# 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.