Circle Internet Financial, LLC
99 High Street
Suite 1701
Boston, MA 02110

March 3, 2023

Office of Science and Technology Policy
Executive Office of the President
725 17th Street NW,
Washington, D.C. 20502

Re: Federal Register Document 2023-01534

To Whom it May Concern:

Circle appreciates the opportunity to provide comments to the White House Office of Science and Technology Policy (OSTP), National Science and Technology Council, National Science Foundation, and the Fast Track Action Committee on Digital Assets Research and Development for the Subcommittee on Networking and Information Technology Research and Development. The establishment of a National Digital Assets Research and Development (R&D) Agenda is an essential foundation to harnessing the crosscutting benefits of cryptographic and blockchain technologies in a manner that supports economic growth and development, protects consumers, fosters responsible innovation, and promotes American competitiveness. Since Circle's founding in 2013, we have prioritized constructive engagement with policymakers and regulators in the United States as well as globally and appreciate this open dialogue in framing the long-term, whole-of-government R&D priorities.

About Circle
Circle is a global financial technology firm that provides internet-native payments and treasury infrastructure on open blockchains. Circle's foundational technology allows for the frictionless exchange of value on the internet. Circle is the sole issuer of USD Coin (USDC), a "digital dollar" also known as tokenized cash or payment stablecoin, with about $43 billion in circulation as of March 3, 2023, and issuance on eight blockchains. Circle is regulated in the United States through state money transmission licenses and USDC is always redeemable on a 1:1 basis for fiat dollars, bankruptcy remote, and fully reserved by high quality liquid assets.

USDC allows for payments that are instantaneous, immutable, cheaper than existing means of payment like wire transfers, and programmable into smart contracts. USDC has been integrated as a settlement option in leading merchant and credit card networks; supports cross-border remittances and humanitarian assistance; and is deployed as a payment option by e-commerce platforms. A full description of Circle's activities, including discussion of its operational risk management practices, terms of use and legal rights, audited financial statements, and filings with the Securities and Exchange Commission (SEC), can be found on our website.

As a financial services company, Circle's response focuses primarily on the benefits and implications of blockchain technology in the financial services industry.

1. Goals, sectors, or applications that could be improved with digital assets and related technologies.

Using public blockchains, payment stablecoins like USDC offer the near instantaneous ability to transfer funds globally with lower fees, greater transparency and finality, and more programmability than existing payment systems. By researching and developing blockchain technology and setting standards, the U.S. has the opportunity to ensure that the global digital economy is rooted in democratic principles that promote U.S. values and support American competitiveness. Circle is already seeing the below benefits being realized and notes, where applicable, where these applications advance the recommendations highlighted in the Treasury Department's September 2022 *"Future of Money and Payments"* report:[1]

Faster, Cheaper Payments with Programmable Money: Current financial architectures rely on often slow and expensive platforms — that necessitate the involvement of multiple intermediaries, parallel messaging through systems like SWIFT, correspondent banking relationships, and other cost-intensive factors — to process a single transaction. However, like the internet itself, the inherently open and peer-to-peer nature of public blockchains allows individuals and businesses to transact globally in seconds with an on-chain transaction cost as low as a few cents.[2] Payment stablecoins simplify that transaction process by serving as a financial instrument automatically written to an immutable ledger, which reduces settlement and credit risk; is inherently traceable; and facilitates real-time market information. USDC was used to settle $4.5 trillion in transactions in 2022, more than three of the top five global credit card companies combined.[3] Furthermore, the use of programmable smart contracts are already generating novel economic activity, for example, by enabling micro-payments for intellectual property and fractionalizing complex property ownership.

Significantly Reducing Transaction Costs for Cross-border Payments and Remittances: Cross-border payments like remittances are plagued by high transaction fees and, at times, delays in processing. But payment stablecoins like USDC and certain decentralized finance protocols drastically reduce costs, helping to support a more inclusive payment landscape, in line with recommendation 2 from the *Future of Money* report. Even in highly competitive remittance corridors such as the U.S.-to-EU, Circle has found that the cost of blockchain-based foreign exchange and conversion can be far lower than that of existing payment rails. A $500 remittance from USD to Euro can cost as low as $4.80 using payment stablecoins and decentralized finance rails, a small fraction relative to the global average cost of $28 through banks and $19[4] through traditional remittance operators.[5] This 80% cost reduction could translate into $30 billion in savings annually for low- and middle-income households.[6] Use of stablecoins for remittances — a $781 billion market in 2021 according to the World Bank — is already seeing significant uptake.[7]

---

[1] U.S. Department of the Treasury, *The Future of Money and Payments*, September 2022, (https://home.treasury.gov/system/files/136/Future-of-Money-and-Payments.pdf).
[2] Circle, *State of the USDC Economy*, January 2023, (https://www.circle.com/hubfs/PDFs/2301StateofUSDCEconomy_Web.pdf), p. 14.
[3] Ibid, *State of the USDC Economy*.
[4] World Bank, *Remittance Prices Worldwide*, (https://remittanceprices.worldbank.org/).
[5] Adams et al., *On-Chain Foreign Exchange and Cross-Border Payments,* January 20, 2023, (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4328948).
[6] Ibid, *On-Chain Foreign Exchange and Cross-Border Payments*.
[7] Knomad and World Bank Group, *Migration and Development Brief 37*, November 2022, (https://www.knomad.org/sites/default/files/publication-doc/migration_and_development_brief_37_nov_2022.pdf).

The largest cryptocurrency exchange platform in Latin America, with more than 3 million users, reported a 400% increase in remittance volume using USDC in 2022, up to $1 billion in remittances, or about 5% of total U.S.-Mexico remittance volume.

Overcoming "Last Mile" Problems with Humanitarian and Charitable Assistance: Due to their inherent versatility and traceability, payment stablecoins are being used to strengthen the delivery and speed of humanitarian assistance; can more effectively mitigate fraudulent abuse of aid; and serve those who lack access to traditional financial services — helping to advance a more inclusive payment landscape for disaster response and aid, in line with recommendation 2 from the *Future of Money* report. In partnership with the United Nations High Commissioner for Refugees (UNHCR) and International Rescue Committee (IRC), Circle launched a pilot program for delivering humanitarian aid to internally displaced persons (IDPs) in Ukraine in November 2022.[8] In addition to cost savings, the program allows multiple points of beneficiary validation and traceability of USDC following receipt by the beneficiary, while also serving as a safer store-of-value to IDPs. For beneficiary institutions and charities, Circle has found that the transaction costs using USDC are reduced by a conservative average of between 1.92% and 2.70% per donation compared with a traditional payment processor. Additionally, the ease and scalability of payment stablecoins attracts marginal donors by lowering the costs of transfer and empowers traditionally untapped populations to donate directly to communities in need, evidenced by the $1.25 million in USDC donated to Ukraine since the start of the Russian invasion[9] and the $500,000 donated to Turkey and Syria in the first week following the catastrophic earthquake in February 2023.[10]

Opens Paths to Financial Access: Roughly 20% of Americans today lack adequate banking services[11] and major banks in the U.S. often require customers to hold large minimum balances in order to waive account fees. Payment stablecoins and blockchain wallets provide a low-cost alternative to cash that serves as both store-of-value and means of access to digital commerce, evidenced by the fact that roughly 75% of wallets holding USDC hold less than $100, lower than all common minimum balance requirements at banks.[12] In addition to offering a cryptographically secure way for individuals to store wealth, users can also exchange their USDC for cash at tens of thousands of locations around the world.[13] Such a solution helps to increase financial access, in line with recommendation 2 from the *Future of Money* report.

Addressing Inefficiencies in the Foreign Exchange (FX) Market: The Bank for International Settlements (BIS) recognizes settlement risk in FX markets as a systemic source of risk that can

---

[8] UNHCR launches pilot Cash-Based Intervention Using Blockchain Technology for Humanitarian Payments to People Displaced and Impacted by the War in Ukraine

[9] Etherscan, USDC held by address, (https://etherscan.io/token/0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48?a=0x165CD37b4C644C2921454429E7F9358d18A45e14).

[10] Etherscan, USDC held by address, (https://etherscan.io/token/0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48?a=0xe1935271D1993434A1a59fE08f24891Dc5F398Cd).

[11] FDIC, 2021 FDIC National Survey of Unbanked and Underbanked Households, (https://www.fdic.gov/analysis/household-survey/index.html)

[12] Wallets surveyed were on Ethereum Virtual Machine (EVM) compatible blockchains only.

[13] Circle, *Coinme Announces USDC-powered Global, Borderless Digital Cash and P2P Payments*, (https://www.circle.com/en/pressroom/coinme-announces-usdc-powered-global-borderless-digital-cash-and-p2p-payments). See also: MoneyGram, *MoneyGram Launches Pioneering Global Crypto-to-Cash Service on the Stellar Network*, (https://ir.moneygram.com/news-releases/news-release-details/moneygram-launches-pioneering-global-crypto-cash-service-stellar).

undermine financial stability, impacting one-third of daily FX turnover, or around $2.2 trillion.[14] The near-instantaneous, or "atomic," nature of payment stablecoins combined with the ability to make payment-versus-payment transactions, facilitated by distributed ledger technology, has the capability to eliminate settlement risk for FX trades. Likewise, "always-on" liquidity and settlement can reduce the chance of flash crashes or after-banking hours distortions that often afflict the FX market.[15] On-chain FX transactions between Circle's USDC and Euro-denominated payment stablecoin, Euro Coin (EUROC), are available 24/7, carry lower fees, and have consistently traded within 0.05% of the USD-Euro exchange rate.[16]

Underpinning Dollar Primacy in the Digital Economy: De-dollarization in the fiat economy has increased in recent years as a result of greater non-USD integration and efforts by countries such as China and Russia to create non-USD settlement infrastructure outside the reach of U.S. sanctions and law enforcement.[17] By contrast, regulated, USD-denominated and -backed stablecoins like USDC import robust compliance measures and the rule-of-law to the digital asset space and ensure that the USD is the reserve currency of the digital economy, which helps to protect national security in line with recommendation 4 from the *Future of Money* report.

2. Goals, sectors, or applications where digital assets introduce risks or harms.

The last year has served as a benchmark not just of the utility value of blockchain-based payment services, but also of the risks that unregulated, opaque, and offshore digital asset firms can pose to consumers and financial markets. As the White House noted in January, however, the risks and behavior seen over the last year are neither novel nor inherent to the underlying cryptographic technology.[18] As a result, many of the most prominent risks in the digital asset space — such as market manipulation, fraud, antitrust, ponzi schemes, etc. — can be effectively mitigated by extending existing financial sector safety and soundness controls, prudential standards, consumer protection, and market conduct constraints to the digital asset sector. Novel risks created or amplified by digital assets include:

Privacy and Information Safeguard Risks: While introducing important benefits in transferability and traceability over physical cash, payment stablecoins create an immutable history of activity that facilitates profiling and targeting of individuals; can be exploited by hacks and cyber fraud; and, can be used for surveillance and unauthorized data collection by criminals and foreign governments. Experts note in the February 2023 St. Louis Federal Reserve Bank Review that, "in contrast to popular belief, permissionless blockchains are completely transparent. All confirmed transactions are publicly observable and stored as part of the blockchain's history."[19] The European Union – as part of efforts to assess the data privacy risks of blockchain technology –

[14] Bank for International Settlements, *FX settlement risk: an unsettled issue*, December 5, 2022, (https://www.bis.org/publ/qtrpdf/r_qt2212i.htm).
[15] Bank for International Settlements, *The sterling 'flash event' of 7 October 2016*, January 2017, (https://www.bis.org/publ/mktc09.pdf)/
[16] Liao, Adams, Lader, Puth, Wan, January 2023, "On-chain Foreign Exchange and Cross-border Payments."
[17] Wall Street Journal, February 2023, "Russia Turns to China's Yuan in Effort to Ditch the Dollar," (https://www.wsj.com/articles/russia-turns-to-chinas-yuan-in-effort-to-ditch-the-dollar-a8111457)
[18] White House, "The Administration's Roadmap to Mitigate Cryptocurrencies' Risks," January 27, 2023 (https://www.whitehouse.gov/nec/briefing-room/2023/01/27/the-administrations-roadmap-to-mitigate-cryptocurrencies-risks/).
[19] Matthias Nadler and Fabian Schar, Federal Reserve Bank of St. Louis Review, February 2023, "Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers," p.1.

has found that public-key information alone can enable the identification of an individual's real-world identity and create a pattern of transaction activity that can be used to single out users.[20] Circle offers recommendations below for public-private cooperation to strike the right balance in preserving individual privacy while still being able to maximize the benefits of blockchain transparency in order to trace illicit activity.

***Illicit Finance**:* While the use of virtual assets for money laundering still remains far below that of fiat currency,[21] 2022 saw a record volume of crime in the digital asset space, with more than $3.8 billion stolen in crypto hacks alone.[22] Based on Circle's review, this stems from two broad risk categories: 1) money laundering from illicit actors seeking to generate or launder the proceeds of crime; and the more prominent risk of 2) fraud, hacks, and other cyber crime directed at cryptocurrency users. Neither risk can be attributed entirely to blockchain technology and instead results from a combination of cybersecurity vulnerabilities, non-compliance with anti-money laundering and countering the financing of terrorism (AML/CFT) controls, and pooling of funds creating "honeypots" for criminals. The pseudonymous nature of blockchain allows for increased traceability using blockchain analytics but also provides a tool for non-compliant users or virtual asset service providers (VASPs) to obscure the movement of funds.

Offshore Exposure: As noted, the most prominent financial risks presented by digital assets already exist in the traditional financial sector. However, the inherently global reach of offshore VASPs amplifies the exposure of U.S. persons to illegal extraterritorial activity. These risks include traditional offshore illicit financial activities such as tax avoidance and obfuscation of beneficial ownership but also direct exposure to antitrust, fraud, money laundering, and market manipulation. These risks are further exacerbated by: the lack of domestic or international framework for digital identity management, particularly among peer-to-peer finance; weak or asymmetric data protection provisions; and differing cybersecurity standards.

***Cybersecurity Risks**:* The illicit finance risks resulting from hacks and cyber crime are most prominent where honeypots are accompanied with cybersecurity vulnerabilities, such as with cross-blockchain bridge protocols or decentralized autonomous organizations. Cross-blockchain transfers alone constituted more than 50% of all crypto crime in 2022 and remain an attractive source for cyber criminals.[23] Actors exploiting such vulnerabilities include cyber criminals and rogue nation-states such as the Lazarus Group, a cybercrime syndicate linked to North Korea.[24]

---

[20] European Parliamentary Research Service, July 2019, "Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?" (https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf).

[21] Treasury Department; February 2022 National Risk Assessment; (https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf), and the September 2022 Action Plan to Address Illicit Financing Risks of Digital Assets (https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf).

[22] Chainalysis, February 1, 2023, "2022 Biggest Year Ever For Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers," (https://blog.chainalysis.com/reports/2022-biggest-year-ever-for-crypto-hacking/).

[23] Chainalysis, February 1, 2023, "2022 Biggest Year Ever For Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers," (https://blog.chainalysis.com/reports/2022-biggest-year-ever-for-crypto-hacking/).

[24] Josh Smith, "Crypto hacks stole record $3.8 billion in 2022, led by North Korea groups - report," (https://www.reuters.com/technology/crypto-hacks-stole-record-38-billion-2022-led-by-north-korea-groups-report-2023-02-01/).

Financial Accessibility: Existing banking infrastructure has created economies of scale that provide transaction cost reductions in proportion to transaction size. However, these cost savings remain regressive: with the greatest efficiencies, discounts, accessibility, and optionality accruing only at the wholesale level. Consumers – particularly the roughly 1-in-5 un- or under-banked Americans[25] — and small businesses in turn pay far higher costs as a percentage of value on domestic and international transfers.[26] While payment stablecoins can lower those costs, a key risk to digital financial accessibility and inclusion is the degree to which the technology is built on, or requires access to, existing banking infrastructure. Requiring a bank account to establish a digital wallet, for example, imports existing socio-economic barriers and biases from the banking sector and transposes patterns of de-risking and de-banking to the digital space.

Environmental Risks*:* The sustainability of blockchain technology remains a comparatively poorly understood risk, with little reliable research assessing the risks across consensus mechanisms or the use of scalability tools such as Layer 2 protocols or rollup architecture.[27] As a result, energy usage estimates differ widely even within a single blockchain. Available data suggests that Proof-of-Work consensus mechanisms can use up to 100,000 times the energy per transaction as a credit card transaction.[28] On the other hand, Proof-of-Stake (PoS)-based transactions can be more than 100 times as energy efficient as a credit card transaction and even degrees-of-magnitude more when batching transactions. Ultimately, more research is needed to standardize risk metrics, understand the environmental impacts, and prioritize technologies to mitigate those risks.

3. Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets.

Circle recommends that the U.S. government introduce research focused on:

Compliant Privacy-Preserving Technologies: The risks accompanying identity management in the digital space exist on a spectrum, requiring an optimum balance that ensures authorities can adequately identify, trace, and prevent illicit activity while preserving consumer financial protections already enshrined in statutes like the Bank Secrecy Act (BSA). Circle recommends that the administration conduct research into technologies that preserve privacy for consumers without sacrificing AML/CFT controls or weakening standards that defend data from leakage or cyber-intrusion. As the 1999 Gramm-Leach Bliley Act makes clear, financial privacy and protections against undue exposure are fundamental rights that should be equally applicable to digital assets. Importantly, these competing risks demand a whole-of-government approach as they cross both policy functions and agency remits.

Given the transparency of most public blockchain infrastructure, users have been forced to rely on unregulated Privacy Enhancing Technologies (PETs) to retain privacy and protect personal

---

[25] FDIC; November 2022; "2021 FDIC National Survey of Unbanked and Underbanked Households;" (https://www.fdic.gov/analysis/household-survey/2021report.pdf).
[26] IMF; K. Kpodar and P. Amir Imam; "How Do Transaction Costs Influence Remittances?" p.8.
[27] Office of Science and Technology Policy, "Climate and Energy Implications of Crypto-Assets in the United States," (https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Crypto-Assets-and-Climate-Report.pd): 13.
[28] IMF Fintech Notes; June 7, 2022; "Digital Currencies and Energy Consumptions;" (https://www.imf.org/en/Publications/fintech-notes/Issues/2022/06/07/Digital-Currencies-and-Energy-Consumption-517866), p. 9.

identifying information (PII), rather than risk exposing sensitive data. PETs are intrinsically "dual-use," and further analysis is needed to lay out standards that preserve legitimate utility. Technical efforts to set standards have been fragmented and heterogeneous, creating a need for best-practices or government-led efforts, similar to NIST's ongoing Privacy Enhancing Cryptography project, focused on data preservation and transparency reference materials.[29] Alternatively, further research into how Layer-1 Zero-Knowledge Proof (ZKP) systems or stealth key setups,[30] harnessing elliptic curve cryptography,[31] could create BSA-compliant means to preserve privacy directly on-chain, in turn reducing the need for consumers to turn to PET solutions in the first place. OSTP should likewise explore the benefit of modernizing Gramm-Leach Bliley by establishing safeguards for centralized actors to avoid the mishandling of data during record-keeping. For example, technology used to collect IP addresses in order to abide by sanctions compliance laws can also aggregate user PII in unsafe ways, creating a data honeypot that is vulnerable to leakage or exploitation.[32]

Digital Identity Solutions: While the permissionless nature of digital asset technologies allows users to conduct transactions without intermediaries, they have also enabled a subset of actors to engage in money laundering, fraud, hacks, and cybercrime with on-chain pseudo-anonymity.[33] Further U.S. R&D on how best to incorporate digital identity tools into online systems – whether involving inherently public goods like a digital driver's license or private tools — would provide a verifiable and tested solution while allowing digital assets to remain scalable, accessible, and interoperable. Both third-party and open-source digital identity solutions can reduce some of the key risks and vulnerabilities identified in the Treasury Department's 2022 *National Money Laundering Risk Assessment* such as cross-border regulatory gaps and non-compliance.[34] Research on digital identity guidance for individual wallet owners, frameworks for credentialing, and the use of third-party KYC tools would also support a reduction in illicit finance while promoting standardization centered on U.S. regulations. Circle has taken the first steps in this effort with Verite, a set of digital identity standards that help users and institutions cryptographically prove claims about their identities to impede the activities of bad actors.[35]

Environmental Concerns: There remains a need for research into the environmental impact of various consensus mechanisms. Circle estimates, for example, that USDC transfers on the Ethereum blockchain required roughly 132.65 MegaWatt-hour (MWh) of energy to process more than 408 million transactions in 2022, equivalent to the running of only 400 refrigerators.[36] This reflects a cost of 6.366 Watt-hours (Wh) of energy per transaction, comparable to the average 1-5

---

[29] NIST Computer Resource Center, "Privacy-Enhancing Cryptography," (https://csrc.nist.gov/projects/pec).

[30] NOTE: A stealth key is a unique address, based off of a receiver's metakey, that allows the recipient to receive private transfers for each transaction without the recipient generating more keys. Elliptic Curve Cryptography is a form of Public Key Cryptography that allows for shorter public addresses while maintaining security. See FN. 29.

[31] Vitalik Buterin, "An incomplete guide to stealth addresses," (https://vitalik.eth.limo/general/2023/01/20/stealth.html).

[32] Getblock, "Blockchain RPC Provider That Won't Track You: Case of Getblock," https://getblock.medium.com/blockchain-rpc-provider-that-wont-track-you-case-of-getblock-6089028a423c.

[33] Chainalysis Team, "2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Hights Amid Surge in Sanctions Designation and Hacking," (https://blog.chainalysis.com/reports/2023-crypto-crime-report-introduction/).

[34] U.S. Department of the Treasury, "National Money Laundering Risk Assessment," https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf): 40-42.

[35] NOTE: Learn more at https://www.circle.com/en/verite.

[36] Ethereum estimates based on the 93.4% of USDC supply located on Ethereum and roughly 5.1% of Ethereum transactions involving USDC. Solana estimates based on an annualized energy cost of 746.738 MWHs and 2.7% of USDC supply.

Wh per credit card transaction estimated by the IMF.[37] By contrast, USDC running on the Solana network requires 0.9 Whs per transaction, consuming less energy than a *single* credit card transaction. Further research by OSTP and standardization of metrics across policy priorities like sustainability and scalability would help measure impact and support government and private efforts to utilize leading technology. This would account for efficiency gains from newer blockchains like Solana or catalog the effects of the transition to PoS on the Ethereum protocol, which recently reduced the network's carbon footprint by 99.98%.[38]

Financial Accessibility Technology: In order to harness the potential for digital assets to increase financial access, the U.S. government should focus R&D efforts on enabling technologies that facilitate payments in non-traditional and underserved contexts. For example, further research into Near Field Communication (NFC)-enabled hardware would allow users to access their digital cash without reliable internet infrastructure and bolster the ease of merchant integration.[39] Coupled with other technologies such as offline "cold-storage" wallets, these innovations could secure funds for disaster relief; support added security for those unable to access traditional banking services; and provide an alternative and safer form of value storage than physical cash.[40]

Cybersecurity Safeguards*:* Smart contract protocols — and in particular bridges — represent a critical but often vulnerable[41] piece of blockchain infrastructure, enabling digital asset interoperability between walled-off networks. While blockchains with sufficiently decentralized validation architecture are generally more secure against direct manipulation, research into more advanced protocol safety and soundness audits, as well as bug detection programs, would prevent exploits of more complex systems, similar to existing Systems and Organizations Controls compliance processes.[42] To solve problems inherent to smart contract bridges, Circle has been developing a new Cross-Chain Transfer Protocol (CCTP) which eliminates the honeypots caused by conventional bridges that amplify security risks.[43] The CCTP instead relies on cryptographic attestations that USDC on the source chain has been burned, minting native USDC at the sender's destination and providing a safer environment for the transfer of value across blockchains. Research into more generalizable standards for cross-chain bridging would help secure asset transfers and cut off a critical supply of illicit financing for America's adversaries.

4. R&D that should be prioritized for digital assets.

Circle suggests the following areas in which OSTP R&D could create cross-functional benefits:

---

[37] IMF Fintech Notes; June 7, 2022; "Digital Currencies and Energy Consumptions;" (https://www.imf.org/en/Publications/fintech-notes/Issues/2022/06/07/Digital-Currencies-and-Energy-Consumption-517866), p. 9.

[38] Digitconomist, "Ethereum Energy Consumption Index," (https://digiconomist.net/ethereum-energy-consumption).

[39] John Kiff, "Taking Digital Currencies Offline," (https://www.imf.org/en/Publications/fandd/issues/2022/09/kiff-taking-digital-currencies-offline).

[40] NOTE: Financial literacy remains a key barrier to accessibility, with a 2014 S&P Global Study estimating only 57% of Americans could be considered financially literate, even among users of financial products. R&D on interoperability involving consumer testing would help bridge this divide, complementing existing literacy initiatives such as OSTP's past Change the Equation, Equal Futures or Tech Inclusion Initiatives.

[41] Chainalysis Team, "Vulnerabilities in Cross-chain Bridge Protocols Emerge as a Top Security Risk," (https://blog.chainalysis.com/reports/cross-chain-bridge-hacks-2022/).

[42] AICPA, "SOC 2 - SOC for Service Organizations: Trust services Criteria," (https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report).

[43] Circle Internet Financial Developers, "Cross-Chain Transfer Protocol," (https://developers.circle.com/stablecoin/docs).

Efficient Post-Quantum Signatures for Blockchains: The U.S. government has taken a number of steps to fortify our economy and critical infrastructure against the emergence of quantum computing, which collectively help keep the U.S. economy at the forefront of technological innovation.[44] NIST's recent post-quantum standardization competition for digital signature schemes was an important first step but further research is needed to adapt the results to the requirements of public blockchains, given the special requirements for blockchain signatures.[45] Until then, quantum vulnerability in blockchain signatures remains a serious threat. To bolster U.S. national security, OSTP should support research designing novel, efficient, post-quantum signature schemes with short signatures that are at least as versatile as the current signature schemes used in the blockchain ecosystem.

Efficient Post-Quantum ZKPs: ZKPs are already used by PETs in the blockchain ecosystem. They allow users to prove useful statements about transactions, such as sanctions compliance, without leaking any private information. However, the current ZKP protocols are vulnerable to quantum algorithms, and any nation or organization that successfully constructs a quantum computer with approximately 3,000 logical qubits would be able to almost instantly compromise applications that use ZKPs. While post-quantum ZKP solutions already exist, they are too inefficient to compete with their more widely used counterparts. Additionally, existing post-quantum ZKP solutions are currently prohibitively costly for real-world applications. Public blockchains generally seek to minimize the computation, storage, and network bandwidth requirements of network operation to maximize node decentralization, and R&D could help design more efficient and secure post-quantum ZKPs for use.

Cryptographic Protocols with Selective Auditing: Mirroring existing BSA standards, financial regulators want to be able to verify that risk management processes and specific transactions meet a certain set of conditions pertaining to financial crimes compliance without receiving information about all lawful transactions. Cryptographic tools based on indistinguishability obfuscation could allow software developers to generate special keys for regulators to check whether blockchain transactions meet certain policies, e.g. "transactions do not include funds originating from X blacklist AND transactions do not include amounts greater than $10,000." Such capabilities would help financial institutions more easily verify blockchain transaction compliance with regulations while preserving the financial privacy of their users without fear of noncompliance with financial regulations.

The same building blocks could also lead to other powerful solutions, such as selective broadcast encryption where a transaction originator could identify specific parties that can read the full information of the transaction. OSTP should consider advancing research into the application of multilinear maps to generate bit-fixing pseudo-random functions as a first step toward creating these tools. Such research would in parallel support development of ZKPs that take transaction details, such as origin or amount, needed to verify compliance with AML rules. The output of the ZKP would then be verified by the regulator or financial institution, which would use a

[44] President Biden recently signed the Quantum Computing Cybersecurity Act which aims to promote research and development of quantum computing and cybersecurity in the United States, and the NSA recently set a 2035 deadline for the adoption of post-quantum cryptography across all national security systems.

[45] For more information about the NIST competition, *see NIST Announces First Four Quantum-Resistant Cryptographic Algorithms*, Jul. 5, 2022, https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.

corresponding set of multilinear maps to check that the proof is valid without requiring access to any further details about the transaction itself. If the proof is valid, the institution, regulator, or law enforcement would have a high degree of confidence that the transaction is compliant with the relevant AML rules, without the potential for spillage of transaction details.

5. Opportunities to advance responsible innovation in the broader digital assets ecosystem.

The advancement of the digital assets ecosystem depends on the development of legal, regulatory, and supervisory models that encourage innovation while ensuring financial stability, protecting consumers, and preventing illicit finance. The U.S. should advance open and democratic principles in the digital assets ecosystem and lead in developing frameworks to create a safe and thriving marketplace for the innovations that protect the rights and interests of end users. To ensure responsible growth, consumer protection, and robust industry oversight, OSTP should focus on three key elements:

1) **The passage of legislation to bring privately-issued dollar digital currencies into the U.S. regulatory perimeter and create an acceptable supervisory framework for these novel technologies, products, and services.** Legislation should include high prudential and conduct standards for digital currency issuers, such as capital, liquidity, cybersecurity, bankruptcy, safety and soundness, and consumer protection rules. Consultations with industry during the rulemaking process following legislative passage would help ensure sound regulation and help shape the international regulatory landscape.
2) **The protection of the rights of end users with safeguards to protect citizens' use of open, secure, and transparent public blockchains and their privacy on those blockchains.** Fundamental American values such as the right to individual privacy, and freedom from unwanted data collection by governments or large corporations should guide efforts to protect users in the digital asset ecosystem. Both government and industry have an obligation to ensure that consumers are protected from harm and informed about their rights and choices when interacting with new technologies and platforms.
3) **The creation of durable frameworks for novel and rapidly evolving technologies.** The regulatory and supervisory frameworks that are ultimately created should be neutral to rapidly changing technologies and new market entrants. Oversight should include the active education and upskilling of regulators; consultation and collaboration with industry through regulatory sandbox efforts; rules to encourage fair market conduct; and public-private partnerships to educate the general public about the design and applications of digital asset technologies and financial services.

Engaging with International Standard-Setting Bodies to Enshrine American Values: The U.S. benefits from a diverse financial services sector, and its capital markets are the largest and most mature in the world due to a combination of legal and regulatory clarity and efficient and competitive markets and capital formation. As such, the U.S. should lead and frame the regulatory dialogue on innovative financial services in international fora and with global standard-setting bodies, such as the BIS, Financial Stability Board, and the the Financial Action Task Force. With the certainty afforded by legislation and regulation, Circle and other responsible industries would be better positioned to promote and defend American standards.

Circle believes that U.S. policymakers and regulators should leverage their participation in international standard setting bodies to ensure USD primacy in international markets and foster

democratic values in the digital economy, such as openness, diversity, and competitiveness. U.S. leadership will be particularly important in striking a global balance between privacy from surveillance and AML/CFT compliance, such as with development of digital ID management; interoperability of public blockchains and wallets; and privacy-preserving compliance tools and enablers such as ZKPs or digital asset mixers. As these technologies proliferate, U.S. leadership in digital asset markets and blockchain-based payments systems will be crucial to the development of standards that can serve as a bulwark against authoritarian regimes which pursue top-down, invasive, and potentially coercive systems using digital assets.

Promoting Resilience and Countering Repression in the Global Digital Economy: As more than 100 countries explore central bank digital currencies (CBDCs) and cross-border CBDC settlement, several countries and international organizations have emerged as leaders in shaping the standards and application of cross-border blockchain infrastructure due to their "first mover" status. Notably, China and other countries are designing and/or piloting their own CBDCs and using the experience and expertise gained to directly feed into the supra-national efforts of organizations like the BIS to design interoperable cross-border CBDC systems.[46] China's central bank, the People's Bank of China, has been a lead collaborator in Project mBridge at the BIS, facilitating the use of its pilot CBDC, the eCNY (e-yuan or e-renminbi) in cross-border trade and investment flows, and driving interoperability between its CBDC system and that of other neighboring states.[47] The U.S. and its allies should actively engage in discussions to prevent de-dollarization and the "soft influence" that imports weak data and privacy controls, sanctions agnosticism, and state-controlled market entry into the global infrastructure governing digital assets and CBDCs.

Promoting Digital Financial Literacy: Alongside these concerns, the U.S. government should seek out ways to make nascent digital asset markets efficient, competitive, and straightforward for end users.[48] Existing financial architecture is built on familiar, but nearly 50-year old standards, and the relative youth of blockchain technology and services related to digital assets has exposed disparities that are not as readily visible in traditional financial services. For example, it can create challenges to both users and regulators in understanding the overlap with existing financial services, particularly in the peer-to-peer space. As digital asset markets mature, the U.S should devote resources and research to determine the ways in which digital asset market participants can make their offerings more accessible; disclose to consumers the potential risks associated with digital assets (including their custody and exchange); and how digital asset platforms can transparently, securely, and easily offer their services to consumers.

[46] Project mBridge: Connecting economies through CBDC, https://www.bis.org/publ/othp59.htm, The Bank for International Settlements. Published: October 26, 2022.
[47] Project mBridge: Ibid.
[48] For an example of digital asset financial literacy initiatives, see: https://www.circle.com/en/pressroom/circle-brings-crypto-literacy-curriculum-to-hbcus-with-circle-u