# Crypto Council for Innovation

March 3, 2023

Dr. Arati Prabhakar
Director, Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, D.C. 20504

*Re: Request for Information regarding Digital Assets Research and Development, 88 FR 5043*

Dear Dr. Prabhakar:

The Crypto Council for Innovation ("CCI") submits this letter in response to a request for information regarding Digital Assets Research and Development, 88 FR 5043.[1] CCI appreciates the opportunity to share its information, expertise, and views on this vital issue. Digital assets represent one of the most significant innovations in finance—and beyond—in many years, with the potential to alter ownership structures, commercial applications, cross-border payments, transaction processing and settlement, access to capital, investment opportunities, and much more. These developments contribute to equitable growth and financial inclusion, as well as investor and consumer choice and security. The development of the digital assets ecosystem, therefore, is an important question for policymakers.

**SUMMARY**

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

- Technological innovation should improve access, efficiency, and equity and empower the average consumer.
- Technical standards should be interoperable and open to facilitate permissionless and composable systems.
- Anti-money laundering regulations should be precise in order to stop illicit activities and there should be privacy-preserving technologies that respect

[1] https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development

national security interests.[2]

Advancements in blockchain technology infrastructure will be key to the evolution of our global financial system. It is paramount that the U.S. remains at the center of this technological leap in digital evolution if we are to maintain our monetary, economic, and political preeminence in the global theater.

## ABOUT CCI

CCI is an alliance of digital asset industry leaders with a mission to communicate the benefits of crypto and demonstrate its transformational promise. CCI members include some of the leading global companies and investors operating in the digital asset industry, including Andreessen Horowitz, Block (formerly Square), Coinbase, Electric Capital, Fidelity Digital Assets, Gemini, Paradigm, OpenSea, and Ribbit Capital, and Spruce Systems. CCI members span the crypto ecosystem and share the goal of encouraging the responsible global regulation of digital assets to unlock economic potential, improve lives, foster financial inclusion, protect national security, and disrupt illicit activity.

## DISCUSSION

### SECTION I: Goals, sectors, or applications that could be improved with digital assets and related technologies

Digital asset research and development can enhance U.S. performance in an increasingly digitized global economy. Rather than focusing on decentralized finance (or DeFi) as an end-state, U.S. policymakers should consider how *decentralized technology stacks* could make financial infrastructure and processes more dynamic, resilient, nimble, and composable. Such an approach to digital infrastructure development will help build the digital assets ecosystem as well as help expand the benefits of the nascent DeFi ecosystem to the broader U.S. consumer economy and spur productivity and innovation for a wider sector of the population.

*Strengthen decentralized technology infrastructure*

The Office of Science and Technology Policy should support funding a series of decentralized financial infrastructure research pilots, conducted in controlled academic environments or through partnerships with research institutions. The pilot research areas should focus on the following use cases:

- Decentralized Exchange Platforms: In this use of decentralized finance, a platform composed of smart contracts allows participants to trade directly between assets without

[2] *See* CCI's Global Regulatory Blueprint in its comment letter to the Financial Stability Board.

any fear of counterparty risk. This type of trading makes it easier for people to trade more quickly and efficiently. OSTP should direct funding toward the development of a testnet blockchain platform run by a consortium of U.S. universities to experiment with various decentralized exchange designs.The research should also explore how retail shareholders can vote directly rather than the current proxy system of voting by mostly large institutional advisors.[3]

- Humanitarian Aid Distribution: The relative speed and efficiency of decentralized finance systems compared to conventional finance should be leveraged for disbursements of humanitarian aid in environments where banking systems are weak or unusable due to natural disaster, war, or political instability. There are multiple real-world examples of crypto-asset funding efforts delivering needed resources in a humanitarian crisis, such as during the beginning of the Russian invasion of Ukraine and after the devastating earthquakes in Turkey and Syria.[4] U.S. academic institutions should partner with the U.S. Agency for International Development to run a pilot that identifies and tests various scenarios of aid distribution. This pilot could help determine technological and operational features to improve global aid distribution.

- Tokenization of Traditional Financial Assets: An innovative way to improve current financial systems would be to apply decentralized finance to established asset classes that are already well-understood and highly regulated. In this research effort, OSTP should work with prudential financial regulators to inform multiple asset tokenization pilots in an academic testnet environment. In each pilot, academic researchers should construct smart contracts that align with and enforce current regulatory requirements for financial products and services. Central banks and mainstream commercial banks around the globe are already experimenting with asset tokenization, such as the New York Fed's recent proof-of-concept with global banks and the SWIFT organization to transfer regulated liabilities over a blockchain ledger.[5] Also, Project Dunbar, led by the Bank for International Settlements (BIS) Innovation Hub in partnership with the central banks of Australia, Malaysia, Singapore, and South Africa, is testing the use of central bank digital currencies (CBDCs) for improving international settlement.[6] Another project is Project Guardian, the Monetary Authority of Singapore's collaborative initiative with the financial industry that seeks to test the feasibility of applications in asset tokenization and decentralized finance (DeFi) while managing risks to financial stability and integrity.[7] These types of experiments are likely to increase globally, especially as the People's Republic of China is leading other multilateral pilots to use blockchain technology for

[3] https://corpgov.law.harvard.edu/2019/11/19/retail-shareholder-participation/
[4] https://cryptoforinnovation.org/crypto-and-humanitarian-aid-reducing-costs-and-improving-speed/; https://cryptoforinnovation.org/crypto-case-study-ukraine/; https://blog.chainalysis.com/reports/cryptocurrency-donations-provide-fast-relief-for-turkey-syria-earthquake-victims/#:~:text=Additionally%2C%20crypto%20businesses%20Binance%2C%20Tether,Turkey%20affected%20by%20the%20earthquakes
[5] https://www.newyorkfed.org/aboutthefed/nyic/facilitating-wholesale-digital-asset-settlement
[6] https://www.bis.org/about/bisih/topics/cbdc/dunbar.htm
[7] https://www.mas.gov.sg/schemes-and-initiatives/project-guardian

cross-border wholesale payments.[8] Failure to stay ahead of innovation on this front may detrimentally affect the United States' ability to conduct R&D in the future.

- Blockchain research on public sector use-cases: Blockchain or distributed ledger technologies provide significant benefits outside of the digital assets space. In this research effort, OSTP should identify the areas where it is appropriate and beneficial to enable and invest in distributed ledger technologies within government agencies. This will identify the technological resources needed at federal government agencies and key use cases for such technology in these agencies. For example, this could include supply chain management purposes (similar to those mentioned above regarding humanitarian aid), data management, personal identity verification (digital identities), and regulatory reporting purposes.

**SECTION II: Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets**

*Ramp up cybersecurity resilience and public-private partnerships*

To mitigate the risks of illicit finance relating to digital assets, the U.S. government cyber agencies should prioritize research into cybersecurity resilience within the crypto-asset ecosystem in order to develop standards and institutions to safeguard users and their assets. Also, U.S. federal law enforcement should partner with the private sector to enhance research on cybercriminal networks and strategies to counter them. The following are key research areas that the U.S. should support:

- Bridge security: The Office of Critical Infrastructure Protection and Compliance Policy (OCIP) at the Department of Treasury, the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security, and the Office of the National Cyber Director at the White House should collaborate to conduct a study on the vulnerabilities and viability of DeFi bridge platforms. Hacks of bridges accounted for almost $2 billion in stolen crypto-assets in 2022.[9] Importantly, engagement with the private sector can yield potential solutions, such as collaboration with Self-Regulatory Organizations (SROs) and white-hat hacker groups. SROs like Financial Industry Regulatory Authority (FINRA) and New York Stock Exchange (NYSE) have long worked with their government counterparts to enforce governance.[10] In February 2023, the DeFi platform Oasis.app was able to recover $140 million in hacked crypto funds based on a back door discovered by a group of white hat hackers.[11] The joint agency cyber study

[8] https://www.lawfareblog.com/mbridge-somewhere-central-banking-having-its-sputnik-moment
[9]https://blog.chainalysis.com/reports/2022-biggest-year-ever-for-crypto-hacking/#:~:text=That%20trend%20intensified%20in%202022,cross%2Dchain%20bridge%20protocols%20specifically
[10]https://www.brookings.edu/research/how-to-improve-regulation-of-crypto-today-without-congressional-action-and-make-the-industry-pay-for-it/
[11] https://www.politico.com/newsletters/digital-future-daily/2023/02/27/when-courts-control-defi-00084610

should include an analysis of the practices and structural problems that led to such hacks and identify how best practices in the traditional financial sector could be transferred to the crypto sector.

- Crypto-asset info-sharing: Treasury should support the formation of information-sharing and analysis centers (ISACs) for crypto-assets by conducting studies that analyze how standards around traditional finance and cybersecurity risk management should be applied to the crypto space.

- Public-private research partnership and exchange: In order to increase the technical expertise on digital assets within US law enforcement and intelligence agencies, OSTP should sponsor a research-focused career exchange program. The exchange should enable members of the digital asset private sector to spend one to two years working within a U.S. law enforcement or intelligence agency and for U.S. national security officials to spend the same amount of time working in the private digital asset space. Participants in these exchanges should research how to best use digital asset technology to improve U.S. safety and security and how to mitigate risks around illicit finance.

**SECTION III: R&D that should be prioritized for digital assets**

*Enable user-focused infrastructure, protocol interoperability, and privacy-enhancing technologies that respect national security*

Digital assets are a broad category, and the U.S. must focus research on some key technical areas to harness decentralized technology's strategic economic, social, and security benefits. OTSP should prioritize the following research areas:

- Smart contracts: An important feature of blockchain technology is the ability to program transactions. Because blockchains are purely software code created on and for the internet, developers can, in many cases, design internet-based functions via blockchains that can not easily or efficiently occur through traditional finance. Various countries have also been using smart contracts in real estate and healthcare. The Republic of Georgia has been developing a blockchain-based land title registry since 2016, and similar projects are underway in the United Arab Emirates.[12] The U.S. should provide funding to deepen the expertise in smart contract design within U.S. educational institutions and enterprises.

- Cross-chain interoperability: Interoperability across blockchains is the major challenge in the crypto ecosystem. Most blockchains were built using different standards and

[12] https://ideas.repec.org/a/tpr/inntgg/v12y2019i3-4p72-78.html; https://dubailand.gov.ae/en/news-media/dubai-land-department-achieves-a-technical-milestone-with-the-adoption-of-blockchain-technology-in-cooperation-with-smart-dubai-and-other-partners/#/

programming bases and are thus not interoperable. Participants have developed workarounds, such as bridges. Intensive research is needed to develop ways for users to operate seamlessly across different blockchain protocols.[13]

- Zero-knowledge proofs: Privacy is a fundamental human right and social good. As people's everyday lives create and reveal more data about themselves, there is a growing need to build technical systems and policies to safeguard 4th amendment protections in the digital age. This also is important for cybersecurity. Privacy-preserving technology allows data computation and targeted analysis while remaining encrypted to those performing the computation and malicious actors who might seek to steal or corrupt that information. Zero-knowledge rollups and configurable privacy blockchains are emerging forms of privacy-preserving technologies that balance individuals' privacy interests with broader public policy and societal requirements, such as effective compliance, transparency, and safety.[14] OSTP should work with the National Institute for Standards and Technology (NIST) in the U.S. Department of Commerce to conduct research on zero-knowledge proofs (ZKPs) and how they could be applied in a variety of digital use-cases where selective disclosure and screening are necessary to balance both privacy and security.

- Digital Identity: In order to help ensure American consumers can operate on the internet more securely and privately, the U.S. government should expand its support of digital identity initiatives that use decentralized and privacy-preserving technology. FinCEN's focus on digital identity should continue, but there should be more focus across agencies on applying digital identity solutions to the areas in which they engage the public. Digital identity plays a key role in modernizing and lowering barriers to access to public services such as those related to healthcare, Social Security, veteran benefits, certifications, and licenses.[15] It has the potential to increase convenience, eliminate unnecessary travel, and lower costs for users through remote online authentication. For the U.S. government, digital identity can boost administrative efficiency and reduce the risks of identity fraud. To ensure user privacy and data security in a wide array of use cases, the U.S. government should gain further understanding of how to apply zero-knowledge proofs (ZKPs) and selective disclosure to identity solutions.[16] To guard against monopolies and walled gardens, research efforts should also seek out the benefits of open and interoperable digital identity systems. In addition, it will be important for the U.S. government to work with the private sector to issue guidance and allow for experimentation with digital identity, including projects that incorporate zero-knowledge

---

[13] See remarks by Acting Comptroller Michael Hsu, https://www.occ.gov/news-issuances/speeches/2022/pub-speech-2022-37.pdf

[14] *See* https://a16zcrypto.com/content/article/privacy-protecting-regulatory-solutions-using-zero-knowledge-proofs-full-paper/

[15] https://www.mckinsey.com/industries/public-and-social-sector/our-insights/how-governments-can-deliver-on-the-promise-of-digital-id

[16] *See* https://a16zcrypto.com/content/article/zero-knowledge-canon/

proofs. CCI would be happy to facilitate such exchanges as part of a public-private research partnership.

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

- Self-hosted Wallets: Wallets (both hosted and self-hosted wallets) are essential to the future of digital assets and are primarily used to store private keys – the passwords that give users access to their cryptocurrencies, NFTs and tokenized assets. Unlike a normal wallet, which can hold actual cash, crypto wallets store digital assets on corresponding blockchains but can only be accessed using a private key. If the users lose their private keys, they lose access to the assets. There have been many hacks over the past few years due to a lack of rigorous research and audits of wallet applications, especially in cybersecurity and access control. OSTP should work with the cryptographic research community and industry players to investigate topics such as multi-party computation (MPC) and programmable access control mechanisms to ensure wallets provide consumer protection and user experience requirements.

- Private key management: Blockchain transactions rely on private cryptographic keys. In order to enhance security and usability for everyday consumers, research is needed on ways to improve the consumer user experience of private key custody, including ways for retail customers to manage their private keys in a safe and efficient manner.

- NFTs: Non-fungible tokens (NFTs) represent unique records minted and tracked on a blockchain that can be used to verify the authenticity and ownership of a particular item asset. Blockchain-based digital identity, in addition to the uses discussed above, can be used to prove ownership of NFTs.[17] While NFTs are useful for developing digital collectibles, OSTP should support research to identify how NFTs could be applied in practical business and public service activities where auditing and verifying asset ownership and provenance are needed. The California Department of Motor Vehicles' pilot using NFTs for title management exemplifies the type of innovative exploration the public sector can undertake by partnering with blockchain firms.[18] In particular, there is significant legal research needed around the policy frameworks that should accompany the growth of NFTs in tracking physical world ownership. OSTP will need to collaborate closely with U.S. legal and audit professional communities on compatibility with existing

[17] https://www.cbinsights.com/research/decentralized-identity-verifiable-credentials/
[18] https://blockworks.co/news/california-pilots-blockchain-car-title-management-system-on-tezos; *see also* https://www.cbinsights.com/research/decentralized-identity-verifiable-credentials/

frameworks. Other jurisdictions—both adversarial and friendly to the United States—are developing strategies to leverage NFTs for public and private sector use cases. For example, the Chinese government is collaborating with software firms to develop NFT-based ownership authentication systems that could be deployed for government records and private sector information-sharing.[19] Japan's majority political party in 2022 released an NFT White Paper to articulate a national NFT strategy for the Web3 era, and guidance to the broader startup and institutional developer community.[20]

**SECTION IV: Opportunities to advance responsible innovation in the broader digital assets ecosystem**

*Explore embedded supervision*

In regulating the DeFi space, the U.S. and other jurisdictions will need to explore and develop methods of regulatory supervision that fit the technology's unique features. One approach to appropriate supervision of DeFi is embedded supervision, in which some regulatory requirements for consumer protection, AML/CFT compliance, and other critical matters are built into the DeFi ecosystem through smart contracts. The Bank for International Settlements published a working paper on this issue in 2019, and there appears to be growing discussion about embedded supervision in regulator circles.[21]

OSTP should work with prudential regulators as well as industry and academic experts to conduct research on applying smart contracts for DeFi supervision. This research should emphasize the technical solutions and the policy decisions and changes which may be necessary for building an appropriate regulatory framework for DeFi. Collaborative efforts across the public and private sectors are necessary to craft policies that keep pace with fast-moving technical advances in the digital assets space.

OSTP should also coordinate with all the US regulatory representatives to the Global Financial Innovation Network (GFIN) to evaluate how each financial regulator is evaluating responsible innovation in their respective sector and to learn from the GFIN representatives what other regulators are doing to promote responsible innovation globally.

**SECTION V: Other information that should inform the R&D Agenda**

*Research private-sector alternatives or complements to a CBDC*

As the U.S. explores the technical and policy possibilities for a central bank digital currency (CBDC), OSTP should prioritize research on how the private sector might achieve or

[19] https://www.lawfareblog.com/chinas-nft-plans-are-recipe-governments-digital-control
[20] https://www.taira-m.jp/Japan%27s%20NFT%20Whitepaper_E_050122.pdf
[21] https://www.bis.org/publ/work811.pdf

complement the aims and functionality being proposed in various CBDC models. In particular, research is needed on the potential for stablecoins, built on open infrastructure, to upgrade and improve US payment systems without constructing a CBDC. Specific topics include researching the validity of stablecoin private issuance, identifying the benefits and risks of such issuance mechanisms (such as 1:1 reserves vs. algorithmic), and the need for licensure among issuers.

*Require greater computer science expertise*

In order to craft and manage effective digital asset policies and regulations, U.S. agencies whose work closely involves digital assets each must hire a substantial number of full-time equivalents (FTEs) with computer science skills and expertise. The number of FTEs may vary by agency but should be based on a formal assessment of current levels of computer science technical skills and a prioritization of current and emerging expertise areas.

*Innovation Centers*

Relevant financial regulatory and policy-making agencies should have centers that enable internal experimentation with blockchain technologies in order to inform rule-making and awareness of use cases for digital asset innovation. In doing so, the U.S. government also needs to consider how to ensure ethics guidance does not preclude officials from having the familiarity with digital assets needed to understand and monitor the ecosystem.

## CONCLUSION

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

Respectfully submitted,

Sheila Warren
Chief Executive Officer
Crypto Council for Innovation