JONES DAY | One Firm Worldwide®

WHITE PAPER

October 2022

Digital Assets Defined: Federal Agencies Weigh Response to President Biden's Executive Order on Digital Assets

On March 9, 2022, President Biden issued Executive Order 14067 ("EO"), "Ensuring Responsible Development of Digital Assets." The EO, which we discussed in "White House Issues Executive Order Calling for Inter-Agency Study of Digital Assets," required a number of federal agencies to issue reports regarding issues raised by digital assets with respect to each agency's area of jurisdiction. Those agencies have now issued nine reports, covering topics ranging from central bank digital currencies ("CBDC") to anti-money laundering ("AML") to the climate and energy implications of creating and using digital assets.

In this *White Paper,* we discuss the high-level takeaways from each report, and what they likely mean for the future development and regulation of digital assets going forward. In two follow-on papers, we will take a closer look at the reports prepared by the White House Office of Science and Technology Policy ("OSTP"), and the U.S. Department of the Treasury.

WHITE HOUSE OFFICE OF SCIENCE AND TECHNOLOGY POLICY

The White House OSTP prepared a technical evaluation of developing a U.S. CBDC system ("Technical Evaluation for a U.S. Central Bank Digital Currency System"). In doing so, the OSTP also set forth the policy objectives of such a system. The report outlines the various choices and limitations that should inform the design and implementation of a "CBDC system" in the United States. Crucially, "CBDC system" includes not only the CBDC itself, but "the public and private sector components built to interact with it, and the laws and regulations that would apply to those components." The term "components" is to be broadly construed and, by way of example, could encompass things such as smart cards, mobile applications, and intermediaries fulfilling various roles in the system.

The report ("Policy Objectives for a U.S. Central Bank Digital Currency System") set forth eight policy objectives, which focus on nuts-and-bolts matters like interoperability with other payment systems as well as higher-level goals such as economic growth, equitable access, national security, and human rights:

1. The CBDC[1] system should include appropriate protections for consumers, investors, and businesses including guardrails against fraud and market failures.
2. The CBDC system should be designed to integrate seamlessly with traditional forms of the U.S. dollar, and be both governable and sufficiently adaptable enough to promote competition and innovation.
3. The CBDC system should provide a good customer experience; make investments and domestic and cross-border fund transfers and payments cheaper, faster, and safer; and include appropriate cybersecurity and incident management so as to be protected against cybersecurity attacks and resilient against other potential disasters or failures. The CBDC system itself should be extensible and upgradeable such that it can be iterated upon quickly to improve and harness new innovation, as well as changing technologies, regulations, and needs.
4. The CBDC system should be appropriately interoperable to facilitate transactions with other currencies and systems, such as physical cash, commercial bank deposits, CBDCs issued by other monetary authorities, and the global financial system.
5. The CBDC system should be available to all and expand equitable access to deposit and payment products and services, as well as credit provided by banks.
6. The CBDC system should promote compliance with anti-money laundering ("AML") and combating the financing of terrorism ("CFT") requirements as well as relevant sanctions obligations.
7. The CBDC system should be designed and used in accordance with civil and human rights, such as those protected by the U.S. Constitution and outlined in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.
8. The CBDC system should adhere to privacy engineering and risk management best practices, including privacy by design and disassociability.

While some of the objectives may be in tension with each other, the document asserts that its aim is not to prioritize or reconcile any of the concepts, or even take a position on whether a U.S. CBDC should be released at all.

In terms of a technical assessment, the report considers various design options and the ways in which they would further or hinder the realization of the above-stated policy objectives. Those options are broken into six different categories: Participants, Governance, Security, Transactions, Data, and Adjustments. In assessing the options, the report is careful to emphasize that it does not make any assumptions, prioritize any design choices, claim the list of design choices is complete, or take any positions on whether a CBDC system would be in the best interests of the United States.

- **Participants:** This section looks at different options for the transport layer and interoperability. The design of the transport layer within a CBDC system determines the degree to which transactions between two parties are intermediated by a third party, and who that third party is. Interoperability determines the extent to which a CBDC system can execute transactions with other payment systems, domestic or international, digital assets vs. nondigital assets, etc.

- **Governance:** This section looks at permissioning, access tiering, identity privacy, and remediation. "Permissioning" determines whether a system is governed by a set of

verified and trusted entities or by a collection of interested participants. Access tiering has to do with the way in which transactions could be parsed and handled differently according to specific attributes. "Identity privacy" relates to who, if anyone, knows the identity of the parties transacting within the CBDC system. And "remediation" has to do with how transaction errors, whether the result of fraud or a simple mistake, are corrected within the system.

- **Security:** This section looks at cryptography and secure hardware. "Cryptography" involves the techniques used to ensure that transactions within the CBDC system are secure. "Secure hardware" considers the extent to which security features within the CBDC system are built into the hardware used to access and operate the system (e.g., smart cards, embedded chips, etc.) vs. managed through software running on general-purpose devices (e.g., computers, tablets, and smartphones).

- **Transactions:** This section looks at signature, transaction privacy, offline transactions, and transaction programmability. "Signatures" concerns how many digital signatures are required to complete a transaction and who must provide them. "Transaction privacy" considers the degree to which transaction details (e.g., account balances, participant location(s), goods sold, etc.) are observable within the system and by whom. "Offline transactions" examines the extent to which parties could effectuate transactions between themselves and then later communicate those transactions to a transaction processor. And "transaction programmability" considers whether third-party developers could develop programs to run within the CBDC system, such as smart contracts.

- **Data:** This section looks at data models and ledger history. "Data models" concerns the way in which ownership records would be stored. "Ledger history" considers whether an ownership and transaction ledger would be stored in a central location or distributed among various locations.

- **Adjustments:** This section looks at fungibility, holding limits, adjustments on transactions, and adjustments on balances. "Fungibility" considers whether a CBDC would have a unique identifier, similar to serial numbers associated with U.S. dollar-denominated bills, or no unique identifier at all. "Holding limits" examines whether to limit entities to holding a set amount of CBDC. And "adjustments on transactions" and "adjustments on balances" looks at whether and how to impose fees on CBDC system users, and whether and how to allow balance adjustments for things like fees and interest, respectively.

A recurring theme in these sections is the sliding scale of privacy vs. AML/CFT compliance, with enhanced privacy making AML/CFT compliance more difficult, and vice versa. The sections also routinely focus on expanding access to the financial system in an equitable manner, and ensuring interoperability with payments systems that currently exist, and that may come into existence in the future.

The White House OSTP also prepared a report on climate and energy implications associated with digital assets ("Climate and Energy Implications of Crypto-Assets in the United States"). The report provides answers to several questions specifically set forth in the EO:

How do digital assets affect energy usage, including grid management and reliability, energy efficiency incentives and standards, and sources of energy supply?

The OSTP finds that crypto-asset networks use electricity to power four major functions: (i) data storage; (ii) computing; (iii) cooling; and (iv) data communications—with computing representing the vast majority of electricity use.[2] It concludes that crypto-assets impact electricity usage and the grid, but that their impact varies depending on the type of crypto-asset. Specifically, the report emphasizes the energy-use differences between proof-of-work ("PoW") and proof-of-stake ("PoS") blockchains. The OSTP points to 2021 research showing that each PoS computing device requires 10 to 500 times less power than a typical rig used for PoW Bitcoin mining.[3] However, the report finds that total power usage from today's crypto-asset networks cannot be directly monitored because many computing or mining centers do not disclose their location or report their electricity usage. Another challenge is that energy usage can fluctuate significantly, based on market value fluctuations of the underlying crypto-asset. Despite these

challenges, the report estimates the United States' PoW mining electricity usage to be in the range of 0.9% to 1.7% of total U.S. electricity usage. It also points to such a large range as suggesting a need for miners to report their actual electricity usage to reduce the uncertainties presented to policymakers.[4]

What is the scale of climate, energy, and environmental impacts of digital assets relative to other energy uses, and what innovations and policies are needed in the underlying data to enable robust comparisons?

This section of the OSTP report focuses on the environmental impact of crypto-assets and finds that crypto-asset mining produces GHG emissions and exacerbates climate change primarily by burning coal, natural gas, or other fossil fuels to generate electricity in: (i) an onsite dedicated power plant; (ii) purchasing electricity from the power grid; and/or (iii) producing and disposing of computers and mining infrastructure, and production of power plant fuels and infrastructure.[5]

What are the potential uses of blockchain technology that could support climate monitoring or mitigating technologies?

The OSTP is not optimistic about the value of distributed ledger technology ("DLT") in certain environmental markets. The report identifies two main types of environmental markets: those created pursuant to a regulatory program and those that are voluntary.[6] While either market requires the type of robust market infrastructure that DLT is adept at providing—trade execution, payments, clearing and settlement, record-keeping, and security—environmental markets are currently highly centralized.[7] Given that DLT is designed to solve issues associated with decentralization, the OSTP finds that there may not be a clear advantage to introducing DLT in environmental markets sufficient to justify the switching cost.

Despite its dim view of DLT in environmental markets, the OSTP appears to see potential for DLT in the context of grid reliability and distributed energy resources, or DERs, such as electric vehicles, fuel cells, residential and commercial battery systems, and solar power systems. The OSTP finds that DLT-supported innovation could help to digitize, automate, and decentralize the operation of an electricity grid that estimates say will have more than 100 million new storage devices connected by 2040.[8] Since such numbers will require greater automation, the OSTP sees smart contracting as a candidate for supporting this aspect of the evolving clean energy marketplace.[9]

What key policy decisions, critical innovations, research and development, and assessment tools are needed to minimize or mitigate the climate, energy, and environmental implications of digital assets?

The OSTP report outlines a number of recommendations to ensure the responsible development of digital assets. These include collaboration among various government entities and the private sector to develop effective performance standards, conduct reliability assessments of crypto-asset mining operations, and analysis of information from crypto-asset miners and electric utilities. They also include promulgating and updating energy conservations standards for crypto-asset mining, encouraging crypto-asset industry associations to publicly report certain information, and promoting and supporting further research and development priorities to improve the environmental sustainability of digital assets.

Overall, the report appears to be aimed at setting the stage for further legislation and regulation that would impact the crypto-asset industry by: (i) informally pressuring the industry to establish certain "best practices" even if such practices are not initially required; (ii) increasing required reporting; and (iii) setting increasingly stringent performance standards.

DEPARTMENT OF THE TREASURY

The Treasury's report on "The Future of Money and Payments" includes three main components: (i) a section setting forth Treasury's overview of the current payment system in place today, including recent developments; (ii) a section evaluating options for the U.S. government to pursue in developing a CBDC; and (iii) its four recommendations for improving the U.S. money and payments system.

The overview of the current payments system covers the different retail and wholesale payments systems in use for domestic and cross-border payments; the consumer choices available for consumer-facing payment systems; the roles that banks

and non-bank intermediaries play in the current system; and recent developments such as stablecoins, FedNow, and ACH's Real Time Payments network.

The section on a future CBDC is largely reminiscent of the OSTP report on the same topic. It lays out a number of choices to be considered in establishing a CBDC system, such as retail vs. wholesale transactions, whether a CBDC would pay interest, the extent of transaction programmability, the nature of the DLT technology underlying the system, interoperability with foreign CBDCs, and single- vs. two-tier intermediation with the Federal Reserve.

Finally, the report sets forth its recommendations for achieving the policy considerations presented in the EO—namely, building the future of money and payments, supporting U.S. global financial leadership, advancing financial inclusion and equity, and minimizing risks. The recommendations are not detailed, but a few items of note are:

- With respect to a CBDC, Treasury considers potential unintended consequences of a CBDC, including a run to CBDC in times of stress and a reduction in credit availability to the extent that CBDC uptake reduces bank deposits and, indirectly, bank lending.
- On the subject of federal payments regulation, Treasury notes that a federal framework would provide a common floor for existing state standards (such as minimum financial resource requirements) and also that it should address run risk, payments risks, and other operational risks consistently and comprehensively.

The Treasury's report on crypto-assets ("Crypto-Assets: Implications for Consumers, Investors, and Businesses") includes four main components: (i) a section setting forth Treasury's overview of the current crypto-assets market; (ii) a section providing a description of current uses of crypto-assets; (iii) a set of risks and exposures for consumers, investors, and businesses in the crypto-asset market, categorized into conduct risks, operational risks, and intermediation risks; and (iv) Treasury's four recommendations to address risks associated with the crypto-asset sector.

The section on the current crypto-assets market describes three categories of relevant entities: crypto-asset platforms, miners and validators, and data aggregators. It also provides four central use cases for crypto-assets: (i) financial markets, products, and services that use native crypto-assets for trading, lending, and collateral activities of other crypto-assets, that are mostly speculative in nature; (ii) use as a medium of exchange for goods and services, in limited cases; (iii) market infrastructure for traditional assets using permissioned blockchains for payments, clearing, and settlement; and (iv) other commercial activities, largely non-fungible tokens ("NFTs").

Treasury views three categories of risks and exposures as the most significant in this space: conduct risks, operational risks, and intermediation risks. Conduct risks include the use of crypto-assets for fraud and scams, information asymmetries between users and platforms, and platforms providing access to bad actors, providing products and services to retail investors without disclosing conflicts or ensuring suitability, and engaging in frontrunning and market manipulation. Operational risks include hacks, difficulty patching bugs in immutable smart contracts, tradeoffs between security and scalability, deanonymization, and misaligned incentives for miners and validators. Intermediation risks include inadequate resources or capabilities for risk mitigation, inability to absorb financial shocks, and bankruptcy/insolvency.

The report asserts that some risk arises from deliberate noncompliance with existing regulation but also from gaps and lack of clarity in the current framework for financial regulation, supervision, and enforcement as it applies to crypto-assets. In that vein, the report makes the following recommendations:

- U.S. regulatory and law enforcement authorities should pursue "vigilant monitoring" of the crypto-asset sector, aggressively pursue investigations, and expand and increase investigations and enforcement, particularly into misrepresentations made to consumers and investors;
- Agencies should review existing regulations and clarify regulatory requirements applicable to crypto-asset products and services, and should act in collaboration with each other while providing guidance in plain language; and
- Agencies should provide education to consumers and investors.

Treasury also issued a report, titled "Action Plan to Address Illicit Financing Risks of Digital Assets" ("Illicit Financing Strategy"), which outlines priorities and action items to ensure that the U.S. government modernizes the U.S. Department of Treasury's anti-money-laundering/countering-the-financing-of-terrorism ("AML/CFT") regime to keep abreast of structural and technological changes to the financial services and markets that result from the increasing issuance and use of digital assets.

Treasury's Illicit Financing Strategy identifies illicit finance and national security risks and proposes a number of action items to address those risks. However, most of the action items are presented in the Illicit Financing Strategy at a high level of generality, and will have to be fleshed out by Treasury, FinCEN, and others going forward before the industry can or should take concrete action in response.

The identified risks are as follows: money laundering, proliferation financing, terrorist financing, cross-border nature and gaps in AML/CFT regimes across countries, anonymity-enhancing technologies, disintermediation, and virtual asset service provider ("VASP") registration and compliance obligations. Treasury identifies a number of go-forward action items for combating and mitigating these identified risks, including: monitoring emerging risks; improving global AML/CFT regulation and enforcement; updating Bank Secrecy Act regulations; strengthening U.S. AML/CFT supervision of virtual asset activities; holding cybercriminals and other illicit actors accountable; engaging with the private sector; supporting U.S. leadership in financial and payments technology; and advancing work on a CBDC, in case one is determined to be in the national interest.

DEPARTMENT OF JUSTICE

As with the other reports discussed in this *White Paper*, the report of the Attorney General on "The Role of Law Enforcement In Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets" was produced in response to the EO. The report gives a brief taxonomy of criminal activity related to digital assets, but—at the direction of the EO—focuses mainly on the role of law enforcement in identifying and investigating crime related to digital assets. The report also adds several potential legislative and regulatory recommendations that could "enhance" DOJ's efforts to disrupt and prosecute digital asset-related criminal activity. Each section is summarized below.

The report begins by noting that the majority of relevant activity resides in three categories: (i) digital assets as a means of payment for or to facilitate criminal activity; (ii) digital assets as a means of concealing criminal activity; and (iii) crimes involving the digital asset ecosystem. The report also flags an emerging area of concern—the rise of decentralized finance ("DeFi"). While there is no agreed-upon definition of "DeFi," in the context of DOJ enforcement, it broadly refers to digital asset protocols and platforms that allow for some form of automated peer-to-peer transactions—usually through the use of smart contracts based on blockchain technology. DOJ is particularly concerned regarding these platforms' application to fraud, investor and consumer protection, and market integrity. Under the DeFi umbrella, the report also notes that the rise of NFTs presents an opportunity for similar exploitation.

With respect to the role of law enforcement, the report notes recent multi-agency efforts to crack down on the illicit use of digital assets, including classic cases like the Silk Road and DOJ's Digital Currency Initiative. The report continues by outlining numerous divisions at DHS, Treasury, and the Secret Service charged with varying duties in monitoring and investigating fraud and other criminal activity related to digital assets. After briefly discussing a particular example involving $10 million in bitcoin, the report concludes with a brief overview of other enforcement mechanisms arising from the SEC, CFTC, CFPB, OCC, FDIC, FTC, and other private-sector partnerships.

Lastly, the report outlines a laundry list of possible regulatory moves that would enhance law enforcement's ability to crack down on illicit digital asset activity. The report designates each with varying levels of priority. DOJ's top priority is an extension of the existing prohibition against disclosing subpoenas to VASPs that operate as money-services businesses. In addition, DOJ also recommends strengthening federal law prohibiting the operation of an unlicensed money-transmitting business and extending the statute of limitations for crimes involving digital assets from five to 10 years. Lower priorities include supporting legislation designed to address the challenges in gathering evidence of such crimes and stronger penalties to further deter criminal digital asset activity.

DEPARTMENT OF COMMERCE

In the Department of Commerce's report on "Responsible Advancement of U.S. Competitiveness in Digital Assets," Commerce sets forth broader conceptual frameworks, with fewer specific recommendations. And Commerce regularly defers to other departmental reports that are discussed above. Commerce's framework sets forth four categories of actions: (i) regulatory approaches; (ii) international engagement; (iii) public–private engagement; and (iv) research and development.

Regulatory Approaches

Commerce takes the position that the SEC is already attempting to apply existing financial regulations to digital assets, and Commerce believes this is critical to future success: "Continued and regular enforcement of applicable financial laws and regulations is a foundational principle of U.S. competitiveness in financial services, including digital assets." Moreover, "Commerce endorses regulators' existing approach that both ensures regulation of the financial sector, including through application of existing law, and responsible innovation that identifies and mitigates risks prior to launch."

International Engagement

Commerce recommends that federal departments and agencies should "continue to engage internationally to promote development of digital asset policies and CBDC technologies consistent with U.S. values and standards." Commerce also recommends engagement with the Organization for Economic Cooperation and Development, multilateral development banks, and Asia-Pacific Economic Cooperation.

Public–Private Engagement

Commerce recommends a number of key issues that warrant public–private engagement: (i) an advisory committee; (ii) consumer and investor protection and education; (iii) diversity, equity, and inclusion; (iv) workforce development; (v) payment system modernization; (vi) sustainability; and (vii) accurate and complete economic statistics on economic activity.

Research and Development

Commerce notes the role of federal agencies in foundational research, and recommends continued promotion of research and development in financial technologies and digital assets to continue U.S. technological leadership.

FINANCIAL STABILITY OVERSIGHT COUNCIL

The Financial Stability Oversight Council's ("FSOC") "Report on Digital Assets Financial Stability Risks and Regulation" assesses the extent to which digital assets might pose systemic risks to the financial system.

The report begins by defining the scope of digital assets—which it defines as CBDCs and crypto-assets. The report focuses primarily on the latter, which it defines as private-sector digital assets that depend primarily on cryptography and distributed ledger or similar technology. Two primary examples, therefore, would be Bitcoin and Ethereum. The report also discusses key technological developments and financial innovations and market developments in this space, including the market capitalization peak of $3 trillion in November 2021 to its current level of around $900 billion.

The report next discusses potential financial stability risks. Those risks are, for the moment, tempered by the lack of significant interconnections between the crypto-asset ecosystem and the traditional financial system. Those interconnections could, however, rapidly grow as the crypto-asset ecosystem continues to evolve. Thus, the report assesses the vulnerabilities within that ecosystem, such as drops in asset prices, financial exposures via interconnections within the ecosystem, operational vulnerabilities, funding mismatches, the risk of runs on assets, and the use of leverage. The report also notes that, interconnections aside, crypto-assets could pose financial stability risks if they were to attain a large enough scale.

The report also discusses regulation of crypto-assets in the context of the above-identified risks. The report observes that the "current regulatory framework, along with the limited overall scale of crypto-asset activities, has helped largely insulate traditional financial institutions from financial stability risks associated with crypto-assets," before going on to discuss various regulators and regulations, and their (potential) applicability to crypto-assets.

The report's more interesting aspects reside in the FSOC's recommendations. There, the report begins by noting that "large parts of the crypto-asset ecosystem are covered by the existing regulatory structure." That may come as a bit of a surprise, given the ongoing legal battles concerning whether certain

crypto-assets are securities, commodities, or something else altogether. It is, however, consistent with recent regulatory enforcement actions in this space, where both the SEC and the CFTC have been increasingly aggressive in asserting their authority over crypto-asset ecosystem participants. The report then notes the "gaps" in the regulation of crypto-asset activities that would benefit from additional attention:

- Limited direct federal oversight of the spot market for crypto-assets that are not securities;
- Opportunities for regulatory arbitrage; and
- Whether vertically integrated market structures can or should be accommodated under existing law and regulations.

The first gap primarily concerns, in the report's eyes, spot markets for bitcoin "and possibly other crypto-assets that are not securities." By the report's own assessment, this market is rather limited. But the report urges additional regulation to "ensure orderly and transparent trading, to prevent conflicts of interest and market manipulation, and to protect investors and the economy more broadly."

The second gap, relating to regulatory arbitrage, characterizes optionality in the existing U.S. regulatory framework as a design defect rather than an intentional feature to permit innovation. FSOC states that opportunities for regulatory arbitrage can occur "when the same activity can be carried out lawfully under more than one regulatory framework." This fact is, of course, a hitherto noncontroversial hallmark of the U.S. banking system, in which banks may choose to be chartered under state or federal law and from a variety of different banking charters, for example. But the FSOC views this flexibility as creating opportunities for crypto-asset providers to "provide financial services that resemble services provided by banks, traditional securities intermediaries, or other financial institutions, but without being subject to, or in compliance with, the same standards and obligations."

The report therefore urges regulators to coordinate with one another in their supervision of crypto-asset entities, especially when "different entities with similar activities may be subject to different regulatory regimes or when no one regulator has visibility across all affiliates, subsidiaries, and service providers of an entity." In a similar vein, the report recommends that the FDIC, FRB, OCC, and state bank regulators use their existing authority to review services provided to banks by crypto-asset service providers. The report also recommends that Congress pass legislation that would create: (i) a comprehensive prudential framework for stablecoin issuers; and (ii) a supervisory framework where regulators have visibility into the activities of all the affiliates and subsidiaries of crypto-asset entities.

The third gap, relating to vertically integrated market structures, largely concerns recent requests by some market participants to disintermediate certain aspects of the market for crypto-assets. Specifically, these participants seek to provide direct retail access to investors. The report's primary concerns stem from consumer protection and managing the risk associated with the leverage or credit offered to retail investors. The report draws particular attention to the practice of managing risk by marking positions to market on a very frequent basis and conducting automatic liquidations where margin calls go unmet. While this may be an effective risk management tool, exposing retail investors to rapid liquidations raises its own set of concerns around disclosures, education, and potential conflicts of interest.

The report is, in some ways, more notable for what it does not say or do. It does not, for instance, provide any additional clarity on whether crypto-assets are securities, commodities, or something else. It also does not call for dramatic regulatory changes. Rather, it essentially calls on the member agencies to keep doing what they are doing. That posture would seem to benefit entities already within the regulatory perimeter, which can explore crypto-asset services and products within a risk management and control framework with which regulators are more comfortable and, in so doing, shape regulatory views on these activities to their advantage. In contrast, firms outside of or unable to gain access to the regulatory perimeter, including would-be "disruptors" to incumbent providers, are more likely to find themselves in an adversarial relationship with regulators.

LAWYER CONTACTS

Jayant W. Tambe
New York
+1.212.326.3604
jtambe@jonesday.com

Jonathan V. Gould
Washington
+1.202.879.3906
jgould@jonesday.com

Nathan S. Brownback
Washington
+1.202.879.3476
nbrownback@jonesday.com

Dorothy N. Giobbe
New York
+1.212.326.3650
dgiobbe@jonesday.com

Abradat Kamalpour
San Francisco
+1.415.875.5860
akamalpour@jonesday.com

Laura S. Pruitt
Washington
+1.202.879.3625
lpruitt@jonesday.com

Mark W. Rasmussen
Dallas
+1.214.220.3939
mrasmussen@jonesday.com

Joshua B. Sterling
Washington
+1.202.879.3769
jsterling@jonesday.com

Samuel L. Walling
Minneapolis
+1.612.217.8871
swalling@jonesday.com

Tyler Fields, Emerald A. Gearing, Timothy M. Villari, Collin L. Waring, and Todd R. Wells contributed to this White Paper.

ENDNOTES

1 News reports indicate that the Department of Justice issued a legal opinion on the Federal Reserve's authority regarding a CBDC, but those legal views have not yet been shared with Congress (or the public).

2 White House Office of Science and Technology Policy, *Climate and Energy Implications of Crypto-Assets in the United States* 13 (Sept. 8, 2022).

3 *Id.*

4 *Id.* at 15.

5 *Id.* at 21.

6 *Id.* at 27.

7 *Id.* at 28.

8 *Id.* at 29.

9 *Id.*