transparency and accountability to previously opaque and inaccessible climate-related markets. Governments should utilize blockchain technology and crypto to unlock novel sustainability solutions and create new market incentives for zero-carbon energy sources.

US-specific principles

State Optionality

19. CCI supports the preservation of optionality between robust state regulatory frameworks and a federal regulatory framework for crypto assets.

[2] https://www.sec.gov/oca/staff-accounting-bulletin-121

We believe that state-based frameworks, especially when coordinated amongst and across each other, can serve as an efficient and effective regulatory model for the industry. We also support concepts like passporting and reciprocity as ways that states can enhance the efficiency of the state-based framework.

The dual banking system in the United States has been a longstanding and effective approach to the chartering of banks, which can opt into state-based or national regimes.

There will be trade offs to opting into various regulatory frameworks, which will be consistent with a competitive marketplace.

Concluding comments

Digital assets represent one of the most significant innovations in the 21st century economy with the potential to alter ownership structures, commercial applications, cross-border payments, transaction processing and settlement, access to capital, investment opportunities, and much more. These developments can contribute to equitable growth and financial inclusion, as well as investor and consumer choice and security.

It is imperative governments, consumers, businesses, and investors become more educated in this rapidly evolving space. Appropriate rules and regulations can be an enabler to nurture innovation, competition and choice but must also provide safeguards for consumers to have trust in both the technology and the ecosystem. As parties become more informed of the transformative potential of digital assets, responsible innovators and policymakers will be well positioned to create products and services that leverage the inherent strengths of blockchain technology within a well understood, globally-aware, mutually beneficial and credible framework

Crypto and blockchain technology will be core to the digital economy for any sovereign jurisdiction regardless of geographic regions and political affiliations. Getting policies and regulation right at this early stage will be key to ensuring that the potential of the technology is fully realized.

Crypto Council for Innovation

August 8, 2022

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

Re: Ensuring Responsible Development of Digital Assets, TREAS-DO-2022-0014-0001

Dear Ms. Li:

The Crypto Council for Innovation ("CCI") submits this letter in response to the request of the Department of the Treasury for comment regarding "Ensuring Responsible Development of Digital Assets" ("Request").[1] The Department issued the Request in connection with its preparation of its report "on the implications of developments and adoption of digital assets and changes in financial market and payment system infrastructures for United States consumers, investors, businesses, and for equitable economic growth," which the President directed the Department to submit to him by September 5, 2022.[2]

CCI appreciates the opportunity to share its information, expertise, and views on this vital issue with the Department, as well as the ongoing engagement that CCI and its member companies have had with Department officials since the issuance of the Executive Order. Cryptocurrency represents one of the most significant innovations in finance—and beyond—in many years, with the potential to alter ownership structures, commercial applications, cross-border payments, transaction processing and settlement, access to capital, investment opportunities, and much more. These developments contribute to equitable growth and financial inclusion, as well as investor and consumer choice and security. The regulation of cryptocurrency, therefore, is an important question for policymakers. Developing an appropriate regulatory framework for cryptocurrency requires an understanding of the technology and careful consideration. Ever since the Financial Crimes Enforcement Network ("FinCEN") became the leading government agency in crypto-related regulatory guidance, the Department has engaged in meaningful public-private sector engagement, with the understanding that doing

[1] Dep't of the Treasury, *Ensuring Responsible Development of Digital Assets* ("Request") TREAS-DO-2022-0014-0001, 87 Fed. Reg. 40,881 (July 8, 2022).
[2] Request, 87 Fed. Reg. at 40,881; *see Executive Order on Ensuring Responsible Development of Digital Assets* § 5(b)(i).

so is critical to getting the regulatory framework right. We look forward to continuing to work with the Department on its report to the President and in the future.

In light of the short deadline for responding to the Request, CCI hopes that the Department will consider information submitted after the comment deadline.[3] Given the breadth and complexity of regulatory issues raised by the emergence of digital assets, these efforts will ensure the Department—and ultimately the President—receive the full benefit of the industry's expertise, information, and views.

SUMMARY

As we discuss in more detail below, cryptocurrencies and blockchain applications more generally are significant and evolving technological innovations with many use cases developed under a variety of business models. These innovations have the potential to bring increased transparency, security, efficiency, and inclusion not only to financial services, but to other sectors as well. As the Department considers what legislation and regulation are appropriate to promote responsible innovation in cryptocurrencies and other digital assets, CCI respectfully submits that the Department should be guided by key principles, including:

- Legislation and regulation should be tailored to address the unique characteristics of cryptocurrencies.
- Legislation and regulation should create a level playing field for all who want to be in the crypto industry.
- Legislation and regulation should promote responsible innovation while putting in place appropriate protections for consumers and investors.
- Legislation and regulation should ensure that innovators can operate in the United States, with certainty about the rules, and take into account that doing so is also paramount to the United States' national and economic security interests.
- Discouraging regulation by enforcement.

In the pages below, CCI provides information on the benefits of cryptocurrencies and blockchain technology more generally. We then elaborate on the principles that we believe should guide legislation and regulation in this area. Finally, we show how those principles should inform policy choices in three important areas: cryptocurrency transfers; stablecoins; and self-hosted wallets.

Developing blockchain technology will serve as the infrastructure of the global digital economy. It is paramount that the U.S. remains at the center of this technological leap in digital evolution if we are to maintain our monetary, economic and political preeminence in the global theater. While the United States has been at the forefront of many of these crypto

[3] In addition to the topics discussed in this response, the treatment of cryptocurrency and digital assets during bankruptcy proceedings is an additional important consideration. CCI intends to continue its engagement with policymakers in the future on this topic.

developments, the current uncertain regulatory climate that developers face in the U.S. is poised to drive overseas the next generation of blockchain-based applications. Indeed, because of the inherently global nature of blockchain technology, this risk is particularly acute in the cryptocurrency context. Regulation that is not sensitive to the unique dynamics of cryptocurrency, combined with the "de-risking" of U.S. financial institutions in developing regions, can also have a significant impact on U.S. national security as U.S. companies become less predominant in the cryptocurrency space.

The absence of U.S. firms from the cryptocurrency payments space can also leave voids that could be filled by other payments technologies, like China's Digital Yuan project, which has the potential to fundamentally reshape the global payments ecosystem in a way that will undoubtedly be detrimental to U.S. interests.

In the face of global competition, U.S. policymakers have an opportunity to counteract these trends, and help realize the promise of crypto. While the economic benefits of keeping cryptocurrency companies in the United States are obvious, it is also a tremendous advantage to U.S. national security and law enforcement to ensure that the cutting edge of innovation remains in this country.

ABOUT CCI

CCI is an alliance of crypto industry leaders with a mission to communicate the benefits of crypto and demonstrate its transformational promise. CCI members include some of the leading global companies and investors operating in the crypto industry, including Andreesen Horowitz, Block (formerly Square), Coinbase, Electric Capital, Fidelity Digital Assets, Gemini, Paradigm, and Ribbit Capital. CCI members span the crypto ecosystem and share the goal of encouraging the responsible global regulation of crypto to unlock economic potential, improve lives, foster financial inclusion, protect national security, and disrupt illicit activity. CCI and its members stand ready and willing to work with the Department and the Administration to accomplish these goals and ensure that the most transformative innovations of this generation and the next are anchored in the United States.

DISCUSSION

I. BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLOGIES

As policymakers consider regulation and legislation related to cryptocurrencies and other applications of blockchain and distributed ledger technologies ("blockchain") to financial services and markets, they should take care not to unintentionally inhibit uses in other, non-financial areas. To do so would arbitrarily limit blockchain applications and deprive the country of their full benefits.

A. TECHNOLOGY BENEFITS

Blockchain technology provides benefits to the transparency, security, and efficiency of an information system. As the Executive Order explains, blockchain "refers to distributed ledger technologies where data is shared across a network that creates a digital ledger of verified transactions or information among network participants and the data are typically linked using cryptography to maintain the integrity of the ledger and execute other functions, including transfer of ownership or value."[4] In other words, a blockchain uses a form of cryptography to create a shared and verified chain of linked data entries to store information.

The blockchain structure has a number of benefits, among them transparency, security, and efficiency.[5] The blockchain is a distributed digital ledger that can be added to and viewed publicly but not edited by any one person. Its name is quite literal: it comprises a series of "blocks" that are linked in a chronological "chain." Each block holds a set of entries, e.g., transactions. Once a block is full, the block is closed and linked to the previous block, and the next block is initiated and timestamped. Thus, the blocks are added in strict chronological order. Further, the blockchain is maintained through a decentralized network. Each node on the network holds a complete copy of the blockchain and participates in the process of adding to and maintaining the blockchain. Decentralization promotes two essential features of the blockchain: stability and fidelity. Through decentralization, the ledger is less vulnerable to failure: if one node on the network fails, the redundancy of the decentralized network enables the data to be retrieved from other nodes on the network. Decentralization also enhances fidelity, i.e., the integrity of the ledger. In order for a blockchain to be edited to, for example, add a transaction, a majority of the nodes on the network must agree to the change; no one node has the power to change a block. Thus, if one node tries to edit a block, the other nodes on the network will reject the change. Blockchains are essentially immutable.

---

[4] Executive Order § 9(a), 87 Fed. Reg. 14143, at 14,151 § 9(a).

[5] *See* U.S. Gov't Accountability Office, GAO-19-704SP, Science & Tech Spotlight: Blockchain & Distributed Ledger Technologies (Sept. 16, 2019), https://www.gao.gov/products/gao-19-704sp; World Bank, Blockchain & Distributed Ledger Technology (DLT) (Apr. 12, 2018), https://www.worldbank.org/en/topic/financialsector/brief/blockchain-dlt.

Blockchain applications have efficiencies from the ability to automate processes and track information without the need for centralized intermediaries. Traditional recordkeeping processes often require a third-party to intermediate a transaction, silo documentation and transaction details, require multiple streams of information that need reconciliation, and produce volumes of paperwork. A blockchain can reduce these frictions. First, blockchains are computerized and certain blockchain-based networks enable the use of smart contracts (blockchain-based software programs that can execute functions), which lessen the risk of human error and reduced costs from manual processing. Second, through the blockchain, the parties can interact directly and maintain a single source of information rather than rely on disparate intermediaries, databases, and file systems. Finally, transaction details and documentation can be linked together permanently on a blockchain.

Bitcoin, as the first application of this technology, has since inspired much of the work that has followed with respect to the technology, including both financial and non-financial use cases as discussed in more detail below.[6]

B. TECHNOLOGICAL APPLICATIONS

Neither the Executive Order nor the Request contemplates the use of blockchain-based systems in contexts other than cryptocurrencies and financial services. But the range of potential applications and benefits of the technology are far broader, and any regulatory approach must be sensitive to the potential impact on the range of applications, many of which are as yet unknown. Similar to the innovation of the internet, blockchain technology is quickly transforming the US financial system into a digital assets-based financial system and the US economy into a true digital economy. In the financial system, in payments, blockchain is being used to transfer value in real-time. This began with the first generation of cryptocurrencies Bitcoin and Ether and has evolved with the next generation of stablecoins, including fiat-backed payment stablecoins. These payment mechanisms power lending and investment tools and other services in decentralized finance ("DeFi"). New types of platforms are emerging to trade crypto products without using expensive and inefficient middlemen such as brokers and market makers. Blockchain's features of transparency and immutability naturally lends itself for identifying, tracing and preventing illicit activities. These same features will also be immensely useful as RegTech tools for financial regulators. Blockchain technology is finding use cases beyond the financial sector, such as healthcare (for transferring sensitive patient data or contracts), music and art (royalties), real estate (title registration), and digital identity - to list a few examples.

1. Governance and Voting

Blockchain and smart contracts implemented via blockchain have the potential to transform the ability of individuals to influence the governance of companies and communities in which they participate. Through smart contracts on the blockchain, the rules and decisions about governance can operate automatically when the smart-contract criteria are met.

---

[6] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf (citing Stuart Haber & W. Scott Stornetta, *How to Time-Stamp a Digital Document*, 3 J. of Cryptology 99 (1991)) (last visited Aug. 5, 2022).

Automation can also reduce the cost of verification and enforcement of a decision for shareholders.[7]

Decentralized autonomous organizations ("DAOs") are an emerging form of membership organization that relies on these concepts. Generally, membership interests in a DAO are represented by tokens, ownership of which can be tracked on blockchains. DAOs then place decision-making in the hands of members who directly exercise those rights by voting with their tokens. DAOs may also deploy smart contracts to govern their operations and execute the decisions made by their members.[8]

2. Recording Ownership and Supply Chains

Blockchains have also been used to record ownership of physical assets. Through registration on a blockchain, the ownership records of physical items are "tokenized" and become a type of non-fungible token ("NFT") viewable on public ledgers. The blockchain creates a tamper-evident record of ownership.[9] The inherent nature of the blockchain effectively creates permanent records of ownership transactions that cannot be altered, forged, or erased. Once recorded on the blockchain, these ownership records may then easily be traded or transferred to follow subsequent ownership transactions. By recording ownership records on the blockchain, users—whether individuals, businesses, or governments—can also ensure that ownership records are in common format, instead of depending on varying internal records and databases.

Blockchains are already being used by companies to track ownership of physical items, particularly where supply chains are fraught with potential human rights abuses, counterfeiting, or other problematic trade practices. For example, in 2018, Starbucks introduced a new blockchain-based tool to trace ownership details of coffee beans from fields all the way to individual stores.[10] In announcing the pilot program, Starbucks highlighted that the traceability benefits allow the farmers to have more financial independence and will benefit broader conservation efforts.[11] The diamond industry is similarly adopting blockchain tools to prevent "conflict diamonds" from entering the marketplace. For example, in 2018, diamond mining company De Beers launched a blockchain-based program that ensures the company does not handle, distribute, or sell conflict diamonds.[12] By recording a unique identifying tag based on

---

[7] Ammol R. Singh and Sirjan Kaur, *Blockchain's Potential for Transforming Corporate Governance*, The Leaflet (Aug. 2, 2022), https://theleaflet.in/blockchains-potential-for-transforming-corporate-governance/.

[8] https://www.governing.com/community/can-we-turn-shareholders-into-public-decision-makers.

[9] *See* Conor Svensson, *Why Blockchain is Great for Records of Ownership*, Web3 Labs (Nov 23, 2020), https://blog.web3labs.com/why-blockchain-is-great-for-records-of-ownership.

[10] *Id*.

[11] Starbucks, *Starbucks to Pilot 'Bean to Cup' Traceability with New Technology* (Mar. 21, 2018), https://stories.starbucks.com/stories/2018/starbucks-to-pilot-bean-to-cup-traceability/.

[12] Wahid Pessarlay, *Blockchains Are Forever: DLT Makes Diamond Industry More Transparent*, CoinTelegraph (May 13, 2022), https://cointelegraph.com/news/blockchains-are-forever-dlt-makes-diamond-industry-more-transparent.

each diamond's clarity, color, and weight, the blockchain enables the diamonds to be traced along the supply chain.

3. Media, Entertainment, and Art

A classic challenge for content creators, entertainers, artists, and other creators is reaching an audience and generating sufficient income. Digital media crystallized this challenge. The internet radically lessens the costs of copying and distributing digitally based work in comparison to its physical counterparts, making it harder for creators to monetize their work. Blockchain applications can help address this challenge. Specifically, non-fungible tokens can help creators manage digital rights to the content they create.

Such NFTs represent unique or quantity-limited digital items (in contrast to the NFTs discussed above representing unique physical items) linked to the blockchain like a work of art or a piece of music. Each individual NFT has a unique identifier. Entries on the blockchain record information about ownership of and associated with the NFT. Subsequent entries can record transactions such as transfer or sale, and creators can embed a function that pays them royalties from secondary market transactions in the work into the smart contract that structures the NFT itself.

NFTs expand opportunities for creators and their audiences to connect directly. Traditional artists like poets and fine artists can reach a broader audience by representing poems or pictures in NFTs than they can by relying solely on books, auctions, and dealers for distribution.[13] For example, the poet Ana Marie Cabellero makes NFTs from spoken-word performances of her award-winning poetry.[14] The blockchain allows her to reach her audience without the need for a third-party seller, which is limited for poetry.[15] Similarly, musicians can sell NFTs incorporating their songs that embed royalty rights in the smart contracts.[16] This allows audiences to support their favorite musicians and feel more connected to the music.[17]

The blockchain can also improve the operation of the secondary market for media to the benefit of the creators. For physical media, it may be difficult for a creator to track resale or transfer of their work or encourage the exchange of it among fans. Tokenizing their work in the form of NFTs may create a more robust market and may facilitate the creation of communities around the work, all to the benefit of the artists and their audience.

---

[13] Shishir Jajoo, *The Creative Artistic and Non-Artistic Utilization of NFT*, Entrepreneur India (Mar. 24, 2022), https://www.entrepreneur.com/article/422999.
[14] *Id*.
[15] *Id*.
[16] Andrew Chow, *Independent Musicians are Making Big Money from NFTs. Can They Challenge the Music Industry?*, Time (Dec. 2, 2021), https://time.com/6124814/music-industry-nft/.
[17] *Id.*

4. Consumer Rewards

Blockchain-based advertising may also upend the traditional web media model by facilitating payments or other rewards to users for their attention to ads. Under a traditional web media model, online users are typically required to view ads before or while viewing the content. Such ads slow access to content, open users to data tracking, and are generally disruptive to user experiences. However, blockchain-based tools offer new avenues that reward users for engagement and encourage participation with advertisements.

An example of this consumer participation model is the Brave Browser. This browser allows users to earn tokens during their usual online activities.[18] After installing the browser, users may opt to see advertisements from the Brave Ads Platform. These advertisements are typically background images and small push notifications, and do not transmit user data back to the advertisers. Users receive Brave's Basic Attention Tokens ("BAT") as they view these ads and can exchange BATs for cash-value gift cards from major retailers, NFTs, and chances to win other prizes through Brave's sweepstakes. For advertisers, this participation model also offers significant benefits. Because Brave uses local machine learning to place ads in optimal locations, users are more likely to interact with ads, confirmed by Brave's anonymous-but-accountable attribution model.[19]

It is clear that the core blockchain technology has a wide range of beneficial uses that go well beyond cryptocurrencies and other types of financial assets. Any approach to regulation or legislation must be cognizant of these uses and must not inordinately interfere with them.

II. CRYPTOCURRENCY BENEFITS

A. Transaction Benefits

Cryptocurrencies provide a medium of exchange that can reduce transaction costs, including fees, time, transfer limits, vulnerability to abusive practices. Cryptocurrencies can also improve access to financial services.

The average cost of a wire transfer is about $26 for domestic and $42 for international.[20] Automated Clearing House ("ACH") transfers typically take at least a few hours to clear and sometimes at least one and up to five days.[21] Although the ACH network permits transfers up to $1 million, many banks limit ACH transfers to around $25,000. Further, both wire transfer and ACH can be completed only during normal business hours. Newer payment apps, such as Zelle, Venmo, and Google Pay are subject to low transfer limits and usually take at least several

---

[18] *See generally,* Brave, BRAVE REWARDS, https://brave.com/brave-rewards (last visited Aug. 8, 2022).

[19] Brave, BRAVE ADS, https://brave.com/brave-ads/ (last visited Aug. 8, 2022).

[20] *See generally,* Matthew Goldberg, *How Much Are Wire Transfer Fees?*, Bankrate (Nov. 4, 2021), https://www.bankrate.com/banking/wire-transfer-fees/#:~:text=Average%20wire%20transfer%20fees,fees%20are%20usually%20%2435%2D50).

[21] *See* David McMillin, *Here's Everything You Need to Know About ACH Payments*, Bankrate (Nov. 13, 2020), https://www.bankrate.com/banking/what-is-ach/.

minutes to complete the transfer.[22] Even with improved speeds, funds transferred by Zelle are generally not accessible until the next business day and funds transferred by Venmo still need to be transferred to the customer's bank account. In contrast, although Bitcoin transfer fees have spiked occasionally, they typically are between $1 and $4,[23] and transaction fees for dollar-backed stablecoins are decreasing as they expand to blockchains other than Ethereum. Crypto transfers can settle in a few minutes, at any time on any day; currently, Bitcoin settlement averages about 8 minutes, for example.[24] And wallet-to-wallet crypto transfers have effectively no limit.

Additionally, the combination of cryptography, the distributed ledger (blockchain), and a high hashrate (the computing power needed to verify and add transactions to the blockchain) can create a highly secure and disintermediated medium of exchange. Some cryptocurrencies, such as Bitcoin, have already achieved those conditions, rendering it highly and increasingly unlikely that any bad actor could apply the level of computing power needed to take over the crypto network and maliciously alter the ledger. This security is enhanced by greater decentralization. And as discussed below, working with industry, regulators could encourage even-more secure practices.[25]

Finally, cryptocurrencies are more widely accessible. In many instances, an internet-enabled device and connection are sufficient to engage in a transaction or make a remittance payment, and a wallet can be created in minutes. In contrast, opening a bank account and establishing the connections needed for bank-to-bank transfers ordinarily can be time-consuming, potentially compromises personal privacy, and excludes from the financial system people who are unable to acquire necessary documentation. Cryptocurrencies and blockchain technologies more generally provide opportunities to make these processes more user-friendly, efficient, and reliable, in part through improved digital identity management, which we discuss in more detail below.

Perhaps because of the entry barriers to traditional financial services, almost one in five U.S. adults is at least partially constrained in their ability to use them: about 5% are unbanked (i.e., no access to a bank account) and another roughly 13% are underbanked (i.e., insufficient

---

[22] *See* Matthew Goldberg and Mary Wisniewski, *7 Best Ways to Send Money*, Bankrate (Dec. 1, 2022), https://www.bankrate.com/banking/best-ways-to-send-money/; Scott Jeffries, *10 Best Payment Apps of 2022*, Go BankingRates (June 8, 2022), https://www.gobankingrates.com/money/business/best-payment-apps-ways-to-send-money/.

[23] Arijit Sarkar, *Bitcoin Average Transaction Fees Lowest in Two Years at $1.04*, Cointelegraph, (Apr. 18, 2022), https://cointelegraph.com/news/bitcoin-average-transaction-fees-lowest-in-two-years-at-1-04; BITCOIN AVERAGE TRANSACTION FEE, https://ycharts.com/indicators/bitcoin_average_transaction_fee (last visited Aug. 5, 2022).

[24] BITCOIN AVERAGE CONFIRMATION TIME, https://ycharts.com/indicators/bitcoin_average_confirmation_time (last visited Aug. 5, 2022).

[25] *See infra* p.22.

access to a bank account to meet financial needs).[26] Most U.S. adults who are unbanked or underbanked represent communities that have historically been the victim of discriminatory or exclusionary financial practices, including low education, low income, and people of color.[27]

Moreover, a distressingly high percentage of historically disadvantaged groups remain unbanked or underbanked: about 40% of families earning less than $50,000 per year, about 40% of Americans with no more than a high school degree, about 27% of Black Americans, and about 21% of Hispanic Americans.[28] Unbanked and underbanked people often turn to alternative financial services, such as money orders, check-cashing services, and payday loans. Such services have a long history of exorbitant fees, fraudulent practices, and other abuses.[29] Cryptocurrencies provide a third way: with lower barriers to entry and without historically exclusionary or abusive practices and stigmas, cryptocurrencies offer people from traditionally excluded or unbanked and underbanked communities new access to secure, low-cost, and effective financial services. Indeed, as discussed below, members of those communities have already shown a strong interest in and adoption of cryptocurrencies.[30]

Further, in many places in the world, especially where people are living under authoritarian regimes or suffer from hyperinflation, crypto can provide a lifeline to store value out of the reach of corrupt or poorly run governments. Indeed, in 2020, digital assets provided one of the few means by which the U.S. government was able to deliver assistance to desperate people in Venezuela.[31] In fact, Venezuelan residents have noted the criticality of crypto assets in the face of hyperinflation.[32] This has been the case in other countries as well. For example, there was significant documented use of crypto in Afghanistan following the Taliban's return to power. Civilians have been using crypto to hedge against sanctions, Taliban seizure of assets, and the absence of reliable financial services, among other reasons.[33] Around the world, crypto

---

[26] Board of Governors of the Federal Reserve System, Economic Well-Being of U.S. Households in 2020 (May 2021), https://www.federalreserve.gov/publications/2021-economic-well-being-of-us-households-in-2020-banking-and-credit.htm. *See also* Silvia Foster-Frau, *Locked Out of Traditional Financial Industry, More People of Color are Turning to Cryptocurrency*, Washington Post (Dec. 1, 2021), https://www.washingtonpost.com/national/locked-out-of-traditional-financial-industry-more-people-of-color-are-turning-to-cryptocurrency/2021/12/01/a21df3fa-37fe-11ec-9bc4-86107e7b0ab1_story.html.

[27] *Id.*

[28] *Id.*

[29] Lisa Lake, *Paying, and Paying, and Paying Payday Loans*, FTC CONSUMER ALERTS (May 22, 2022), https://consumer.ftc.gov/consumer-alerts/2020/05/paying-and-paying-and-paying-payday-loans.

[30] *See infra* p.17.

[31] Nikhilesh De, *US Government Enlists USDC for 'Global Foreign Policy Objective' in Venezuela: Circle CEO*, CoinDesk (Nov. 20, 2020), https://www.coindesk.com/markets/2020/11/20/us-government-enlists-usdc-for-global-foreign-policy-objective-in-venezuela-circle-ceo/

[32] Carlos Hernández, Opinion, *Bitcoin Has Saved My Family*, N.Y. Times, Feb. 3, 2019, https://www.nytimes.com/2019/02/23/opinion/sunday/venezuela-bitcoin-inflation-cryptocurrencies.html

[33] Anamaria Silic, *Afghans Turn to Cryptocurrencies Amid U.S. Sanctions*, BBC (Mar. 15, 2022), https://www.bbc.com/news/world-asia-60715707; Eltaf Najafizada & Bloomberg, *Afghan Crypto Buyers Aren't Trying to Strike It Rich. They're Just Trying to Keep What They Have Out of the Taliban's Reach*, Fortune (Apr. 24, 2022), https://fortune.com/2022/04/24/afghan-crypto-buyers-keep-money-out-of-taliban-reach-stablecoin-herat/; *Crypto Provides Fix for Some in Crisis-hit Afghanistan*, AFP (Mar. 21, 2022), https://www.aljazeera.com/news/2022/3/21/crypto-provides-fix-for-some-in-crisis-hit-afghanistan.

has been a tool in enabling advocates of democracy—particularly in areas where free speech and dissidence are not protected.

Similarly, cryptocurrencies are increasingly used in countries where access to financial institutions is slow and cumbersome, or where such access has been otherwise significantly depleted because of war or terrorism. Recent events in Ukraine present one such example: following the start of the war, the crypto community quickly galvanized to provide aid to the Ukrainian government. Working with a local exchange, the Ukrainian government was able to receive and use the cryptocurrency quickly to buy essential items for the war effort. Michael Chobanian, a Ukrainian entrepreneur and president of the Blockchain Association of Ukraine, testified before the U.S. Congress in May 2022, describing the essential nature of the crypto relief campaign, detailing how "the minute the crypto landed on these addresses, the government could use them so immediately. No bureaucracy." Further, he explained that "[f]or my country, which is fighting right now with bare hands, time is vital," and that "[t]he faster we buy helmets, the faster we buy bulletproof vests, the faster we buy aid kits, the more people I can save in my country." In short, Chobanian emphasized, blockchain and crypto "will be the technology that we're going to use to rebuild our country."[34]

Crypto has also provided immediate aid in other high-stakes crisis situations. Following the second wave of COVID-19 in India, the crypto community quickly mobilized to raise money for the "India COVID Crypto Relief Fund." Several key players in the space donated and encouraged others to do the same. This included a donation from Ethereum co-founder Vitalik Buterin that was worth over $1B at the time of donation. The funds have been used for beds, training, and augmenting the public health infrastructure in India. Importantly, the fund was community driven and the funds went towards local, grassroots COVID relief efforts.[35]

Remittances—estimated to reach $630 billion in 2022—represent another significant opportunity. According to the World Bank's Remittance Prices Worldwide Database, the global average cost of sending $200 was 6.4 percent in the first quarter of 2021, which is more than double the Sustainable Development Goal target of 3 percent by 2030.[36] Crypto operators around the world have stepped in to provide these services at a lower cost. For example, in sub-Saharan Africa, banks are the most expensive agents for sending money to sub-Saharan Africa, charging 10.2 percent in fees on average. This is closely followed by 7.7 percent from money transfer operators and post offices at 5.5 percent. Meanwhile, crypto service providers such as

---

[34] Benjamin Pimentel & the Fintech Team, *Ukraine Makes Crypto's Case in Washington*, Protocol (Mar. 18, 2022), https://www.protocol.com/newsletters/protocol-fintech/crypto-ukraine-senate-hearing.

[35] Nina Bambyscheva, *Ethereum's Co-Founder Vitalik Buterin Donates Over $1 Billion to India Covid Relief Fund and Other Charities*, Forbes (May 12, 2021), https://www.forbes.com/sites/ninabambysheva/2021/05/12/ethereums-co-founder-vitalik-buterin-donates-over-1-billion-to-india-covid-relief-fund-and-other-charities/?sh=4a804cb36548.

[36] Press Release, The World Bank, Remittance Flows Register Robust 7.3 Growth in 2021 (Nov. 17, 2021), https://www.worldbank.org/en/news/press-release/2021/11/17/remittance-flows-register-robust-7-3-percent-growth-in-2021.

BitPesa, LocalBitcoins, and Paxos can process remittance payments with 1 to 3 percent in fees on average, representing significant cost savings for those who need them most.[37]

1. New Market Infrastructure Benefits

Since the release of Bitcoin almost fourteen years ago, blockchain technology has driven the evolution of financial services and products, including cryptocurrencies as an option for many who traditionally have been marginalized from or reluctant to use traditional financial services. Policymakers should not stand in the way of consumers and investors who choose cryptocurrencies.

Consumer choice is a foundational tenet of the market for financial products and consumer protection. Indeed, it is not the role of policymakers to make financial decisions for individual consumers and investors, who are in the best position to know their own financial needs. The decision of which financial product to purchase is left to consumers and investors, and policymakers should focus on maintaining an open and competitive market. Policymakers should take the same tact for cryptocurrencies.

It is especially important to preserve and enhance opportunities for crypto access because of the capacity for cryptocurrencies to bring benefits to groups who traditionally have avoided or been locked out of financial services, particularly the underbanked, people of color, and young workers.[38] Cryptocurrencies are proving instrumental in drawing such groups[39] in and could provide a unique—perhaps once-in-a-generation—way to build wealth and take increased control their financial futures.[40] However, adverse policy could lock consumers and investors out of the ability to access crypto and its attendant benefits.

B. Conditions for Increasing Use

Cryptocurrency adoption is rapidly increasing. According to an analysis of worldwide cryptocurrency adoption, based off an examination of on-chain value transactions, on-chain retail transactions, and peer-to-peer ("P2P") trade volume, global adoption increased by over 2,300%

---

[37] Kingsley Obinna Alo, *How Bitcoin is Helping African Migrant Workers and Their Families Save Money*, Forkast (Mar. 9, 2020), https://forkast.news/cryptocurrencies-remittance-africa-blockchain-bitcoin-money-transfers-fees/.

[38] *See* Foster-Frau *supra* note 26; Suzanne Woolley, *Plan for Retirement? Millennials Don't See the Point*, Bloomberg (Mar. 18, 2022), https://www.bloomberg.com/news/articles/2022-03-18/retirement-planning-45-of-millennials-gen-z-don-t-see-the-point.

[39] Michael J. Hsu, Comptroller, OCC, Remarks Before the British American Business Transatlantic Finance Forum 1-2 (Jan. 13, 2022), https://www.occ.treas.gov/news-issuances/speeches/2022/pub-speech-2022-2.pdf (people of color own crypto assets at rates comparable to, and sometimes higher than, White Americans); Nasdaq, *The Importance of Women in Crypto Leadership Positions* (Apr. 29, 2022), https://www.nasdaq.com/articles/the-importance-of-women-in-crypto-leadership-positions; Andrew Perrin, *16% of Americans say They Have Ever Invested In, Traded or Used Cryptocurrency*, Pew Rsch. Ctr. (Nov. 11, 2021), https://www.pewresearch.org/fact-tank/2021/11/11/16-of-americans-say-they-have-ever-invested-in-traded-or-used-cryptocurrency/.

[40] *See* BITCOIN TO UNITED STATES DOLLAR, https://www.google.com/finance/quote/BTC-USD?window=5Y (last visited Aug. 8, 2022); ETHER TO UNITED STATES DOLLAR, https://www.google.com/finance/quote/ETH-USD?window=5Y (last visited Aug. 8, 2022).

since Q3 2019 and over 881% since Q3 2020.[41] This growth is primarily occurring due to increases in P2P platforms and is driven by usage in emerging markets without access to centralized exchanges, including Kenya, Nigeria, and Vietnam. In the United States, however, cryptocurrency growth is slowing. While the United States remains a top country for cryptocurrency transactions overall, one study suggested that a lack of P2P transactions contributes to a slowing adoption number and may indicate increasing professionalization and institutionalization of the cryptocurrency industry.[42]

While such institutionalization of cryptocurrency is not inherently a hindrance to widespread cryptocurrency adoption, full realization of the benefits for most consumers will require the right regulatory, technological, and consumer-awareness conditions. Without these positive conditions, crypto adoption is likely to move overseas.

To ensure that the American public can fully benefit from cryptocurrency opportunities and unlock the promise of web3, the U.S. government must work towards implementing legislative and regulatory frameworks that provide certainty and promote innovation. As discussed in Section V *infra*, creating a regulatory framework that is cognizant of crypto's unique characteristics is critical. Further, any legislative or regulatory framework should foster a diverse cryptocurrency ecosystem rather than choosing the specific types of entities that can participate. Provided that legislation and regulation is guided by these overarching principles, the crypto industry will be able to continue to innovate and meet the needs of the greatest number of users.

Additionally, it will require continued technological developments. Cryptocurrency presents significant opportunities for consumer investment and transactional purposes. CCI supports increased technological partnerships between the crypto industry and law enforcement to stop illicit activities and increase consumer confidence in the legitimate uses of cryptocurrency. CCI has advocated for FinCEN to adopt new, crypto-informed mechanisms to identify and mitigate financial crime risk and works with the private sector to help develop new structures of public/private and private/private partnerships to address illicit activity to ensure that even smaller financial institutions are able to identify and prevent emerging illicit threats.[43]

Finally, consumer education regarding the benefits and opportunities of crypto is also important. Cryptocurrency is still an emerging technology. Bitcoin, the oldest and most widely adopted cryptocurrency, is still only 13 years old. Cryptocurrency is still seen by many as untested or too new to be an investment tool or to be used for regular transactions. The crypto industry and government policymakers can work in tandem to educate consumers about safe cryptocurrency usage. For example, as CCI noted in its comment letter to the Department of Labor, CCI is broadly in support of allowing more plan fiduciaries to offer information to

---

[41] Chainalysis, *2021 Global Crypto Adoption Index: Worldwide Adoption Jumps Over 880% with P2P Platforms Driving Cryptocurrency Usage in Emerging Markets* (Oct. 14, 2021), https://blog.chainalysis.com/reports/2021-global-crypto-adoption-index/.

[42] *Id*.

[43] *See* Letter from CCI to Himamauli Das, Acting Director, FinCEN (Feb. 13, 2022), https://www.regulations.gov/comment/FINCEN-2021-0008-0140.

consumers about cryptocurrency benefits.[44] By increasing the amount of reliable information about cryptocurrency that consumers have access to, the greater number of consumers will be able to make responsible and informed choices about whether to use cryptocurrency for investments purposes or in daily P2P transactions.

III. CRYPTOCURRENCY RISK MANAGEMENT

A. Cybersecurity

Responsible crypto companies like CCI members and the New York Department of Financial Services ("NYDFS")[45] have developed robust cybersecurity programs for themselves and their regulated entities. Other regulators like the California Department of Financial Protection and Innovation have also emphasized attention to cyber risk in the current threat environment.[46] Federal standards, developed with the private sector, could provide uniformity and nationwide safeguards from malicious actors for both companies and customers.

Recognizing the threat to financial-services companies from "nation-states, terrorist organizations and independent criminal actors,"[47] the NYDFS promulgated cybersecurity requirements for banking, insurance, and certain other financial services companies licensed in the state.[48] NYDFS explains, "It is critical for all regulated institutions that have not yet done so to move swiftly and urgently to adopt a cybersecurity program and for all regulated entities to be subject to minimum standards with respect to their programs. The number of cyber events has been steadily increasing and estimates of potential risk to our financial services industry are stark."[49] Under the NYDFS regulations, covered entities, which include regulated crypto firms engaging in crypto activity in New York, must maintain a cybersecurity program and policy, conduct self-assessments and testing of cyber defenses, and establish an incident response plan, among other requirements.[50] These standards are in place to protect both the company and its customers from malicious actors.

Crypto companies and their customers face cyber risks on several fronts. First, cybercriminals target cryptocurrencies and other crypto assets themselves. Recently, for

---

[44] *See* Letter from CCI to Ali Khawar, Acting Assistant Sec'y, Employee Benefits Security Admin. (June 14, 2022), https://cryptoforinnovation.org/wp-content/uploads/2022/06/Crypto-Council-for-Innovation-Department-of-Labor-Response-Letter_Final.pdf.

[45] Indeed, NYDFS continues to update these standards. *See* NYDFS, Proposed Second Amendment to 23 NYCRR 500 (July 29, 2022), https://www.dfs.ny.gov/system/files/documents/2022/07/pre_proposed_draft_23nycrr500_amd2.pdf.

[46] *See e.g.*, California DFPI, *Obligations Regarding Situation in Ukraine and Russia*, (Mar. 4, 2022), https://dfpi.ca.gov/wp-content/uploads/sites/337/2022/03/Guidance-to-FIs-re-Russia-Ukraine-jt_pjl.pdf.

[47] N.Y. Comp. Codes R. & Regs. tit. 23 § 500.0.

[48] *Id.* § 500.1(c).

[49] *Id.* § 500.0.

[50] *Id.* § 500.2(a).

example, hackers stole $600 million or more worth of crypto assets in a single attack.[51] Second, crypto companies may also have access to valuable traditional assets like customer funds, company funds, or files and data, which could also be vulnerable to attack. Third, crypto companies are susceptible to the threats that traditional companies have long endured. Malicious actors target crypto companies' systems for ransom.[52] In addition to bad actors that might attempt to penetrate a company's defenses from the outside, crypto companies (like traditional financial companies) are also vulnerable to insider threats, where authorized personnel of a company abuse or misuse their access.[53] For example, an employee may use their access to the company's databases to steal customers' financial information.[54]

CCI members and other responsible crypto companies have recognized these risks and developed sophisticated cybersecurity programs, including programs like those required by NYDFS. These companies have put in place layers of protection like account security protocols, internal controls, asset security protocols, and compliance and certifications assessments. Further, those CCI members and other crypto companies that control customer assets have taken specific steps to protect against the misappropriation of those assets, including requiring the assent of multiple personnel before certain transactions with customer assets, using "cold storage" of private keys in media that are not connected to the Internet to reduce the risk of theft, and establishing backup systems. Robust cybersecurity programs like these are a necessary response to the potential costs of a successful cyber-attack. Not only are there direct costs from theft or harm to the company's systems, but there are also indirect costs from missed transactions during the downtime and lost goodwill if customers or others are also affected, and these indirect costs can be substantial and long-lasting.

For the benefit of all consumers and other market participants, federal policymakers should work with the private sector on uniform cybersecurity requirements and protections for participants in the cryptocurrency ecosystem.

---

[51] *See, e.g.*, Jonathan Ponciano, *Second Biggest Crypto Hack Ever: $600 Million In Ether Stolen From NFT Gaming Blockchain*, Forbes (Mar. 29, 2022), https://www.forbes.com/sites/jonathanponciano/2022/03/29/second-biggest-crypto-hack-ever-600-million-in-ethereum-stolen-from-nft-gaming-blockchain/?sh=4f855a5b2686; Jonathan Ponciano, *More Than $600 Million Stolen in Ethereum and Other Cryptocurrencies—Marking One of Crypto's Biggest Hacks Ever*, Forbes (Aug. 10, 2021), https://www.forbes.com/sites/jonathanponciano/2021/08/10/more-than-600-million-stolen-in-ethereum-and-other-cryptocurrencies-marking-one-of-cryptos-biggest-hacks-ever/?sh=2f5851217f62.

[52] *See* Edward Segal, *A Majority of Surveyed Companies Were Hit by Ransomware Attacks In 2021—and Paid Ransom Demands*, Forbes (Feb. 03, 2022), https://www.forbes.com/sites/edwardsegal/2022/02/03/a-majority-of-surveyed-companies-were-hit-by-ransomware-attack-in-2021-and-paid-ransom-demands/?sh=57c7e085b8c6.

[53] Nat'l Inst. of Standards and Tech,, NIST Special Pub. 800-53, *Security and Privacy Controls for Information Systems and Organizations*, 406 (rev. Sept. 2020), https://doi.org/10.6028/NIST.SP.800-53r5.

[54] *See, e.g.*, James Rundle & Catherine Stupp, *Capital One Breach Highlights Dangers of Insider Threats*, Wall St. J. (July 31, 2019), https://www.wsj.com/articles/capital-one-breach-highlights-dangers-of-insider-threats-11564565402.

B. Illicit Finance

Traditional banking services are by no means free from abuse. For example, a recent survey by the Federal Reserve reports that 65% of U.S. adults have experienced fraudulent transactions in connection with their banking services.[55] Cryptocurrency's transparency and security benefits provide opportunities to combat fraudulent practices and illicit finance in novel ways that may improve on approaches currently taken in traditional financial services.

In fact, the cryptocurrency industry has already made major strides in developing compliance programs reasonably designed to prevent, detect, and report illicit finance. Cryptocurrency businesses that are covered financial institutions under the Bank Secrecy Act ("BSA") are required to develop anti-money laundering ("AML") compliance programs. Responsible cryptocurrency businesses that are money services businesses ("MSBs") typically develop AML compliance programs that include customer identification and verification, customer risk rating, and customer due diligence procedures that go beyond what is required by the letter of the law.

Cryptocurrency business AML programs increasingly consist of the components of AML programs at other financial institutions such as banks and broker-dealers.[56] These include the components prescribed by law:

- A designated BSA/AML compliance officer;
- Policies, procedures, and controls, including:
    - Customer identification and verification; and
    - Customer due diligence at onboarding and on an ongoing basis, including through transaction monitoring for suspicious activity;
- Training; and
- Independent testing.

In addition, these programs also include components that, while not necessarily specified directly in regulation, are components that regulators expect to see, such as:

- A tone from senior managers emphasizing the importance of compliance;
- A statement regarding risk assessment and risk tolerance; and
- Performance evaluations that include the employee's contributions to compliance.

As the cryptocurrency industry has matured, several firms have arisen to assist cryptocurrency businesses in meeting their compliance obligations. In particular, several firms have developed, and continue to enhance, sophisticated transaction-monitoring tools to identify

[55] *See* Fed *supra* note 26.

[56] *See e.g.*, N.Y. Comp. Codes R. & Regs. tit. 23, § 200.15 (requiring a risk-based AML program for holders of the virtual currency business activity license).

suspicious activity, even if the cryptocurrency business using the tools does not have full insight into the identities of the parties engaged in the transactions. Some cryptocurrency businesses use more than one of these tools.

In addition, U.S. cryptocurrency businesses and employees are required—as are all U.S. persons and companies—to comply with U.S. sanctions. To meet this requirement, U.S. cryptocurrency businesses have adopted sanctions-compliance programs. Such programs, while not required by statute or regulation, are a prudent measure to mitigate the risk that the business would be exploited by individuals or entities subject to sanctions, thereby causing the business inadvertently to violate the sanctions. Some cryptocurrency businesses have adopted controls such as "geoblocking" to block customers in comprehensively sanctioned jurisdictions from accessing their services. Some cryptocurrency businesses are also taking steps to identify individuals and entities that seek to mask or spoof their internet protocol ("IP") address to evade the geoblocking tools.[57]

Additionally, the unique properties of the blockchain, on which all transactions are generally publicly available, presents opportunities to improve upon traditional approaches to anti-money laundering compliance. As cryptocurrency applications proliferate, an increasing portion of economic activity will likely take place on publicly observable blockchains. Just as in the past, where the government recognized that the private sector has access to information to identify suspicious activity, hosted wallet providers and cryptocurrency exchanges, in partnership with others such as blockchain-analytics firms, may today be better positioned than governments to develop techniques to analyze activity on the blockchain and to identify specific typologies of illicit activity.

The government, by contrast, may have access to a broader range of information that can be used to confirm the identities of individual wallet-holders involved in potentially suspicious activity and to inform an analysis of financial crime trends. Therefore, FinCEN has already worked in partnership with the private sector to establish the necessary "feedback loops," (through FinCEN Exchange and the issuance of typologies for threat identification and mitigation) that Acting Director Das has said is one of FinCEN's current goals.[58] Continued utilization of these mechanisms is crucial.

There are many examples of this kind of public-private partnership producing results. For example, cooperation between a private-sector blockchain-analytics firm and federal law

---

[57] NYDFS, Guidance on Use of Blockchain Analytics, April 28, 2022 ("OFAC notes: 'Transaction monitoring and investigation software can be used to identify transactions involving virtual currency addresses or other identifying information (e.g., originator, beneficiary, originating and beneficiary exchanges, and underlying transactional data) associated with sanctioned individuals and entities listed on the SDN List or other sanctions lists, or located in sanctioned jurisdictions.'").

[58] Him Das, Acting Director, FinCEN, Prepared Remarks, American Bankers Association/American Bar Association Financial Crimes Enforcement Conference (Jan. 13, 2022), https://www.fincen.gov/news/speeches/prepared-remarks-fincen-acting-director-him-das-delivered-virtually-american-bankers.

enforcement led to the October 2021 arrest of a major suspect in child sexual exploitation crimes.[59] Another example is the government's recovery of the ransom paid in Bitcoin by Colonial Pipeline Co. In that instance, the Department of Justice was able to seize the majority of the ransom, in part, by using the traceability of Bitcoin on the blockchain.[60] Still another example is the government seizure of stolen virtual currency and the arrest of suspects charged with laundering virtual currency stolen from Bitfinex. In announcing the seizure and arrests, the government acknowledged its work with a "coalition of the willing to unravel these technical fraud schemes and identify the perpetrators."[61]

In our February 2022 Response to FinCEN's Request for Information on the Modernization of U.S. AML/CFT Regulatory Regime, CCI offered a number of suggestions and guiding principles that the government should adopt to develop the opportunity to improve upon the traditional approach to AML compliance. These included:

- principles around threat identification and dissemination through public-private partnerships; and
- novel approaches to customer identification, verification, due diligence, and record retention.

Rather than repeat those responses in full here, CCI attaches its complete response to the FinCEN RFI as **Appendix A** and incorporates it herein by reference. We wish to note a few salient details about that response, however:

- The need for speed in identifying and disseminating emerging typologies of money laundering, terrorist finance, and other forms of illicit activity call for a deeper and more operational private-public approach to fighting illicit finance that will require the government to look to and leverage the best features of existing private-public platforms; and
- The potential that technological innovations such as digital identification tokens, zero-knowledge proofs, and sophisticated forms of encryption present for improved approaches to customer identification and verification, including the ability for customers to gain more control over their digital identities and, for example, to be able to satisfy successive financial institutions that their identity already has been verified without having to provide sensitive personal information to yet another financial institution.

---

[59] Andy Greenberg, *Inside the Bitcoin Bust That Took Down the Web's Biggest Child Abuse Site*, Wired (Apr. 7, 2022), https://www.wired.com/story/tracers-in-the-dark-welcome-to-video-crypto-anonymity-myth.

[60] *See* Brett Wolf, *Recovery of Colonial Pipeline Ransom Funds Highlights Traceability of Cryptocurrency*, Thomson Reuters (Jun. 23, 2021), https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/colonial-pipeline-ransom-funds.

[61] Press Release, Dep't of Justice, "Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency (Feb. 8, 2022), https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency.

These principles and technological developments should equally inform the government's approach in the case of self-custodied wallets. The rulemaking appeared in the recent Spring 2022 Unified Agenda, with an expected "Final Action" in March of 2023.[62] Many commenters, including CCI members, already engaged at length with the December 2020 proposed "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets" ("Proposal") when it was published. We note a small sample here.[63] In the almost two years since December 2020, the industry has seen sustained and rapid growth, including related to the advances in combating illicit finance discussed above. The industry would likely continue apace through any finalization of the Proposal. The Proposal is outdated at this point, and a final rule further in the future is not positioned to account for these developments.[64] If the Department is considering finalizing any version of the Proposal, we strongly urge further engagement before doing so.

IV. KEY PRINCIPLES THAT SHOULD GUIDE ANY CRYPTOCURRENCY LEGISLATION OR REGULATION

CCI supports the goals of the Executive Order, including:

- Responsible innovation;
- Equitable growth;
- Financial inclusion;
- Mitigating illicit finance and national security risks;
- US leadership in the global financial system;
- US prominence in technology; and
- Consumer choice and protection.

Appropriate legislation and regulation can be important to realizing these goals. However, inappropriate legislation and regulation, alongside regulation through enforcement, could prevent consumers, investors, and the economy as a whole from realizing these goals and the full benefits of cryptocurrencies and other digital assets. Accordingly, CCI believes it is important that legislation and regulation be guided by key principles, including:

- Legislation and regulation should be tailored to address the unique characteristics of digital assets.

---

[62] Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets , 85 F.R. §83840 (2022), https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202204&RIN=1506-AB47.

[63] *See e.g.*, Comment from Andreesen Horowitz, Re: FinCEN-2020-0020, RIN 1506-AB47, Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets (Jan. 4, 2021); Comment from Andreesen Horowitz, Re: FINCEN-2020-0020, RIN 1506–AB47, Reporting Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets (March 29, 2021).

[64] *See, e.g.*, HM Treasury, Response to the Consultation, Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on Payer) Regulations 2017 Statutory Instrument 2022, at 28 ("there is not good evidence that unhosted wallets present a disproportionate risk of being used in illicit finance").

- Legislation and regulation should create a level playing field for all who want to be in the crypto industry.
- Legislation and regulation should promote responsible innovation while putting in place appropriate protections for consumers and investors.
- Legislation and regulation should ensure that innovators can operate in the United States, with certainty about the rules, and take into account that doing so is also paramount to the United States' national and economic security interests.
- Discouraging regulation by enforcement.

A. Principle 1: Legislation and Regulation of Cryptocurrency Should Be Tailored to Address the Unique Characteristics of Cryptocurrency

Cryptocurrencies are a once-in-a-generation opportunity to realize benefits such as trust, immutability, and resilience arising from recording transactions on a distributed network. Accordingly, any legislation or regulation of cryptocurrencies should be tailored to address the unique characteristics of cryptocurrencies.

In cases of previous financial innovations, Congress has responded with legislation tailored to the specific risks and benefits of those activities. For example, after the creation of low-cost electronic funds transfers, Congress responded with the Electronic Fund Transfers Act (EFTA). EFTA helped make possible the widespread adoption of such low-cost payments, in part by limiting the liability of consumers for unauthorized or erroneous transfers.

It is true that in some cases of financial innovation, Congress and regulators have found it possible to meet policy objectives by expanding or applying existing statutory and regulatory approaches. For example, after the creation and increased success of the consumer credit card, Congress responded by expanding the Truth in Lending Act (TILA) to make clear that it covered the extension of consumer credit via a card or other device, and regulators similarly have responded by amending and expanding TILA's implementing regulation, Regulation Z. That approach works best, however, when the new financial activity is quite similar to a previously regulated activity (in the case of TILA, extending consumer credit). In contrast, cryptocurrency is profoundly different from preexisting financial tools and therefore requires a different regulatory approach.

A challenge for policy makers is to know when a financial innovation is sufficiently like a previous activity that it can be safely and appropriately regulated within existing statutory authority merely by expanding existing regulation to cover it, and when a financial innovation is sufficiently different that it requires a new, or largely new, approach. CCI respectfully submits that cryptocurrency activities tend to be sufficiently different in their characteristics, risks, and benefits that a new approach will often be warranted.

One reason that this is important is that certain legacy regulatory frameworks may be ill-suited for addressing the unique characteristics of cryptocurrencies. "Shoe-horning" cryptocurrencies into legacy regulatory frameworks may create unanticipated risks and prevent

full realization of the benefits of cryptocurrency. For example, cryptocurrency is not an access-device, as that term is defined under the EFTA and Regulation E. Further, it has special characteristics, including cryptographic protections and, depending on the cryptocurrency, simultaneous publication to a distributed ledger. Addressing the risk of unauthorized or erroneous transfers through, say, the EFTA and Regulation E could undermine the security that cryptocurrency applications achieve by introducing doubt as to whether a transaction published to the ledger can be relied on by other market participants without the uncertainty that the transaction will be unwound after a period of time. To be clear, CCI is not suggesting that unauthorized transfers of cryptocurrency can never occur. Rather, CCI's view is that cryptocurrency users should have the ability to choose a technology that was designed to address this risk through other means.

B. Principle 2: Legislation and Regulation of Cryptocurrency Should Create a Level Playing Field for All Who Want to Be in the Crypto Industry

CCI believes that consumers and investors should have a chance to choose the responsible innovations that work best for them. Currently, many different types of businesses engage in cryptocurrency activities through a variety of business models and product offerings. Although some product offerings may share some characteristics with legacy products, the government should carefully consider the full range of characteristics of the offerings, rather than allow one or a few characteristics to drive a conclusion that they may be offered only by entities permitted to offer similar legacy products. For example, if a cryptocurrency product has some characteristics in common with products offered by banks, that should not mean that only banks should be permitted to offer the cryptocurrency products. Any legislation or regulation should create a level playing field for all who want to be responsible innovators in the crypto industry, rather than artificially or unnecessarily constraining which entities may participate.

C. Principle 3: Legislation and Regulation of Cryptocurrency Should Promote Responsible Innovation While Putting in Place Appropriate Protections for Consumers and Investors

As the President's Executive Order makes clear, any new legislation and regulation of the cryptocurrency industry should promote responsible innovation, rather than curtail, restrict, or preclude it. At the same time, the Executive Order makes clear the Administration's goal of putting in place appropriate protections for consumers and investors. CCI strongly supports both of these goals so that consumers, businesses, and investors can receive the full benefits of cryptocurrencies and the technologies that support them, while being appropriately informed of and protected from the risks.

D. Principle 4: Legislation and Regulation of Cryptocurrency should ensure that innovators can operate in the United States, with certainty about the rules, and take into account that doing so is also paramount to the United States' national and economic security interests.

As discussed, cryptocurrency and blockchain technologies more generally represent a once-in-a-generation, potentially transformative innovation for the financial sector. For decades, the United States and the U.S. financial system have been at the center of the global financial system, with essential consequences for U.S. economic and national security. It is paramount that the United States remain at the center of the global financial system going forward. If the center of financial innovation through cryptocurrency and blockchain technologies more generally moves outside of the United States, it would have serious, adverse consequences for the United States. Accordingly, legislators and regulators should focus on common sense, pro-business policies to support private sector activity and thereby secure America's leadership in the emerging digital global financial system.

American leadership in the international economic system has been crucial to United States national and economic security both past and present.[65] The importance of the U.S. Dollar to the global economy provides the United States unique tools to protect national and economic security. For example, foreign countries and individuals hold U.S. dollars as a source of financial resources and to facilitate transactions internationally. Those non-U.S. accounts and transactions require access to U.S. dollars and U.S. markets to function. The centrality of the U.S. dollar allows the Treasury Department to exercise significant reach that it might not otherwise have.

Other countries may be moving ahead in crypto technology, regulation, and talent that could threaten continued United States leadership. For instance, China has made significant investments in digital currencies and blockchain technologies.[66] Countries around the world, including the European Union, have made significant moves towards regulatory clarity.[67] Finally, while the overall developer ecosystem for web3 is growing, the United States is losing its market share – with significant growth in emerging markets like Russia and India.[68]

The significant policy and regulatory uncertainty to date is a drag on private sector innovation and a detriment to continued American leadership in the international financial system. As just one example, companies must contend with an alphabet soup of potential regulators, including the Securities and Exchange Commission, Commodity Futures Trading

---

[65] Douglas A. Rediker, *Why US Multilateral Leadership was Key to the Global Financial Crisis Response*, Brooking Inst. (Sept. 12, 2018), https://www.brookings.edu/blog/future-development/2018/09/12/why-us-multilateral-leadership-was-key-to-the-global-financial-crisis-response; Eric Milstein & David Wessel, *What did the Fed do in Response to the COVID-19 Crisis?*, Brooking Inst. (Dec. 17, 2021), https://www.brookings.edu/research/fed-response-to-covid19.

[66] Frederick Kempe, *Why the US Can't Afford to Fall Behind in the Global Digital Currency Race,* The Atlantic Council (Feb. 28, 2021), https://www.atlanticcouncil.org/content-series/inflection-points/why-the-us-cant-afford-to-fall-behind-in-the-global-digital-currency-race/.

[67] Chris Matthews, *U.S. is 'Behind the Curve' on Crypto Regulations, says SEC Commissioner Peirce*, MarketWatch (Apr. 7, 2022), https://www.marketwatch.com/story/u-s-is-behind-the-curve-on-crypto-regulations-says-sec-commissioner-peirce-11617824160.

[68] Enrique Herreros, @eherrerosj, Twitter (May 10, 2022, 11:32 AM) https://twitter.com/eherrerosj/status/1524049725103742977?s=20&t=ZjpUp5dCFAFZXBq52NLcqw.

Commission, U.S. Department of the Treasury, prudential banking regulators, the Consumer Financial Protection Bureau, and others with ambiguous and potentially competing jurisdictional authority. Innovators are reluctant to develop technologies in the United States in the event that new, evolving regulations threaten their investments, market opportunities, and ability to maximize revenue. Policymakers can greatly enhance the potential for innovation by facilitating coordination among agencies to develop a more streamlined and predictable approach—without sacrificing any regulatory oversight deemed necessary.

E. Principle 5: Discouraging Regulation by Enforcement

Legislators and regulators should provide clear, forward-looking rules of the road for cryptocurrencies rather than rely on enforcement actions to create new law and policy. This would improve policy development, treat the individuals involved in an enforcement action fairly, and provide a strong foundation for private sector innovation. First, setting out clear policy for cryptocurrencies in advance of taking an enforcement action allows policymakers to marshal the broadest expertise and to consider all parts of an issue holistically. In enforcement, the outcome is driven by the parties, based on the information that they choose to submit, and limited to the issues in dispute. Second, clear rules in advance enforcement action is necessary for a fair proceeding. Finally, regulation by enforcement further harms innovation. Innovators are unlikely to pursue their ideas without the certainty that clear rules, established in advance of enforcement, provide.

* * *

In the next parts of this letter, we apply these principles to three important policy areas: cryptocurrency transfers, stablecoins, and bankruptcy. However, the principles could be – and should be – used to guide policymaking approaches in a wide range of areas related to cryptocurrency and blockchain.

V. APPLICATION OF GUIDING PRINCIPLES

A. Cryptocurrency Transfers

Cryptocurrency transfers are a good example of how the guiding principles should be applied. The current approach at the federal level and in many states is to treat any cryptocurrency business engagement in the transfer or exchange of cryptocurrency as a money transmitter subject to federal registration and state licensing requirements.

This approach may seem reasonable where an entity's business is the movement of funds and where cryptocurrency is the store of value or one of the stores of value used. In the case of such entities, it is reasonable to require them to have a money transmitter license (although, as discussed below, a pathway for national regulation could be more efficient than regulation by each of the 49 states and the District of Columbia). Such requirements serve important policy

interests implicated by the nature of the entity's activity, such as protecting originators and beneficiaries by ensuring the entity has sound, reputable management and has posted sufficient capital reserves to make good on payments in the event the entity was to fail while payments were mid-transmission.

But this does not mean that all use cases involving money transmission should be limited to "money transmitters" and, indeed, they are not currently. Money transmission law has long recognized that other types of entities may engage in money transmission without being subject to state licensing or federal registration. For example, banks are permitted to transmit money without being licensed as a money transmitter. As another example, in many states, non-financial businesses such as grocery stores are permitted to accept funds from consumers to pay utility bills under the "agent of the payee" exemption. As an additional example, the federal rules recognize exemptions from registration for business where the movement of funds is integral to the provisions of goods or services or where the business operates as a settlement mechanism between other entities that are covered financial institutions under the BSA. Accordingly, where a cryptocurrency business is not engaged primarily in the transfer of funds between individuals or entities, but changes in the ownership of a cryptocurrency occur as a result of the activity, the business may not necessarily need to be regulated as a money transmitter.

In fact, although CCI supports goals of protecting originators and beneficiaries from unscrupulous or insolvent firms through the regulation of money transmission, there may be other, more efficient regulatory approaches for digitally native firms that move money via cryptocurrency networks through smartphone applications and websites and do not have physical stores in any state. Such firms can be—and often are—national, if not international, in their reach from start-up. Providing a pathway for national regulation of such firms would make sense given their operations. It would also eliminate confusion and uncertainty that arises when a business is exempt from the definition of money transmitter at the federal level, but there is no explicit equivalent exemption in one or more of the states. Further, it would promote competition and innovation by providing optionality for start-ups not in a position to spend the time and expense of securing money transmission licenses in each of the 49 states that require them, while ensuring they are still subject to regulatory oversight.

B. Stablecoins

A stablecoin is a crypto asset whose value is pegged to another currency, commodity, or other financial instrument to reduce its volatility and thus to enhance its suitability for making payments, hedging against volatility in other types of assets, and participating in decentralized finance among other uses. Accordingly, policymakers should not make artificial distinctions between who may issue stablecoins or how they reduce fluctuations in their value. Rather, they should follow the principles of tailoring and non-exclusion when designing any regulatory controls for stablecoin. The government should not limit the ability to issue stablecoins to banks or, as has been suggested more recently, affiliates of banks; it should allow responsible bank and non-bank entities alike to issue stablecoins. Nor should it pick a winner among the different methods to reduce fluctuations in value; instead, policymakers should allow reasonable

alternatives to develop subject to the demands of consumers, recognizing that different types of stable coins (*e.g.*, fiat backed versus algo backed) may require different regulatory approaches.

1. Issuers

A diverse ecosystem of private stablecoin issuers would permit different business models to meet the varied needs of the market. The existing market for payments has generally thrived this way, which bodes well if policymakers maintain this practice for stablecoins.

a. Private Entities

Currently, many different types of entities compete in the market for issuing stablecoins. These include banks and affiliates of banks, but also other types of entities, such as national trust banks, state-chartered special-purpose trust companies, and money transmitters. Not all these entities are engaged in the business of banking—that is, both accepting deposits and extending credit. Rather, they focus on various business models, and generally may issue the stablecoins for use in specific applications, such as allowing consumers to send remittances to other countries without exchange-rate conversion fees or uncertainty.

A banking license, or corporate affiliation with a bank, is not necessary to issue stablecoins safely and effectively. Banks offer a distinctive service (demand deposit accounts) and engage in maturity transformation by lending with deposits. The combination of short-term liabilities (demand deposits) and long-term assets (loans) can result in runs on a bank and raise concerns about liquidity or credit risk. Banks are also distinctly, and highly, regulated against these risks, which increases the costs of operation while mitigating the risk of customers losing their account funds. Though not banks themselves, bank affiliates have a close relationship with a bank or banks, may offer services closely tied to banking, and benefit from that relationship without taking on the full cost of bank regulation or being in competition with banks for deposits.

Safely issuing a stablecoin requires neither a banking license nor bank affiliation. Unlike the core business of banking, which traditionally relies on maturity transformation, a stablecoin issuer might not engage in lending or necessarily hold user funds itself. In that case, the application of bank capital and liquidity regulation to guard against investment losses or an inability to immediately withdraw funds may serve no useful purpose but would artificially restrict competition among issuers. Instead, tailored legislation and regulation would recognize and target the risks relevant to the business model. In a case where a nonbank issues stablecoins for use in payments by account holders at banks, the banks providing the accounts that custody the reserves would be subject to regulation and the funds in the accounts insured by the FDIC. The stablecoin issuer would be regulated and supervised in accordance with its transfer function, including to mitigate operational risk. In other cases, a nonbank stablecoin issuer may transfer value without the need for (or in some cases access to) a bank, as in the case of remittance transfers.

For example, nonbank stablecoin issuers could replicate prepaid or stored-value cards like gift cards, government benefit cards, or payroll cards. Stored-value cards provide users a

method of transacting electronically without a bank account. The card is loaded by either the user or a third-party and may then be used for purchases at either a single merchant (in a closed loop) or multiple merchants (open loop). Recipients of government nutrition benefits may use an "Electronic Benefits Transfer" card to receive and use Supplemental Nutrition Assistance Program funds, parents may buy prepaid cards for children, and wage earners who lack a bank account may receive their income through a payroll card rather than a check. In these cases, the full suite of banking regulation would be unnecessary, and stablecoins could be spent like the value stored on a card. In addition to accruing the broad benefits of cryptocurrencies discussed above, stablecoins could provide an alternative to a physical card and its consequent risk of loss. Stablecoin stored-value products could be of particular benefit to the unbanked and underbanked and advance financial inclusion.

In sum, banks that issue stablecoin should continue to be regulated as banks, albeit with examination procedures for their stablecoin issuance businesses that are tailored to the specific technologies associated with issuing stablecoin. State chartered trust companies that issue stablecoins subject to consumer protection regulations, capital reserve requirements, cybersecurity requirements, and AML and banking compliance standards set and examined by a state financial regulator, should also continue to be regulated under such a framework. Money transmitters that issue stablecoins for the purpose of facilitating safer, more secure, and more reliable remittances without exchange-rate risk should continue to be regulated as money transmitters. For them, requirements to post capital sufficient to cover payments in mid transmission should continue to be sufficient to safeguard the interests of originators and beneficiaries.

2. Collateral

As with issuers, policymakers should not hastily or haphazardly limit potential mechanisms to reduce fluctuations in value. Because of the range of possible stablecoin designs, the analysis necessary to categorically exclude potential mechanisms to reduce fluctuations in value could unnecessarily stifle innovation. Instead, policymakers should encourage continued innovation in stablecoin technology and diversification in application. The benefits and risks presented by different arrangements may be appropriate for different circumstances and meet varied market needs.

Stablecoins aim to reproduce a certain value—a "peg"—and maintain the peg through some mechanism, either by collateralization (holding assets equal to or greater than the value of the outstanding coins) or by another mechanism, like an algorithm designed to ensure the peg. In the case of a single-currency stablecoin, the peg could be the US Dollar with collateral chosen to support the peg.

In a single-currency stablecoin, the stablecoin would represent a 1:1 exchange-rate against the reference currency, i.e., one stablecoin would equal one US Dollar. A common purpose for this arrangement could be to reproduce virtual money and transact electronically in an easily understood unit of account or for assets also valued in the given currency. To maintain the peg, the issuer would require assets with a total value in US Dollars equal to or greater than the sum of outstanding stablecoins. If the value of the assets fell below the necessary level, the

issuer would risk the inability to redeem the outstanding stablecoins in full and "breaking the buck," until the value of the assets increased above the threshold. A US Dollar stablecoin issuer might hold US Dollars, US Treasuries, short-term US Dollar-denominated debt, or other assets to support the peg.

Another approach is the single-commodity stablecoin. Rather than representing the value of a currency, the single-commodity stablecoin represents the value of a particular commodity, like gold. A single-currency stablecoin might allow a user to trade on the monetary value of gold or in actual gold, if for example a gold-backed stablecoin were redeemable for the physical commodity. Similar to the above example, to maintain the value of the single-commodity stablecoin, the issuer would maintain assets equivalent to the value of the outstanding stablecoins either in the commodity itself or in other assets.

This pattern could be reproduced with other cryptocurrencies and crypto assets as either the peg or the collateralized assets. For example, an issuer might develop a basket of currencies, commodities, or both as the peg for a stablecoin. Such stablecoins could be less sensitive to the relative value of a single currency or commodity.

To this point, we have assumed that an issuer maintains a peg by maintaining assets at a value equal to or greater than the value of the outstanding stablecoins. That is not the only mechanism to maintain a stable value. Other mechanisms may as well, either in full or in part. So-called algorithmic or synthetic stablecoins rely on calculations and computer operations to maintain their value. For example, some may deploy principles of supply-and-demand to periodically alter the supply of tokens outstanding so that each maintains a stable value or may create demand for a stablecoin by discounting the price of purchasing an asset associated with the stablecoin relative to the value of the peg. Others might combine aspects of an algorithmic stablecoin and asset-backed stablecoin to maintain a peg.

Policymakers should not take it upon themselves to limit permissible pegs or collateral categorically. Rather, issuers should select the appropriate peg in light of the purpose and design of their stablecoin. Then, regulators could assess the risks associated with the selected peg or collateral—an important supervisory role for which regulators would have the relevant expertise.

3. Recommendations

In sum, policymakers should follow the twin principles of tailoring and non-exclusion. Policymakers should not exclude nonbanks from becoming stablecoin issuers. Instead, nonbank issuers should be subject to regulation and supervision tailored to the risks of the nonbank's activities. Policymakers should also refrain from limiting the options for issuers to minimize the fluctuations in the value of a stablecoin. Issuers are best positioned to select collateral in particular cases with supervision of the issuer's risk-management practices by relevant regulators.

A. **Self-Hosted Wallets**

Policymakers should refrain from arbitrarily limiting self-hosted wallets, either directly by prohibition or indirectly by imposing unnecessary and burdensome regulatory requirements upon users. Self-hosted wallets represent for users a spirit of financial self-reliance, not illicit behavior.

In December 2020, FinCEN proposed "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets" ("December 2020 Proposal").[69] The proposal would impose a reporting requirement for certain cryptocurrency transactions deemed to be "a virtual currency analogue to the [current] CTR [Currency Transaction Report] reporting requirement"[70] under the existing regulations implementing the BSA.[71] Despite the proposal languishing for nearly two years unfinalized, the rulemaking continues to be listed among top regulatory priorities. The rulemaking appeared in the recent Spring 2022 Unified Agenda, with an expected "Final Action" in March of 2023.[72]

Commenters have already explained at length the December 2020 Proposal's foundational misunderstanding and the resulting harm that it would cause to the cryptocurrency ecosystem and its users.[73] Specifically, the proposed rule erroneously equates the use of an unhosted wallet with illicit activity, in contrast to users of wallets hosted by financial institutions.[74] As a result, the proposed rule errs when it proposes similar reporting obligations on publicly recorded and immutable blockchain transactions as exist for ephemeral cash transactions. For instance, the UK government after its consultation with regulators, industry

---

[69] *See Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets*, 85 Fed. Reg. 83,840 (proposed Dec. 23, 2020) ("December 2020 Proposal"), https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28437.pdf.

[70] December 2020 Proposal at 83,844, n.31.

[71] 31 C.F.R. § 1010.311.

[72] TK, https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202204&RIN=1506-AB47.

[73] As of early January, over 7,000 comments were submitted, including comments from Andreesen Horowitz, Block (formerly Square), US Chamber of Commerce, MIT Digital Currency Initiative, CrossTower, Coin Center, Blockchain Association, Chamber of Digital Commerce. Nikhilesh De, *65K Comments and Counting: Crypto Industry Fights 'Arbitrary' Treasury Rule*, CoinDesk (Jan. 7, 2021), https://www.coindesk.com/65k-comments-and-counting-crypto-industry-fights-arbitrary-treasury-rule.

[74] December 2020 Proposal at 83,841 n.4 ("For example, across 2017 and 2018, FinCEN observed at least seventeen separate transactions over $10,000 conducted between U.S. financial institutions and unhosted wallets affiliated with the Lazarus Group, a malign actor engaged in efforts to steal and extort CVC as a means of generating and laundering large amounts of revenue for the North Korean regime. Generally, FinCEN has observed that, following initial receipt of the funds, the perpetrator may then engage in multiple transactions between unhosted wallets before exchanging the CVC for fiat currency."); *id.* at 83,843-44 ("Hosted wallets are provided by account-based money transmitters that receive, store, and transmit CVC on behalf of their account holders. … By contrast, the term unhosted wallet describes when a financial institution is not required to conduct transactions from the wallet … The Treasury Department has previously noted that "[a]nonymity in transactions and funds transfers is the main risk that facilitates money laundering."); *id.* at 83,853 ("FinCEN expects that malign actors may exploit such a delay by moving assets to unhosted wallets and away from regulated financial institutions to escape financial transparency")

and academics decided to abandon its plans of introducing a KYC rule for self-hosted wallets in its implementation of the travel rule:

> "The government does not agree that unhosted wallet transactions should automatically be viewed as higher risk; many persons who hold cryptoassets for legitimate purposes use unhosted wallets due to their customizability and potential security advantages (e.g., cold wallet storage), and there is no good evidence that unhosted wallets present a disproportionate risk of being used in illicit finance."[75]

The Department should consider these and other similar concerns rather than proceed with the rulemaking in its current form.

Contrary to the depiction in the rule of self-hosted wallets as inherently suspicious, self-hosted wallets represent a way to take control of one's own financial life. Cryptocurrencies developed in the aftermath of a financial crisis that undermined the trust necessary for a functioning financial system that serves all. Many of the well-known financial institutions that Americans relied on were suddenly at great risk. In contrast, self-hosted wallets enable individuals to participate in financial activity without relying on the same banks and brokers at the center of the financial crisis. Many people find blockchains—which are open source and distributed—more trustworthy than traditional banks. Anyone, including government agencies, can review a blockchain's transaction history that is already in public view, providing assurances to all of the integrity of the blockchain.

The Department and FinCEN should not unreasonably burden self-hosted wallet users with unnecessary recordkeeping and reporting obligations. Instead, FinCEN should take advantage of the transparency provided by blockchains and reconsider the proposed rule to tailor the regulation accordingly.

CONCLUSION

In conclusion, cryptocurrencies and blockchain applications have already delivered and promise further to deliver great benefits to consumers, investors, businesses, and the economy as a whole. As the Department considers how to promote responsible innovation in this area, we hope the Department will be guided by the key principles outlined above. So guided, CCI is confident that responsible innovators in this field will continue to create products and services that leverage the inherent strengths of blockchain technology and bring the benefits of transparency, security, and efficiency to a range of users and sectors.

Moreover, the United States has been the industry leader in blockchain technology and digital assets. The United States needs to construct policies, laws and regulations that ensure U.S. global competitiveness. In addition, it is paramount for U.S. economic and national security

---

[75] Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 Statutory Instrument 2022 (UK), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1083351/MLRs_SI_2022_-_Consultation_Response_final.pdf.

that the U.S. financial system remain at the center of the global financial system. The United States should not allow leadership in the potentially transformative technologies of cryptocurrency and other blockchain applications to move outside of the United States. Rather, legislators and regulators should focus on common sense, pro-business policies to support private sector activity and thereby secure America's leadership in the emerging digital global financial system, promoting responsible innovation, economic growth, safety, inclusion and equity, and economic and national security.

Sincerely,

Sheila Warren
Chief Executive Officer
Crypto Council for Innovation

Appendix A

BY U.S. MAIL AND ELECTRONIC SUBMISSION

Himamauli Das
Acting Director, Financial Crimes Enforcement Network
Policy Division
P.O. Box 39
Vienna, VA 22183

February 13, 2022

RE: FinCEN Docket No. FINCEN-2021-0008, Response to FinCEN's Request for Information on the Modernization of U.S. AML/CFT Regulatory Regime

Dear Acting Director Das,

The Crypto Council for Innovation ("CCI") appreciates the opportunity to comment on the Financial Crimes Enforcement Network's ("FinCEN") request for information ("RFI") regarding ways to "streamline, modernize, and update the anti-money laundering and countering the financing of terrorism ("AML/CFT") regime of the United States,"[1] specifically with respect to the Bank Secrecy Act and its implementing regulations (collectively, the "BSA").[2]

CCI is an alliance of crypto industry leaders with a mission to communicate the benefits of crypto and demonstrate its transformational promise. CCI members include some of the leading global companies and investors operating in the cryptocurrency industry, including Andreesen Horowitz, Block (formerly Square), Coinbase, Fidelity Digital Assets, Paradigm, and Ribbit Capital. CCI members span the crypto ecosystem and share the goal of encouraging the responsible global regulation of crypto to unlock economic potential, improve lives, foster financial inclusion, protect national security, and disrupt illicit activity. CCI and its members stand ready and willing to work with FinCEN and other government agencies to accomplish these goals to ensure that the most transformative innovations of this generation and the next are anchored in the United States.

I. *Introduction and Overview*

CCI welcomes FinCEN's interest in modernizing AML/CFT regulation and strongly believes that the technological revolution of the last decade has made the current moment a unique opportunity to reexamine how the United States counters the threat of financial crime and

[1] Press Release, FinCEN, *FinCEN Seeks Comments on Modernization of U.S. AML/CFT Regulatory Regime* (Dec. 14, 2021), https://www.fincen.gov/news/news-releases/fincen-seeks-comments-modernization-us-amlcft-regulatory-regime; Review of Bank Secrecy Act Regulations and Guidance, 86 Fed. Reg. 71,201 (Dec. 15, 2021), https://www.govinfo.gov/content/pkg/FR-2021-12-15/pdf/2021-27081.pdf.

[2] The BSA is codified at 31 U.S.C. § 5311 *et seq.*, and the BSA implementing regulations are codified at 31 C.F.R. § 1010, *et seq.*

to explore new ways to deploy technology to address emerging threats. Specifically, as FinCEN embarks on the process of modernizing the BSA, it should consider how to harness the innovation that blockchain and other new technologies facilitate to accomplish the objectives of the BSA in novel ways that make law enforcement investigations more efficient while also better protecting individuals' security and privacy.

We commend FinCEN for embracing innovative approaches to financial crime compliance in a number of ways over the last several years. Embracing innovative approaches will undoubtedly lead to the provision of more, and better, financial products and services to a greater number of people, and, in turn, to broader financial inclusion and economic empowerment. By encouraging novel approaches to regulation, instead of imposing duplicative reporting requirements that focus on collecting sensitive personal data,[3] FinCEN can better protect privacy, make law enforcement efforts more effective, and ensure that the United States is not left out of the next generation of innovation in financial services.

Two areas offer particularly fertile ground for reevaluating the traditional approaches to AML/CFT activity: (i) how government and the private sector can identify and mitigate financial crime risk while bringing more people into the financial system; and (ii) the ways in which financial institutions verify customer identities.

Threat Identification. From the adoption of the BSA in 1970, the U.S. AML/CFT framework was grounded in the recognition that the private sector has important perspectives on, and an important role to play in identifying, illicit finance risks. The statute therefore imposed recordkeeping and reporting requirements that would facilitate the provision of information from financial institutions to the government under specified circumstances. Indeed, the main objective of the BSA was to require banks "to maintain prudent practices with respect to identification of their customers, reporting of unusual cash transactions, and general recordkeeping,"[4] in order to provide information that is "highly useful" to "criminal, tax, or regulatory investigations" or to "intelligence or counterintelligence activities."[5] With respect to blockchain-based transactions, however, much of this data is *already* publicly available. Thus, a new paradigm of compliance should focus on creating mechanisms for the public and private sectors to leverage technology to *utilize* this publicly available information – rather than requiring duplicative, burdensome reporting.

While a paradigm of threat identification grounded in financial institution recordkeeping and reporting requirements is important, in an era where cryptocurrency transactions take place over public ledgers, there are more effective ways for the public and private sectors to identify and mitigate risk. Specifically, instead of a model of threat identification focused solely on investigating individuals and groups through subpoenas or other requests for specific records held by financial institutions (much of which may already be publicly available on the blockchain), the threat identification paradigm in blockchain-based environments should focus

[3] *See* Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 86 Fed. Reg. 3,897 (proposed Jan. 15, 2021), https://www.govinfo.gov/content/pkg/FR-2021-01-15/pdf/2021-01016.pdf.
[4] 115 Cong. Rec. 36,769, 36,770 (Dec. 3, 1969) (statement of Rep. Patman).
[5] 31 U.S.C. § 5311(1).

on the identification of typologies, tactics, and techniques of financial crime based on blockchain data. These efforts can leverage the comparative advantages of the private sector in blockchain and data analytics, and the government's comparative advantages in threat-related intelligence, to develop typologies and risk indicators that can be broadly disseminated throughout the industry to enhance threat identification and suspicious activity reporting, particularly by smaller financial institutions in the blockchain ecosystem.

Identity Management. Similarly, the Treasury Department came, over time, to impose requirements under the BSA for financial institutions to verify the identities of their customers.[6] These requirements mandate that every financial institution at which a customer opens an account collect and verify the same information previously collected and verified by every other financial institution at which the customer holds an account, causing costly duplication of effort. New technologies and methodologies for verifying and managing identity can make this process more effective and more efficient, opening the financial services industry to a broader range of actors that can deliver services to new individuals and communities, including those historically excluded from the financial sector because established institutions have not been able or willing to serve them. These new methods could potentially protect customer information more effectively and provide ways to verify identity for those who may lack access to traditional government issued IDs (or whose information is not available in the commercial databases typically used to verify identity). They could also reduce the amount of personal information potentially vulnerable to release in the event of a breach, thus protecting privacy and security. FinCEN and the federal banking regulators have begun the process of encouraging financial institutions to embrace innovation in identity management,[7] but work should continue to encourage accelerated innovation in this space.

---

[6] *See* Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks, 68 Fed. Reg. 25,090 (May 9, 2003), https://www.govinfo.gov/content/pkg/FR-2003-05-09/pdf/03-11019.pdf, and Customer Identification Programs for Broker-Dealers, 68 Fed. Reg. 25,113 (May, 9, 2003), https://www.govinfo.gov/content/pkg/FR-2003-05-09/pdf/03-11017.pdf (requiring banks and broker-dealers, respectively, to implement reasonable procedures to verify the identity of any person seeking to open an account, maintain records of the information used to verify the person's identity, and determine whether the person appears on any lists of known or suspected terrorists or terrorist organizations).

[7] *See, e.g.*, Board of Governors of the Federal Reserve System ("FRB"), Federal Deposit Insurance Corporation ("FDIC"), FinCEN, National Credit Union Administration("NCUA"), and Office of the Comptroller of the Currency ("OCC"), Interagency Statement on Sharing Bank Secrecy Act Resources (Oct. 3, 2018), https://www.fincen.gov/sites/default/files/2018-10/Interagency%20Statement%20on%20Sharing%20BSA%20Resources%20-%20%28Final%2010-3-18%29%20%28003%29.pdf; FRB, FDIC, FinCEN, NCUA, OCC, Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing (Dec. 3, 2018), https://www.fincen.gov/sites/default/files/2018-12/Joint Statement on Innovation Statement (Final 11-30-18)_508.pdf; Press Release, FinCEN, *FinCEN to Host Innovation Hours Program Workshop on Digital Identity Services and Technologies* (Aug. 31, 2021), https://www.fincen.gov/news/news-releases/fincen-host-innovation-hours-program-workshop-digital-identity-services-and#:~:text=WASHINGTON%E2%80%94The%20Financial%20Crimes%20Enforcement,that%20undermine%20the%20integrity%20and; Press Release, FinCEN, *FDIC and FinCEN Launch Digital Identity Tech Sprint* (Jan. 11, 2022), https://www.fincen.gov/news/news-releases/fdic-and-fincen-launch-digital-identity-tech-sprint.

II. *Technology and the Current Moment*

It is particularly important for FinCEN, and the broader U.S. regulatory community, to take up this work now because we sit today at the convergence of two significant developments.

First, cryptocurrencies, and blockchain-based technology more broadly, are disrupting a wide and expanding range of economic activity. Born in the aftermath of the financial crisis, cryptocurrencies and the blockchain represent the simple but powerful idea that individuals should be able to store value and engage in economic exchange without having to use only centralized institutions to execute transactions. Because blockchain-based transactions are recorded on public ledgers, the paradigm of recordkeeping and reporting established by the BSA can be supplemented by enhanced analysis of publicly available blockchain transactional data to identify and curtail illicit activity. These approaches could complement the identity verification measures already taken by banks and other exchanges at the on and off ramps that bridge the cryptocurrency and fiat currency worlds. Compliance capabilities have also benefited from significant technological advancements in recent years. In particular, the rise of data analytics and artificial intelligence (along with related applications like machine learning and natural language processing) has improved general AML compliance potential.[8]

Second, similar technological developments can be used to manage and verify identities more securely, obviating the need to create large repositories of personally identifiable information ("PII") at financial institutions that can be hacked or misused, empowering customers, and increasing the efficiency and effectiveness of identity verification throughout the financial sector.

The economic impact of meeting this technological moment will be significant. By the end of 2022, the number of crypto users is expected to break one billion for the first time,[9] and the rise of cryptocurrency is poised to improve the lives of underprivileged communities. The World Bank reports that close to one-third of adults, 1.7 billion people, remain unbanked,[10] and cryptocurrency has already demonstrated the potential to change this landscape for the better. Crypto's lower barriers to entry and "low cost, nearly instantaneous, borderless, peer-to-peer transfers of actual value,"[11] creates an unparalleled opportunity to bolster financial inclusion by helping underserved communities worldwide access the financial system.

---

[8] *See* Financial Action Task Force (FATF), Opportunities and Challenges of New Technologies for AML/CFT (July 2021), https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.

[9] *Global Crypto Owners Near 300 Million, Predicted to Hit 1 Billion by the End of 2022*, Crypto.com (Jan. 19, 2022), https://blog.crypto.com/global-crypto-owners-near-300-million-predicted-to-hit-1-billion-by-the-end-of-2022.

[10] *See* World Bank, Financial Inclusion, Overview, https://www.worldbank.org/en/topic/financialinclusion/overview#1 (last visited Feb. 10, 2022).

[11] Andreesen Horowitz, The web3 Landscape at 10 (Oct. 2021), https://a16z.com/wp-content/uploads/2021/10/The-web3-Readlng-List.pdf.

Underbanked communities in the United States, particularly those comprising minority populations, have shown a particular interest in crypto,[12] a trend recently recognized by the Acting Comptroller of the Currency, Michael Hsu. When describing crypto's appeal to these communities, Hsu noted the fact that "37 percent of the underbanked indicated they own cryptocurrency, compared to 10 percent of the fully banked."[13] Several members of Congress have also recently remarked on cryptocurrency's ability to bring traditionally underbanked individuals into the financial system.[14] For many of these underbanked and minority communities, the traditional financial system has generally not been tailored to their financial needs.[15] In comparison, cryptocurrency, with its decentralized infrastructure and ease of access, provides a much-needed alternative for these individuals to take control of their financial present – and future.[16] Crypto therefore has the potential to democratize finance and expand access and ownership opportunities for these individuals and communities.

While the United States has been at the forefront of many of these developments, the current uncertain regulatory climate that developers face in the U.S. is poised to drive overseas the next generation of blockchain-based applications. Indeed, because of the inherently global nature of blockchain technology, this risk is particularly acute in the cryptocurrency context. Regulation that is not sensitive to the unique dynamics of cryptocurrency, combined with the

---

[12] *See e.g.*, Silvia Foster-Frau, *Locked Out of Traditional Financial Industry, More People of Color Are Turning to Cryptocurrency*, Wash. Post (Dec. 1, 2021), https://www.washingtonpost.com/national/locked-out-of-traditional-financial-industry-more-people-of-color-are-turning-to-cryptocurrency/2021/12/01/a21df3fa-37fe-11ec-9bc4-86107e7b0ab1_story.html; Kori Hale, *Why Black Investors Seemingly Prefer Cryptocurrencies Over Traditional Stocks*, Forbes (Aug. 10, 2021), https://www.forbes.com/sites/korihale/2021/08/10/why-black-investors-seemingly-prefer-cryptocurrencies-over-traditional-stocks/?sh=16d66c906839.

[13] Michael J. Hsu, Acting Comptroller, OCC, *Remarks Before the BritishAmerican Business Transatlantic Finance Forum Executive Roundtable: "The Future of Crypto-Assets and Regulation"* (Jan. 13, 2022), https://www.occ.treas.gov/news-issuances/speeches/2022/pub-speech-2022-2.pdf.

[14] *See e.g.,* Sam Sutton, *Four Takeaways From the House Stablecoin Hearing*, PoliticoPro (Feb. 8, 2022) ("Several Republicans and some Democrats urged caution against cracking down on privately backed digital tokens that have become a resource for underbanked communities. New York Democratic Reps. Ritchie Torres and Gregory Meeks noted that Black and Hispanic communities have moved more quickly to embrace crypto and decentralized finance platforms as a form of financial services."); Kollen Post, *What We Learned at Congress' Much-Anticipated Summit of Crypto Execs,* The Block (Dec. 8, 2021), https://www.theblockcrypto.com/post/126866/what-we-learned-at-congress-much-anticipated-summit-of-crypto-execs ("[S]everal Democrats who entered the committee this year seemed more interested in crypto's potential positive impacts. Rep. Ritchie Torres asked the witnesses how stablecoins could help the large immigrant population in his district in the South Bronx facilitate cheaper remittances.").

[15] Samuel Haig, *Minority Communities Are Investing in Crypto to Escape Financial Discrimination*, Cointelegraph (Aug. 17, 2021), https://cointelegraph.com/news/minority-communities-are-investing-in-crypto-to-escape-financial-discrimination.

[16] Cryptocurrency also has the potential to reduce the cost of remittances, especially low-value remittances, the average cost of which the World Bank has pegged at 6.3%. *See* World Bank, Remittance Prices Worldwide, Quarterly, Issue 39, at 5 (Sept. 2021), https://remittanceprices.worldbank.org/sites/default/files/rpw_main_report_and_annex_q321.pdf. Technologies such as Celo, which offers a consumer-facing mobile application that integrates with a native stablecoin platform, enables remittances to be confirmed in seconds and securely transferred, allowing for faster, cheaper, and more energy efficient cross-border transactions. *See* Evan Kereiakes, *Rethinking Remittances with Blockchain Technology and Celo*, Celo Blog (May 28, 2020), https://medium.com/celoorg/rethinking-remittances-with-blockchain-technology-720c978084d4.

"de-risking" of U.S. financial institutions in developing regions, can also have a significant impact on U.S. national security as U.S. companies become less predominant in the cryptocurrency space.[17]

Specifically, as described in this letter, productive relationships between crypto financial institutions and law enforcement agencies are critical to mitigating financial crime risk, but those relationships, and the exchanges of information they facilitate, may be put at risk if crypto financial institutions move offshore. This is because crypto financial institutions are required to collect information about their customers both at onboarding and throughout the lifecycle of the customer relationship. Law enforcement agencies can combine this information, obtained with subpoenas or other forms of lawful process, with information obtained from the blockchain to identify specific perpetrators of illicit activity. To the extent crypto financial institutions move overseas, the ability of U.S. law enforcement agencies to obtain expediently the pieces of the puzzle that cannot be obtained from public blockchains will likely be reduced commensurately, to the detriment of the U.S. law enforcement and national security communities. Just as the U.S. benefits from the fact that large global telecommunications, Internet, and social media companies are headquartered here, U.S. law enforcement—and thus the American people—will lose out if cryptocurrency financial institutions leave the United States or are never established here in the first place.

The absence of U.S. firms from the cryptocurrency payments space can also leave voids that could be filled by other payments technologies, like China's Digital Yuan project, which has the potential to fundamentally reshape the global payments ecosystem in a way that will undoubtedly be detrimental to U.S. interests.

In the face of global competition, U.S. regulators have an opportunity to counteract these trends, and help realize the promise of crypto. While the economic benefits of keeping cryptocurrency companies in the United States are obvious, it is also a tremendous advantage to U.S. national security and law enforcement to ensure that the cutting edge of innovation remains in this country.

III. *The AMLA, Public-Private Partnerships, and Identity Management*

Congress recognized the potential for technology to transform the U.S. AML/CFT regime in the Anti-Money Laundering Act of 2020 ("AMLA").[18] Title LXII of the AMLA in particular focuses on modernizing the AML/CFT system—the topic of this RFI—and contains several sections relating to leveraging technology and innovation to improve the effectiveness and

[17] ClearingHouse, A New Paradigm: Redesigning the U.S. AML/CFT Framework to Protect National Security and Aid Law Enforcement (Feb. 2017), https://bpi.com/wp-content/uploads/2018/07/20170216_tch_report_aml_cft_framework_redesign.pdf.

[18] The AMLA is contained in Div. F of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, Div. F, 134 Stat. 3388, 4547 (2021).

efficiency of the current AML/CFT framework.[19] We encourage FinCEN to capitalize on this pivotal moment and reimagine how to conduct core BSA activities consistent with the spirit of the statute and the possibilities that now exist.

In Part II of this comment letter, we focus on how FinCEN and the private sector can develop novel mechanisms of threat identification, which go beyond recordkeeping and reporting requirements, and leverage public and private resources to develop typologies and risk indicators of financial crime that can be disseminated throughout the industry. In Part III, we explain why FinCEN should encourage the adoption of novel approaches to identity management. Collectively, these approaches can reduce financial crime risk while better protecting customer privacy.

In the half-century since the adoption of the BSA, the U.S. AML/CFT regime has evolved to adapt to changing threats and changing opportunities. By leveraging technology to improve threat identification, and adopting novel approaches to identity management, the U.S. can set the tone for how governments and transnational bodies manage financial crime risk globally for the next generation.

IV. *FinCEN Should Foster Innovative Frameworks to Identify and Mitigate Financial Crime Risk Related to Blockchain-Based Transactions.*

The original intent of the BSA of 1970 was to mitigate money laundering risk by instituting a set of preventative measures that put financial institutions on the front lines of the fight against financial crime. At the outset of the statutory regime, the BSA centered on ensuring banks maintained the requisite records to provide information that is "highly useful" to government investigations and that banks submitted reports on otherwise-ephemeral cash transactions. The BSA has since been refreshed periodically to address new threats through new mechanisms of a regime fundamentally grounded in recordkeeping and reporting; examples include formal Suspicious Activity Report ("SAR") requirements and, after 9/11, Sections 314(a) and 314(b) of the USA PATRIOT Act.

The explosive growth of cryptocurrencies marks another inflection point and can facilitate a new, and improved, mechanism to identify and mitigate financial crime risk. Specifically, because blockchains are generally public and reveal transaction histories, it is possible to analyze those transactional records to identify typologies of high-risk behavior, specific high-risk addresses, risk indicators, and the tactics and techniques that illicit actors use

[19] *See e.g.,* AMLA, § 6207 (adding a Subcommittee on Innovation and Technology to the BSAAG to advise FinCEN and other federal and state regulators on how to most effectively encourage and support technological innovation in the area of AML/CFT and reduce any obstacles to innovation that may arise from existing regulations); *id.* § 6208 (establishing Bank Secrecy Act Innovation Officers to advise public and private sector stakeholders on innovative methods, processes, and new technologies that may assist with AML/CFT compliance and provide technical assistance and guidance regarding their implementation); *id.* § 6209 (requiring standards by which financial institutions must test the new technologies); *id.* § 6210 (requiring FinCEN to conduct an analysis of the impact of the new technologies on financial crimes compliance); *id.* § 6211 (establishing a global financial crimes tech symposium focused on how the new technologies can be used to more effectively combat financial crimes and other illicit activities).

to launder ill-gotten funds (like the ways in which ransomware actors "hop" among multiple blockchains to attempt to hide the proceeds of their criminal activity)[20] on the basis of publicly available information,[21] while mitigating impacts on privacy.

Private sector actors are generally well-positioned to leverage their expertise in blockchain analytics to identify this activity and can combine it with specific intelligence from government agencies about threats to ensure the work is maximally impactful. Working together, government and the private sector can develop typologies of illicit activity that can be shared among a broad range of participants in the blockchain ecosystem to ensure that even smaller financial institutions can have up-to-date information to identify and prevent emerging illicit threats. And, importantly, because this kind of preventive risk management is less dependent on recordkeeping and reporting, it poses fewer privacy challenges. SARs remain a vital law enforcement tool, and we envision a regime to complement and support SARs by sharing threat typologies and risk indicators widely across members of the blockchain industry subject to the BSA to help ensure those SARs are impactful by permitting financial institutions to situate the activity they are seeing in the context of broader threats.

The power of blockchain data to provide information about transactions is especially noteworthy when viewed in light of recent proposals to expand the scope of suspicionless reports like Currency Transaction Reports ("CTRs") to require reporting of certain transactions between cryptocurrency exchanges and self-hosted wallets.[22] Traditional CTRs may have been appropriate when they related exclusively to cash transactions, information about which would have been lost if not captured contemporaneously. But, as described in this letter, much of the information about transaction histories that would have been required by recent proposals to expand CTR requirements, such as the date and time, amount, source and destination wallet address of transactions, and transaction hash, is *already* available on blockchains.[23] This reality means proposals to report this data to FinCEN are duplicative and unnecessary, while at the same time posing serious privacy and security risks to consumers.

---

[20] This practice is often referred to as "chain hopping"—a practice often used by illicit actors to obfuscate the origin of their funds by converting one cryptocurrency into a different cryptocurrency at least once before moving the funds to another service or platform. *See* FinCEN, Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021 (Oct. 2021), https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf.

[21] For example, the Statement of Facts released in connection with the two arrests made for an alleged conspiracy to launder cryptocurrency stolen during the Bitfinex hack in 2016 includes a number of statements about the government's reliance on public blockchain data to identify the alleged perpetrators. U.S. Dep't of Justice, Statement of Facts at 2 & n.7 (Feb. 7, 2022), https://www.justice.gov/opa/press-release/file/1470211/download ("U.S. authorities traced the stolen funds on the BTC blockchain," which is "a public transaction ledger that includes a record of every BTC transaction that has ever occurred").

[22] Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 85 Fed. Reg. 83,840 (proposed Dec. 23, 2020) ("NPRM"), https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28437.pdf; *see also* 86 Fed. Reg. 3,897 (Jan. 15, 2021) (reopening comment period) ("January NPRM"), https://www.govinfo.gov/content/pkg/FR-2021-01-15/pdf/2021-01016.pdf; 86 Fed. Reg. 7,352 (Jan. 28, 2021) (extending comment period), https://www.govinfo.gov/content/pkg/FR-2021-01-28/pdf/2021-01918.pdf.

[23] *See* Coinbase Comment, Dkt. No. FINCEN-2020-0020 (Mar. 25, 2021), https://www.regulations.gov/comment/FINCEN-2020-0020-8248.

To the extent recent proposals related to CTRs requested information not directly available on blockchains, like the "name and physical address of each counterparty to the transaction of the financial institution's customer,"[24] FinCEN's proposal to collect and retain that data in large government repositories, as opposed to simply mandating that financial institutions retain those records internally, poses serious privacy and security concerns. Such concerns are especially sharp with respect to CTR requirements that would link a person's PII with their blockchain addresses, which, if accessed without authorization, could reveal their entire blockchain transaction history. That proposal also used the same $10,000 threshold for cryptocurrency CTRs without fully considering the differences between cryptocurrency and cash transactions. This makes particularly clear that simply grafting traditional recordkeeping and reporting requirements onto the blockchain is at best inappropriate – an unlawfully obtained fiat currency CTR is unlikely to reveal a customer's entire financial history, but an unlawfully leaked crypto CTR linking a person's real identity with his or her blockchain address could have significant privacy and security consequences.

In light of these concerns, FinCEN and the rest of the U.S. regulatory community should prioritize the development of systems to identify illicit financial activity that leverage the unique properties of publicly available blockchain data, instead of expanding existing reporting requirements in a manner that poses significant privacy and security concerns without commensurate benefits. Doing so will not only give law enforcement agencies better tools but will also free up compliance resources at cryptocurrency exchanges to focus on important value-added activities, like SAR investigations, and is consistent with a "risk-based approach to AML/CFT regulation" that will mark a departure from the status quo.[25]

V. *The Foundations of the Modern Recordkeeping and Reporting System*

A core insight of the BSA is that the private sector has an inherent comparative advantage in recognizing certain forms of suspicious activity. The modern AML system, where financial institutions must report certain categories of transactions through CTRs and SARs, in particular, is rooted in the idea that "the creation of a meaningful system for detection and prevention of money laundering is impossible without the cooperation of financial institutions,"[26] because "it is representatives of financial institutions, rather than law enforcement, who see the money launderers first."[27] Moreover, "because money laundering

---

[24] January NPRM, 86 Fed. Reg. at 3,899.

[25] Himamauli Das, Acting Director, FinCEN, *Prepared Remarks of FinCEN Acting Director Him Das, Delivered Virtually at the American Bankers Association/American Bar Association Financial Crimes Enforcement Conference* (Jan. 13, 2022), https://www.fincen.gov/news/speeches/prepared-remarks-fincen-acting-director-him-das-delivered-virtually-american-bankers.

[26] *See* FinCEN; Proposed Amendment to the Bank Secrecy Act Regulations—Requirement of Money Transmitters and Money Order and Traveler's Check Issuers, Sellers, and Redeemers to Report Suspicious Transactions, 62 Fed. Reg. 27,900, 27,901 (proposed May 21, 1997) (finalized on Mar. 2, 2000), https://www.govinfo.gov/content/pkg/FR-1997-05-21/pdf/97-13303.pdf (proposing to amend the BSA regulations to require money transmitters, and issuers and sellers of money orders to report suspicious transactions to further the "creation of a comprehensive system . . . for the reporting of suspicious transactions," *id.* at 27,900).

[27] FinCEN, Advisory, *Court Interprets "Safe Harbor" Provisions*, (Aug. 1, 1996), https://www.fincen.gov/resources/advisories/fincen-advisory-issue-5.

transactions are designed to appear legitimate in order to avoid detection,"[28] bank "officials . . . are more likely than government officials to have a sense as to which transactions appear to lack commercial justification or otherwise cannot be explained as falling within the usual methods of legitimate commerce."[29]

Because the government understood that financial institutions were often better positioned than official agencies to identify suspicious transactions, it followed that financial institutions should be required to retain records about those transactions and to report them to the government. The specific regulatory requirements that implement this core idea and govern the private sector's role have evolved over time.

VI. *BSA Recordkeeping and Reporting Requirements*

In 1970, the BSA imposed recordkeeping requirements and required the filing of reports for certain types of transactions. The statute noted that records of the identities of accountholders,[30] and of cash transactions,[31] which were by nature ephemeral, were of particular value because "[r]eports of domestic currency transactions will be quite helpful in limiting the use of secret foreign financial facilities for illegal purposes. These reports will also facilitate domestic law enforcement transactions . . . If certain cash transactions are required to be reported to the Treasury Department, law enforcement agencies, particularly in the income tax field, will have a useful tool in their investigations and proceedings. "[32]

VII. *Suspicious Activity Reports*

In 1992, the Annunzio-Wylie Anti-Money Laundering Act granted the Treasury broad authority to require financial institutions to report suspicious transactions.[33] Pursuant to this authority, a "single integrated system" was created that reflected, among other things, the "mutual desire" of Treasury and financial regulators to "simplify and reduce the burdensomeness of the reporting process," while "increas[ing] the effectiveness of counter-money laundering efforts."[34] Over time, FinCEN expanded SAR requirements to other types of financial institutions, including, among others, money services businesses ("MSBs").[35]

VIII. *Information Sharing under 314(a) and 314(b)*

In response to the 9/11 attacks, Congress adopted the USA PATRIOT Act, aimed at combatting terrorism more effectively. Sections 314(a) and 314(b) of that statute inaugurated a

---

[28] 62 Fed. Reg. at 27,901; *see also* Proposed Amendment to the Bank Secrecy Act Regulations—Requirement to Report Suspicious Transactions, 60 Fed. Reg. 46,556, 46,558 (proposed Sept. 7, 1995), https://www.govinfo.gov/content/pkg/FR-1995-09-07/pdf/95-22223.pdf.
[29] 62 Fed. Reg. at 27,901.
[30] Currency and Foreign Transactions Reporting Act, Pub. L. No. 91-508, § 101, 84 Stat. 1114, 1114-15 (1970).
[31] Currency and Foreign Transactions Reporting Act, § 221.
[32] 116 Cong. Rec. 16,949, 16,954 (May 25, 1970) (remarks of Rep. Patman).
[33] Annunzio-Wylie Anti-Money Laundering Act, Pub. L. No. 102-550, tit. XV, § 1517(b), 106 Stat. 3672, 4059-60 (1992).
[34] 60 Fed. Reg. at 46,558.
[35] *See* 31 C.F.R. § 1022.320.

new paradigm in information sharing to fight money laundering and terrorist financing. Each provision facilitates the flow of information among relevant participants in the financial ecosystem – between government and financial institutions under 314(a), and on a voluntary basis among financial institutions under 314(b).

Taken together, these components of the BSA—SAR and CTR reporting, along with 314(a) and 314(b)—establish a recordkeeping and reporting regime that originated in the context of fiat currency transactions. As noted above, however, the blockchain obviates the need for reporting on certain types of data, and as explained further below, it also opens new opportunities for government and the private sector to identify threats and risks in a way that is scalable and often immediate.

IX. *The Blockchain Informational Advantage*

Certain types of reports, like high-value SARs, will always be important to the identification and mitigation of financial crime. But blockchain technology unlocks new potential forms of threat identification based on the same foundational idea that history demonstrates has always animated BSA information reporting processes: the private sector has unique insight about risks that are valuable and important to the government in combating criminal activity. In the blockchain era, it will remain the case that "[n]o system for the reporting of suspicious transactions can be effective unless information flows *from* as well as *to* the government."[36] But the ways in which public and private sector efforts leverage their comparative advantages to fight financial crime should be adapted to the unique advantages of blockchain technology.

The AML regime should therefore be augmented with structures to facilitate the identification of threat typologies and risk indicators, with an eye toward sharing them broadly to prevent financial crime. This approach would leverage the unique properties of the blockchain, on which all transactions are generally publicly available. And as cryptocurrency applications proliferate, an increasing portion of economic activity will likely take place on publicly observable blockchains. Just as in the past, where the government recognized that the private sector has the unique capacity to identify suspicious activity, hosted wallet providers and cryptocurrency exchanges, in partnership with others such as blockchain analytics firms, may today be better positioned than government to develop techniques to analyze activity on the blockchain, and to identify specific typologies of illicit activity. The government, by contrast, may have access to a broader range of information that can be used to confirm the identities of individual wallet-holders involved in potentially suspicious activity, and to inform an analysis of financial crime trends. Therefore, it is critical for the government to work in partnership with the private sector to establish the necessary "feedback loop[s]" for threat identification and mitigation that Acting Director Das has said is one of FinCEN's goals.[37]

There are a range of possibilities for the specific shape novel frameworks to identify and mitigate financial crime risk with respect to blockchain-based technologies could take, but below

[36] 60 Fed. Reg. at 46,559.
[37] Das, *supra* note 25.

we describe key principles any such regime should embrace. A structure that leverages the strengths of the public and private sectors fueled by modern data analytics and the blockchain would be powerful and could complement existing mechanisms of information-sharing like 314(a), 314(b), and SARs, which are, by their nature, retrospective. The AMLA took an important step in the right direction by mandating the creation of a Subcommittee on Innovation and Technology in the Bank Secrecy Act Advisory Group ("BSAAG"),[38] tasked with encouraging and supporting technological innovation.[39] The statute also required the Secretary of the Treasury to convene a group of public and private sector experts "to examine strategies to increase cooperation between the public and private sectors for purposes of countering illicit finance," which can be leveraged for these purposes.[40]

X. *Threat Identification – Core Principles*

A framework for threat identification aimed at the specific challenge of identifying and mitigating financial crime risk in blockchain-based transactions should be constructed with reference to a set of core principles. These kinds of partnerships should: (i) focus on typology development and rapidly disseminate those typologies and threat indicators across the industry and to global Financial Intelligence Unit ("FIU") partners; (ii) harness the power of technology; and (iii) leverage the full range of available administrative structures.

Importantly, this kind of framework will make it easier for law enforcement agencies to engage in global investigations quickly—a significant improvement over investigative capabilities with respect to fiat currency transactions today. At present, law enforcement agencies must rely on legal processes like subpoenas to gain access to transactional records held at financial institutions. Collecting and analyzing these records takes time, even when the transactions occur domestically at financial institutions that have been identified. If transactions related to criminal activity took place through financial institutions abroad, obtaining the records through Mutual Legal Assistance Treaty ("MLAT") requests can take months or years, if they yield relevant records at all.

With cryptocurrency, the history of wallet addresses is available for law enforcement to analyze—and even to seize directly, as the Department of Justice recently did with the proceeds of the Bitfinex hack, unraveling "a labyrinth of cryptocurrency transactions" on the path to a significant prosecution.[41] The approach we propose in this letter also allows law enforcement to invert the typical investigative process, and start by identifying high-risk transactions on the blockchain (*e.g.*, a wallet that interacted with a known criminal network), and to work from there to identify the individuals involved in the activity. Law enforcement agencies do not need to

[38] The BSAAG was established pursuant to Section 1654 of the Annunzio-Wylie Anti-Money Laundering Act of 1992, as a means by which the Treasury receives advice on the BSA. The Director of FinCEN serves as the chair of BSAAG and is responsible for ensuring that relevant issues are placed before the BSAAG for review, analysis, and discussion. Annunzio-Wylie Anti-Money Laundering Act, § 1564(a)-(b).
[39] AMLA, § 6207.
[40] AMLA, § 6211.
[41] Press Release, U.S. Dep't of Justice, *Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency* (Feb. 8, 2022), https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency.

wait for SARs to be filed to pursue bad actors. And during the course of ongoing investigations, law enforcement agents can use blockchain records to identify additional persons and entities with whom the subjects transacted, wherever in the world they may be, without waiting on MLAT requests that may or may not be granted.

These possibilities illustrate the power of devoting public and private sector resources to developing structures to fully utilize the potential of blockchain-based records, instead of imposing reporting requirements on cryptocurrency exchanges that cover records that are already available publicly.

Develop typologies that can be disseminated broadly. As noted above, core BSA structures were designed to require recordkeeping and reporting to support government investigations of individuals, entities, and networks. These requirements, especially as they relate to SARs, are and will remain important. But they should be supplemented with alternative structures that leverage unique properties of blockchains to reduce financial crime risk.

While in some circumstances these structures could be used to advance individual investigations—and, as noted above, to identify high-risk wallet addresses—these structures would be designed to create the tools to empower cryptocurrency financial institutions to more effectively identify indicators of specific types of financial crime risk. These may include typologies of criminal activity that would illustrate, for example, how bad actors use techniques like "chain-hopping" to obfuscate the links between specific crypto assets and unlawful activity.

These typologies and tools can broadly promulgate information to a wide range of actors in the crypto ecosystem so they can monitor for such activity on their networks. This approach would complement efforts to interdict the particular perpetrators of specific criminal acts and would help facilitate the development of a broad cohort of financial institutions equipped with the ability to identify and interdict illicit activity that interacts with their platforms. This approach would also permit smaller financial institutions to benefit from the work of these partnerships even if they lack the resources to participate directly. And focusing on typologies also has the salutary effect of buttressing consumer privacy because the focus would not be on collecting and reporting information about individual financial institution customers.

These kinds of partnerships can also allow rapid iteration of typology development as threats emerge, based on information that originates either with the government or with the private sector. They can also leverage FinCEN's power to connect with its global FIU partners to expand the exchange of financial intelligence that is relevant to the development of the kinds of impactful typologies discussed here.[42]

---

[42] *See* FinCEN, The Egmont Group of Financial Intelligence Units, https://www.fincen.gov/resources/international/egmont-group-financial-intelligence-units (last visited Feb. 11, 2022) (describing the Egmont Group as an international networks of FIUs designed to "improve communication, information sharing, and training coordination amongst its FIU members" and which supports its FIU members by "helping them to expand and systematize the exchange of financial intelligence and information, improve expertise and capabilities of personnel, and enable secure communication with one another").

Harness the power of technology. This type of work is enabled by the nature of the blockchain—purposefully designed to create an immutable record of transactions—which allows for open-source traceability and accountability of each transaction, regardless of the identity or location of the participants. Records of fiat currency transactions have traditionally been siloed at financial institutions, but because the transactions that take place on the blockchain are public, new tools can be used to analyze those transactions on an aggregated basis to identify typologies and threats.

In the past decade, compliance technology also has developed rapidly, with quantum leaps made in areas such as data analytics, artificial intelligence, and machine learning, which can help to better identify risks and communicate, monitor, and address suspicious activity.[43] These technologies are evolving at a rapid pace. The ideal mechanism would therefore leverage the comparative advantages of public and private to marry the government's information about threats and bad actors with the private sector's expertise in analytics, and access to additional types of information about transactions and relationships.

Leverage a range of administrative frameworks. This effort will depend not only on new substantive approaches to financial crime threat mitigation, but also on new administrative structures for doing so. FinCEN has long had the authority to grant exceptive relief from its regulations,[44] and to provide administrative rulings on the implications of proposed activity under the BSA.[45] FinCEN has also recently published a report noting that it should embark on a rulemaking process to adopt a framework to grant no-action relief.[46] And several U.S. states have developed regulatory sandboxes to help facilitate the incubation of new ways to provide financial services.[47] One can envision the use of these authorities to create novel structures that combine features of, for example, 314(a) and 314(b) to facilitate the development and dissemination of typologies and risk indicators.

---

[43] FATF, Opportunities and Challenges of New Technologies for AML/CFT (July 2021), https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.
[44] 31 U.S.C. § 5318(a)(7); 31 C.F.R. § 1010.970(a).
[45] FinCEN has the authority to issue administrative rulings interpreting regulations promulgated under the BSA pursuant to 31 C.F.R. § 1010.710. For a list of published administrative rulings, *see* FinCEN, Administrative Rulings, https://www.fincen.gov/resources/statutes-regulations/administrative-rulings (last visited Feb. 11, 2022).
[46] FinCEN, Assessment of No-Action Letters in Accordance with Section 6305 of the Anti-Money Laundering Act of 2020 (June 28, 2021), https://www.fincen.gov/sites/default/files/shared/No-Action%20Letter%20Report%20to%20Congress%20per%20AMLA%20for%20ExecSec%20Clearance%20508.pdf .
[47] Multiple states have launched a "regulatory sandbox" for innovative financial products or services, including Arizona, Nevada, Utah, Florida, West Virginia, Hawaii, and North Carolina. *See e.g.*, Ariz. Rev. Stat. Ann. §§ 41-5601 *et seq.*; S.B. 161, 2019 Leg., 80th Sess. (Nev. 2019) (pending statutes); Utah Code Ann. §§ 13-55-101 *et seq*; Fla. Stat. Ann. § 559.952; W. Va. Code Ann. §§ 31A-8G-1 *et seq.*; Press Release, Gov. David Y. Ige, *DCCA News Release: Hawaii Launches First Sandbox for Digital Currency* (Mar. 17, 2020), https://governor.hawaii.gov/newsroom/latest-news/dcca-news-release-hawaii-launches-first-sandbox-for-digital-currency; N.C. Gen. Stat. § 169-1 *et seq*.

XI. *Examples of Public-Private Partnerships*

There are several extant frameworks that could serve as a model for what we propose, but FinCEN should leverage the structures described above, including the BSAAG and the consultation structure required by the AMLA, to consult with industry on how to establish these kinds of mechanisms.

NCFTA. The National Cyber-Forensics and Training Alliance ("NCFTA")—a Pittsburgh-based non-profit organization focused on identifying, mitigating, and neutralizing cybercrime threats globally—is one potential model for the type of public-private partnership we envision. NCFTA was initially established by the Federal Bureau of Investigation ("FBI") in 1997 and operates through strategic alliances and partnerships with subject matter experts in the public, private, and academic sectors.[48] NCFTA focuses on enabling "near real-time"[49] information sharing among members—some of which have staff permanently located at NCFTA—and fostering close collaboration among law enforcement, the private sector, and academia.

As the FBI describes it, the NCFTA essentially works as an early-warning system that leverages the power of real-time information sharing.[50] For example, a major banking institution that discovers a new kind of malware attacking its network can disseminate that information to other NCFTA members, which can then develop strategies to mitigate the threat. FBI agents and analysts from NCFTA can also use the information to open new or support existing investigations, often in concert with law enforcement partners globally. This model encourages not only information sharing between the government and the private sector, but also among private sector partners themselves.[51] Between 2015 and 2021, NCFTA produced 26,945 intelligence reports and referred 4,184 cases to law enforcement, ultimately resulting in the prevention of $12.25 billion in financial losses.[52]

JMLIT. The United Kingdom's Joint Money Laundering Intelligence Taskforce ("JMLIT") is another innovative public-private partnership, established in 2015, that can serve as a reference for the type of public-private partnership we propose. JMLIT is a partnership between law enforcement and financial institutions to exchange information relating to money laundering and wider economic threats. JMLIT members include financial institutions, the Financial Conduct Authority (the United Kingdom's principal financial regulatory body), Cifas (a United Kingdom fraud prevention organization), and various law enforcement agencies.

A particularly strong feature of JMLIT is its mechanism for public-private information sharing, which is actively used by law enforcement agencies to enhance their access to financial

---

[48] *The NCFTA: Combining Forces to Fight Cyber Crime*, FBI News (Sept. 16, 2011), https://www.fbi.gov/news/stories/the-ncfta-combining-forces-to-fight-cyber-crime.
[49] *See* NCFTA, About Us, https://www.ncfta.net/home-2/about-us (last visited Feb. 6, 2022).
[50] *The NCFTA: Combining Forces to Fight Cyber Crime*, FBI News (Sept. 16, 2011), https://www.fbi.gov/news/stories/the-ncfta-combining-forces-to-fight-cyber-crime.
[51] Christopher Wray, Dir., FBI, *The FBI and the Private Sector: Battling the Cyber Threat Together* (Jan. 28, 2021), https://www.fbi.gov/news/speeches/the-fbi-and-the-private-sector-battling-the-cyber-threat-together-012821.
[52] *See* NCFTA, Home, https://www.ncfta.net (last visited Feb. 6, 2022).

intelligence, facilitate interagency cooperation, and enhance their understanding of the ever-evolving money laundering landscape. Through JMLIT, law enforcement agencies can obtain information from multiple sources and quickly develop a comprehensive intelligence picture.[53] While JMLIT access is only granted to certain financial institutions, it has developed alerts that are distributed to the wider industry and non-JMLIT banks have filed SARs based on information learned from these alerts.[54]

Through its Operations Group, JMLIT facilitates weekly meetings among law enforcement agencies and financial institution representatives, supporting more iterative/real-time interactions. Private sector members of JMLIT are also encouraged to refer cases to the Operations Group using an information sharing gateway which complements the mandatory obligations imposed by the SAR filing regime. Since 2015, JMLIT has supported more than 950 law enforcement investigations and contributed to more than 280 arrests and the seizures or restraints of more than £86 million. In particular, JMLIT's private sector members have identified more than 7,400 suspicious accounts and commenced more than 6,000 internal investigations.[55]

XII. *FinCEN Should Encourage Novel Approaches to Identity Management*

Identity management is another area in which evolving technology can help accelerate changes to BSA processes. Traditionally, the core manifestation of the regulatory expectation that a financial institution must Know Your Customer ("KYC") was the Customer Identification Program ("CIP"). The policy rationale behind KYC and CIP is simple: financial institutions must know with whom they are dealing by obtaining and verifying customer information, including name, date of birth, address, and personal identification number (*e.g.*, taxpayer identification number),[56] to mitigate money laundering and terrorist financing risk.[57]

But, at present, and with some notable exceptions, financial institutions must each collect and verify this information independently on customers who establish accounts across multiple institutions. And they must do so using the same basic framework that has been in place since the advent of CIP requirements. Indeed, Congress has noted the need for "anti-money laundering, countering the financing of terrorism, and sanctions policies . . . that . . . do not unduly hinder or delay legitimate access to the international financial system for underserved

---

[53] FATF, *Mutual Evaluation Report for United Kingdom's Anti-money Laundering and Counter-terrorist Financing Measures* (Dec. 2018), https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf.

[54] *Id.*

[55] *See* National Crime Agency, NECC, Joint Money Laundering Intelligence Taskforce, https://www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre (last visited Feb. 11, 2022).

[56] *See* 31 C.F.R. § 1020.220(a)(2)(i)(A).

[57] *See* FinCEN; Customer Identification Programs for Certain Banks (Credit Unions, Private Banks and Trust Companies) That Do Not Have a Federal Functional Regulator, 67 Fed. Reg. 48,299, 48,302 (July 23, 2002), https://www.govinfo.gov/content/pkg/FR-2002-07-23/pdf/02-18193.pdf ("Obtaining sufficient information to verify a customer's identity can reduce the risk that a bank will be used as a conduit for money laundering and terrorist financing.").

individuals, entities, and geographic areas[.]"[58] The persistence of these challenges is particularly troubling given that technology has evolved significantly, and we have access to additional data and tools to verify identity efficiently and effectively.[59]

FinCEN should therefore help encourage novel approaches to identity management, including the use of blockchain technology, and the use of shared services and platforms, consistent with the forward-leaning, innovative solutions FinCEN and the FDIC are seeking to foster in their tech sprint on digital identity.[60]

Novel approach to storing and proving identifying information. FinCEN should consider encouraging the exploration of novel approaches to identity management that would permit financial institutions to meet the policy objective behind KYC and CIP requirements while allowing financial institutions to increase effectiveness and efficiency and better protect consumers' personal information.

FinCEN specifically could establish a process to evaluate the way novel mechanisms can be used to create and maintain digital identity records, including (but not limited to) the adoption of digital identity verification techniques that can use a combination of decentralized blockchain-based technologies and secure "off-chain" data repositories. Specifically, there are tools under development that can allow digital identity information to be stored securely, and that use digital markers or tokens to enable the persons whose identity information is requested to confirm for a financial institution at onboarding that their identity *has been* verified, without providing the sensitive PII itself. This provides a mechanism for a customer to control the dissemination of information about his or her identity, thus better protecting privacy, while also enabling access to financial services.[61]

There are even more novel ways of confirming identities without revealing identities that are under development through the use of zero-knowledge proofs and other sophisticated forms

---

[58] AMLA, § 6215(a)(8).

[59] *See, e.g.,* FATF, Digital Identity (Mar. 2020), http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf (broad discussion of evolving technologies available to facilitate digital identity management).

[60] FDIC, FDITECH, Measuring the Effectiveness of Digital Identity Proofing for Digital Financial Services, https://www.fdic.gov/fditech/techsprints/measuring-effectiveness.html (last visited Feb. 11, 2022) ("What is a scalable, cost-efficient, risk-based solution to measure the effectiveness of digital identity proofing to ensure that individuals who remotely (i.e., not in person) present themselves for financial activities are who they claim to be?").

[61] Traditionally, a user must register for an account for every service provider. Each service provider serves as the central authority for managing user identity. With novel identity management frameworks, the user can receive credentials proving identity from multiple issuers, such as government agencies, universities, and employers, and store them in a digital wallet. When a need for identity verification arises, the user can then present proofs of their identity to any company that requests it and these companies can verify the proofs are true. *See e.g.,* CAPCO, Decentralized Identity: How Digital Transformation and Distributed Ledger Technology is Disrupting KYC (2020), https://www.capco.com/-/media/CapcoMedia/Capco-2/PDFs/Decentralized_Identity_Disrupting_KYC.ashx; Darren Shou, *How Decentralized Identity Is Reshaping Privacy for Digital Identities*, Forbes (Dec. 10, 2021), https://www.forbes.com/sites/forbestechcouncil/2021/12/10/how-decentralized-identity-is-reshaping-privacy-for-digital-identities/?sh=247c3e6e3226.

of encryption.[62] These technologies would allow a customer to confirm that she is who she says she is, without revealing her specific identity. Doing so would be accomplished by the customer leveraging a token or other digital marker that only she possesses that would confirm she has unique access to a particular body of identifying information that is stored in encrypted form. This approach to identity management could potentially supplement existing CIP mechanisms that require the dissemination of large amounts of PII to numerous financial institutions. And it could do so while allowing individuals to keep their PII private and safe from theft or manipulation.

With time, many of the techniques described here could also incorporate non-traditional forms of identifying information (*e.g.*, mobile device identifiers) that would facilitate access to financial services for those who may lack government-issued photo IDs. While these technologies are likely a long way away from maturity, now is the time to allow experimentation and testing of these types of products to incentivize research into how they may scale over time.

Leverage shared services and shared platforms and collaboration among financial institutions. FinCEN should also further encourage financial institutions to leverage shared services and shared platforms in conducting identity management. On October 3, 2018, FinCEN and the federal banking regulators—FRB, FDIC, NCUA, and OCC—issued the *Interagency Statement on Sharing Bank Secrecy Act Resources* (the "2018 Interagency Statement"). Congress endorsed this approach in the AMLA, expressly encouraging financial institutions to enter the types of arrangements described in the statement.[63] The 2018 Interagency Statement was published "to address instances in which banks may decide to enter into collaborative arrangements to share resources to manage their [BSA] and [AML] obligations more efficiently and effectively."[64] FinCEN and the federal banking regulators defined collaborative arrangements as "two or more banks with the objective of participating in a common activity or pooling resources to achieve a common goal. Banks use collaborative arrangements to pool human, technology, or other resources to reduce costs, increase operational efficiencies, and leverage specialized expertise."[65] The 2018 Interagency Statement recognized that, although each financial institution faces a unique set of threats and risks, there are efficiencies to be gained by collaborating—including potentially in "reviewing and developing risk-based customer identification and account monitoring processes."[66]

---

[62] Howard Wu, *How the Coming Privacy Layer Will Fix the Broken Web*, Future (June 15, 2021), https://future.a16z.com/a-privacy-layer-for-the-web-can-change-everything/; Pamela Dingle, *Advancing Privacy with Zero-Knowledge Proof Credentials*, Microsoft: Identity Standards Blog (July 22, 2020), https://techcommunity.microsoft.com/t5/identity-standards-blog/advancing-privacy-with-zero-knowledge-proof-credentials/ba-p/1441554.

[63] *See* AMLA, § 6213 ("[i]n order to more efficiently comply with the requirements of this subchapter, 2 or more financial institutions may enter into collaborative arrangements, as described in the statement entitled 'Interagency Statement on Sharing Bank Secrecy Act Resources'").

[64] FRB, FDIC, FinCEN, NCUA, OCC, Interagency Statement on Sharing Bank Secrecy Act Resources at 1 (Oct. 3, 2018), https://www.fincen.gov/sites/default/files/2018-10/Interagency%20Statement%20on%20Sharing%20BSA%20Resources%20-%20%28Final%2010-3-18%29%20%28003%29.pdf.

[65] *Id.*

[66] *Id.*

More can be done, however, to build on the 2018 Interagency Statement. Regulators indicated that "[c]ollaborative arrangements as described in this statement generally are most suitable for banks with a community focus, less complex operations, and lower-risk profiles for money laundering or terrorist financing."[67] However, any financial institution that properly manages the risk of adopting an innovative approach to identity management should be able to do so, which would free resources to manage other financial crime compliance activities.

Identity management and CIP are precisely the kinds of requirements that the ideas embodied in the 2018 Interagency Statement could helpfully address because each financial institution at which a customer opens an account must collect and verify information identical to that previously collected and verified by the other financial institutions at which the customer has opened an account—a duplication of effort that can be reduced. Indeed, this type of approach to relying on data not contained at the relevant financial institution has historical precedent, as the BSA has permitted certain financial institutions to rely on the CIP of another financial institution in certain circumstances.[68] And a recent Government Accountability Office report on de-risking mandated by the AMLA noted the potential for shared KYC utilities to increase banking access for vulnerable groups, like humanitarian organizations and MSBs that cater to cross-border transfers.[69] It should be noted that FinCEN has not yet formally expanded the concept of reliance to MSBs—a category of financial institution that includes many cryptocurrency companies—but such an expansion could be warranted.

Customer due diligence. A final area where blockchain technology will play an important role is with respect to customer due diligence. As described above, transactional histories are generally publicly available on blockchains for analysis. It will be increasingly important for financial institutions of all types to leverage the information about transaction history that is available through blockchain forensic tools. These kinds of tools can identify transactions with high-risk counterparties or other kinds of high-risk activities and will be an indispensable component of customer due diligence on an ongoing basis.

XIII. *Conclusion*

The last decade has witnessed unprecedented dynamism in the ways financial products and services are delivered, largely as a result of the development of blockchain technology. As FinCEN reexamines the BSA, it faces an opportunity to similarly reimagine how AML compliance processes take place. One of the core ways it can do so is by supplementing the BSA's paradigm of recordkeeping and reporting with new frameworks for the public and private sectors to identify and mitigate financial crime risks. Anchored in the comprehensive public record of transactions recorded on the blockchain, and enabled by advances in forensic tools to analyze those records, the public and private sectors have opportunities to employ novel approaches to identify and disseminate typologies of illicit finance threats. Similarly, blockchain

[67] *Id.*
[68] *See, e.g.,* 31 C.F.R. § 1020.220(a)(6).
[69] U.S. Gov't Accountability Office, GAO-22-104792, Bank Secrecy Act: Views on Proposals to Improve Banking Access for Entities Transferring Funds to High-Risk Countries at 29-31 (Dec. 2021), https://www.gao.gov/assets/gao-22-104792.pdf,

technology and advanced cryptography have the potential to reinvent identity management and customer due diligence while protecting privacy and making those processes more effective. We look forward to continuing to collaborate with FinCEN to accomplish these shared objectives.

Respectfully submitted,

/s/ Sheila Warren

Sheila Warren

Chief Executive Officer

Crypto Council for Innovation

Crypto
Council for
Innovation

June 14, 2022

Ali Khawar
Acting Assistant Secretary
Employee Benefits Security Administration
200 Constitution Ave NW
Suite N-5677
Washington, DC 20210
khawar.ali@dol.gov

Re: Compliance Assistance Release No. 2022-01, 401(k) Plan Investments in "Cryptocurrencies"

Dear Mr. Khawar:

The Crypto Council for Innovation ("CCI") submits this letter to the Department of Labor in response to the Department's "Compliance Assistance Release No. 2022-01, 401(k) Plan Investments in 'Cryptocurrencies'" ("Release").[1] CCI is deeply concerned that the Release in effect categorically precludes 401(k) administrators from including crypto investment options in their plans, based on a factually and legally flawed analysis. Therefore, we urge the Department to rescind the Release and clarify that retirement plan administrators may offer crypto investment options consistent with their ordinary fiduciary duties under the Employee Retirement Income Security Act of 1974 ("ERISA"). We also urge the Department to commence a more open, inclusive, and deliberative process to develop guidance for the inclusion of crypto assets on 401(k) investment menus, consistent with the President's "Executive Order on Ensuring Responsible Development of Digital Assets."[2] Finally, we request that the Department consider the information in this letter as it participates in the interagency process prescribed by the Executive Order and develops appropriate guidance regarding crypto assets.

CCI shares the Department's commitment to "ensur[ing] the security of the retirement, health, and other workplace-related benefits of America's workers and their families" and supports the Department's effort to do so "by developing effective regulations; assisting and educating workers, plan sponsors, fiduciaries and service providers; and vigorously enforcing the law."[3] However, we respectfully submit that the position reflected in the Release (as well as in recent public statements by senior Department officials) is not fully aligned with this commitment or the Administration's approach to cryptocurrencies embodied in the Executive Order or established legal standards because it:

---

[1] Dep't of Labor, Compliance Assistance Release No. 2022-01, 401(k) Plan Investments in "Cryptocurrencies" (Mar. 10, 2022), https://www.dol.gov/agencies/ebsa/employers-and-advisers/plan-administration-and-compliance/compliance-assistance-releases/2022-01.

[2] Executive Order, Executive Order on Ensuring Responsible Development of Digital Assets (Mar. 9, 2022), https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/.

[3] Dep't of Labor, Employee Benefits Security Administration, About Us, "Our Mission," https://www.dol.gov/agencies/ebsa/about-ebsa/about-us/mission-statement (last accessed June 13, 2022).

- Departs from the text of ERISA and judicial precedents and Department regulations interpreting that text by replacing the ordinary fiduciary duty of prudence with a new standard of "extreme care."
- Narrowly considers only the risks of cryptocurrencies while disregarding their potential benefits, including growth and portfolio diversification. As with any other type of investment option, plan fiduciaries must consider both the risks *and* the potential benefits of cryptocurrencies.
- Invents an approach that, because of its exclusive consideration of risks, would deter plan fiduciaries from including myriad other types of investment options in their plans—because all investment options have risks—even though such options have long been appropriately included in plans and have generated significant returns for many plan participants.
- Ignores interest from investors, including plan participants, for assets with features offered by cryptocurrencies, such as assets that are supply inelastic or that are tied to the performance of one or more currencies; and
- Is inconsistent with the Executive Order's directive to conduct an interagency process to support the responsible development of digital assets.

We provide more detail on each of these points below.

ABOUT CCI

CCI is an alliance of crypto industry leaders with a mission to communicate the benefits of crypto and demonstrate its transformational promise. CCI members include some of the leading global companies and investors operating in the crypto industry, including Andreesen Horowitz, Block (formerly Square), Coinbase, Electric Capital, Fidelity Digital Assets, Gemini, Paradigm, and Ribbit Capital. CCI members span the crypto ecosystem and share the goal of encouraging the responsible global regulation of crypto to unlock economic potential, improve lives, foster financial inclusion, protect national security, and disrupt illicit activity. CCI and its members stand ready and willing to work with the Department and the Administration to accomplish these goals and ensure that the most transformative innovations of this generation and the next are anchored in the United States.

INTRODUCTION

The Release takes a one-sided, highly negative view of crypto assets, seeing (and amplifying) only their risks without acknowledging the opportunities they offer or placing them in context with other investment options, which pose their own risks.[4] Accordingly, the Release admonishes fiduciaries to exercise "extreme care" with respect to such crypto investment options. Unfortunately, the Release is silent on how to properly manage these potential issues and how they compare to those associated with other potential classes of investment. Rather, the Release threatens enforcement for any deployment of assets into cryptocurrencies (or into assets

[4] Although the Release's title refers to "cryptocurrencies," the Release states that "the same reasoning and principles also apply to a wide range of 'digital assets' including those marketed as 'tokens,' 'coins,' 'crypto assets,' and any derivatives thereof." Release at n. 1.

whose value is tied to them), stating that the Department "expects to conduct an investigative program aimed at plans that offer participant investments in cryptocurrencies and related products."[5] And its condemnation of crypto will lay a foundation for plan participants to hold fiduciaries personally liable for any losses resulting from crypto investments.[6]

Few, if any, fiduciaries will be willing to assume the risk of public and private enforcement and personal liability, and therefore the Release as a practical matter bans crypto investment options categorically from use in 401(k) plans—even where a fiduciary might conclude that it would be appropriate to include a crypto-related investment option consistent with ordinary fiduciary duties after taking into consideration not only the risks of crypto but also the opportunity for gain and the options for risk diversification crypto may afford. Moreover, the Release gives this effective ban a sweeping scope by applying its position not only to "cryptocurrencies" but also to "related products" and "other products whose value is tied to cryptocurrencies"[7]—vague and undefined terms that could cover a wide range of investment options, given some companies' deployment of assets into cryptocurrencies or related products or businesses. Consequently, the Release could broadly chill cryptocurrency investments by a significant proportion of American investors.

The Release's posture toward crypto is at odds with many of the Biden Administration's policy priorities, including reinforcing the country's leadership in the development of digital assets, facilitating increased retirement planning, and expanding access to financial services for underbanked and underserved people. The Release is also at odds with the interests of plan participants, who would be unable to take advantage of benefits provided by cryptocurrencies, and correspondingly with fiduciaries' overarching ERISA duty to serve plan participants' interests by offering a diverse and balanced array of investment options after careful consideration of both their risks and their potential benefits.

The Release's many weaknesses presumably reflect its hasty development and adoption. On March 9, 2022, President Biden directed the Department (and other agencies) to study various issues relating to cryptocurrency and to prepare a report with policy recommendations, including actions to "support expanding access to safe and affordable financial services" within 180 days.[8] Yet, the very next day the Department issued the Release. Further, the Department sought no public comment on the Release, despite the benefits of, and norms supporting the solicitation of, public comment on significant administrative policymaking.[9] Indeed, the

---

[5] Release ¶5.
[6] 29 U.S.C. §1109(a); *see* Release ¶2.
[7] Release ¶4.
[8] Executive Order §5(b)(i).
[9] *See, e.g.*, Cass Sunstein, *"Practically Binding": General Policy Statements and Notice-and-Comment Rulemaking*, 68 ADMIN. L. REV. 491, 500 (2016) ("notice-and-comment … promotes legitimacy …: Policymakers might find out that their plan is in one or another respect misdirected"); Michael Asimow, *On Pressing McNollgast to the Limits: The Problem of Regulatory Costs*, 57 LAW & CONTEMP. PROBS. 127, 129 (1994) ("rulemaking procedures are refreshingly democratic: people who care about legislative outcomes produced by agencies have a structured opportunity to provide input into the decisionmaking process"); Mark Seidenfeld, *A Civil Republican Justification for the Bureaucratic State*, 105 HARV. L. REV. 1512, 1515 (1992) ("having administrative agencies set government policy provides the best hope of implementing civic republicanism's call for deliberative decisionmaking informed by the values of the entire polity").

Department's procedural shortcut has already prompted a lawsuit to invalidate the Release.[10] Recent statements by senior Department officials to the media and at industry conferences have compounded the Release's problems by reinforcing the threat of enforcement for offering crypto investment options while further clouding the precise standards and expectations to which plan fiduciaries will be subject.[11] The regulatory climate created by the Release and the Department's recent accompanying public statements harms both plan fiduciaries and plan participants.

Given the Release's potentially far-reaching consequences, the Department should rescind the Release, clarify that retirement plan administrators could include cryptocurrency investment options consistent with their fiduciary duties, and commence a more open, inclusive, and deliberative process to develop guidance for the inclusion of cryptocurrency on 401(k) investment menus.

The Release Impermissibly Changes the Fiduciary Duties of Plan Administrators in the Cryptocurrency Context

The Labor Department's Release is at odds with the duties of 401(k) plan fiduciaries under ERISA—as stated in the statute and as interpreted by both the courts and the Department's own regulations—in a number of ways. In fact, by strongly discouraging plan fiduciaries from offering crypto investment options, based on a purely negative view of their potential, the Release will pressure fiduciaries to act contrary to the interests of plan participants and their ERISA duties.

First, the Release indicates that the Department intends to require greater caution with respect to cryptocurrencies than ERISA requires. Under ERISA, retirement plan fiduciaries owe participants a duty to act with "the care, skill, prudence, and diligence under the circumstances then prevailing that a prudent [person] acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims."[12] The courts have generally recognized that this means that an ERISA plan fiduciary must act as an ordinary prudent trustee.[13] Similarly, the Department's regulations recognize that ERISA requires "reasonable" prudence.[14]

Yet, the Release "cautions plan fiduciaries to exercise extreme care before they consider adding a cryptocurrency option."[15] ERISA does not require "extreme care," and the Department

---

[10] Complaint, *ForUsAll, Inc. v. Dep't of Labor*, 1:22-cv-01551 (D.D.C. June 2, 2022), ECF No. 1.
[11] *See, e.g.*, Sam Sutton, *Bitcoin's crashing. The Biden administration wants to keep it out of your 401(k)*, Politico (May 13, 2022), https://www.politico.com/news/2022/05/13/bitcoin-crashing-fidelity-401k-00031241.
[12] 29 U.S.C. §1104(a)(1)(B).
[13] *See, e.g.*, *Skelton v. Radisson Hotel Bloomington*, 33 F.4th 968, 976 (8th Cir. 2022) ("ERISA fiduciaries have a duty of prudence—to exercise care and skill as a man of ordinary prudence would."); *In re Unisys Corp. Retiree Med. Benefit "ERISA" Litig.*, 242 F.3d 497, 509 (3d Cir. 2001), *as amended* (Mar. 20, 2001) ("The law requires only that a fiduciary deal fairly with his beneficiaries and, in doing so, that it exercise such care and skill as a man of ordinary prudence would exercise in his own affairs."); *Teamsters Loc. 282 Pension Tr. Fund v. Angelos*, 839 F.2d 366, 372 (7th Cir. 1988) (ERISA requires "ordinary prudence"); *Morse v. Stanley*, 732 F.2d 1139, 1145 (2d Cir. 1984) (ERISA imposes "a duty to exercise such care and skill as a person of ordinary prudence would exercise in dealing with his own property"); 29 C.F.R. §2550.404a-1(b)(2).
[14] 29 C.F.R. §2550.404a-1(b)(2).
[15] Release ¶1.

cannot impose a higher standard of care on fiduciaries generally or with respect to a specific asset class than ERISA sets.[16]

Second, the Release suggests that, with respect to cryptocurrencies, the Department intends to impose a duty that is different in kind from ERISA's duty of prudence. Under ERISA, the duty "focuses on a fiduciary's conduct in arriving at an investment decision, not on its results, and asks whether a fiduciary employed the appropriate methods to investigate and determine the merits of a particular investment."[17] Correspondingly, Department regulations state that in selecting investment options, plan fiduciaries fulfill their fiduciary duty under ERISA by "giv[ing] appropriate consideration to [the relevant] facts and circumstances" and "act[ing] accordingly."[18]

The Release, however, threatens enforcement action against plan fiduciaries based on the *substance* of particular investment decisions—to offer crypto investment options—rather than the process used by fiduciaries to select and offer such assets. The Department cannot alter the fundamental nature of the duty imposed by ERISA or impose an additional duty beyond those defined by ERISA.[19]

Third, the Release would interfere with plan fiduciaries' performance of their ERISA duty to make investment decisions based on a holistic analysis of each investment option. Under ERISA, "the prudence of each investment is not assessed in isolation but, rather, as the investment relates to the portfolio as a whole."[20] Thus, Department regulations mandates that plan fiduciaries "give[] appropriate consideration to … the role the investment or investment course of action plays in … the plan's investment portfolio."[21] That includes considering whether the investment option is "reasonably designed … to further the purposes of the plan, taking into consideration" both the investment option's "risk of loss" and its "opportunity for gain" "compared to" to the alternative options' potential for loss or gain.[22]

By threatening enforcement action based on the inclusion of digital asset options in a plan, however, the Release strongly deters plan fiduciaries from giving crypto investment options the holistic consideration required by ERISA. Fiduciaries could face enforcement liability—or at a minimum, the burden and expense of defending against an enforcement action—for including digital asset options in their plans, even if they had determined that such options were appropriate. Conversely, fiduciaries apparently could safeguard themselves against Department enforcement action by categorically excluding digital asset options, again even if they

---

[16] *See, e.g.*, *Chamber of Com. of U.S. of Am. v. United States Dep't of Labor*, 885 F.3d 360, 368 (5th Cir. 2018) (invalidating Labor Department regulation because it "expanded the statutory term 'fiduciary'"); *National Fed'n of Indep. Bus. v. Occupational Safety & Health Admin.*, 142 S. Ct. 661, 665 (2022) (per curiam) ("Administrative agencies are creatures of statute. They accordingly possess only the authority that Congress has provided.").
[17] *Pension Ben. Guar. Corp. ex rel. St. Vincent Cath. Med. Ctrs. Ret. Plan v. Morgan Stanley Inv. Mgmt. Inc. ("PBGC")*, 712 F.3d 705, 716 (2d Cir. 2013); *see also, e.g.*, *Stegemann v. Gannett Co.*, 970 F.3d 465, 474 (4th Cir. 2020); *Sweda v. Univ. of Penn.*, 923 F.3d 320, 329 (3d Cir. 2019); *Fink v. Nat'l Sav. & Tr. Co.*, 772 F.2d 951, 955 (D.C. Cir. 1985).
[18] 29 C.F.R. §2550.404a-1(b)(1).
[19] *See supra* note 16.
[20] *PBGC*, 712 F.3d at 717.
[21] 29 C.F.R. §2550.404a-1(b)(1)(i).
[22] 29 C.F.R. §2550.404a-1(b)(2)(i).

determined that such assets were appropriate and superior to the alternatives in specific circumstances. Put another way, the Release discourages plan fiduciaries from exercising their best judgment in selecting investment options—when the Department should be *encouraging* fiduciaries to exercise such judgment.

Moreover, the analysis of cryptocurrencies on which the Release bases its threat of enforcement action does not reflect the type of rational, holistic assessment required by ERISA. The Release treats cryptocurrencies as categorically dangerous investments, exclusively and repeatedly discussing their risk of loss without ever mentioning their opportunities for gain. Like plan fiduciaries in making investment decisions, the Department cannot blind itself to the opportunity cost of risk aversion to plan participants in providing guidance or making enforcement decisions.

Relatedly, fiduciaries must "diversify[] the investments of the plan so as to minimize the risk of large losses, unless under the circumstances it is clearly prudent not to do so."[23] Diversification itself is a sensitive and multi-factor analysis regarding the plan, the portfolio, and the investment options.[24] In contrast, the Release focuses on *one* consideration: whether a fiduciary includes crypto investments. Under some circumstances, digital asset options could enhance a plan's diversification, enabling participants to protect against some risks, or to balance a generally lower-risk portfolio. By categorically condemning crypto investment options and threatening enforcement action for including them in retirement plans, however, the Release will prevent fiduciaries from taking advantage of crypto investment options to diversify their plans' offerings.

The Department Should Not Disregard the Administration's More Balanced Approach to Cryptocurrencies

In contrast to the approach reflected in the Release, the Executive Order and subsequent statements about its implementation by the Secretary of the Treasury reflect a view of cryptocurrency that focuses not on the risks involved in the asset class, but rather on getting the cryptocurrency regulatory framework right in light of a full appreciation of both risk and potential benefits. The Department should embrace this holistic and balanced approach so it does not lose sight of the potential benefits of cryptocurrency as it continues to develop its position on digital assets.

The day before the Department issued its Release, the President issued the Executive Order charting a whole-of-government effort to ensure that all Americans have "expand[ed] access to safe and affordable financial services."[25] The Executive Order embodies an "approach to digital assets … that encourages innovation but mitigates the risks."[26] The Executive Order

[23] 29 U.S.C. §1104(a)(1)(C).
[24] *PBGC*, 712 F.3d at 717.
[25] Executive Order §1(e).
[26] Executive Office of the President, Statement by NEC Director Brian Deese and National Security Advisor Jake Sullivan on New Digital Assets Executive Order ¶2 (Mar. 9, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/09/statement-by-nec-director-brian-deese-and-national-security-advisor-jake-sullivan-on-new-digital assets -executive-order/.

promotes "United States leadership in the global financial system [that] will sustain United States financial power and promote United States economic interests."[27] It also expresses hope that digital assets can assist "those Americans underserved by the traditional banking system" and that they can help "ensur[e] that the benefits of financial innovation are enjoyed equitably by all."[28] Through the Executive Order, the President specifically directed the Department to work with the Secretary of the Treasury and other agencies to develop recommendations to expand access to safe and affordable financial services.[29] To do so, the President declared, the Department must consider "the risks *and opportunities*" that wide adoption of different types of digital assets "might present to United States consumers, investors, and businesses."[30]

In a recent speech, the Secretary of the Treasury, Janet Yellen, articulated her approach to digital assets and implementing the Executive Order, which mirrors the President's and is focused on "responsible innovation."[31] This includes evaluation of both the downside and upside potential of digital assets. Like the Department of Labor, Secretary Yellen recognized that crypto assets can be used for fraudulent ends, just as traditional financial products can be, and agrees that the government should guard against such misuse.[32] She ended her statement, however, with optimism about the future predicated on the benefits of crypto assets: "Think of the development of the national highway system, the space race, the creation of the internet, or the ongoing revolution in biotechnology. All of these innovations have transformed the way we live our lives."[33] So too, she said, could digital assets, which have already "opened a world of possibilities and risks that would have seemed fantastical only a few decades ago."[34]

The Many Benefits of Including Cryptocurrencies in Retirement Plans

Instead of taking the approach embodied in the Release, the Department should consider some of the many benefits of cryptocurrency *alongside the risks* as it crafts its response to the Executive Order and its policies with respect to cryptocurrency more broadly. The Department's position should recognize the significant growth that crypto assets can experience despite their volatility and risk. Long-term retirement investors in particular could benefit from this growth potential. Crypto assets also hold significant appeal to categories of investors who have historically been marginalized from or reluctant to use traditional retirement planning options. These potential benefits dovetail for younger workers, who have tended to avoid retirement planning but who have shown a strong interest in crypto assets and have a long investment horizon. Retirement plan administrators, therefore, could include cryptocurrencies in a risk-appropriate manner to help encourage younger and underserved investors to participate in the retirement savings system.

---

[27] Executive Order §2(d).
[28] *Id.* §2(e).
[29] *Id.* §3.
[30] *Id.* §5(b)(i) (emphasis added).
[31] Dep't of the Treasury, Remarks from Secretary of the Treasury Janet L. Yellen on Digital Assets at American University's Kogod School of Business Center for Innovation §I (Apr. 7, 2022), https://home.treasury.gov/news/press-releases/jy0706.
[32] *Id.* §III ¶2 ("For example, consumers, investors, and businesses should be protected from fraud and misleading statements regardless of whether assets are stored on a balance sheet or distributed ledger.").
[33] *Id.* §V ¶1.
[34] *Id.* ¶4.

The Volatility of Crypto Assets Can Provide Long-Term Opportunities for Growth

To provide enough money for retirement, a portfolio must increase in value. The longer the investment term, the less sensitive investors can be to short-term volatility and the more they can benefit from compounding growth. Thus, a common retirement strategy is to change the portfolio's mix of asset types over time, starting with higher-reward investments—even if riskier or more volatile—and later transitioning into lower-risk and lower-volatility investments to capitalize on the opportunity for large growth early on and to protect the gains as the investor approaches the time for withdrawing funds.[35] The Release acknowledges this venerable wisdom,[36] yet charts a regulatory position that disregards it.

Crypto investments could easily fit this paradigm as a growth asset, especially for long-term investors. For example, a fiduciary could compare the opportunity for growth from a given crypto investment to available equities, which are the traditional high-growth asset.[37] In one scenario, incorporating cryptocurrencies as a small part of a moderately aggressive long-term portfolio of 70% stocks and 30% bonds from 2017 to 2021 would have led to 42 percent higher investment returns over the period.[38]

The Department expressed concern about the volatility of crypto assets. However, even accounting for volatility, crypto assets may continue to grow over the medium- to long-term. For example, as of June 13, 2022, BTC's price has increased by about 4,600 percent since May 2016 (from $500 to more $23,000).[39] Similarly, ETH's price has increased about 11,000 percent since April 2016 (from $11 to more $1,200).[40] These growth figures are net of the recent market decline (which many other asset classes also experienced), and thus illustrate the potential for cryptocurrencies' growth over the long time horizons retirement planning contemplates. These are the kinds of data and analysis that a fiduciary exercising reasonable prudence ordinarily would consider when evaluating whether an investment option is an appropriate addition to a retirement plan—and here, these data suggest that cryptocurrencies may well be appropriate options. Categorically excluding crypto assets, by contrast, could deny retirement savers the opportunity to reap the potential rewards of crypto investments and leave them worse off.

---

[35] Javier Simon, *How to Manage Your Portfolio's Asset Allocation at Any Age* ¶1, SMART ASSET (May 11, 2022), https://smartasset.com/investing/asset-allocation-by-age.
[36] Release ¶4 (noting that "those approaching retirement" may be more sensitive to asset volatility).
[37] Simon ¶5, *supra* note 35 ("One common asset allocation rule of thumb has been dubbed "The 100 Rule." It simply states that you should take the number 100 and subtract your age. The result should be the percentage of your portfolio that you devote to equities like stocks.").
[38] Geoff Williams, *Should You Invest in Cryptocurrencies or the Stock Market?* ¶3, MONEYGEEK (April 15, 2022), https://www.moneygeek.com/investing/crypto/cryptocurrency-or-stocks/ (analyzing the performance of a market-cap weighted index of crypto assets, the S&P 500 stock, and the S&P US Aggregate Bond Index).
[39] Kat Tretina, *10 Best Cryptocurrencies of June 2022*, FORBES ADVISOR (June 6, 2022), https://www.forbes.com/advisor/investing/cryptocurrency/top-10-cryptocurrencies/.
[40] *Id.*

Crypto Could Usefully Diversify Retirement Portfolios

Crypto assets could also be a useful addition to some portfolios by diversifying their assets. All markets and all investment options have risks, including traditional assets,[41] and diversifying the mix of assets in a portfolio is important to achieving stable long-term growth. The equities market is famously volatile. Speculation and over-investment in internet companies created the "dotcom bubble" of the late 1990s.[42] The NASDAQ Composite Index vaulted from 751 in January 1995 to 5,048.62 in March 2000.[43] The bubble then burst, and the NASDAQ lost $5 trillion in market value as a result.[44]

Commodities markets are similarly not safe from turmoil and are based on the availability of physical resources or natural events. Crop prices are a good example. Over multiple periods in recent decades, crop prices spiked and plummeted repeatedly due to changes in overseas demand, domestic supply, weather, and the prices of other commodities, among other factors.[45] During one saga in the 1970s, the prices for grains and oilseeds shot up and then remained volatile for an extended period.[46] Increased global demand for imports from countries with a large volume of petrodollars to spend coupled with poor crop yields globally due to poor weather conditions put pressure on prices to increase.[47] Prices of wheat, corn, and soybeans doubled or tripled during this period before declining sharply.[48] The prices rose substantially again, as governments, farmers, and consumers responded with export restrictions, ramped-up production, and lower consumption, respectively.[49] The cycle of price volatility continued throughout the decade before prices finally settled into a new equilibrium.[50]

Neither are gold and currencies safe from risk and volatility. Gold markets are often viewed as a haven in times of instability and a stable store of value.[51] But gold prices fluctuate

---

[41] *See, e.g.*, Kate Davidson & Aubree Eliza Weaver, *'Talk about clueless': Calabria unloads on Washington* ¶7, POLITICO (May 17, 2022) (quoting a former FHFA director that currently "the risk in the mortgage market is of magnitudes far greater than anything we're seeing in crypto or stablecoins"), https://www.politico.com/newsletters/morning-money/2022/05/17/talk-about-clueless-calabria-unloads-on-washington-00032946.

[42] *See* Int'l Banker, History of Financial Crises, *The Dotcom Bubble Burst (2000)* ¶1 (Sept. 29, 2021), https://internationalbanker.com/history-of-financial-crises/the-dotcom-bubble-burst-2000/.

[43] *Id.* ¶2.

[44] *Id.*

[45] May Peters et al., Feature: Crops, *Agricultural Commodity Price Spikes in the 1970s and 1990s: Valuable Lessons for Today*, USDA ECON. RSCH. SERV. (Mar. 1, 2009), https://www.ers.usda.gov/amber-waves/2009/march/agricultural-commodity-price-spikes-in-the-1970s-and-1990s-valuable-lessons-for-today/.

[46] *Id.* ¶7 ("National Agricultural Statistics Service and World Agricultural Supply and Demand Estimates, 2008.").

[47] *Id.* ¶¶7-12.

[48] *Id.* ¶7 ("National Agricultural Statistics Service and World Agricultural Supply and Demand Estimates, 2008."), ¶22.

[49] *Id.*

[50] *Id.* ¶¶7, 21.

[51] *See, e.g.*, Vicky McKeever, *Why People Consider Fold to be a 'Safe Haven' in Crises Like the Coronavirus* ¶4, CNBC (Apr. 20, 2020) ("It is in such times of uncertainty that gold is touted as a "safe haven" for those looking for shelter from more traditionally volatile investments, like stocks."), https://www.cnbc.com/2020/04/20/coronavirus-why-gold-is-seen-as-a-safe-haven-investment-in-a-crisis.html.

significantly in response to fears and panic—rational or irrational.[52] Fear and uncertainty can drive the price of gold up as some investors attempt a flight to safety; gold prices can then plummet when the panic evaporates. A strong dollar and other countervailing pressures can also lower the price of gold even when it might otherwise rise, such as during periods of inflation or uncertainty.[53] Currencies—even those of highly stable countries—also fluctuate, sometimes due to inflation, and occasionally they crash, as the British Pound Sterling notoriously did in the early 1990s.[54] The UK had entered into a common exchange rate agreement with other European countries that linked the values of their respective currencies.[55] However, the link between the currencies was frustrated by the differences in the countries' individual economies.[56] As a result of the differences, the UK withdrew from the agreement, which was viewed as a sign of further inflation, and the Pound lost about a sixth of its value against the German Mark overnight.[57]

Volatility in assets is therefore hardly unique to crypto, and volatility alone should not be—and, indeed, has not been—cause to exclude those assets from a well-balanced portfolio. Rather, the appropriate response, as ERISA itself recognizes, is diversification, so that the risks posed by some asset classes are mitigated by the benefits of other classes, and vice versa. Crypto assets provide another opportunity to diversify the risks inherent in other types of investment options, just as other types of investment options can provide a mechanism to mitigate risks posed by crypto assets.

Including Cryptocurrency in Retirement Plan Options May Make Saving for Retirement More Attractive to Younger Americans

Having access to retirement plan options that include cryptocurrency is particularly important for younger Americans, who have the most to gain from potentially high-growth assets like crypto and who tend to have a stronger interest in crypto than some traditional options. An advantage of investing at a young age is that there are more years of compounding returns. Yet, until at least quite recently, a significant portion of younger generations have shown little interest in saving for retirement.[58] Younger workers who fail to save appropriately for retirement permanently forgo the significant opportunity of compounding returns, potentially necessitating that they continue to work past retirement age, put a greater proportion of their earnings into investments in hopes of compensating for the lost compounding later in life, or experience greater precarity in old age.

---

[52] CME Grp., *Introduction to Gold Volatility Trading* ¶7 (Mar. 15, 2018), https://www.cmegroup.com/education/articles-and-reports/introduction-to-gold-volatility-trading.html.
[53] Arundhati Sarkar, *Gold Pressured by Stronger Dollar, Faster Fed Taper Bets* ¶¶1-2, Reuters (Nov. 22, 2021), https://www.reuters.com/markets/europe/gold-pressured-by-stronger-dollar-faster-fed-taper-bets-2021-11-22/.
[54] *See generally* Larry Elliott et al., *September 17 1992: Pound drops out of ERM*, The Guardian (Sept. 16, 1992), https://www.theguardian.com/business/1992/sep/17/emu.theeuro.
[55] *Id.*
[56] Craig R. Whitney, *Blaming the Bundesbank* ¶4, N.Y. Times Magazine (Oct. 17, 1993), https://www.nytimes.com/1993/10/17/magazine/blaming-the-bundesbank.html.
[57] *Id.* ¶4.
[58] Suzanne Woolley, *Plan for Retirement? Millennials Don't See the Point*, Bloomberg (Mar. 18, 2022), https://www.bloomberg.com/news/articles/2022-03-18/retirement-planning-45-of-millennials-gen-z-don-t-see-the-point#:~:text=Not%20only%20have%20many%20Americans,according%20to%20a%20new%20survey.

In contrast to this bleak picture, a sizable portion of younger workers today have shown interest in crypto and are already including crypto investments in their financial planning. Thirty-one percent of Americans ages 18-29 and twenty-one percent of Americans ages 30-49 have invested in, traded, or used a cryptocurrency compared to eight percent of Americans ages 50-64 and three percent of Americans over 65.[59] Thus, locking crypto investments out of retirement plans not only could deny workers the opportunity to choose an investment option they want but also could perniciously discourage younger Americans from saving as much as prudence counsels.

Crypto Assets Could be a Tool for Expanding Financial Inclusion and a Path to Building Wealth for Those Historically Excluded From the Traditional Financial System

Crypto investments have also proven attractive to communities of color and other communities that have historically been locked out of the traditional financial sector.

People of color have historically faced significant roadblocks to accessing means to accumulate wealth that were available to White Americans. Government policies and private actors long excluded people of color not only from home ownership,[60] but also from avenues to save for retirement on par with White Americans. For example, communities of color have faced discrimination in the ability to secure employment that provides access to stable retirement plans. As the Department recently highlighted, Black employees are 15 percent less likely than their White counterparts to have access to a job-based retirement plan.[61] In addition, 62 percent of Black working-age households lack assets in a retirement account, in contrast with 37 percent of White households in the same situation.[62] Even when workers of color can access a retirement plan or otherwise save for retirement, the wealth gap persists. Three-quarters of Black households ages 25-64 have less than $10,000 in retirement savings, compared to only half of White households, and among those close to retirement, households of color have one-fourth the average retirement savings ($30,000) of White households ($120,000).[63]

In contrast, communities of color and those who have been historically excluded from full access to the traditional financial system have not faced the same obstacles to owning crypto assets. Indeed, such groups have shown great enthusiasm for purchasing cryptocurrencies. As the Acting Comptroller of the Currency, Michael Hsu, recently noted, people of color own crypto

---

[59] Andrew Perrin, *16% of Americans say they have ever invested in, traded or used cryptocurrency* ¶3, Pew Rsch. Ctr. (Nov. 11, 2021), https://www.pewresearch.org/fact-tank/2021/11/11/16-of-americans-say-they-have-ever-invested-in-traded-or-used-cryptocurrency/.

[60] Sylvia Foster-Frau, *Locked Out of Traditional Financial Industry, More People of Color are Turning to Cryptocurrency* ¶16, Wash. Post (Dec. 1, 2021), https://www.washingtonpost.com/national/locked-out-of-traditional-financial-industry-more-people-of-color-are-turning-to-cryptocurrency/2021/12/01/a21df3fa-37fe-11ec-9bc4-86107e7b0ab1_story.html.

[61] Dep't of Labor Advisory Council on Employee Welfare & Pension Benefit Plans, Report to the Honorable Martin Walsh, U.S. Sec'y of Labor, Gaps in Retirement Savings Based on Race, Ethnicity and Gender 28-29 (Dec. 2021), https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2021-gaps-in-retirement-savings-based-on-race-ethnicity-and-gender.pdf.

[62] *Id.*

[63] *Id.*

assets at rates comparable to, and sometimes higher than, White Americans.[64] Eighteen percent of Black Americans and twenty percent of Hispanic Americans own crypto, in comparison to eleven percent of White Americans.[65] In addition, the underbanked own crypto at a higher rate (thirty-seven percent) than the fully banked (ten percent).[66] Some people of color report their experience with crypto as a "unique opportunity to even the playing field" and to get in on the ground floor of a growing sector.[67] Because crypto is a new sector, it affords the opportunity to guard against the bias and discrimination in the traditional financial system.[68] As one policy leader put it, speaking of people of color, crypto offers opportunities long denied to build wealth "for your community[and] … for the next generation."[69]

The ability to choose crypto assets in a retirement plan could be particularly important for groups that have for too long faced discrimination, including in financial services, and have been unable to build wealth as a result. Excluding crypto assets could be particularly pernicious given the tax benefits and opportunities for financial planning associated with retirement plans. For example, in the case of pre-tax contributions from both the employee and employer, these benefits help savers grow the value of their portfolio, take advantage of compounding returns, and reduce taxable income until funds are withdrawn. In a Roth IRA, the employee would receive the tax benefits on the back end, when the funds are withdrawn. These are the types of strategies that build wealth, and categorically excluding cryptocurrency from those plans could discourage historically underserved communities from participating in them.

Plan Fiduciaries and Other Experts Can Help Retirement Savers Understand and Manage Risks Associated With Crypto Investment Options

Although certain methods of holding crypto investments may be difficult for some investors, and some investors may benefit from additional education about the nature of crypto investments,[70] the Department fundamentally misunderstands the role retirement plan administrators can play in the cryptocurrency ecosystem. Just as plan administrators have helped participants understand and account for the risks inherent in other types of investment options, administrators can also help with respect to crypto risks, such as by providing a safe place to store crypto assets and a structured channel to communicate risk considerations to investors that will allow them to make informed choices about how to allocate their assets. For many investors today, the alternative is increasingly to invest in crypto directly, *without* the structure afforded by regulated 401(k) plans and administrators subject to strong fiduciary duties. For these reasons, the Department should *encourage* rather than *discourage* plan administrators to include cryptocurrencies in their retirement plans when they deem it appropriate.

In the last few years, retirement funds, insurers, and others in the retirement sector have begun incorporating crypto into the retirement landscape and building additional infrastructure to

[64] Michael J. Hsu, Comptroller, OCC, Remarks before the British American Business Transatlantic Finance Forum 1-2 (Jan. 13, 2022), https://www.occ.treas.gov/news-issuances/speeches/2022/pub-speech-2022-2.pdf.
[65] *Id.*; Nasdaq, *The Importance of Women in Crypto Leadership Positions* ¶5 (Apr. 29, 2022), https://www.nasdaq.com/articles/the-importance-of-women-in-crypto-leadership-positions.
[66] Hsu, *supra* note 64.
[67] Foster-Frau ¶34, *supra* note 60.
[68] *Id.* ¶12.
[69] *Id.* ¶6.
[70] Release ¶4.

support crypto-investing for retirement. For example, CalPERS, Pimco, the Houston Firefighters' Relief and Retirement Fund, and the Fairfax County (Virginia) Police Officers Retirement System have all begun investing directly in crypto assets like Bitcoin or in crypto-related companies or investment funds.[71] In addition, MassMutual is in the process of offering new technology platform to help registered investment advisors provide advice and support for digital asset investments, and is developing solutions to simplify billing.[72]

It is easy to see why retirement plans are entering the cryptocurrency market. Retirement plan administrators can help participants by selecting appropriate crypto investments as options and are likely better positioned than an average plan participant to assess individual investment options and to diversify risk.[73] This is as true of cryptocurrency investments as it is of equity, debt, and other traditional investments. Retirement plan administrators may also have the benefit of economies of scale to secure expert advice and institutional infrastructure.[74]

Plan administrators also have the resources to invest in cryptocurrencies through institutional-grade platforms like custodians, which can provide a safer option for people who want to make cryptocurrency a part of their saving and investment strategy than would be available to individual retail cryptocurrency holders. Indeed, while individual retail investors may have to store cryptocurrency as "lines of computer code" in individual self-housed wallets,[75] retirement plan administrators are likely to choose professional custodians.

With all these resources, administrators can ensure that participant funds are well safeguarded.

* * *

The Department's Release appears to have considered none of these important advantages to crypto or their implications for the proper discharge of plan administrators' fiduciary duties. The Release contains no discussion of the opportunity for gain, just the risk of loss; no discussion of the distributional consequences of a practical bar on crypto investments by retirement plans; and no discussion of whether retirement plans may be *superior* vehicles for Americans to gain exposure to cryptocurrency investments as opposed to the alternatives. Instead, the Department offers an ill-considered promise of enforcement against plan administrators who seek to help their participants gain exposure to an asset class from which

---

[71] Lawrence Wintermeyer, *Pension And Sovereign Wealth Funds Eye Crypto As Regulators Focus On A Global Crypto Framework*, FORBES (Dec. 30, 2021), https://www.forbes.com/sites/lawrencewintermeyer/2021/12/30/pension-and-sovereign-wealth-funds-eye-crypto-as-regulators-focus-on-a-global-crypto-framework/?sh=330216cc7399.

[72] Samuel Steinberger, *MassMutual Launches Crypto Subsidiary for RIAs* ¶1, WEALTHMANAGEMENT.COM (Sept. 30, 2021), https://www.wealthmanagement.com/technology/massmutual-launches-crypto-subsidiary-rias.

[73] Dep't of Labor, *Meeting your Fiduciary Responsibilities* 2 (Sept. 2021) ("The duty to act prudently is one of a fiduciary's central responsibilities under ERISA. It requires expertise in a variety of areas, such as investments."), https://www.dol.gov/sites/dolgov/files/ebsa/about-ebsa/our-activities/resource-center/publications/meeting-your-fiduciary-responsibilities.pdf.

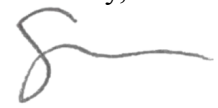
[74] *Id.* ("Lacking that expertise, a fiduciary will want to hire someone with that professional knowledge to carry out the investment and other functions.").

[75] Release ¶4.

they may benefit. That threat is neither supported by the facts nor consonant with the Administration's priorities.

For all the foregoing reasons, we urge the Department to rescind the Release, clarify that retirement plan administrators may offer crypto investment options consistent with their ordinary fiduciary duties under ERISA, and commence a more open, inclusive, and deliberative process to develop guidance for the inclusion of cryptocurrency on 401(k) investment menus.

Sincerely,



Sheila Warren, Esq.
Chief Executive Officer
Crypto Council for Innovation

cc: Timothy Hauser, Deputy Assistant Secretary for Program Operations, Employee Benefits Security Administration, hauser.timothy@dol.gov

November 3, 2022

Jon Fishman
Assistant Director
Office of Terrorist Financing and
Financial Crimes
U.S. Department of the Treasury
1500 Pennsylvania Ave., NW
Washington, DC 20220

RE: Response to September 20, 2022, U.S. Department of the Treasury Request for Comment Regarding Ensuring Responsible Development of Digital Assets

Dear Mr. Fishman:

The Crypto Council for Innovation ("CCI") submits this letter in response to the September 20, 2022, U.S. Department of the Treasury ("Treasury") request for comment regarding "Ensuring Responsible Development of Digital Assets" (the "Request").

I. Introduction and Overview

CCI is an alliance of digital asset industry leaders with a mission to communicate the benefits of digital assets and demonstrate their transformational promise. CCI members include some of the leading global companies and investors operating in the digital asset industry, including Andreessen Horowitz, Block (formerly Square), Coinbase, Electric Capital, Fidelity Digital Assets, FTX, Gemini, Paradigm, and Ribbit Capital. CCI members span the digital asset ecosystem and share the goal of encouraging the responsible global regulation of digital assets to unlock economic potential, improve lives, foster financial inclusion, protect national security, and disrupt illicit activity. CCI and its members stand ready and willing to work with Treasury and the U.S. Government (the "USG") to accomplish these goals

and ensure that the most transformative innovations of this generation and the next are anchored in the United States.

CCI supports the goals articulated by President Biden in Executive Order 14067 of March 9, 2022, "Ensuring Responsible Development of Digital Assets" ("Executive Order"),[1] particularly the stated goals of (i) reinforcing U.S. leadership in the global financial system and in technological and economic competitiveness, including through the responsible development of payment innovations and digital assets; (ii) promoting access to safe and affordable financial services; and (iii) supporting technological advances that promote the responsible development and use of digital assets. We believe that digital asset technologies and services can and will be developed in a way that advances these goals while protecting consumers, investors, and businesses, safeguarding the U.S. and global financial system, and mitigating the risks posed to U.S. national security by illicit finance.

As we described in our August 8, 2022, letter in response to Treasury's request for comment *TREAS-DO-2022-0014-0001* regarding "Ensuring Responsible Development of Digital Assets" (the "August 2022 Letter"),[2] digital assets based on blockchain technology represent some of the most significant innovations in finance in many years, with the potential to alter ownership structures, commercial applications, cross-border payments, transaction processing and settlement, access to capital, investment opportunities, and much more. In the United States, digital assets have the promise to provide critical payment services to the unbanked or underbanked. Beyond our shores, in countries that have collapsing economies or authoritarian regimes, digital assets can provide a financial – and literal – lifeline. Recent events including Russia's invasion of Ukraine and popular movements in opposition to authoritarian regimes demonstrate the urgency of establishing payment methods that cannot be intercepted or monitored by despotic regimes. For these reasons alone, it is imperative that the USG and private industry work together to foster these innovative technologies.

This letter builds on the August 2022 Letter and our February 13, 2022, letter responding to the Financial Crimes Enforcement Network ("FinCEN") Request for Information on the Modernization of U.S. AML/CFT Regulatory Regime (the "February 2022 Letter")[3] and focuses on two of Treasury's questions included in the

---

[1] 87 Fed. Reg. 14143, March 14, 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/

[2] The August 2022 Letter is included as Exhibit A.

[3] The February 2022 Letter is included as Exhibit B.

Request that we believe are particularly important in fostering the conditions that will enable the USG and the digital asset community to work collaboratively to achieve the goals articulated by the President:

> **Question D. 1.** "How can the U.S. Department of the Treasury, in concert with other government agencies, improve guidance and public-private communication on AML/CFT and sanctions obligations with regard to digital assets?"
>
> **Question D. 2.** "How can Treasury maximize public-private and private-private information sharing on illicit finance and digital assets?"

We provide our thoughts and recommendations related to these questions in Parts II and III. Part IV describes how public-private partnerships and improved education can help reduce the risk that USG action may have unintended consequences that could undermine the President's goals in the Executive Order, such as by impeding law enforcement efforts, creating privacy concerns, further excluding the unbanked and underbanked populations from the global financial system, and stifling innovation. Part V provides a summary of our recommendations responsive to the questions above and certain other questions in the Request.

II. Question D. 2. "How can the U.S. Department of the Treasury, in concert with other government agencies, improve guidance and public-private communication on AML/CFT and sanctions obligations with regard to digital assets?"

We appreciate the efforts Treasury and the USG have undertaken in recent years to learn more about the benefits and risks of digital assets and other blockchain technologies. The President's call in the Executive Order to the various USG executive agencies to further understand the unique promise and challenges of digital assets underscores the continued importance of understanding the history of the digital asset ecosystem, the underlying technologies, and available tools that can make digital assets and related technologies safer and more effective.

a. Two-way public-private sector communication is imperative to ensure that the solutions to potential illicit finance risks incorporate the latest developments in the digital asset space and the unique features of digital assets.

Key players in the digital asset ecosystem and the USG, including law enforcement, FinCEN and the Office of Foreign Assets Control ("OFAC"), should continue to establish and foster open communication to find effective solutions to the

challenges posed by illicit finance. Frequent dialogue between the USG and major private sector players like CCI and our members will enable the USG to better understand the technologies and how responsible innovation – not just regulation – can solve many of the problems related to illicit finance that the government is seeking to address. Additionally, the digital asset community can gain insights from the USG, which will often have access to information that the industry does not. In this regard, we would appreciate frequent advisories and guidance from U.S. regulators like FinCEN and OFAC on relevant financial crime typologies. Prior advisories and guidance papers from these agencies in 2013, 2019 and 2021, respectively, have been instrumental in establishing an understanding of the applicability of financial regulations to different digital asset and blockchain business types and has led to consistency in how compliance controls are implemented across the industry.

Moreover, given the rapid innovation and deployment of a wide array of digital asset and other blockchain technologies in recent years, including cryptocurrencies, decentralized finance ("DeFi"), stablecoins, non-fungible tokens ("NFTs"), and decentralized autonomous organizations, any regulatory approach to these technologies should acknowledge and account for each asset or technology's unique and evolving characteristics. For example, fungible digital asset tokens are not the same thing as NFTs. NFTs are not only unique, but they are almost always associated with rich metadata, such as artwork or media, which is a key differentiator from fungible digital asset tokens and may therefore warrant a different regulatory approach. Similarly, DeFi protocols provide a myriad of products and services that vary significantly, ranging from products that mirror traditional financial services (e.g., lending, borrowing and exchange activity) to prediction markets, yield lotteries, and liquidity pools, with new business models emerging every day. There is also a wide range of decentralization in the DeFi space that makes it difficult, if not impossible, to impose the same regulatory requirements on all DeFi protocols. These examples demonstrate the importance of tailoring regulation to the specific product or service, particularly as digital asset products and business models continue to evolve, becoming increasingly complex and distinctive.

Private sector academics, technologists, businesspeople, and entrepreneurs who are innovating such technologies are best positioned to provide insights into this changing landscape. As described in our August 2022 Letter, the USG has long recognized that traditional financial institutions, like banks and money transmitters, have access to information and technology necessary to enable the USG to identify and prevent illicit activity. Major players in the digital asset ecosystem are similarly positioned to help the government to innovate and develop techniques to help combat illicit finance through responsible innovation that is fit for purpose.

b. Building consumer financial and digital literacy can make the digital asset ecosystem safer and more beneficial for all users.

We strongly support efforts to build financial and digital asset literacy among the public. We think that we can build a safer, and more resilient ecosystem by educating the public who seek to reap the benefits of digital assets. We also believe that transparency is key to ensuring that consumers receive the full benefits of the digital asset space and the technologies that support them. The general public should fully understand how digital assets work (and do not work), the key players in the space, how trust is earned and maintained, and the potential risks that digital assets may share with other financial products, as well those that are unique to the digital asset space. Armed with this knowledge, consumers will be well equipped to make informed decisions based on their own goals and risk tolerance—decisions that make the digital asset ecosystem safer and more beneficial to all.

c. The USG should consider exceptive relief and regulatory sandboxes to afford the digital asset industry opportunity to innovate to solve the challenges posed by illicit finance.

We believe that increasing our collective understanding of the risks and benefits of digital assets will require allowing technologies room to grow. It is only by providing the players in this space opportunities to innovate that we will begin to understand the full potential of this technology. Beyond keeping open lines of communication with the digital asset industry, as we described in our August 2022 Letter, the USG should consider the use of exceptive relief and regulatory sandboxes to allow for experimentation that could enable public and private partners to gather knowledge and pursue effective, innovative regulation. For example, several U.S. states have established regulatory sandboxes to help foster responsible innovation and explore the potential expansion of financial products and services that digital assets can offer their residents.[4] These sandboxes provide a safe space for the digital asset industry to explore the potential benefits that their innovation can bring to consumers and the broader financial system, while providing the necessary legal and regulatory guardrails in this space.

By fostering open dialogue, consumer financial and digital asset literacy, and the use of exceptive relief and regulatory sandboxes, we believe that the United States

---

[4] *See e.g.*, Ariz. Rev. Stat. Ann. §§ 41-5601 *et seq.*; Fla. Stat. Ann. §§ 559.952 *et seq.*; Utah Code Ann. §§ 13-55-101 *et seq.*; W. Va. Code Ann. §§ 31A-8G-1 *et seq.*; Wyo. Stat. Ann. §§ 40-28-103 *et seq.*

can position itself as the world leader in digital asset innovation and remain the central player in the global financial system.

III. Question D. 1. "How can Treasury maximize public-private and private-private information sharing on illicit finance and digital assets?"

Existing initiatives and partnerships such as FinCEN Exchanges and other programs have served to increase public-private sector collaboration and coordination. However, we think that additional and more robust public-private information sharing frameworks would facilitate stronger management of illicit finance risks in the digital asset ecosystem.

a. Treasury should consider establishing industry-hosted and other bidirectional information sharing programs to expand the USG's understanding of the digital asset ecosystem.

We believe that collaboration between the public and private sectors would be most effective if information flows more freely in both directions. As such, while the FinCEN Exchange program has been a very useful starting point for facilitating USG-led discussions, we propose FinCEN Exchanges hosted and led by industry leaders to further expand the USG's understanding of the industry and relevant technologies. The private sector is well-equipped and committed to provide the USG with insight into the industry's perspective on the digital asset landscape to assist in the investigation and prosecution of financial crimes. These meetings should include a safe harbor for private industry participants so that they feel empowered to share insights freely with the USG. Conversely, we hope that the USG will provide more frequent and useful information to digital asset industry partners to ensure the private sector is best positioned to detect and prevent illicit finance.

The Treasury-led Financial and Banking Information Infrastructure Committee ("FBIIC") and Financial Services Sector Coordinating Council ("FSSCC") are examples of successful public-private collaboration. Another example of successful information sharing efforts between national government and industry players is the UK's Joint Money Laundering Intelligence Taskforce ("JMLIT"). JMLIT, which we previously discussed in our February 2022 Letter, demonstrates the power of two-way law enforcement and financial sector partnerships. JMLIT, which is part of the UK's National Economic Crime Centre, is a private-public coalition of over 40 financial institutions collaborating with five law enforcement agencies and other UK regulators to facilitate information sharing on new typologies, existing vulnerabilities, and live tactical intelligence. Since its inception in 2015, JMLIT has supported nearly 1,000 law enforcement investigations leading to more than 280 arrests and the seizure of

over £86 million.[5] Through JMLIT, the UK has also identified over 7,400 suspect accounts linked to money laundering activities and has commenced over 6,000 internal investigations.[6] To facilitate the two-way flow of information, the UK government has shared over 60 "JMLIT Alert" reports with the broader financial industry to deepen the industry-government partnership and enhance monitoring and enforcement of financial crimes nationwide.[7] JMLIT is widely viewed as an international example of best practice for government-private sector information sharing, and we recommend the USG consider creating a similar body or program in the United States to enable the private sector to serve as a more effective first line of defense against illicit finance.

b. Treasury should establish a public-private 24/7 rapid-response communication network to monitor for and share intelligence on illicit finance risks.

We propose that FinCEN consider establishing and hosting a 24/7 public-private rapid response communications network across national boundaries. FinCEN currently participates in similar – albeit governmental-only – networks, such as the Rapid Response Program ("RRP"). RRP facilitates partnership between FinCEN, U.S. law enforcement, and foreign agencies to help victims and their financial institutions recover funds stolen as a result of cyber-enabled financial crime schemes, including business email compromise.[8] We understand the RRP activates when a criminal complaint is reported, and then proceeds to open an investigation and coordinate sharing of financial intelligence with financial intelligence units ("FIUs") of allied foreign countries. Through such information sharing, FinCEN encourages foreign authorities to intercept fraudulent transactions, freeze funds, and recall payments under the authority of their own respective legal and regulatory frameworks. Thanks to the RRP's efforts, FinCEN has assisted in the successful recovery of over $1.1 billion across 70 jurisdictions.

While public-sector only networks like RRP are a good start, including private sector actors can allow FinCEN and other USG agencies to have fuller insight into

---

5 Nat'l Econ. Crime Ctr., *Successes of JMLIT*, Nat'l Crime Agency, https://www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre (last visited Oct. 21, 2022).

6 *Id.*

7 *Id.*

8 *FinCEN Fact Sheet: Fact Sheet on the Rapid Response Program (RRP)*, Fin. Crimes Enf't Network, at 1 (Feb. 11, 2022), https://www.fincen.gov/sites/default/files/shared/RRP%20Fact%20Sheet%20Notice%20FINAL%20508.pdf.

real-time threats impacting industry. With the participation of the U.S. Department of Justice, Federal Bureau of Investigation, and other USG agencies, along with the private sector, a similar network in the digital asset context could facilitate swift and coordinated action to address illicit finance risks.

c. We recommend that the USG strategically leverage sections 314(a) and 314(b) of the USA PATRIOT Act to deepen engagement with the digital asset industry.

While real-time information sharing through the proposed 24/7 communication network will be critical to combat financial crimes in the digital asset space in the United States and worldwide, we also propose that the USG strategically leverage sections 314(a) and 314(b) of the USA PATRIOT Act[9] to engage industry participation more deeply. Through regulations established under these provisions of the USA PATRIOT Act, federal, state, local, and European Union law enforcement agencies have already connected with approximately 14,000 financial institutions to identify accounts and transactions of individuals likely to be involved in terrorism or money laundering.[10] However, these legal frameworks may need to be modified to better serve and account for the interests of both law enforcement and the digital asset community. For example, the type of personally identifying information shared with financial institutions for screening and the mechanisms used to share such information may need to be tailored to the digital asset space.

We encourage the USG to work with Congress and the industry to enhance these existing information sharing frameworks.

d. The USG should consider creating international digital asset coordination centers to combat illicit finance in the digital asset space and promote and understand innovation.

Finally, newly created national and international digital asset coordination centers could be used as a focal point for combating illicit finance and promoting and understanding innovation. These centers could facilitate public and private sector

---

[9] Pub. L. No. 107-56, §§ 314(a), (b), 115 Stat. 272, 307, 308 (2001). Section 314(a) requires the Secretary of the Treasury to encourage regulatory and law enforcement authorities to share information with financial institutions regarding individuals, entities, and organizations engaged in or suspected to be engaged in terrorist or money laundering activities. Section 314(b) permits financial institutions to share information with one another to identify and report these parties to the federal government.

[10] *FinCEN's 314(a) Fact Sheet*, Fin. Crimes Enf't Network, at 1 (Oct. 18, 2022), https://www.fincen.gov/sites/default/files/shared/314afactsheet.pdf.

training, enable real-time information sharing, and promote the dissemination of shared analysis related to criminal networks and emerging money laundering typologies. While such coordinated information sharing typically takes place through mutual legal assistance treaties ("MLAT"), the MLAT process is often unable to match the pace of international financial criminals. Cross-border digital asset coordination centers could help address gaps in enforcement left outstanding by the MLAT process.

The Egmont Group is a prime example of a public-private collaborative project. The Egmont Group is a body of 66 FIUs that collaborate to facilitate and prompt the exchange of information, knowledge, and cooperation among FIUs globally.[11] The Egmont Group has achieved particular success in countering terrorist financing and money laundering crimes by groups such as ISIS and Al Qaeda.[12] While we recognize that certain limitations on information sharing may exist due to local data protection and secrecy laws in various jurisdictions, we recommend that Treasury and the USG look to organizations such as the Egmont Group and FinCEN's RRP as models for overcoming or operating within such constraints.

Whether through additional FinCEN exchanges led by U.S. industry partners, increased cross-border collaboration through coalitions or collaborative centers, or some combination of these options, we see a wide breadth of opportunity for increased cooperation between the private and public sectors. With increased two-way information sharing between both groups, greater transparency and effectiveness and criminal enforcement in the digital asset space is achievable. Our objective remains to support and partner with the USG toward these goals and we would welcome the opportunity to further discuss any of these proposals.

IV. Avoiding Unintended Consequences

Active public-private sector communications, consumer education, exceptive relief and regulatory sandboxes, and robust information sharing frameworks have the promise of not only making the digital asset ecosystem safer and more beneficial for all, but reducing the chances that USG actions may have unintended consequences that could stifle innovation, fracture the digital asset community, and push legitimate actors out of the ecosystem.

---

[11] Egmont Grp. Fin. Intel. Units, https://egmontgroup.org/ (last visited Oct. 21, 2022).

[12] *Annual Report 2014-2015*, Egmont Grp. Fin. Intel. Units, at 14 (2015), https://egmontgroup.org/wp-content/uploads/2021/09/Egmont_Group_Annual_Report_2014-2015.pdf.

The CCI fully supports the USG's efforts to combat illicit activity and protect consumers and businesses. These efforts should be grounded in a thorough understanding of the technologies that underlay the ecosystem and should be targeted to ensure that they reduce the risk of bad behavior while maximizing innovation that is beneficial to consumers and the wider economy. For instance, many perceived OFAC's recent designation of Tornado Cash as an attack on the entire digital asset ecosystem even if it may have been well-intentioned. This designation has had repercussions far beyond its effect on a single technology. Today, innovators are worried that their technology may be OFAC's next target or the target of other USG agencies. Such a trend has the potential to stifle innovation and push digital asset innovation outside of the United States where it will be more difficult for the USG to have a positive impact on this space.

a. Regulating the digital asset industry exactly like the traditional financial industry – notwithstanding the unique and distinct features of digital assets – may fracture the digital asset market by pushing innovators and business offshore.

Active dialogue between the USG and innovators can help reduce the risk of ineffective or even detrimental regulations and shift the focus to innovations that can help address and identify risks successfully. As an example, as we previously discussed in our February and August 2022 Letters, proposals such as requiring reporting of certain transactions between digital asset exchanges and self-hosted wallets, similar to Currency Transaction Reports ("CTRs") in the cash context, would likely be ineffective and unnecessary.[13] Unlike cash transactions, anyone, including USG agencies, can review a blockchain's transaction history to understand how wallets are being used and track their transaction history. Applying CTR-like requirements to digital asset transactions will not yield the information the government seeks and will only serve to unduly burden innovation and slow progress.

Similarly, requiring know-your-customer ("KYC") verification by VASPs of third-party self-hosted wallets with whom VASPs have no contractual relationship could be equally detrimental to the U.S. digital asset community. Contrary to a common depiction of self-hosted wallets as inherently suspicious, these wallets simply

---

[13] In December 2020, FinCEN proposed "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets." The proposal would impose a reporting requirement for certain digital asset transactions deemed to be a "virtual currency analogue to the [current] CTR reporting requirement under existing regulations implementing the BSA. *See* 31 C.F.R. § 1010.311. The rulemaking appeared in the recent Spring 2022 Unified Agenda, with an expected "Final Action" in March of 2023. https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202204&RIN=1506-AB47

enable individuals to participate in financial activity without relying on traditional, legacy financial institutions. It would be very difficult and expensive, if not technologically impossible in some circumstances, for otherwise compliant and well-intentioned VASPs to effectively KYC all self-hosted wallets they may interact with, leaving VASPs with no choice but to either de-risk self-hosted wallets or to exit the U.S. market.

As a result, attempts by the USG to regulate the digital assets industry in the same manner as the traditional financial sector could lead to the unintentional fracturing of the digital asset ecosystem into two markets. One market would likely be dominated by existing financial institutions that are compliant but may be reluctant to transact with entities they consider to be "higher risk," such as DeFi platforms, self-hosted wallets, and underserved and unbanked individuals. The other market would be comprised of all other entities in the ecosystem—even otherwise legitimate businesses—that may be driven offshore or underground to survive.

b. A fractured digital assets market can undermine the USG's enforcement efforts and have other detrimental effects.

A fractured digital assets market will deny the USG and the broader financial system the benefits of the innovative products and extensive insights ousted industry players could have provided had they been able to continue operating in the U.S. Also, entities driven underground would pose a greater threat to the U.S. financial system and would be more likely to facilitate illicit activity.

Such a division of the digital asset ecosystem will have other potentially unintended consequences, including:

- Impeding law enforcement by driving innovative products or providers like DeFi, NFTs, certain VASPs, and certain wallet providers offshore beyond the reach and collaboration of U.S. law enforcement;

- Creating substantial privacy and security issues, for instance, by requiring consumers to turn over sensitive personal data to numerous businesses;

- Further excluding underserved and unbanked persons, particularly those in developing countries, from the global financial system; and

- Stifling innovation in new technologies that may allow for KYC-like controls while protecting privacy.

c. Before imposing new regulations, the USG should work with the digital asset industry to leverage innovative technologies to address illicit finance risks.

We recommend that Treasury and the USG work more proactively with private industry to explore innovative approaches that could enable companies to comply with existing regulations. Such innovations can include digital identification tokens, zero-knowledge proof credentials, and sophisticated forms of encryption that may allow for KYC while also protecting privacy. Zero-knowledge proof credentials show particular promise. These credentials can allow a customer to confirm, through an individualized token or other unique digital marker, that they are who they say they are without revealing their specific identity. As more companies continue to create decentralized identities, this can be an innovative approach to consider. By allowing further development of these technologies, such as through the use of regulatory sandboxes and exceptive relief, they could incorporate non-traditional forms of identifying information that could both protect privacy interests and facilitate access to not only digital asset services but also the traditional financial system.

There is a pressing need for the USG to work with the private sector to achieve privacy and compliance solutions extending beyond the mere imposition of new KYC requirements. As we discussed in our August 2022 Letter, many U.S. adults who are underbanked or unbanked represent communities that have historically been victim to discriminatory or exclusionary financial practices. This history of discrimination and exclusion has led many to distrust legacy financial institutions. As an alternative, many underbanked and unbanked people have turned to services like check-cashing services and payday loans, services that are more likely to be associated with fraud and predatory practices.[14] The over-regulation or mis-regulation of the digital asset industry could lead to the same mistrust of the new innovative products and solutions that the digital asset industry has to offer, suffocating the ecosystem before it has the opportunity to reach and benefit underbanked or unbanked individuals. Through collaboration, the USG and industry can develop mechanisms to realize the full benefits of digital assets to benefit underbanked people at home and those fighting tyranny and oppression abroad.

V. Recommendations

For your convenience, we have summarized our recommendations below, and keyed each recommendation to one or more questions in the Request.

---

[14] https://consumer.ftc.gov/consumer-alerts/2020/05/paying-and-paying-and-paying-payday-loans

a. The USG should collaborate with the private sector to establish and foster open communication to find effective solutions to the challenges posed by illicit finance. *Questions C.1., D. 2., D.5. , and D.6.*

b. Prioritize financial literacy for private sector businesses and consumers to ensure that they understand the risks associated with illicit finance and are able to make informed decisions. *Question D. 2.*

c. Allow for experimentation through exceptive relief and regulatory sandboxes, which can facilitate the development of crypto-native tools that leverage blockchain technology and transparency to create a compliant ecosystem that effectively combats illicit finance. *Questions D. 2., D.3., D.5., and D. 7.*

d. Establish industry-hosted and other bidirectional information sharing programs to expand the USG's understanding of the digital asset ecosystem. *Questions D. 1., D.2., and D.6.*

e. Establish a FinCEN-hosted 24/7 rapid-response communications network to monitor for and share intelligence on illicit finance risks. *Questions D. 1. and D.6.*

f. Strategically leverage authorities under Sections 314(a) and 314(b) of the USA PATRIOT Act to deepen engagement with the digital asset industry. *Questions D. 1. and D.6.*

g. Create international digital asset coordination centers to combat illicit finance in the digital asset space and promote and understand innovation. *Questions C.1. and D. 1.*

h. Before imposing new regulations, the USG should work with the digital asset industry to leverage innovative technologies to address illicit finance risks. *Questions B.1., C.1., and D.1.*

VI. Conclusion

We thank Treasury for the opportunity to weigh in on these critical issues. We believe the Request, and this response, is part of the larger dialogue between public and private institutions we seek. Ultimately, the President's goals articulated in the Executive Order can be best achieved through sensible regulation and responsible innovation. As we respectfully submitted in the August 2022 Letter, legislators and regulators should focus on common sense, pro-business policies to support private

sector activity and thereby secure America's leadership in the emerging digital global financial system, promoting responsible innovation, economic growth, safety, inclusion and equity, and economic and national security. By continuing to work together and learn from each other, we believe that we can and will continue to innovate in the digital asset ecosystem to find solutions that will make the financial system more secure, innovative, inclusive, and safer for all Americans.

Respectfully submitted,

Sheila Warren
Chief Executive Officer
Crypto Council for Innovation

Exhibits:

A. August 2022 Letter

B. February 2022 Letter

Crypto
Council for
Innovation

BY U.S. MAIL AND ELECTRONIC SUBMISSION

Himamauli Das
Acting Director, Financial Crimes Enforcement Network
Policy Division
P.O. Box 39
Vienna, VA 22183

February 13, 2022

RE: FinCEN Docket No. FINCEN-2021-0008, Response to FinCEN's Request for Information on the Modernization of U.S. AML/CFT Regulatory Regime

Dear Acting Director Das,

The Crypto Council for Innovation ("CCI") appreciates the opportunity to comment on the Financial Crimes Enforcement Network's ("FinCEN") request for information ("RFI") regarding ways to "streamline, modernize, and update the anti-money laundering and countering the financing of terrorism ("AML/CFT") regime of the United States,"[1] specifically with respect to the Bank Secrecy Act and its implementing regulations (collectively, the "BSA").[2]

CCI is an alliance of crypto industry leaders with a mission to communicate the benefits of crypto and demonstrate its transformational promise. CCI members include some of the leading global companies and investors operating in the cryptocurrency industry, including Andreesen Horowitz, Block (formerly Square), Coinbase, Fidelity Digital Assets, Paradigm, and Ribbit Capital. CCI members span the crypto ecosystem and share the goal of encouraging the responsible global regulation of crypto to unlock economic potential, improve lives, foster financial inclusion, protect national security, and disrupt illicit activity. CCI and its members stand ready and willing to work with FinCEN and other government agencies to accomplish these goals to ensure that the most transformative innovations of this generation and the next are anchored in the United States.

I. Introduction and Overview

CCI welcomes FinCEN's interest in modernizing AML/CFT regulation and strongly believes that the technological revolution of the last decade has made the current moment a unique opportunity to reexamine how the United States counters the threat of financial crime and to explore new ways to deploy technology to address emerging threats. Specifically, as

---

[1] Press Release, FinCEN, *FinCEN Seeks Comments on Modernization of U.S. AML/CFT Regulatory Regime* (Dec. 14, 2021), https://www.fincen.gov/news/news-releases/fincen-seeks-comments-modernization-us-amlcft-regulatory-regime; Review of Bank Secrecy Act Regulations and Guidance, 86 Fed. Reg. 71,201 (Dec. 15, 2021), https://www.govinfo.gov/content/pkg/FR-2021-12-15/pdf/2021-27081.pdf.

[2] The BSA is codified at 31 U.S.C. § 5311 *et seq.*, and the BSA implementing regulations are codified at 31 C.F.R. § 1010, *et seq.*

FinCEN embarks on the process of modernizing the BSA, it should consider how to harness the innovation that blockchain and other new technologies facilitate to accomplish the objectives of the BSA in novel ways that make law enforcement investigations more efficient while also better protecting individuals' security and privacy.

We commend FinCEN for embracing innovative approaches to financial crime compliance in a number of ways over the last several years. Embracing innovative approaches will undoubtedly lead to the provision of more, and better, financial products and services to a greater number of people, and, in turn, to broader financial inclusion and economic empowerment. By encouraging novel approaches to regulation, instead of imposing duplicative reporting requirements that focus on collecting sensitive personal data,[3] FinCEN can better protect privacy, make law enforcement efforts more effective, and ensure that the United States is not left out of the next generation of innovation in financial services.

Two areas offer particularly fertile ground for reevaluating the traditional approaches to AML/CFT activity: (i) how government and the private sector can identify and mitigate financial crime risk while bringing more people into the financial system; and (ii) the ways in which financial institutions verify customer identities.

Threat Identification. From the adoption of the BSA in 1970, the U.S. AML/CFT framework was grounded in the recognition that the private sector has important perspectives on, and an important role to play in identifying, illicit finance risks. The statute therefore imposed recordkeeping and reporting requirements that would facilitate the provision of information from financial institutions to the government under specified circumstances. Indeed, the main objective of the BSA was to require banks "to maintain prudent practices with respect to identification of their customers, reporting of unusual cash transactions, and general recordkeeping,"[4] in order to provide information that is "highly useful" to "criminal, tax, or regulatory investigations" or to "intelligence or counterintelligence activities."[5] With respect to blockchain-based transactions, however, much of this data is *already* publicly available. Thus, a new paradigm of compliance should focus on creating mechanisms for the public and private sectors to leverage technology to *utilize* this publicly available information – rather than requiring duplicative, burdensome reporting.

While a paradigm of threat identification grounded in financial institution recordkeeping and reporting requirements is important, in an era where cryptocurrency transactions take place over public ledgers, there are more effective ways for the public and private sectors to identify and mitigate risk. Specifically, instead of a model of threat identification focused solely on investigating individuals and groups through subpoenas or other requests for specific records held by financial institutions (much of which may already be publicly available on the blockchain), the threat identification paradigm in blockchain-based environments should focus

---

[3] *See* Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 86 Fed. Reg. 3,897 (proposed Jan. 15, 2021), https://www.govinfo.gov/content/pkg/FR-2021-01-15/pdf/2021-01016.pdf.

[4] 115 Cong. Rec. 36,769, 36,770 (Dec. 3, 1969) (statement of Rep. Patman).

[5] 31 U.S.C. § 5311(1).

on the identification of typologies, tactics, and techniques of financial crime based on blockchain data. These efforts can leverage the comparative advantages of the private sector in blockchain and data analytics, and the government's comparative advantages in threat-related intelligence, to develop typologies and risk indicators that can be broadly disseminated throughout the industry to enhance threat identification and suspicious activity reporting, particularly by smaller financial institutions in the blockchain ecosystem.

Identity Management. Similarly, the Treasury Department came, over time, to impose requirements under the BSA for financial institutions to verify the identities of their customers.[6] These requirements mandate that every financial institution at which a customer opens an account collect and verify the same information previously collected and verified by every other financial institution at which the customer holds an account, causing costly duplication of effort. New technologies and methodologies for verifying and managing identity can make this process more effective and more efficient, opening the financial services industry to a broader range of actors that can deliver services to new individuals and communities, including those historically excluded from the financial sector because established institutions have not been able or willing to serve them. These new methods could potentially protect customer information more effectively and provide ways to verify identity for those who may lack access to traditional government issued IDs (or whose information is not available in the commercial databases typically used to verify identity). They could also reduce the amount of personal information potentially vulnerable to release in the event of a breach, thus protecting privacy and security. FinCEN and the federal banking regulators have begun the process of encouraging financial institutions to embrace innovation in identity management,[7] but work should continue to encourage accelerated innovation in this space.

---

[6] *See* Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks, 68 Fed. Reg. 25,090 (May 9, 2003), https://www.govinfo.gov/content/pkg/FR-2003-05-09/pdf/03-11019.pdf, and Customer Identification Programs for Broker-Dealers, 68 Fed. Reg. 25,113 (May, 9, 2003), https://www.govinfo.gov/content/pkg/FR-2003-05-09/pdf/03-11017.pdf (requiring banks and broker-dealers, respectively, to implement reasonable procedures to verify the identity of any person seeking to open an account, maintain records of the information used to verify the person's identity, and determine whether the person appears on any lists of known or suspected terrorists or terrorist organizations).

[7] *See, e.g.*, Board of Governors of the Federal Reserve System ("FRB"), Federal Deposit Insurance Corporation ("FDIC"), FinCEN, National Credit Union Administration("NCUA"), and Office of the Comptroller of the Currency ("OCC"), Interagency Statement on Sharing Bank Secrecy Act Resources (Oct. 3, 2018), https://www.fincen.gov/sites/default/files/2018-10/Interagency%20Statement%20on%20Sharing%20BSA%20Resources%20-%20%28Final%2010-3-18%29%20%28003%29.pdf; FRB, FDIC, FinCEN, NCUA, OCC, Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing (Dec. 3, 2018), https://www.fincen.gov/sites/default/files/2018-12/Joint Statement on Innovation Statement (Final 11-30-18)_508.pdf; Press Release, FinCEN, *FinCEN to Host Innovation Hours Program Workshop on Digital Identity Services and Technologies* (Aug. 31, 2021), https://www.fincen.gov/news/news-releases/fincen-host-innovation-hours-program-workshop-digital-identity-services-and#:~:text=WASHINGTON%E2%80%94The%20Financial%20Crimes%20Enforcement,that%20undermine%20the%20integrity%20and; Press Release, FinCEN, *FDIC and FinCEN Launch Digital Identity Tech Sprint* (Jan. 11, 2022), https://www.fincen.gov/news/news-releases/fdic-and-fincen-launch-digital-identity-tech-sprint.

A. *Technology and the Current Moment*

It is particularly important for FinCEN, and the broader U.S. regulatory community, to take up this work now because we sit today at the convergence of two significant developments.

First, cryptocurrencies, and blockchain-based technology more broadly, are disrupting a wide and expanding range of economic activity. Born in the aftermath of the financial crisis, cryptocurrencies and the blockchain represent the simple but powerful idea that individuals should be able to store value and engage in economic exchange without having to use only centralized institutions to execute transactions. Because blockchain-based transactions are recorded on public ledgers, the paradigm of recordkeeping and reporting established by the BSA can be supplemented by enhanced analysis of publicly available blockchain transactional data to identify and curtail illicit activity. These approaches could complement the identity verification measures already taken by banks and other exchanges at the on and off ramps that bridge the cryptocurrency and fiat currency worlds. Compliance capabilities have also benefited from significant technological advancements in recent years. In particular, the rise of data analytics and artificial intelligence (along with related applications like machine learning and natural language processing) has improved general AML compliance potential.[8]

Second, similar technological developments can be used to manage and verify identities more securely, obviating the need to create large repositories of personally identifiable information ("PII") at financial institutions that can be hacked or misused, empowering customers, and increasing the efficiency and effectiveness of identity verification throughout the financial sector.

The economic impact of meeting this technological moment will be significant. By the end of 2022, the number of crypto users is expected to break one billion for the first time,[9] and the rise of cryptocurrency is poised to improve the lives of underprivileged communities. The World Bank reports that close to one-third of adults, 1.7 billion people, remain unbanked,[10] and cryptocurrency has already demonstrated the potential to change this landscape for the better. Crypto's lower barriers to entry and "low cost, nearly instantaneous, borderless, peer-to-peer transfers of actual value,"[11] creates an unparalleled opportunity to bolster financial inclusion by helping underserved communities worldwide access the financial system.

---

[8] *See* Financial Action Task Force (FATF), Opportunities and Challenges of New Technologies for AML/CFT (July 2021), https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.

[9] *Global Crypto Owners Near 300 Million, Predicted to Hit 1 Billion by the End of 2022*, Crypto.com (Jan. 19, 2022), https://blog.crypto.com/global-crypto-owners-near-300-million-predicted-to-hit-1-billion-by-the-end-of-2022.

[10] *See* World Bank, Financial Inclusion, Overview, https://www.worldbank.org/en/topic/financialinclusion/overview#1 (last visited Feb. 10, 2022).

[11] Andreesen Horowitz, The web3 Landscape at 10 (Oct. 2021), https://a16z.com/wp-content/uploads/2021/10/The-web3-Readlng-List.pdf.

Underbanked communities in the United States, particularly those comprising minority populations, have shown a particular interest in crypto,[12] a trend recently recognized by the Acting Comptroller of the Currency, Michael Hsu. When describing crypto's appeal to these communities, Hsu noted the fact that "37 percent of the underbanked indicated they own cryptocurrency, compared to 10 percent of the fully banked."[13] Several members of Congress have also recently remarked on cryptocurrency's ability to bring traditionally underbanked individuals into the financial system.[14] For many of these underbanked and minority communities, the traditional financial system has generally not been tailored to their financial needs.[15] In comparison, cryptocurrency, with its decentralized infrastructure and ease of access, provides a much-needed alternative for these individuals to take control of their financial present – and future.[16] Crypto therefore has the potential to democratize finance and expand access and ownership opportunities for these individuals and communities.

While the United States has been at the forefront of many of these developments, the current uncertain regulatory climate that developers face in the U.S. is poised to drive overseas

---

[12] *See e.g.*, Silvia Foster-Frau, *Locked Out of Traditional Financial Industry, More People of Color Are Turning to Cryptocurrency*, Wash. Post (Dec. 1, 2021), https://www.washingtonpost.com/national/locked-out-of-traditional-financial-industry-more-people-of-color-are-turning-to-cryptocurrency/2021/12/01/a21df3fa-37fe-11ec-9bc4-86107e7b0ab1_story.html; Kori Hale, *Why Black Investors Seemingly Prefer Cryptocurrencies Over Traditional Stocks*, Forbes (Aug. 10, 2021), https://www.forbes.com/sites/korihale/2021/08/10/why-black-investors-seemingly-prefer-cryptocurrencies-over-traditional-stocks/?sh=16d66c906839.

[13] Michael J. Hsu, Acting Comptroller, OCC, *Remarks Before the BritishAmerican Business Transatlantic Finance Forum Executive Roundtable: "The Future of Crypto-Assets and Regulation"* (Jan. 13, 2022), https://www.occ.treas.gov/news-issuances/speeches/2022/pub-speech-2022-2.pdf.

[14] *See e.g.,* Sam Sutton, *Four Takeaways From the House Stablecoin Hearing*, PoliticoPro (Feb. 8, 2022) ("Several Republicans and some Democrats urged caution against cracking down on privately backed digital tokens that have become a resource for underbanked communities. New York Democratic Reps. Ritchie Torres and Gregory Meeks noted that Black and Hispanic communities have moved more quickly to embrace crypto and decentralized finance platforms as a form of financial services."); Kollen Post, *What We Learned at Congress' Much-Anticipated Summit of Crypto Execs,* The Block (Dec. 8, 2021), https://www.theblockcrypto.com/post/126866/what-we-learned-at-congress-much-anticipated-summit-of-crypto-execs ("[S]everal Democrats who entered the committee this year seemed more interested in crypto's potential positive impacts. Rep. Ritchie Torres asked the witnesses how stablecoins could help the large immigrant population in his district in the South Bronx facilitate cheaper remittances.").

[15] Samuel Haig, *Minority Communities Are Investing in Crypto to Escape Financial Discrimination*, Cointelegraph (Aug. 17, 2021), https://cointelegraph.com/news/minority-communities-are-investing-in-crypto-to-escape-financial-discrimination.

[16] Cryptocurrency also has the potential to reduce the cost of remittances, especially low-value remittances, the average cost of which the World Bank has pegged at 6.3%. *See* World Bank, Remittance Prices Worldwide, Quarterly, Issue 39, at 5 (Sept. 2021), https://remittanceprices.worldbank.org/sites/default/files/rpw_main_report_and_annex_q321.pdf. Technologies such as Celo, which offers a consumer-facing mobile application that integrates with a native stablecoin platform, enables remittances to be confirmed in seconds and securely transferred, allowing for faster, cheaper, and more energy efficient cross-border transactions. *See* Evan Kereiakes, *Rethinking Remittances with Blockchain Technology and Celo*, Celo Blog (May 28, 2020), https://medium.com/celoorg/rethinking-remittances-with-blockchain-technology-720c978084d4.

the next generation of blockchain-based applications. Indeed, because of the inherently global nature of blockchain technology, this risk is particularly acute in the cryptocurrency context. Regulation that is not sensitive to the unique dynamics of cryptocurrency, combined with the "de-risking" of U.S. financial institutions in developing regions, can also have a significant impact on U.S. national security as U.S. companies become less predominant in the cryptocurrency space.[17]

Specifically, as described in this letter, productive relationships between crypto financial institutions and law enforcement agencies are critical to mitigating financial crime risk, but those relationships, and the exchanges of information they facilitate, may be put at risk if crypto financial institutions move offshore. This is because crypto financial institutions are required to collect information about their customers both at onboarding and throughout the lifecycle of the customer relationship. Law enforcement agencies can combine this information, obtained with subpoenas or other forms of lawful process, with information obtained from the blockchain to identify specific perpetrators of illicit activity. To the extent crypto financial institutions move overseas, the ability of U.S. law enforcement agencies to obtain expediently the pieces of the puzzle that cannot be obtained from public blockchains will likely be reduced commensurately, to the detriment of the U.S. law enforcement and national security communities. Just as the U.S. benefits from the fact that large global telecommunications, Internet, and social media companies are headquartered here, U.S. law enforcement—and thus the American people—will lose out if cryptocurrency financial institutions leave the United States or are never established here in the first place.

The absence of U.S. firms from the cryptocurrency payments space can also leave voids that could be filled by other payments technologies, like China's Digital Yuan project, which has the potential to fundamentally reshape the global payments ecosystem in a way that will undoubtedly be detrimental to U.S. interests.

In the face of global competition, U.S. regulators have an opportunity to counteract these trends, and help realize the promise of crypto. While the economic benefits of keeping cryptocurrency companies in the United States are obvious, it is also a tremendous advantage to U.S. national security and law enforcement to ensure that the cutting edge of innovation remains in this country.

B. *The AMLA, Public-Private Partnerships, and Identity Management*

Congress recognized the potential for technology to transform the U.S. AML/CFT regime in the Anti-Money Laundering Act of 2020 ("AMLA").[18] Title LXII of the AMLA in particular focuses on modernizing the AML/CFT system—the topic of this RFI—and contains several sections relating to leveraging technology and innovation to improve the effectiveness and

[17] ClearingHouse, A New Paradigm: Redesigning the U.S. AML/CFT Framework to Protect National Security and Aid Law Enforcement (Feb. 2017), https://bpi.com/wp-content/uploads/2018/07/20170216_tch_report_aml_cft_framework_redesign.pdf.

[18] The AMLA is contained in Div. F of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, Div. F, 134 Stat. 3388, 4547 (2021).

efficiency of the current AML/CFT framework.[19] We encourage FinCEN to capitalize on this pivotal moment and reimagine how to conduct core BSA activities consistent with the spirit of the statute and the possibilities that now exist.

In Part II of this comment letter, we focus on how FinCEN and the private sector can develop novel mechanisms of threat identification, which go beyond recordkeeping and reporting requirements, and leverage public and private resources to develop typologies and risk indicators of financial crime that can be disseminated throughout the industry. In Part III, we explain why FinCEN should encourage the adoption of novel approaches to identity management. Collectively, these approaches can reduce financial crime risk while better protecting customer privacy.

In the half-century since the adoption of the BSA, the U.S. AML/CFT regime has evolved to adapt to changing threats and changing opportunities. By leveraging technology to improve threat identification, and adopting novel approaches to identity management, the U.S. can set the tone for how governments and transnational bodies manage financial crime risk globally for the next generation.

II. FinCEN Should Foster Innovative Frameworks to Identify and Mitigate Financial Crime Risk Related to Blockchain-Based Transactions.

The original intent of the BSA of 1970 was to mitigate money laundering risk by instituting a set of preventative measures that put financial institutions on the front lines of the fight against financial crime. At the outset of the statutory regime, the BSA centered on ensuring banks maintained the requisite records to provide information that is "highly useful" to government investigations and that banks submitted reports on otherwise-ephemeral cash transactions. The BSA has since been refreshed periodically to address new threats through new mechanisms of a regime fundamentally grounded in recordkeeping and reporting; examples include formal Suspicious Activity Report ("SAR") requirements and, after 9/11, Sections 314(a) and 314(b) of the USA PATRIOT Act.

The explosive growth of cryptocurrencies marks another inflection point and can facilitate a new, and improved, mechanism to identify and mitigate financial crime risk. Specifically, because blockchains are generally public and reveal transaction histories, it is possible to analyze those transactional records to identify typologies of high-risk behavior, specific high-risk addresses, risk indicators, and the tactics and techniques that illicit actors use

[19] *See e.g.,* AMLA, § 6207 (adding a Subcommittee on Innovation and Technology to the BSAAG to advise FinCEN and other federal and state regulators on how to most effectively encourage and support technological innovation in the area of AML/CFT and reduce any obstacles to innovation that may arise from existing regulations); *id.* § 6208 (establishing Bank Secrecy Act Innovation Officers to advise public and private sector stakeholders on innovative methods, processes, and new technologies that may assist with AML/CFT compliance and provide technical assistance and guidance regarding their implementation); *id.* § 6209 (requiring standards by which financial institutions must test the new technologies); *id.* § 6210 (requiring FinCEN to conduct an analysis of the impact of the new technologies on financial crimes compliance); *id.* § 6211 (establishing a global financial crimes tech symposium focused on how the new technologies can be used to more effectively combat financial crimes and other illicit activities).

to launder ill-gotten funds (like the ways in which ransomware actors "hop" among multiple blockchains to attempt to hide the proceeds of their criminal activity)[20] on the basis of publicly available information,[21] while mitigating impacts on privacy.

Private sector actors are generally well-positioned to leverage their expertise in blockchain analytics to identify this activity and can combine it with specific intelligence from government agencies about threats to ensure the work is maximally impactful. Working together, government and the private sector can develop typologies of illicit activity that can be shared among a broad range of participants in the blockchain ecosystem to ensure that even smaller financial institutions can have up-to-date information to identify and prevent emerging illicit threats. And, importantly, because this kind of preventive risk management is less dependent on recordkeeping and reporting, it poses fewer privacy challenges. SARs remain a vital law enforcement tool, and we envision a regime to complement and support SARs by sharing threat typologies and risk indicators widely across members of the blockchain industry subject to the BSA to help ensure those SARs are impactful by permitting financial institutions to situate the activity they are seeing in the context of broader threats.

The power of blockchain data to provide information about transactions is especially noteworthy when viewed in light of recent proposals to expand the scope of suspicionless reports like Currency Transaction Reports ("CTRs") to require reporting of certain transactions between cryptocurrency exchanges and self-hosted wallets.[22] Traditional CTRs may have been appropriate when they related exclusively to cash transactions, information about which would have been lost if not captured contemporaneously. But, as described in this letter, much of the information about transaction histories that would have been required by recent proposals to expand CTR requirements, such as the date and time, amount, source and destination wallet address of transactions, and transaction hash, is *already* available on blockchains.[23] This

---

[20] This practice is often referred to as "chain hopping"—a practice often used by illicit actors to obfuscate the origin of their funds by converting one cryptocurrency into a different cryptocurrency at least once before moving the funds to another service or platform. *See* FinCEN, Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021 (Oct. 2021), https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf.

[21] For example, the Statement of Facts released in connection with the two arrests made for an alleged conspiracy to launder cryptocurrency stolen during the Bitfinex hack in 2016 includes a number of statements about the government's reliance on public blockchain data to identify the alleged perpetrators. U.S. Dep't of Justice, Statement of Facts at 2 & n.7 (Feb. 7, 2022), https://www.justice.gov/opa/press-release/file/1470211/download ("U.S. authorities traced the stolen funds on the BTC blockchain," which is "a public transaction ledger that includes a record of every BTC transaction that has ever occurred").

[22] Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 85 Fed. Reg. 83,840 (proposed Dec. 23, 2020) ("NPRM"), https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28437.pdf; *see also* 86 Fed. Reg. 3,897 (Jan. 15, 2021) (reopening comment period) ("January NPRM"), https://www.govinfo.gov/content/pkg/FR-2021-01-15/pdf/2021-01016.pdf; 86 Fed. Reg. 7,352 (Jan. 28, 2021) (extending comment period), https://www.govinfo.gov/content/pkg/FR-2021-01-28/pdf/2021-01918.pdf.

[23] *See* Coinbase Comment, Dkt. No. FINCEN-2020-0020 (Mar. 25, 2021), https://www.regulations.gov/comment/FINCEN-2020-0020-8248.

reality means proposals to report this data to FinCEN are duplicative and unnecessary, while at the same time posing serious privacy and security risks to consumers.

To the extent recent proposals related to CTRs requested information not directly available on blockchains, like the "name and physical address of each counterparty to the transaction of the financial institution's customer,"[24] FinCEN's proposal to collect and retain that data in large government repositories, as opposed to simply mandating that financial institutions retain those records internally, poses serious privacy and security concerns. Such concerns are especially sharp with respect to CTR requirements that would link a person's PII with their blockchain addresses, which, if accessed without authorization, could reveal their entire blockchain transaction history. That proposal also used the same $10,000 threshold for cryptocurrency CTRs without fully considering the differences between cryptocurrency and cash transactions. This makes particularly clear that simply grafting traditional recordkeeping and reporting requirements onto the blockchain is at best inappropriate – an unlawfully obtained fiat currency CTR is unlikely to reveal a customer's entire financial history, but an unlawfully leaked crypto CTR linking a person's real identity with his or her blockchain address could have significant privacy and security consequences.

In light of these concerns, FinCEN and the rest of the U.S. regulatory community should prioritize the development of systems to identify illicit financial activity that leverage the unique properties of publicly available blockchain data, instead of expanding existing reporting requirements in a manner that poses significant privacy and security concerns without commensurate benefits. Doing so will not only give law enforcement agencies better tools but will also free up compliance resources at cryptocurrency exchanges to focus on important value-added activities, like SAR investigations, and is consistent with a "risk-based approach to AML/CFT regulation" that will mark a departure from the status quo.[25]

A. *The Foundations of the Modern Recordkeeping and Reporting System*

A core insight of the BSA is that the private sector has an inherent comparative advantage in recognizing certain forms of suspicious activity. The modern AML system, where financial institutions must report certain categories of transactions through CTRs and SARs, in particular, is rooted in the idea that "the creation of a meaningful system for detection and prevention of money laundering is impossible without the cooperation of financial institutions,"[26]

---

[24] January NPRM, 86 Fed. Reg. at 3,899.

[25] Himamauli Das, Acting Director, FinCEN, *Prepared Remarks of FinCEN Acting Director Him Das, Delivered Virtually at the American Bankers Association/American Bar Association Financial Crimes Enforcement Conference* (Jan. 13, 2022), https://www.fincen.gov/news/speeches/prepared-remarks-fincen-acting-director-him-das-delivered-virtually-american-bankers.

[26] *See* FinCEN; Proposed Amendment to the Bank Secrecy Act Regulations—Requirement of Money Transmitters and Money Order and Traveler's Check Issuers, Sellers, and Redeemers to Report Suspicious Transactions, 62 Fed. Reg. 27,900, 27,901 (proposed May 21, 1997) (finalized on Mar. 2, 2000), https://www.govinfo.gov/content/pkg/FR-1997-05-21/pdf/97-13303.pdf (proposing to amend the BSA regulations to require money transmitters, and issuers and sellers of money orders to report suspicious transactions to further the "creation of a comprehensive system . . . for the reporting of suspicious transactions," *id.* at 27,900).

because "it is representatives of financial institutions, rather than law enforcement, who see the money launderers first."[27] Moreover, "because money laundering transactions are designed to appear legitimate in order to avoid detection,"[28] bank "officials . . . are more likely than government officials to have a sense as to which transactions appear to lack commercial justification or otherwise cannot be explained as falling within the usual methods of legitimate commerce."[29]

Because the government understood that financial institutions were often better positioned than official agencies to identify suspicious transactions, it followed that financial institutions should be required to retain records about those transactions and to report them to the government. The specific regulatory requirements that implement this core idea and govern the private sector's role have evolved over time.

1. *BSA Recordkeeping and Reporting Requirements*

In 1970, the BSA imposed recordkeeping requirements and required the filing of reports for certain types of transactions. The statute noted that records of the identities of accountholders,[30] and of cash transactions,[31] which were by nature ephemeral, were of particular value because "[r]eports of domestic currency transactions will be quite helpful in limiting the use of secret foreign financial facilities for illegal purposes. These reports will also facilitate domestic law enforcement transactions . . . If certain cash transactions are required to be reported to the Treasury Department, law enforcement agencies, particularly in the income tax field, will have a useful tool in their investigations and proceedings. "[32]

2. *Suspicious Activity Reports*

In 1992, the Annunzio-Wylie Anti-Money Laundering Act granted the Treasury broad authority to require financial institutions to report suspicious transactions.[33] Pursuant to this authority, a "single integrated system" was created that reflected, among other things, the "mutual desire" of Treasury and financial regulators to "simplify and reduce the burdensomeness of the reporting process," while "increas[ing] the effectiveness of counter-

---

[27] FinCEN, Advisory, *Court Interprets "Safe Harbor" Provisions*, (Aug. 1, 1996), https://www.fincen.gov/resources/advisories/fincen-advisory-issue-5.

[28] 62 Fed. Reg. at 27,901; *see also* Proposed Amendment to the Bank Secrecy Act Regulations—Requirement to Report Suspicious Transactions, 60 Fed. Reg. 46,556, 46,558 (proposed Sept. 7, 1995), https://www.govinfo.gov/content/pkg/FR-1995-09-07/pdf/95-22223.pdf.

[29] 62 Fed. Reg. at 27,901.

[30] Currency and Foreign Transactions Reporting Act, Pub. L. No. 91-508, § 101, 84 Stat. 1114, 1114-15 (1970).

[31] Currency and Foreign Transactions Reporting Act, § 221.

[32] 116 Cong. Rec. 16,949, 16,954 (May 25, 1970) (remarks of Rep. Patman).

[33] Annunzio-Wylie Anti-Money Laundering Act, Pub. L. No. 102-550, tit. XV, § 1517(b), 106 Stat. 3672, 4059-60 (1992).

money laundering efforts."[34] Over time, FinCEN expanded SAR requirements to other types of financial institutions, including, among others, money services businesses ("MSBs").[35]

3. *Information Sharing under 314(a) and 314(b)*

In response to the 9/11 attacks, Congress adopted the USA PATRIOT Act, aimed at combatting terrorism more effectively. Sections 314(a) and 314(b) of that statute inaugurated a new paradigm in information sharing to fight money laundering and terrorist financing. Each provision facilitates the flow of information among relevant participants in the financial ecosystem – between government and financial institutions under 314(a), and on a voluntary basis among financial institutions under 314(b).

Taken together, these components of the BSA—SAR and CTR reporting, along with 314(a) and 314(b)—establish a recordkeeping and reporting regime that originated in the context of fiat currency transactions. As noted above, however, the blockchain obviates the need for reporting on certain types of data, and as explained further below, it also opens new opportunities for government and the private sector to identify threats and risks in a way that is scalable and often immediate.

B. *The Blockchain Informational Advantage*

Certain types of reports, like high-value SARs, will always be important to the identification and mitigation of financial crime. But blockchain technology unlocks new potential forms of threat identification based on the same foundational idea that history demonstrates has always animated BSA information reporting processes: the private sector has unique insight about risks that are valuable and important to the government in combating criminal activity. In the blockchain era, it will remain the case that "[n]o system for the reporting of suspicious transactions can be effective unless information flows *from* as well as *to* the government."[36] But the ways in which public and private sector efforts leverage their comparative advantages to fight financial crime should be adapted to the unique advantages of blockchain technology.

The AML regime should therefore be augmented with structures to facilitate the identification of threat typologies and risk indicators, with an eye toward sharing them broadly to prevent financial crime. This approach would leverage the unique properties of the blockchain, on which all transactions are generally publicly available. And as cryptocurrency applications proliferate, an increasing portion of economic activity will likely take place on publicly observable blockchains. Just as in the past, where the government recognized that the private sector has the unique capacity to identify suspicious activity, hosted wallet providers and cryptocurrency exchanges, in partnership with others such as blockchain analytics firms, may today be better positioned than government to develop techniques to analyze activity on the blockchain, and to identify specific typologies of illicit activity. The government, by contrast, may have access to a broader range of information that can be used to confirm the identities of individual wallet-

[34] 60 Fed. Reg. at 46,558.

[35] *See* 31 C.F.R. § 1022.320.

[36] 60 Fed. Reg. at 46,559.

holders involved in potentially suspicious activity, and to inform an analysis of financial crime trends. Therefore, it is critical for the government to work in partnership with the private sector to establish the necessary "feedback loop[s]" for threat identification and mitigation that Acting Director Das has said is one of FinCEN's goals.[37]

There are a range of possibilities for the specific shape novel frameworks to identify and mitigate financial crime risk with respect to blockchain-based technologies could take, but below we describe key principles any such regime should embrace. A structure that leverages the strengths of the public and private sectors fueled by modern data analytics and the blockchain would be powerful and could complement existing mechanisms of information-sharing like 314(a), 314(b), and SARs, which are, by their nature, retrospective. The AMLA took an important step in the right direction by mandating the creation of a Subcommittee on Innovation and Technology in the Bank Secrecy Act Advisory Group ("BSAAG"),[38] tasked with encouraging and supporting technological innovation.[39] The statute also required the Secretary of the Treasury to convene a group of public and private sector experts "to examine strategies to increase cooperation between the public and private sectors for purposes of countering illicit finance," which can be leveraged for these purposes.[40]

C. *Threat Identification – Core Principles*

A framework for threat identification aimed at the specific challenge of identifying and mitigating financial crime risk in blockchain-based transactions should be constructed with reference to a set of core principles. These kinds of partnerships should: (i) focus on typology development and rapidly disseminate those typologies and threat indicators across the industry and to global Financial Intelligence Unit ("FIU") partners; (ii) harness the power of technology; and (iii) leverage the full range of available administrative structures.

Importantly, this kind of framework will make it easier for law enforcement agencies to engage in global investigations quickly—a significant improvement over investigative capabilities with respect to fiat currency transactions today. At present, law enforcement agencies must rely on legal processes like subpoenas to gain access to transactional records held at financial institutions. Collecting and analyzing these records takes time, even when the transactions occur domestically at financial institutions that have been identified. If transactions related to criminal activity took place through financial institutions abroad, obtaining the records through Mutual Legal Assistance Treaty ("MLAT") requests can take months or years, if they yield relevant records at all.

---

[37] Das, *supra* note 25.

[38] The BSAAG was established pursuant to Section 1654 of the Annunzio-Wylie Anti-Money Laundering Act of 1992, as a means by which the Treasury receives advice on the BSA. The Director of FinCEN serves as the chair of BSAAG and is responsible for ensuring that relevant issues are placed before the BSAAG for review, analysis, and discussion. Annunzio-Wylie Anti-Money Laundering Act, § 1564(a)-(b).

[39] AMLA, § 6207.

[40] AMLA, § 6211.

With cryptocurrency, the history of wallet addresses is available for law enforcement to analyze—and even to seize directly, as the Department of Justice recently did with the proceeds of the Bitfinex hack, unraveling "a labyrinth of cryptocurrency transactions" on the path to a significant prosecution.[41] The approach we propose in this letter also allows law enforcement to invert the typical investigative process, and start by identifying high-risk transactions on the blockchain (*e.g.*, a wallet that interacted with a known criminal network), and to work from there to identify the individuals involved in the activity. Law enforcement agencies do not need to wait for SARs to be filed to pursue bad actors. And during the course of ongoing investigations, law enforcement agents can use blockchain records to identify additional persons and entities with whom the subjects transacted, wherever in the world they may be, without waiting on MLAT requests that may or may not be granted.

These possibilities illustrate the power of devoting public and private sector resources to developing structures to fully utilize the potential of blockchain-based records, instead of imposing reporting requirements on cryptocurrency exchanges that cover records that are already available publicly.

Develop typologies that can be disseminated broadly. As noted above, core BSA structures were designed to require recordkeeping and reporting to support government investigations of individuals, entities, and networks. These requirements, especially as they relate to SARs, are and will remain important. But they should be supplemented with alternative structures that leverage unique properties of blockchains to reduce financial crime risk.

While in some circumstances these structures could be used to advance individual investigations—and, as noted above, to identify high-risk wallet addresses—these structures would be designed to create the tools to empower cryptocurrency financial institutions to more effectively identify indicators of specific types of financial crime risk. These may include typologies of criminal activity that would illustrate, for example, how bad actors use techniques like "chain-hopping" to obfuscate the links between specific crypto assets and unlawful activity.

These typologies and tools can broadly promulgate information to a wide range of actors in the crypto ecosystem so they can monitor for such activity on their networks. This approach would complement efforts to interdict the particular perpetrators of specific criminal acts and would help facilitate the development of a broad cohort of financial institutions equipped with the ability to identify and interdict illicit activity that interacts with their platforms. This approach would also permit smaller financial institutions to benefit from the work of these partnerships even if they lack the resources to participate directly. And focusing on typologies also has the salutary effect of buttressing consumer privacy because the focus would not be on collecting and reporting information about individual financial institution customers.

These kinds of partnerships can also allow rapid iteration of typology development as threats emerge, based on information that originates either with the government or with the private sector. They can also leverage FinCEN's power to connect with its global FIU partners

[41] Press Release, U.S. Dep't of Justice, *Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency* (Feb. 8, 2022), https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency.

to expand the exchange of financial intelligence that is relevant to the development of the kinds of impactful typologies discussed here.[42]

Harness the power of technology. This type of work is enabled by the nature of the blockchain—purposefully designed to create an immutable record of transactions—which allows for open-source traceability and accountability of each transaction, regardless of the identity or location of the participants. Records of fiat currency transactions have traditionally been siloed at financial institutions, but because the transactions that take place on the blockchain are public, new tools can be used to analyze those transactions on an aggregated basis to identify typologies and threats.

In the past decade, compliance technology also has developed rapidly, with quantum leaps made in areas such as data analytics, artificial intelligence, and machine learning, which can help to better identify risks and communicate, monitor, and address suspicious activity.[43] These technologies are evolving at a rapid pace. The ideal mechanism would therefore leverage the comparative advantages of public and private to marry the government's information about threats and bad actors with the private sector's expertise in analytics, and access to additional types of information about transactions and relationships.

Leverage a range of administrative frameworks. This effort will depend not only on new substantive approaches to financial crime threat mitigation, but also on new administrative structures for doing so. FinCEN has long had the authority to grant exceptive relief from its regulations,[44] and to provide administrative rulings on the implications of proposed activity under the BSA.[45] FinCEN has also recently published a report noting that it should embark on a rulemaking process to adopt a framework to grant no-action relief.[46] And several U.S. states have developed regulatory sandboxes to help facilitate the incubation of new ways to provide

---

[42] *See* FinCEN, The Egmont Group of Financial Intelligence Units, https://www.fincen.gov/resources/international/egmont-group-financial-intelligence-units (last visited Feb. 11, 2022) (describing the Egmont Group as an international networks of FIUs designed to "improve communication, information sharing, and training coordination amongst its FIU members" and which supports its FIU members by "helping them to expand and systematize the exchange of financial intelligence and information, improve expertise and capabilities of personnel, and enable secure communication with one another").

[43] FATF, Opportunities and Challenges of New Technologies for AML/CFT (July 2021), https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.

[44] 31 U.S.C. § 5318(a)(7); 31 C.F.R. § 1010.970(a).

[45] FinCEN has the authority to issue administrative rulings interpreting regulations promulgated under the BSA pursuant to 31 C.F.R. § 1010.710. For a list of published administrative rulings, *see* FinCEN, Administrative Rulings, https://www.fincen.gov/resources/statutes-regulations/administrative-rulings (last visited Feb. 11, 2022).

[46] FinCEN, Assessment of No-Action Letters in Accordance with Section 6305 of the Anti-Money Laundering Act of 2020 (June 28, 2021), https://www.fincen.gov/sites/default/files/shared/No-Action%20Letter%20Report%20to%20Congress%20per%20AMLA%20for%20ExecSec%20Clearance%20508.pdf.

financial services.[47] One can envision the use of these authorities to create novel structures that combine features of, for example, 314(a) and 314(b) to facilitate the development and dissemination of typologies and risk indicators.

D. *Examples of Public-Private Partnerships*

There are several extant frameworks that could serve as a model for what we propose, but FinCEN should leverage the structures described above, including the BSAAG and the consultation structure required by the AMLA, to consult with industry on how to establish these kinds of mechanisms.

NCFTA. The National Cyber-Forensics and Training Alliance ("NCFTA")—a Pittsburgh-based non-profit organization focused on identifying, mitigating, and neutralizing cybercrime threats globally—is one potential model for the type of public-private partnership we envision. NCFTA was initially established by the Federal Bureau of Investigation ("FBI") in 1997 and operates through strategic alliances and partnerships with subject matter experts in the public, private, and academic sectors.[48] NCFTA focuses on enabling "near real-time"[49] information sharing among members—some of which have staff permanently located at NCFTA—and fostering close collaboration among law enforcement, the private sector, and academia.

As the FBI describes it, the NCFTA essentially works as an early-warning system that leverages the power of real-time information sharing.[50] For example, a major banking institution that discovers a new kind of malware attacking its network can disseminate that information to other NCFTA members, which can then develop strategies to mitigate the threat. FBI agents and analysts from NCFTA can also use the information to open new or support existing investigations, often in concert with law enforcement partners globally. This model encourages not only information sharing between the government and the private sector, but also among private sector partners themselves.[51] Between 2015 and 2021, NCFTA produced 26,945

---

[47] Multiple states have launched a "regulatory sandbox" for innovative financial products or services, including Arizona, Nevada, Utah, Florida, West Virginia, Hawaii, and North Carolina. *See e.g.*, Ariz. Rev. Stat. Ann. §§ 41-5601 *et seq.*; S.B. 161, 2019 Leg., 80th Sess. (Nev. 2019) (pending statutes); Utah Code Ann. §§ 13-55-101 *et seq*; Fla. Stat. Ann. § 559.952; W. Va. Code Ann. §§ 31A-8G-1 *et seq.*; Press Release, Gov. David Y. Ige, *DCCA News Release: Hawaii Launches First Sandbox for Digital Currency* (Mar. 17, 2020), https://governor.hawaii.gov/newsroom/latest-news/dcca-news-release-hawaii-launches-first-sandbox-for-digital-currency; N.C. Gen. Stat. § 169-1 *et seq*.

[48] *The NCFTA: Combining Forces to Fight Cyber Crime*, FBI News (Sept. 16, 2011), https://www.fbi.gov/news/stories/the-ncfta-combining-forces-to-fight-cyber-crime.

[49] *See* NCFTA, About Us, https://www.ncfta.net/home-2/about-us (last visited Feb. 6, 2022).

[50] *The NCFTA: Combining Forces to Fight Cyber Crime*, FBI News (Sept. 16, 2011), https://www.fbi.gov/news/stories/the-ncfta-combining-forces-to-fight-cyber-crime.

[51] Christopher Wray, Dir., FBI, *The FBI and the Private Sector: Battling the Cyber Threat Together* (Jan. 28, 2021), https://www.fbi.gov/news/speeches/the-fbi-and-the-private-sector-battling-the-cyber-threat-together-012821.

intelligence reports and referred 4,184 cases to law enforcement, ultimately resulting in the prevention of $12.25 billion in financial losses.[52]

JMLIT. The United Kingdom's Joint Money Laundering Intelligence Taskforce ("JMLIT") is another innovative public-private partnership, established in 2015, that can serve as a reference for the type of public-private partnership we propose. JMLIT is a partnership between law enforcement and financial institutions to exchange information relating to money laundering and wider economic threats. JMLIT members include financial institutions, the Financial Conduct Authority (the United Kingdom's principal financial regulatory body), Cifas (a United Kingdom fraud prevention organization), and various law enforcement agencies.

A particularly strong feature of JMLIT is its mechanism for public-private information sharing, which is actively used by law enforcement agencies to enhance their access to financial intelligence, facilitate interagency cooperation, and enhance their understanding of the ever-evolving money laundering landscape. Through JMLIT, law enforcement agencies can obtain information from multiple sources and quickly develop a comprehensive intelligence picture.[53] While JMLIT access is only granted to certain financial institutions, it has developed alerts that are distributed to the wider industry and non-JMLIT banks have filed SARs based on information learned from these alerts.[54]

Through its Operations Group, JMLIT facilitates weekly meetings among law enforcement agencies and financial institution representatives, supporting more iterative/real-time interactions. Private sector members of JMLIT are also encouraged to refer cases to the Operations Group using an information sharing gateway which complements the mandatory obligations imposed by the SAR filing regime. Since 2015, JMLIT has supported more than 950 law enforcement investigations and contributed to more than 280 arrests and the seizures or restraints of more than £86 million. In particular, JMLIT's private sector members have identified more than 7,400 suspicious accounts and commenced more than 6,000 internal investigations.[55]

III. FinCEN Should Encourage Novel Approaches to Identity Management

Identity management is another area in which evolving technology can help accelerate changes to BSA processes. Traditionally, the core manifestation of the regulatory expectation that a financial institution must Know Your Customer ("KYC") was the Customer Identification Program ("CIP"). The policy rationale behind KYC and CIP is simple: financial institutions must know with whom they are dealing by obtaining and verifying customer information, including

---

[52] *See* NCFTA, Home, https://www.ncfta.net (last visited Feb. 6, 2022).

[53] FATF, *Mutual Evaluation Report for United Kingdom's Anti-money Laundering and Counter-terrorist Financing Measures* (Dec. 2018), https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf.

[54] *Id.*

[55] *See* National Crime Agency, NECC, Joint Money Laundering Intelligence Taskforce, https://www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre (last visited Feb. 11, 2022).

name, date of birth, address, and personal identification number (*e.g.*, taxpayer identification number),[56] to mitigate money laundering and terrorist financing risk.[57]

But, at present, and with some notable exceptions, financial institutions must each collect and verify this information independently on customers who establish accounts across multiple institutions. And they must do so using the same basic framework that has been in place since the advent of CIP requirements. Indeed, Congress has noted the need for "anti-money laundering, countering the financing of terrorism, and sanctions policies . . . that . . . do not unduly hinder or delay legitimate access to the international financial system for underserved individuals, entities, and geographic areas[.]"[58] The persistence of these challenges is particularly troubling given that technology has evolved significantly, and we have access to additional data and tools to verify identity efficiently and effectively.[59]

FinCEN should therefore help encourage novel approaches to identity management, including the use of blockchain technology, and the use of shared services and platforms, consistent with the forward-leaning, innovative solutions FinCEN and the FDIC are seeking to foster in their tech sprint on digital identity.[60]

Novel approach to storing and proving identifying information. FinCEN should consider encouraging the exploration of novel approaches to identity management that would permit financial institutions to meet the policy objective behind KYC and CIP requirements while allowing financial institutions to increase effectiveness and efficiency and better protect consumers' personal information.

FinCEN specifically could establish a process to evaluate the way novel mechanisms can be used to create and maintain digital identity records, including (but not limited to) the adoption of digital identity verification techniques that can use a combination of decentralized blockchain-based technologies and secure "off-chain" data repositories. Specifically, there are tools under development that can allow digital identity information to be stored securely, and that use digital markers or tokens to enable the persons whose identity information is requested to confirm for a financial institution at onboarding that their identity *has been* verified, without

---

[56] *See* 31 C.F.R. § 1020.220(a)(2)(i)(A).

[57] *See* FinCEN; Customer Identification Programs for Certain Banks (Credit Unions, Private Banks and Trust Companies) That Do Not Have a Federal Functional Regulator, 67 Fed. Reg. 48,299, 48,302 (July 23, 2002), https://www.govinfo.gov/content/pkg/FR-2002-07-23/pdf/02-18193.pdf ("Obtaining sufficient information to verify a customer's identity can reduce the risk that a bank will be used as a conduit for money laundering and terrorist financing.").

[58] AMLA, § 6215(a)(8).

[59] *See, e.g.,* FATF, Digital Identity (Mar. 2020), http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf (broad discussion of evolving technologies available to facilitate digital identity management).

[60] FDIC, FDITECH, Measuring the Effectiveness of Digital Identity Proofing for Digital Financial Services, https://www.fdic.gov/fditech/techsprints/measuring-effectiveness.html (last visited Feb. 11, 2022) ("What is a scalable, cost-efficient, risk-based solution to measure the effectiveness of digital identity proofing to ensure that individuals who remotely (i.e., not in person) present themselves for financial activities are who they claim to be?").

providing the sensitive PII itself. This provides a mechanism for a customer to control the dissemination of information about his or her identity, thus better protecting privacy, while also enabling access to financial services.[61]

There are even more novel ways of confirming identities without revealing identities that are under development through the use of zero-knowledge proofs and other sophisticated forms of encryption.[62] These technologies would allow a customer to confirm that she is who she says she is, without revealing her specific identity. Doing so would be accomplished by the customer leveraging a token or other digital marker that only she possesses that would confirm she has unique access to a particular body of identifying information that is stored in encrypted form. This approach to identity management could potentially supplement existing CIP mechanisms that require the dissemination of large amounts of PII to numerous financial institutions. And it could do so while allowing individuals to keep their PII private and safe from theft or manipulation.

With time, many of the techniques described here could also incorporate non-traditional forms of identifying information (*e.g.*, mobile device identifiers) that would facilitate access to financial services for those who may lack government-issued photo IDs. While these technologies are likely a long way away from maturity, now is the time to allow experimentation and testing of these types of products to incentivize research into how they may scale over time.

Leverage shared services and shared platforms and collaboration among financial institutions. FinCEN should also further encourage financial institutions to leverage shared services and shared platforms in conducting identity management. On October 3, 2018, FinCEN and the federal banking regulators—FRB, FDIC, NCUA, and OCC—issued the *Interagency Statement on Sharing Bank Secrecy Act Resources* (the "2018 Interagency Statement"). Congress endorsed this approach in the AMLA, expressly encouraging financial institutions to enter the types of arrangements described in the statement.[63] The 2018

---

[61] Traditionally, a user must register for an account for every service provider. Each service provider serves as the central authority for managing user identity. With novel identity management frameworks, the user can receive credentials proving identity from multiple issuers, such as government agencies, universities, and employers, and store them in a digital wallet. When a need for identity verification arises, the user can then present proofs of their identity to any company that requests it and these companies can verify the proofs are true. *See e.g.,* CAPCO, Decentralized Identity: How Digital Transformation and Distributed Ledger Technology is Disrupting KYC (2020), https://www.capco.com/-/media/CapcoMedia/Capco-2/PDFs/Decentralized_Identity_Disrupting_KYC.ashx; Darren Shou, *How Decentralized Identity Is Reshaping Privacy for Digital Identities*, Forbes (Dec. 10, 2021), https://www.forbes.com/sites/forbestechcouncil/2021/12/10/how-decentralized-identity-is-reshaping-privacy-for-digital-identities/?sh=247c3e6e3226.

[62] Howard Wu, *How the Coming Privacy Layer Will Fix the Broken Web*, Future (June 15, 2021), https://future.a16z.com/a-privacy-layer-for-the-web-can-change-everything/; Pamela Dingle, *Advancing Privacy with Zero-Knowledge Proof Credentials*, Microsoft: Identity Standards Blog (July 22, 2020), https://techcommunity.microsoft.com/t5/identity-standards-blog/advancing-privacy-with-zero-knowledge-proof-credentials/ba-p/1441554.

[63] *See* AMLA, § 6213 ("[i]n order to more efficiently comply with the requirements of this subchapter, 2 or more financial institutions may enter into collaborative arrangements, as described in the statement entitled 'Interagency Statement on Sharing Bank Secrecy Act Resources'").

Interagency Statement was published "to address instances in which banks may decide to enter into collaborative arrangements to share resources to manage their [BSA] and [AML] obligations more efficiently and effectively."[64] FinCEN and the federal banking regulators defined collaborative arrangements as "two or more banks with the objective of participating in a common activity or pooling resources to achieve a common goal. Banks use collaborative arrangements to pool human, technology, or other resources to reduce costs, increase operational efficiencies, and leverage specialized expertise."[65] The 2018 Interagency Statement recognized that, although each financial institution faces a unique set of threats and risks, there are efficiencies to be gained by collaborating—including potentially in "reviewing and developing risk-based customer identification and account monitoring processes."[66]

More can be done, however, to build on the 2018 Interagency Statement. Regulators indicated that "[c]ollaborative arrangements as described in this statement generally are most suitable for banks with a community focus, less complex operations, and lower-risk profiles for money laundering or terrorist financing."[67] However, any financial institution that properly manages the risk of adopting an innovative approach to identity management should be able to do so, which would free resources to manage other financial crime compliance activities.

Identity management and CIP are precisely the kinds of requirements that the ideas embodied in the 2018 Interagency Statement could helpfully address because each financial institution at which a customer opens an account must collect and verify information identical to that previously collected and verified by the other financial institutions at which the customer has opened an account—a duplication of effort that can be reduced. Indeed, this type of approach to relying on data not contained at the relevant financial institution has historical precedent, as the BSA has permitted certain financial institutions to rely on the CIP of another financial institution in certain circumstances.[68] And a recent Government Accountability Office report on de-risking mandated by the AMLA noted the potential for shared KYC utilities to increase banking access for vulnerable groups, like humanitarian organizations and MSBs that cater to cross-border transfers.[69] It should be noted that FinCEN has not yet formally expanded the concept of reliance to MSBs—a category of financial institution that includes many cryptocurrency companies—but such an expansion could be warranted.

---

[64] FRB, FDIC, FinCEN, NCUA, OCC, Interagency Statement on Sharing Bank Secrecy Act Resources at 1 (Oct. 3, 2018), https://www.fincen.gov/sites/default/files/2018-10/Interagency%20Statement%20on%20Sharing%20BSA%20Resources%20-%20%28Final%2010-3-18%29%20%28003%29.pdf.

[65] *Id.*

[66] *Id.*

[67] *Id.*

[68] *See, e.g.,* 31 C.F.R. § 1020.220(a)(6).

[69] U.S. Gov't Accountability Office, GAO-22-104792, Bank Secrecy Act: Views on Proposals to Improve Banking Access for Entities Transferring Funds to High-Risk Countries at 29-31 (Dec. 2021), https://www.gao.gov/assets/gao-22-104792.pdf,

Customer due diligence. A final area where blockchain technology will play an important role is with respect to customer due diligence. As described above, transactional histories are generally publicly available on blockchains for analysis. It will be increasingly important for financial institutions of all types to leverage the information about transaction history that is available through blockchain forensic tools. These kinds of tools can identify transactions with high-risk counterparties or other kinds of high-risk activities and will be an indispensable component of customer due diligence on an ongoing basis.

IV. Conclusion

The last decade has witnessed unprecedented dynamism in the ways financial products and services are delivered, largely as a result of the development of blockchain technology. As FinCEN reexamines the BSA, it faces an opportunity to similarly reimagine how AML compliance processes take place. One of the core ways it can do so is by supplementing the BSA's paradigm of recordkeeping and reporting with new frameworks for the public and private sectors to identify and mitigate financial crime risks. Anchored in the comprehensive public record of transactions recorded on the blockchain, and enabled by advances in forensic tools to analyze those records, the public and private sectors have opportunities to employ novel approaches to identify and disseminate typologies of illicit finance threats. Similarly, blockchain technology and advanced cryptography have the potential to reinvent identity management and customer due diligence while protecting privacy and making those processes more effective. We look forward to continuing to collaborate with FinCEN to accomplish these shared objectives.

Respectfully submitted,

/s/ Sheila Warren

Sheila Warren

Chief Executive Officer

Crypto Council for Innovation

Crypto Council for Innovation

Oct 28, 2022

Senator Andrew Bragg
Liberal Senator for New South Wales
PO Box 6100
Senate
Parliament House
Canberra ACT 2600

Re: The Digital Assets (Market Regulation) Bill 2022

Dear Senator Bragg:

The Crypto Council for Innovation ("CCI") submits this letter in response to the The Digital Assets (Market Regulation) Bill 2022.[1] CCI appreciates the opportunity to share its information, expertise, and views on this vital issue with your team. Digital assets represent one of the most significant innovations in finance—and beyond—in many years, with the potential to alter ownership structures, commercial applications, cross-border payments, transaction processing and settlement, access to capital, investment opportunities, and much more. These developments contribute to equitable growth and financial inclusion, as well as investor and consumer choice and security. The regulation of this space, therefore, is an important question for policymakers.

SUMMARY

As we discuss in more detail below, cryptocurrencies and blockchain applications more generally are significant and evolving technological innovations with many use cases developed under a variety of business models. These innovations have the potential to bring increased transparency, security, efficiency, and inclusion not only to financial services, but to other sectors as well. As your team considers what legislation and regulation are appropriate to promote responsible innovation in cryptocurrencies and other digital assets, CCI respectfully submits that the policies should be guided by key principles, including:

- Legislation and regulation should be tailored to address the unique characteristics of digital assets – and carefully consider the nuances within the space.
- Legislation should take a strategic and forward-looking approach.

[1] https://www.andrewbragg.com/digital-assets-market-regulation-bill-2022

- Legislation and regulation should create a level playing field for all who want to be in the industry.
- Legislation and regulation should promote responsible innovation while putting in place appropriate protections for consumers and investors.
- Legislation should take a deliberate and thoughtful approach to definitions and categorization.

The following letter provides our thinking on these principles, followed by policy and regulatory considerations for each. We note that these principles are high-level and may be applied to this or any future legislation.

Crypto and blockchain technology will be core to the digital economy for any sovereign jurisdiction regardless of geographic regions and political affiliations. Getting policies and regulation right at this stage will be key to ensuring that the potential of the technology is realized.

The space is moving quickly and in many exciting directions. The Crypto Council for Innovation hopes to be a resource to policymakers and regulators to navigate this evolving space.

ABOUT CCI

CCI is an alliance of crypto industry leaders with a mission to communicate the benefits of crypto and demonstrate its transformational promise. CCI members include some of the leading global companies and investors operating in the crypto industry, including Andreesen Horowitz, Block (formerly Square), Coinbase, Electric Capital, Fidelity Digital Assets, FTX.US Gemini, Paradigm, and Ribbit Capital. CCI members span the crypto ecosystem and share the goal of encouraging the responsible global regulation of crypto to unlock economic potential, improve lives, foster financial inclusion, protect national security, and disrupt illicit activity.

DISCUSSION

I. Legislation and regulation should be tailored to address the unique characteristics of digital assets – and carefully consider the nuances within the space.

Digital assets represent a once-in-a-generation opportunity to realize benefits such as trust, immutability, and resilience arising from recording transactions on a distributed network. Accordingly, any legislation or regulation of cryptocurrencies should be tailored to address the unique characteristics of cryptocurrencies.

A challenge is to understand when a financial innovation is sufficiently like a previous activity that it can be safely and appropriately regulated within existing statutory authority merely by expanding existing regulation to cover it, and when a financial innovation is

sufficiently different that it requires a new, or largely new, approach. CCI respectfully submits that digital assets activities tend to be sufficiently different in their characteristics, risks, and benefits that a new approach will often be warranted.

Crypto and blockchain technology are underpinned by fundamentally new operational, technical, and business models. This fundamentally new innovation has opened a new model for peer-to-peer value exchange in the digital economy. Though the first use case was financial, the innovation found in the Bitcoin white paper[2] has opened a world of possibilities. Conversations about central bank digital currencies (CBDCs),[3] digital art and non-fungible tokens (NFTs),[4] digital identity,[5] and decentralized finance[6] would not be possible without this fundamental transformation.

One reason that this is important is that certain legacy regulatory frameworks may be ill-suited for addressing the unique characteristics of cryptocurrencies. "Shoe-horning" cryptocurrencies into legacy regulatory frameworks may create unanticipated risks and prevent Cryptocurrencies from providing a medium of exchange that can reduce transaction costs, including fees, time, transfer limits, vulnerability to abusive practices. Cryptocurrencies can also improve access to financial services.

Policy and regulatory considerations

Scope

Given the wide range of use cases and applications covered within the digital assets space, legislation should be appropriately tailored. As we have seen with proposals from the European Union, Financial Stability Board, and the United States Congress, it may be appropriate to have separate legislation and considerations for crypto, stablecoins, and central bank digital currencies (CBDCs), given the differences in their uses and technical underpinnings. Even within certain categories, such as stablecoins, a recognition of sub-categories may be necessary.

This bill aims to tackle both stablecoins and the digital yuan, among other aspects of crypto and blockchain technology. While both topics are important, combining their legislation may not allow for the nuance that is necessary to address such different and quickly-evolving spaces. We recommend the digital yuan be treated separately.

Licensing

Many financial regulations have historically been based on an entities-based approach requiring licensing or chartering of a legal entity to conduct permissible financial activities. An

[2] https://bitcoin.org/bitcoin.pdf

[3] https://www.bis.org/publ/bppdf/bispap125.htm

[4] https://time.com/5947720/nft-art/

[5] https://www.coindesk.com/podcasts/coindesks-money-reimagined/getting-internet-identity-right-30-years-on/

[6] https://www.weforum.org/whitepapers/decentralized-finance-defi-policy-maker-toolkit

entities-based approach, however, is less suited to blockchain-based financial services and products, which are more distributed than traditional finance and may have no specific entity with unilateral control of the financial product or service.

A licensing regime may not be suitable for many crypto products and services. Rather it may be more fruitful to identify who are the key parties involved with the provision of the crypto asset-related product or service. These key parties, such as the development team, blockchain infrastructure, banks, token holders, validators, etc., may not have unilateral control over the service or product, but they can provide important information about the roles they play in the provision of the service or product.

Finally, a licensing regime may not be suitable for all crypto-related financial services or products because in the near future a large portion of the global financial system will be running on blockchain technologies. Crypto will be mainstream and will not be considered a category apart from traditional financial services. Thus, a separate licensing regime for crypto asset-related entities may not be a future-proof approach to regulation. Regulating and enforcing all crypto assets under existing securities law may cause inadvertent harm to the overall digital asset ecosystem and Australia's innovation competitiveness as it compares to other regional jurisdictions in Asia and abroad.

A study of regional licensing regimes and crypto asset classification research as guidance may be useful, as well as exploring collaboration opportunities with jurisdictional partners and regulatory counterparts. Where applicable, CCI will be honored to facilitate such conversations within our network and connections with global policy makers.

II. Legislation should take a strategic and forward-looking approach.

Given the nascency of the crypto and digital assets space, there is a great deal of activity and developments are moving very quickly. As such, policies should take a strategic and forward-looking approach. In addition to considering the nuances in the space, as discussed, it is important that policy is not driven by news cycles. A proactive approach will set countries apart in this emerging space. For policymakers, it will be critical to consider which innovations and applications are a priority and legislate accordingly.

Policy and regulatory considerations

Tailored approaches

Australia may choose to learn from the examples of other countries that have worked towards tailored approaches for various use cases and applications. For example:

1. Monetary Authority of Singapore - Guidelines on Provision of Digital Payment Token Services to the Public[7]
2. FINMA (Switzerland) - Utility and Payment tokens classification and guidelines[8]

Global alignment

This cross-jurisdictional information-sharing and learning is also critical to ensure that there are consistent rules of the road across the world. Gaps in legislation or regulation may lead to regulatory arbitrage. At the same time, vastly different regimes from country to country may mean that service providers are not able to scale and serve customers around the world.

III. Legislation and regulation should create a level playing field for all who want to be in the industry.

CCI believes that consumers and investors should have a chance to choose the responsible innovations that work best for them. Currently, many different types of businesses engage in digital assets activities through a variety of business models and product offerings. Although some product offerings may share some characteristics with legacy products, the government should carefully consider the full range of characteristics of the offerings, rather than allow one or a few characteristics to drive a conclusion that they may be offered only by entities permitted to offer similar legacy products. For example, if a product has some characteristics in common with products offered by banks, that should not mean that only banks should be permitted to offer these products. Any legislation or regulation should create a level playing field for all who want to be responsible innovators in the industry, rather than artificially or unnecessarily constraining which entities may participate.

IV. Legislation and regulation should promote responsible innovation while putting in place appropriate protections for consumers and investors.

Any new legislation and regulation of the industry should promote responsible innovation, rather than curtail, restrict, or preclude it. At the same time, it is important to put in place appropriate protections for consumers and investors. CCI strongly supports both of these goals so that consumers, businesses, and investors can receive the full benefits of cryptocurrencies and the technologies that support them, while being appropriately informed of and protected from the risks. CCI agrees that we should work towards consumers having proper disclosures, appropriate safeguarding controls and measures, protections and a clear process for when something goes wrong.

---

[7] https://www.mas.gov.sg/regulation/guidelines/ps-g02-guidelines-on-provision-of-digital-payment-token-services-to-the-public

[8] https://www.finma.ch/en/documentation/dossier/dossier-fintech/entwicklungen-im-bereich-fintech/

Policy and regulatory considerations

Parsable disclosures

At the end of the day, consumer protection is about ensuring that average consumers can make informed decisions within a set of choices that work for them. Information should be presented in a manner that doesn't require a law degree or technical background to understand. Specifically, we support the creation of a meaningful and practical disclosure regime that includes information regarding material risks and conflicts of interest. Fair communication and advertising standards will also give investors and consumers transparency into financial tools and products and the entities which may be facilitating them.

V. Legislation should take a deliberate and thoughtful approach to definitions and categorization.

Given the diversity in the space, definitions will matter. Whether and how a service can operate will be determined by its categorization. As such, getting this right at the outset is of critical importance. This includes capturing the diversity of decisions around economic incentives, governance, and technology. Moreover, a dedicated effort will carefully consider both the policy and regulatory implications – including who should regulate a given project and why – as well as technical standards and how this plays into the classification of assets and technical projects.

Policy and regulatory considerations

Definitions

We appreciate the efforts to provide clarity on definitions. However, the bill leaves unclear precise definitions of how digital assets can and should be classified – a question that we are seeing playing out globally. We have followed Australia's efforts towards "token mapping," which could prove to be an essential step before assigning regulators and classifying various crypto projects.[9] Classifying some tokens and not others may be problematic down the road for those that are not expressly enumerated. To date, regulation by enforcement or reactive regulation has not worked well, with significant implications for consumers.

Studies

Around the world, policymakers have recognized that there are some aspects of digital assets that may be challenging to legislate or categorize at this moment in time. As such, they have commissioned studies on these areas to ensure that legislation does not inadvertently stifle innovation. For example, the European Union's Markets in Crypto Assets (MiCA) Regulation commissions studies on decentralized finance (DeFi) and non-fungible tokens (NFTs), which

[9] https://www.coindesk.com/policy/2022/08/22/australia-to-use-token-mapping-as-framework-for-crypto-regulation/

will be used to inform future legislation. These may be used as critical policy-making tools in addition to efforts like the token mapping exercise.

Stablecoin categorization

We also recommend evaluating stablecoin licensing requirements based on different characteristics and underlying mechanics of stablecoin issuance. Not all stablecoins are designed equally, and varying design decisions can affect factors like volatility, liquidity, and accountability. There are four primary stablecoin types (fiat-backed, crypto-backed, commodity-backed, and algorithmic) and each may require different considerations.

CCI believes fiat-backed payment tokens, whether they be CBDCs or private stablecoins, can power the ecosystem, and must be treated as cash-equivalent under laws, regulation and accounting. These payment tokens should be backed 1:1, be secure, and have sufficient risk management practices. Consumers and investors should have the right to redemption.

CONCLUSION

In conclusion, cryptocurrencies and blockchain applications have already delivered and promise further to deliver great benefits to consumers, investors, businesses, and the economy as a whole. As Australia considers how to promote responsible innovation in this area, we hope your team will be guided by the key principles outlined above. So guided, CCI is confident that responsible innovators in this field will continue to create products and services that leverage the inherent strengths of blockchain technology and bring the benefits of transparency, security, and efficiency to a range of users and sectors.

Sincerely,

/s/ Linda Jeng

Linda Jeng
Chief Global Regulatory Officer & General Counsel
Crypto Council for Innovation

Crypto Council for Innovation

UNIVERSAL PRINCIPLES FOR INDUSTRY OPERATING STANDARDS AND LEGISLATION THAT PROTECTS CRYPTO CUSTOMERS IN INSOLVENCY

1. Balanced Priorities and Predictable Results

- Insolvency rules currently cover “exchanges” and other now-existing and to-be-created platforms for the holding and transfer of crypto assets by customers, but these rules should be flexible enough to take into account the different types of crypto exchanges, platforms, and assets.
    - Insolvency rules should consider that exchanges, brokers, dealers or similar entities that facilitate trading may hold customer assets in order to facilitate trading and that those assets may be held on different terms than assets held by a custodian in cold storage.
- Insolvency rules regarding entities that transact with crypto customers should:
    - Balance customer protections with customer and counterparty transactional flexibility.
        - Customer protections will necessarily limit flexibility because segregation of and limits on use of crypto assets will constrain leveraged, derivative, and other transactions.
        - Flexibility is a hallmark of crypto as an emerging asset class and creating crypto-specific rules is an opportunity to match those rules with the particulars of the asset class.
    - Not force an entity with crypto customers to liquidate in order to avail itself of bankruptcy protections; chapter 11 reorganization of such an entity should be permitted.

2. Private Commercial Law

- Entities that transact with crypto customers should honor commercially-agreed terms for crypto assets to uphold predictable results during a bankruptcy
    - Entities and their customers desire both the freedom to agree among themselves and the ability to rely on agreed commercial terms.
    - Operational standards should work in unison with commercially-agreed terms in order to ensure compliance with contractual expectations.
- Private commercial law assigns rights to creditors, and as these laws are updated, they may implicate bankruptcy protections
    - Private commercial laws are being revised or have been revised in light of crypto assets.
        - For example, in the US, the Uniform Commercial Code is adopting a new Article 12 and a new term: “Controllable Electronic Forms,”and the UK Law Commission is proposing a third asset class: “Data Objects’ to be added to the property classes of “tangible assets” and “intangible assets.

2. Default Customer Protections and Opt-Out Flexibility

- Commercially-agreed terms should:
    - Define the specifics of the relationship between entities that transact with crypto customers and those customers.
    - Provide customers with the ability to "opt-out" of a "default" relationship and its protections
        - The ability to "opt-out" should be conducted preferably by different legal entities to reduce contagion.
        - The "default" relationship will trigger mandatory customer protections (see below for specifics).
            - The "default" will provide the best route for a customer to quickly and fully access its positions with the entity, either through a transfer to a different entity or through the ability to transact with the existing entity during the entity's insolvency.
        - "Opt-out" of the default relationship will allow innovation in business models and transactions, creating potential for greater returns / lower pricing but at higher risk.
            - For example, opt-out will allow entities to encumber or leverage customer assets for the growth of the entity's business and will result in a customer having only a general contractual claim against the entity.
            - Nevertheless, opt-out will still require proper accounting for customer claims.
            - Opt-out will likely diminish the amount to be recovered by a customer in any entity insolvency and will likely increase the time before a customer receives any distribution from an entity insolvency.
    - Industry should take steps to incorporate these default protections in its customer contracts.

3. Default Protections: Segregation; Fast and Easy Netting and Transfer/Return of Custodial Crypto Assets

- Default protections for crypto assets should:
    - Mandate segregation of customer crypto assets from proprietary assets, which can be achieved through the custodian's books and records.
    - In limited cases, permit or require the relevant crypto entity to add or assign proprietary assets to the customer asset pool to faciliate customer activity.
        - These assets would be treated as customer assets and would NOT be treated as proprietary assets in an insolvency of the relevant crypto entity. They would only revert to the insolvency estate of that entity after all customer claims are satisfied.
        - Assets in the customer asset pool would not be commingled with operating assets of the entity and could not be used for any purposes other than facilitating customer activity.
        - Permit the use of omnibus accounts in lieu of requiring individual segregation on a customer-by-customer level, subject to accounting in the

books and records of the entity that would provide precise traceability of all assets in the customer asset pool.
    - Prohibit encumbrances on the crypto assets, other than as directed by and for the benefit of the customer.
    - Allow for the fast and easy:
        - netting of customer positions in crypto assets at the entity, whether upon the commencement of an entity insolvency (in a liquidation) or in the ordinary course (in a reorganization); and
        - transfer of net crypto assets to a different entity, return of net crypto assets to customers, or, in the case of an entity reorganization, maintenance of net crypto assets with customer protections remaining in place.

4. Separation of Crypto Asset Insolvency Rules from Other Insolvency Rules

- Insolvency rules for crypto assets should not disrupt, but should also be distinct/exempt from, insolvency rules for cash/deposit accounts, securities/securities accounts, or commodities/commodities accounts.
- However, the drafting of the crypto rules should draw upon the existing regulatory and legislative framework as appropriate to achieve consistency and to make use of tested procedures for delivering transactional freedom and customer protection. It may be appropriate for insolvency rules for crypto assets to work together with insolvency rules for existing products where the activities are conducted out of the same legal entity.
- International conflicts of laws in bankruptcy - including over where the case should be handled and who should be in charge of the assets- should be predictable.