CATO INSTITUTE | CENTER FOR MONETARY AND FINANCIAL ALTERNATIVES

March 3, 2023

Rachel Wallace
Deputy General Counsel
Office of Science and Technology Policy
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, DC 20504

Re: *Document Number: 2023-01534*
Request for Information; Digital Assets Research and Development

Dear Ms. Wallace:

My name is Jack Solowey, and I am a financial technology policy analyst at the Cato Institute's Center for Monetary and Financial Alternatives. I appreciate the opportunity to comment on the Office of Science and Technology Policy's (OSTP's) Request for Information regarding Digital Assets Research and Development (RFI).[1] The Cato Institute is a public policy research organization dedicated to the principles of individual liberty, limited government, free markets, and peace, and the Center for Monetary and Financial Alternatives focuses on identifying, studying, and promoting alternatives to centralized, bureaucratic, and discretionary financial regulatory systems. The opinions I express here are my own.

The RFI posed several important questions regarding the research and development of digital assets to further responsible innovation in line with American values. This letter specifically addresses topics 1, 2, and 4.

* * *

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

Cryptographically secure software—including private cryptocurrencies and the distributed ledgers that enable them (crypto technology)—can not only be tools for enhanced financial infrastructure, but also for furthering democratic civil society.[2]

[1] Office of Science and Technology Policy, "Request for Information; Digital Assets Research and Development," 2023-01534, 88 FR 5043, January 26, 2023.
[2] The following summaries of a few key applications that can be enhanced by crypto technology should not be taken as an exhaustive survey.

Enhanced private financial infrastructure

At a basic level, cryptocurrencies enable faster transaction settlement times, allowing fund transfers to occur within minutes instead of days, as is typical of legacy payment rails.[3] In addition, cryptocurrencies facilitate borderless international payments.[4] While these benefits often are held out as either speculative or immaterial, with the charge leveled that cryptocurrencies serve no real-world function, their utility has been revealed in high-stakes situations where practicality is the primary criterion.

Within one month of Russia's invasion of Ukraine, crypto donations to Ukraine reached nearly $100 million.[5] Fast, cross-border settlement times were a critical part of cryptocurrencies' appeal. According to Ukraine's Deputy Minister of Digital Transformation, in the early days of the war, Ukraine's national bank was "not really operating" and crypto donations were "essential," due in no small part to "fast transfers" that got "results almost immediately."[6] Throughout the world—from Venezuela to Vietnam—cryptocurrencies have been valued for their utility as an alternative to deficient traditional financial institutions.[7]

Crypto transfers can work in the absence of a functioning central bank because they enable peer-to-peer transactions that settle directly on distributed public ledgers without necessary reliance on intermediaries.[8] These technologies also enable decentralized marketplaces for financial instruments, which mitigate by design the classic risks that financial intermediaries present to trustworthy asset custody and faithful trade execution.[9] Decentralized crypto exchanges (DEXs) allow users to self-custody their assets (i.e., control their holdings with their own private keys) and to arrange transactions with a series of smart contracts (i.e., software designed to self-execute when specific conditions are satisfied), mitigating risks of theft and fraud by middlemen.[10] As my colleague Jennifer Schulp has explained, "while DEXs do have human programmers, DEXs do not rely on a middleman keeping his word because they are composed of smart contracts that are open and auditable."[11]

---

[3] Nicholas Anthony, "Congress Should Welcome Cryptocurrency Competition," Cato Institute Briefing Paper no. 138, May 2, 2022.
[4] Nicholas Anthony, "What Do Cryptocurrencies Mean for Liberty?" *Cato at Liberty* (blog), Cato Institute, January 7, 2022.
[5] Illia Polosukhin, "How Cryptocurrency Is Helping Ukraine," *Wall Street Journal*, March 23, 2022.
[6] Id.
[7] Jennifer J. Schulp et al., "Overstating Crypto Crime Won't Lead to Sound Policy," *Cato at Liberty* (blog), Cato Institute, January 27, 2023.
[8] See Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System.
[9] See Jack Solowey and Jennifer J. Schulp, "What Congress Should Do about Crypto Exchanges," *Cato at Liberty* (blog), Cato Institute, December 15, 2022.
[10] Id.
[11] Jennifer J. Schulp, "Testimony Before the United States Senate Committee on Banking, Housing, and Urban Affairs Hearing on "Crypto Crash: Why the FTX Bubble Burst and the Harm to Consumers'," December 14, 2022.

Achieving financial policy goals of individual autonomy and data portability

In the United States, crypto technology already has made great strides toward achieving longstanding domestic policy goals. Since the passage of the Dodd-Frank Act in 2010, realizing "open-banking" goals (i.e., that consumers should have default access to their own financial transaction data) has been a U.S. policy objective.[12] Final rules on the subject are expected no sooner than 2024.[13] Recently, Consumer Financial Protection Bureau (CFPB) Director Rohit Chopra summarized well the goals of open banking and consumer financial data portability. These included "a decentralized, open ecosystem," a diminished ability for "incumbents to build moats and for middlemen to serve as gatekeepers," that no one person or entity "'owns' critical infrastructure," and achieving "more seamless integration."[14]

These very priorities describe some of the core capabilities of decentralized finance (DeFi) enabled by crypto technology.[15] Cryptocurrencies are natively decentralized, with transactions not recorded by trusted intermediaries but by a global network of computers incentivized to validate a cryptographically secure distributed ledger (a blockchain).[16] Cryptocurrencies are permissionless, with users free to self-custody their assets and access their complete, pseudonymous transaction histories without relying on middlemen.[17] Financial rails based on open-source, decentralized software protocols are perhaps the first true alternative to critical financial infrastructure being "owned" by one person or entity.[18] Lastly, crypto projects are composable, as open-source software allows protocols and applications to be more readily interoperable.[19]

Furthering democratic civil society

These same features and capabilities not only serve to further U.S. financial policy goals, but also democratic civil society at home and abroad.[20] The permissionless, pseudonymous, and censorship resistant properties of blockchains make them strong tools for securely recording information essential to civic life. For example, when law enforcement pressured the pro-democracy *Apple Daily* newspaper in Hong Kong to shutter in connection with the Chinese Communist Party's application of an authoritarian "national security law," private individuals

---

[12] 12 U.S.C. § 5533. See also Jack Solowey, "A Tale of Two Documents: How the Bitcoin White Paper Outperformed Dodd-Frank," *Cato at Liberty* (blog), Cato Institute, November 4, 2022.
[13] Rohit Chopra, "Director Chopra's Prepared Remarks at Money 20/20," Consumer Financial Protection Bureau, October 25, 2022.
[14] Id.
[15] Jack Solowey, "A Tale of Two Documents: How the Bitcoin White Paper Outperformed Dodd-Frank," *Cato at Liberty* (blog), Cato Institute, November 4, 2022. See also Jack Solowey, "Crypto's Useful Future Was Vivified By the Correction," *RealClearMarkets*, August 23, 2022.
[16] Id.
[17] Id.
[18] Id.
[19] Id.
[20] Jack Solowey, "America, Don't Be the Anti-Network State: Crypto Policy for the Leader of the Free World," *Cato at Liberty* (blog), Cato Institute, December 22, 2022.

were able to backup archives of the journalistic outlet using secure blockchain technology.[21] In the U.S., blockchain technology has been leveraged to preserve the testimony of genocide survivors.[22] Critically, the RFI asks how a digital asset ecosystem can both embody and further democratic values. The answer is through private crypto technology that supports the preservation of vital political and historical speech, expression, and witness.

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

Private sector innovation can address cybersecurity risks

No technology is perfect, and it is unwise to ignore software vulnerabilities generally. While the cryptographically secure distributed ledgers at the heart of cryptocurrencies, such as the Bitcoin blockchain, have historically resisted hacking, aspects of the crypto ecosystem such as bridges (for communicating across blockchains) and smart contracts (as described above) have been vulnerable to attack.[23] Crypto technologies do not "introduce" these risks so much as, like other networked software, experience them to varying degrees.

The question then is how to address or mitigate these risks. Here, the crypto ecosystem has native resiliencies that should be embraced, not thwarted. The permissionless and composable qualities of open-source software can support ongoing iterative improvements and the dissemination and adoption of best practices.[24] Moreover, the public nature of crypto protocols makes them auditable by design, facilitating threat detection and identification of patchable vulnerabilities. Therefore, diminishing the speed of the iteration cycle and the default openness of the U.S. crypto ecosystem (e.g., through prescriptive regulations that create prior restraint, or regulation by enforcement that nudges innovation in crypto technology out of the U.S.) also can diminish the development of cybersecurity safeguards in the U.S.

Central Bank Digital Currencies are not compatible with a free and democratic society

The risks that Central Bank Digital Currencies (CBDCs) present to a free and democratic society vastly exceed any potential benefits. A CBDC (i.e., a digital national currency that is a direct liability of the Federal Reserve) should not be developed in the United States.[25]

---

[21] Pak Yiu, "Hong Kong's Apple Daily to live on in blockchain, free of censors," *Reuters*, June 24, 2021. See also Javier C. Hernández, "Harsh Penalties, Vaguely Defined Crimes: Hong Kong's Security Law Explained," *New York Times*, June 30, 2020.

[22] "Starling Lab: Establishing Trust for Humanity's Data," Filecoin, June 10, 2021.

[23] Jack Solowey, "Dissent Is a Part of Crypto," *Cato at Liberty* (blog), Cato Institute, August 19, 2022 citing Is Bitcoin secure? Has this network ever been hacked?" Coinbase, last visited March 2, 2023. See also "Blockchain bridges," Ethereum, last updated March 1, 2023; "Introduction to Smart Contracts," Ethereum, last updated September 1, 2022; and Corin Faife, "Nomad crypto bridge loses $200 million in 'chaotic' hack," *The Verge*, August 2, 2022.

[24] Jack Solowey, "Dissent Is a Part of Crypto," *Cato at Liberty* (blog), Cato Institute, August 19, 2022 citing Sonal Chokshi et al., "Bridge Hack, Wallet Hack," *Web3 with a16z* (podcast), August 11, 2022.

[25] Nicholas Anthony and Norbert Michel, "Central Bank Digital Currency," Cato Institute Briefing Paper no. 145, January 10, 2023.

As my colleagues Norbert Michel and Nicholas Anthony explain, the purported benefits of a CBDC are outweighed by serious risks across several areas of concern: financial inclusion, faster payments, the dollar's status as the global reserve currency, monetary and fiscal policy, financial privacy, financial freedom, private enterprise, and cybersecurity.

With respect to financial inclusion, a CBDC would not resolve, and would risk exacerbating, the privacy and trust concerns that lead some Americans to eschew bank accounts.[26] A CBDC also would provide no unique advantage in faster payments over existing private financial technology solutions, such as stablecoins or the Real-Time Payments (RTP) Network.[27] Moreover, the dollar's reserve currency status is due to the strength of the U.S. economy, rule of law, and property rights; another central bank merely deploying a CBDC while the Federal Reserve refrains from doing so is unlikely to jeopardize the dollar's reserve currency status, particularly where those other central banks are in jurisdictions with weak or nonexistent legal protections.[28]

That the central bank could use a CBDC to impose negative interest rates or penalize savings is a threat to financial autonomy and property rights.[29] In addition, a CBDC would risk undermining retail banking, both by limiting private banks' ability to extend credit due to decreased consumer deposits, as well as by creating run risks where a CBDC serves as a substitute for private banks during times of stress.[30] What's more, a CBDC would be a prominent target for hackers, and a single federal database would pose even greater cybersecurity risk than would the potential breach of a private financial institution with limited market share.[31]

A CBDC would further erode Americans' limited financial privacy, giving the federal government direct visibility into Americans' financial lives. In addition to Orwellian surveillance risk, a CBDC would provide the federal government with "countless opportunities . . . to control citizens' financial transactions," risking levels of control over private economic and civic life that are fundamentally incompatible with a liberal democratic society.[32]

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

This letter identifies research areas worth the attention and consideration of the OSTP to support the Office's advisory mission in light of the whole-of-government approach to digital

[26] Id. at 2, citing Federal Deposit Insurance Corporation, "2021 FDIC National Survey of Unbanked Households," October 2022.
[27] Id. at 2.
[28] Id. at 2 citing Christopher Waller, "The U.S. Dollar and Central Bank Digital Currencies," Board of Governors of the Federal Reserve System, October 14, 2022.
[29] See Id. at 2-3.
[30] Id. at 3 citing Lael Brainard, "Cryptocurrencies, Digital Currencies, and Distributed Ledger Technologies: What Are We Learning?," Board of Governors of the Federal Reserve System, May 15, 2018.
[31] Id. at 3.
[32] Id. at 3.

assets underway pursuant to Executive Order 14067, "Ensuring Responsible Development of Digital Assets."[33] The research priorities included in this response are not intended to be exhaustive, nor should they be construed as support for taxpayer-subsidized risk taking. To the contrary, the techniques and applications discussed below already have been advanced through private research and development.[34] Consistent with OSTP's mission, the Office should explore these areas by engaging with external partners—in both the for-profit and non-profit sectors—in a learning capacity in order to be able to advise the President and the Executive Office of the President on risk-based digital asset policy. Lastly, the OSTP should bear in mind the inherent unpredictability of disruptive innovations before drawing firm conclusions on the ultimate course of the crypto ecosystem's evolution.[35]

Zero-knowledge technologies

The RFI identifies zero-knowledge (ZK) proofs as a potential privacy-enhancing technology (PET). ZK proofs are indeed critical to the advancement of PET research and development. In addition, the OSTP should consider the potential of ZK proofs and related technologies to further additional goals of the crypto ecosystem: disintermediation, democratization of infrastructure governance, and financial inclusion.

ZK proofs enable a party (the prover) to prove the validity or truth of a statement to an additional party (the verifier) without having to disclose further information beyond that the statement itself is true.[36] Such "statements" can include that the prover is in possession of certain knowledge (e.g., personally identifying information (PII), a credential, or private key), which in turn can be used to verify the prover's identity without requiring the disclosure of specific PII to the verifier. Here, the potential of ZK proofs as a PET are on full display, as an individual can prove his or her identity, or an aspect of thereof, without having to reveal more PII than necessary, helping to mitigate both privacy and security risks. A common demonstrative example is that ZK proofs would enable an individual to prove that his or her age meets or exceeds a relevant threshold (e.g., voting age) without having to reveal one's exact date of birth to the verifier.

ZK proofs' ability to verify statements without revealing those statements' contents also can help to improve the scalability and overall decentralization of crypto networks. In essence, the statement that a ZK proof would be validating in that context is the proper execution and recording of a transaction over a cryptocurrency network (e.g., that a cryptocurrency transfer

[33] Executive Office of the President, "Ensuring Responsible Development of Digital Assets," E.O. 14067, 2022-05471, 87 FR 14143, March 14, 2022.
[34] See "What are zero-knowledge proofs?" Ethereum, March 1, 2023; and Colin Harper, "Multisignature Wallets Can Keep Your Coins Safer (If You Use Them Right)," *CoinDesk*, November 10, 2020.
[35] See Jack Solowey, "Don't Push Crypto Offshore, Don't Outlaw Disruptive Innovation," *Cato at Liberty* (blog), Cato Institute, February 24, 2023.
[36] "What are zero-knowledge proofs?" Ethereum, March 1, 2023; and Glossary: Zero-Knowledge Proof, Computer Security Resource Center, National Institute of Standards and Technology, U.S. Department of Commerce, last visited March 2, 2023.

has not involved double spending of the same tokens).[37] This can improve a crypto network's scalability in multiple ways.

For example, such proofs can be leveraged to process verifiable transactions using computing resources beyond the nodes composing primary (i.e., layer 1) blockchains, improving throughput while providing a method to validate transactions' legitimacy before they are recorded to those layer 1 blockchains.[38] In addition, ZK technology and related cryptography can enable the further development and adoption of light clients—crypto network nodes that are less capital and resource intensive.[39] While designs vary, light clients can verify transaction records without needing to download or store complete copies of a blockchain, as a full node would.[40]

The OSTP wisely prioritizes the advancement of democratic values and financial inclusion in its RFI. Crypto network scaling and light client solutions enabled by ZK technology could support both priorities. Increased transaction processing capacity directly addresses a core critique of crypto networks: that they have limited ability to process large numbers of transactions per second.[41] The benefits of crypto payments and DeFi—as discussed in response to topic 1 above—can become more widely available where those constraints are overcome.

Similarly, light clients have the potential to open participation in crypto networks to a broader group of individuals by making the ability to run a node less capital intensive. Light clients could help nodes run on ubiquitous consumer-grade devices, like notebooks, tablets, and smartphones, as opposed to hardware requiring specialized Graphics Processing Units (GPUs) and Application-Specific Integrated Circuits (ASICs) that support certain full nodes.[42] Not only would this have financial inclusion benefits, but also could serve to further democratize participation in network design, as more individuals from more diverse backgrounds became able to choose the software clients on a crypto network.[43]

In terms of advancing U.S. competitiveness and leadership, light clients are just one example of crypto technologies devolving infrastructure decisions to network edges. Where global adoption of decentralized software protocols continues apace, those concerned with seeing U.S. interests represented in the architecture of global financial infrastructure should be wary

---

[37] See Zero-Knowledge Rollups: Validity proofs, Ethereum, last updated January 23, 2023.
[38] "What are zero-knowledge proofs? Verifiable computation," Ethereum, last updated March 1, 2023.
[39] See "Nodes and Clients: Light node," Ethereum, last updated February 3, 2023. See also Polygon, "How Zero Knowledge Proofs, Aggregation Layers, and Light Nodes Can Improve Web3 Experience and Structure?," *Medium*, November 23, 2022.
[40] Id. See also, Vitalik Buterin, "Re: My first impressions of web3," Reddit, January 8, 2022; and Etan Kissling, "Light Clients After the Merge," Devcon Archive (video), October 14, 2022.
[41] "Scaling," Ethereum, last updated January 5, 2023.
[42] See "Blockchain client types," Coinbase, January 26, 2022. See also "Nodes and Clients: Light node," Ethereum, last updated February 3, 2023; and Polygon, "How Zero Knowledge Proofs, Aggregation Layers, and Light Nodes Can Improve Web3 Experience and Structure?," *Medium*, November 23, 2022.
[43] Jack Solowey, "Don't Push Crypto Offshore, Don't Outlaw Disruptive Innovation," *Cato at Liberty* (blog), Cato Institute, February 24, 2023.

of the risks of an unfavorable regulatory climate nudging crypto activity offshore. Americans being represented in the governance of crypto networks requires crypto policy that allows Americans to participate—as entrepreneurs, developers, and users—in those very same crypto networks.[44]

Multi-signature technologies

The RFI aptly identifies the importance of digital asset security. The OSTP should consider the ability of multi-signature arrangements to enhance security in the crypto ecosystem. This includes risks related to digital asset holdings, as well as to unauthorized modifications of protocol software.

Multi-signature (or multisig) methods help to secure crypto transactions and networks by requiring that two or more private key holders sign crypto transactions before they are executed or authorize access to crypto wallets or smart contracts.[45] These methods can be readily analogized to those for securing physical facilities, like vaults, with locks that require multiple different keys held by multiple different parties to permit access. Whether it's physical keys unlocking a vault made of steel-reinforced concrete, or private keys for signing crypto transactions, dispersing keys to multiple holders helps to reduce the risks of unauthorized access or tampering. In the software context, multisig arrangements can be set with different parameters. For example, two out of three private keys may be required to sign a transaction, which mitigates risks from unauthorized access, as well as from a lost key resulting in permanent asset loss.

Multisig methods also can be used to support different use cases within the crypto ecosystem. Gating a crypto wallet with multiple keys can enable a form of secure account recovery. On a broader scale, similar arrangements can be used to support secure crypto asset custody by centralized crypto exchanges, helping to guard customer assets against the types of risks exemplified by the mismanagement of FTX.[46] In addition, multiple signatures can be required before deploying upgrades to a crypto network's core code, which can not only help to prevent malicious activity but also to formalize governance procedures of decentralized projects, imposing limits on discretionary changes.

* * *

[44] Id.

[45] See Colin Harper, "Multisignature Wallets Can Keep Your Coins Safer (If You Use Them Right)," *CoinDesk*, November 10, 2020.

[46] See Jack Solowey and Jennifer Schulp, "Don't punish crypto for the sins of SBF's FTX," *New York Daily News*, November 29, 2022.

Thank you for the opportunity to comment on a national digital assets research and development agenda. I am happy to answer any questions or further engage on this topic.

Sincerely,

Jack Solowey
Financial Technology Policy Analyst
Center for Monetary and Financial Alternatives
Cato Institute