MITRE's Response to the OSTP RFI Supporting a National Digital Assets R&D Agenda

March 3, 2023

For additional information about this response, please contact:

Duane Blackburn
Center for Data-Driven Policy
The MITRE Corporation
7596 Colshire Drive
McLean, VA 22102-7539

policy@mitre.org
(434) 964-5023

©2023 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited. Case Number 22-01891-17.

About MITRE

MITRE is a not-for-profit company that works in the public interest to tackle difficult problems that challenge the safety, stability, security, and well-being of our nation. We operate multiple federally funded research and development centers (FFRDCs); participate in and lead public-private partnerships across national security and civilian agency missions; and maintain an independent technology research program in areas such as artificial intelligence, intuitive data science, quantum information science, health informatics, policy and economic expertise, trustworthy autonomy, cyber threat sharing, and cyber resilience. MITRE's 10,000-plus employees work in the public interest to solve problems for a safer world, with scientific integrity being fundamental to our existence. We are prohibited from lobbying, do not develop or sell products, have no owners or shareholders, and do not compete with industry. Our multidisciplinary teams (including engineers, scientists, data analysts, organizational change specialists, policy professionals, and more) are thus free to dig into problems from all angles, with no political or commercial pressures to influence our decision making, technical findings, or policy recommendations.

Over the past several years, MITRE has provided unbiased, trusted advice to multiple federal agencies and U.S. policymakers who seek to better understand rapidly changing technology developments across the full spectrum of digital and crypto-assets from cryptocurrencies, stablecoins, Central Bank Digital Currencies (CBDCs), and non-fungible tokens (NFTs). We have developed partnerships on key digital asset topics with industry, academia, and the nonprofit sector to understand, research, or develop capabilities—for example for the development of high-throughput, reliable, safe, and private payment systems; the interconnectivity of the digital assets system with the traditional financial system to illuminate contagion and system risks; the unmasking and retrieval of sophisticated money laundering activities enabled by illicit use of cryptocurrencies; and examination of how digital assets could impact U.S. economic and national security. Specifically, over the past two years MITRE has held several digital assets technical exchange meetings, bringing together the digital assets industry, government, and nonprofit sector to share insights and deepen a collective understanding of policy goals, challenges, and the current state of technology developments to gain a more holistic view of how the government and industry should tackle the many challenges in the digital assets ecosystem.

Introduction and Overarching Recommendations

MITRE supports the government's efforts in developing a National Digital Assets Research and Development Agenda to drive important research on key digital asset technology topics. We recommend this Agenda focus not only on advancing the state of the art but also on providing data and experiences in maximizing opportunities or mitigating risks that can guide future operational and policy decisions in a data-driven manner.

<u>Strategic Structure</u>. MITRE recommends that the Fast Track Action Committee ensures that the Agenda will strategically drive federal activities and enable the Executive Office of the President (EOP) to assess individual activities and holistic progress toward its unifying vision. It may help

to use a strategic planning framework that is consistent with the Government Performance and Results Act.

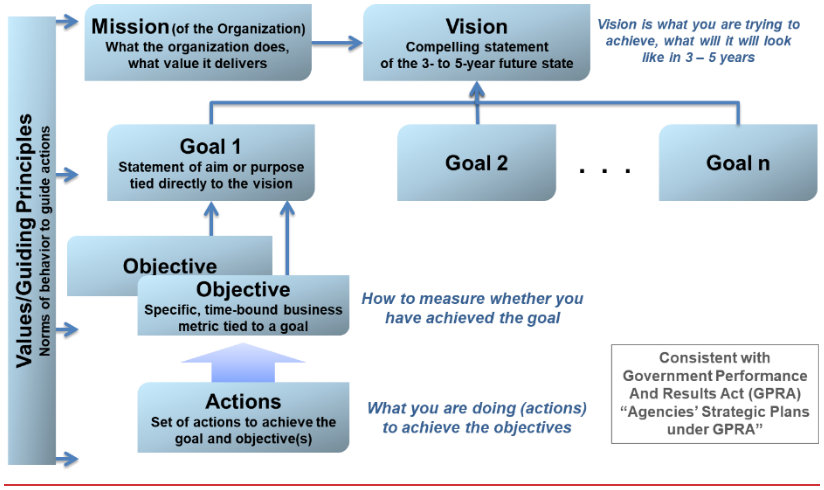

Values/Guiding Principles
Norms of behavior to guide actions
Mission (of the Organization)
What the organization does, what value it delivers
Vision
Compelling statement of the 3- to 5-year future state
Vision is what you are trying to achieve, what will it will look like in 3 – 5 years
Goal 1
Statement of aim or purpose tied directly to the vision
Goal 2
. . .
Goal n
Objective
Objective
Specific, time-bound business metric tied to a goal
How to measure whether you have achieved the goal
Actions
Set of actions to achieve the goal and objective(s)
What you are doing (actions) to achieve the objectives
Consistent with Government Performance And Results Act (GPRA) "Agencies' Strategic Plans under GPRA"

Figure 1. Strategic Planning Framework with Values/Guiding Principles

Such a structured planning framework provides:

- A set of values and principles that guides all subsequent activities
- A universal and compelling vision for the future of digital assets research
- A series of goals that collectively enables the vision to be met
- Subordinate objectives and strategies that are specific and time-bound and that both help drive activities to successfully meet goals and provide the EOP the ability to measure progress

Organizing Taxonomy. The Agenda will also benefit greatly with an organizing taxonomy (or Glossary) that establishes a common government digital assets vernacular and will aid in increasing meaning and control as new technologies are introduced. An organizing taxonomy will also aid in R&D activities such as, but not limited to, 1) building virtual models to simulate the kinds of markets that digital assets might enable and how they may interact with the traditional financial markets, 2) addressing increasing adoption of digital assets that undermine national security and intelligence missions as well as criminal and civil investigations, 3) prototyping simplified interfaces for consumers to access digital assets, and 4) testing approaches to balance privacy and identity across multiple government authorities. While doing so is not a common National Science and Technology Council activity, there are examples where it has been beneficially executed—including in issuing policy for agencies to consistently leverage this terminology in their science and technology (S&T) activities.[1]

[1] D. Blackburn and M. Garris. A National Science and Technology Council for the 21st Century. 2021. MITRE, https://www.mitre.org/sites/default/files/2021-09/pr-21-2388-national-science-technology-council.pdf.

Questions Posed in the RFI

1. *Goals, sectors, or applications that could be improved with digital assets and related technologies*: Information about goals, sectors, or applications where digital assets could provide significant value to the public, and examples of where benefits are already being delivered.

Digital assets and related technologies hold significant promise to decrease costs, increase trust and security, and more equitably share value creation. Like the advent of other new technologies, however, there is often a considerable amount of overpromising and underdelivering on what digital asset technology can transform, at least at this stage of its development. Below we discuss several areas where digital assets and related technologies could provide benefits.

Finance, Payments Systems, and U.S. Dollar (USD) Demand. Most digital assets projects to date have aimed to transfer value more quickly, efficiently, and securely compared with the current financial system while simultaneously improving access. Stablecoins utilizing public blockchain infrastructure have enabled inexpensive, secure, nearly instant, and stable cross-border transactions. Prior to stablecoins, there was no mechanism for retail investors to access the USD and preserve their purchasing power. Digital assets may also provide important opportunities for disadvantaged populations around the world by improving the efficiency and cost-effectiveness of international remittances sent by migrant workers back to family members in their home countries. It is estimated there are currently 100+ cryptocurrency remittance companies that aim to provide alternatives to traditional wire transfer services.

Supply Chain. As globalization has fragmented supply chains across the world, it is increasingly difficult to ascertain the provenance of components and subcomponents of the technology we consume. Digital asset technology has the potential to provide a unique new way to unequivocally track the aggregation of intellectual property, manufacturing data, and testing regimes for hardware and software.[2] From software libraries underpinning an enterprise application to bias testing performed on a machine learning model, the U.S. can help ruggedize our supply chains with transparency and illumination. Further, global shipping logistics are increasingly looking toward digital asset technology for solutions, as a large portion of those transactions remain rooted in analog bill of lading mechanisms.

Healthcare. Current approaches struggle to ensure individuals' ownership and control of their own Electronic Medical Records (EMRs) and personal health data, thus risking adverse usage of this sensitive information. A digital asset technology solution for EMR data, however, could dramatically improve patient care through secure, electronically portable, and consistent health records. An early example of such a system is MIT Media Lab's MedRec.[3] Medical research might also be accelerated by compensating users for contributing their data to retrospective trials and population health studies, much as individual participation in prospective, interventional clinical trials is compensated, and hence incentivized, today.

[2] MITRE supported a 2022 National Institute of Standards and Technology/National Cybersecurity Center of Excellence study on "Blockchain and Related Technologies to Support Manufacturing Supply Chain Traceability." Available on request.

[3] MedRec: Blockchain for Medical Data Access, Permission Management and Trend Analysis. 2014. Massachusetts Institute of Technology, https://www.media.mit.edu/publications/medrec-blockchain-for-medical-data-access-permission-management-and-trend-analysis/. Last accessed February 27, 2023.

Digital Property Rights and the Metaverse. One of the fundamental building blocks of digital asset technology is the concept of digital property rights. NFTs existing on decentralized public infrastructure make the idealized concept of sovereign ownership of unique digital property a reality. As the public increasingly values digital assets alongside physical assets, the metaverse can become an environment in which to uniquely interact with these wholly digital assets.[4]

2. *Goals, sectors, or applications where digital assets introduces risks or harms*: Information about goals, sectors, or applications where digital assets might introduce risks or harms, and examples of where risks or harms are already being manifested.

Cryptocurrency's Role in Facilitating Ransomware Attacks. Cryptocurrency has become the ransomware payment instrument of choice for cyber actors targeting individuals; federal, state, local, tribal, and territorial governments; critical infrastructure operators; small and medium businesses; and the cyber insurance (and re-insurance) markets. The explosion of ransomware attacks in recent years has made victims in virtually every sector of commerce and elements of government at all levels,[5,6] driving reliance on cyber insurance. Individuals and businesses are also harmed through crypto scams in a variety of ways outside of ransomware. These include crypto pump-and-dump schemes, private key compromises, smart contract compromise or misuse, and a host of other illegal or unethical schemes against both sophisticated and unsophisticated cryptocurrency users.

Digital Assets' Introduction of Various Threat Vectors for National Security. Digital assets can diminish the efficacy of U.S. economic policy through introducing mechanisms to transfer value outside of the USD and outside of the U.S. and partner-based financial infrastructure. Cryptocurrencies are a unique problem because they are a complete payment system that avoids infrastructure like the Society for Worldwide Interbank Financial Telecommunications, which the U.S. relies on to implement financial sanctions. North Korea has profited from this in a major way, utilizing cryptocurrency-enabled ransomware to fund their WMD program.[7] Russian oligarchs were also able to use cryptocurrencies to evade financial sanctions after the Ukrainian invasion. Russian cryptocurrency miners were able to continue to mine bitcoin, taking advantage

[4] R. Belk, et al. Money, Possessions, and Ownership in the Metaverse: NFTs, Cryptocurrencies, Web3 and Wild Markets. 2022. Journal of Business Research, https://www.sciencedirect.com/science/article/abs/pii/S0148296322007147. Last accessed February 27, 2023.

[5] Ransomware Threats against Local Agencies Shows No Sign of Slowing in 2022. 2022. StateScoop, https://statescoop.com/ransomware-threats-against-local-agencies-shows-no-sign-of-slowing-in-2022/. Last accessed February 20, 2023. This recently released report paints a bleak picture of the prevalence of ransomware in government, at both the central government and local government levels.

[6] Three Affiliated Tribes Hit by Ransomware Attack, Holding Tribal Information Hostage. 2021. Native News Online, https://nativenewsonline.net/currents/three-affiliated-tribes-hit-by-ransomware-attack-holding-tribal-information-hostag. Last accessed February 20, 2023. Tribal governments have been hit by ransomware, disrupting tribes' access to their email and other information systems.

[7] U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats. 2022. U.S. Department of the Treasury, https://home.treasury.gov/news/press-releases/jy0768. Last accessed February 27, 2023.

of the country's combination of cool weather and cheap electricity. Iran has also explored the use of cryptocurrency to facilitate international trade.[8]

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

Addressing Digital Asset Tax Compliance Needs. Public Law No. 117-58 (November 2021) requires brokers (e.g., cryptocurrency exchanges, peer-to-peer money transmitters, financial institutions that provide crypto investing services) to report all digital asset transactions (e.g., cost basis, sales) beginning in January 2024. In simple terms, individual taxpayers engaged in digital asset trading and the businesses that facilitate digital asset trading must file tax returns to report the values of those trades, and the Internal Revenue Service must enforce the reporting requirements for those exchanges. Because digital asset values are considerably more volatile than physical assets, but are significantly easier to trade and occur in higher daily volumes, there is a significantly higher overhead for both voluntary compliance and enforcement. To help mitigate this overhead for taxpayers, research should be conducted to explore techniques that can automate the tracking of digital asset basis—especially for transactions that occur on decentralized exchanges and transactions that involve transfers across multiple exchanges. To support tax enforcement efforts, additional research is required to determine how digital assets can be used to advance abusive tax shelter strategies.

Anti-Money Laundering (AML)/Combating the Financing of Terrorism (CFT). Whether cryptocurrencies, stablecoins, CBDC, or other digitized forms of value, due diligence standards for identifying and reporting illicit finance, sanction-evasion, and fraud activities must be based on a reasonableness standard to associate the asset with an entity (i.e., person, business, or other form of entity). The current AML/CFT and sanctions regime is based on the principle that the financial intermediary (e.g., bank, MSB, fiduciary) will and should have adequate controls in place to associate the value to the entity for the specified purpose (e.g., AML/CFT, sanctions, fraud). Regardless of whether a financial regulator has jurisdiction over a particular form of digital asset, development of a reasonableness standard framework for association of "the who to the asset" is imperative. The framework should lay out the key variations of responsibilities for diligence monitoring by the community—from those where there is a clear fiduciary intermediary to those where there is not where a reasonable intermediary. For those digital assets that are truly decentralized—where no one entity has insight into due diligence AML/CFT and sanctions monitoring—not-for-profits/nongovernmental organizations could be authorized to perform the due diligence. R&D specifically into the types of entities that could be established and funded to perform fully decentralized AML/CFT and sanctions monitoring is an area for exploration.

Equitable Access. To help underserved communities harness the benefits of digital assets while reducing their risks, barriers to adoption must be understood. These barriers must be considered across several dimensions, including access and financial inclusion, usability, security, privacy, and interoperability. MITRE identified 11 key user-centered issues that need to be further

[8] D. Dudley. Iran Dabbles in Crypto for Cross-Border Trade, in Effort to Bypass Sanctions. 2022. Forbes, https://www.forbes.com/sites/dominicdudley/2022/08/10/iran-dabbles-in-crypto-for-cross-border-trade-in-effort-to-bypass-sanctions. Last accessed February 27, 2023.

researched to achieve an equitable and usable token-based CBDC wallet (please see detailed discussion in Appendix A).[9] For example, offline capabilities address barriers of particular importance for both usability and access across all populations. By addressing these barriers and incorporating user-centered digital wallet design, all citizens—especially those who have been underserved by the traditional banking system—can leverage digital assets more efficiently, effectively, and safely.

4. *R&D that should be prioritized for digital assets*: Information about Federal research opportunities that could be introduced or modified to (a) advance the development of digital assets and/or (b) protect communities and U.S. national interests from risks or harms that digital assets might present.

Maximizing the Benefits of a New Decentralized Payment System while Mitigating Illicit Financial Activities. These new easily accessible peer-to-peer payment systems and distributed applications fueled by a myriad of digital assets can allow for greater distribution of economic wealth. However, they present an economic and technical hurdle to a number of government missions. For instance, an explosion of broadly adopted digital assets and investments through decentralized finance might in some circumstances also erode the standing of the U.S. dollar as the global reserve currency and provide a new mechanism to scale illicit financial activities that can undermine trust in the overall financial ecosystem. To make that less likely, the following questions should be explored:

1. How can adversaries combine cyber and economic techniques, tactics, and procedures to compromise national security and government services? Addressing this issue requires research to develop sensors, ontologies of behavior, and systems/environments for modeling and empirical experimentation. These building blocks can form the basis of varieties of mechanisms for effects across government missions, such as degrading criminals' logistical capabilities, avoiding systemic economic tipping points, and creating secure blockchain resources.
2. What data science techniques can be developed to track illicit actor use of privacy-enhancing coins such as Monero and Zcash?
3. What extensions are required to existing threat-sharing intelligence standards, such as Common Vulnerabilities and Exposures/Common Weakness Enumeration, to capture digital asset-based illicit financial activities and exploits?
4. How can unique government authorities be asserted upon decentralized payments without violating their underlying transaction mechanisms?
5. What cryptography advances can help increase the speed of computational algorithms used in tools for law enforcement interdiction?
6. How can legitimate users be guided away from illicit environments while offering them similar privacy?
7. How can on and off ramps into the digital assets ecosystem be improved to better enforce Know Your Customer (KYC) standards?

[9] B. Scollan and E. Darling. Designing Digital Currency Wallets for Broad Adoption. 2023. Journal of Payments Strategy & Systems, 17(1), forthcoming.

8. How can government play a role in setting standards for the safety of code that defines these socio-technical systems, such as smart contracts in decentralized autonomous organizations?
9. What challenges need to be overcome to better enable cross-agency sharing of digital asset data and intelligence?

Research Strategies to Reduce Systemic Financial Risk from Decentralized Finance. Regulatory agencies such as the Commodity Futures Trading Commission and Securities and Exchange Commission are facing a host of new challenges to address the stability issues associated with digital asset markets.[10] Traditional approaches that involve applying regulatory controls such as asset risk disclosures, liquidity minimums, and trading rules to centralized intermediaries such as stock exchanges don't translate well for digital assets that trade in decentralized market systems. In these complex economic systems, small perturbations can have cascading effects in unpredictable ways and can undermine the stability and integrity of the system as a whole in short order. The following are topics of recommended research to mitigate these risks:

1. Determine interdependencies between decentralized protocols that can lead to financial contagion in digital asset markets.
2. Discover which controls can be applied to detect and mitigate potential contagion.
3. Research which real-time data extract, transform, and load techniques can help quickly identify digital asset liquidity fragmentation across centralized/decentralized protocols and market participants.
4. Promote research efforts to develop modeling and simulation tools that can test the impact of regulatory "what-if" scenarios on the behaviors of market participants.
5. Conduct research to uncover fundamental economic mechanisms in digital asset protocols that can result in a "run on the bank" and corresponding "death spiral" of liquidity.

Advancing Global Decentralized Digital Identity and Digital Data Research to Protect Citizen Privacy and Enable the Evolution of Governance. The need to protect individual privacy and the need for service providers to comply with KYC, Customer Due Diligence, and AML regulations are conflicting goals that require solutions that balance private interests with national security. At the heart of this conflict is the need to prevent abuse or misuse of individual identities and data. Given the advent of decentralized identity technologies, portable and verifiable KYC credentials and zero-knowledge proof (ZKP) research should be prioritized to explore the potential to achieve a good balance. In particular:

1. How can ZKPs be scaled to provide customized citizen services while preserving the privacy of transactions? This should include statements about measuring whether a given transaction or action is allowed without revealing the contents and making statements describing quantities, materials, and identities of involved parties (e.g., this transaction contains no bad actors) without revealing any of this data to others?
2. What are the technical and social barriers to growing and adopting decentralized identity solutions? How can they be overcome?

[10] There have been many congressional hearings on this topic over the past year, such as a February 14 Senate Committee hearing on "Crypto Crash: Why Financial System Safeguards Are Needed for Digital Assets."

3. How can the computational overhead of privacy-enhancing technologies (PETs) such as homomorphic encryption, secure multiparty computation, differential privacy, blind signatures, and ring signatures be reduced to enable solutions for larger problem sets?
4. How can PETs allow industry to exchange data in a secure and privacy-enhanced way, as well as to comply with state, national, and international data protection regulations?
5. How can PETs help government agencies monitor privacy risk, meet privacy compliance requirements, and strategically address privacy policy and technology challenges?
6. How can post-quantum cryptography (PQC) be used to perform digital asset transactions?
7. How can identity and transaction delegation via Attribute Based Encryption or Identity Based Encryption be performed using PQC?

The Potential of Digital Assets to Meet the Needs of the Underbanked/Unbanked. The U.S. Treasury Department's Strategic Plan for Fiscal Years 2022–26[11] calls for progress on financial innovation with a deliberate emphasis on financial inclusion. Unfortunately, many of the current use cases for digital assets are centered on investment opportunities and may not align directly with the needs of underbanked or unbanked populations. That said, digital assets may have considerable potential to help disadvantaged populations, not least in providing a possible future way to accelerate, target, and mitigate fraud, waste, and abuse in disbursements of government economic stimulus or crisis response aid. The underlying web3 technologies may also help reduce financial transaction fees—thus also potentially helping the underbanked—and help make possible more viable or safer alternatives to predatory inclusion services such as payday lending and title loans. Research efforts should explore the following:

1. Can peer-to-peer decentralized financial payment systems benefit communities located in domestic banking deserts?
2. If government grants were administered using a decentralized ledger, would this help reduce fraud, waste, and abuse?
3. Can digital asset-based decentralized lending protocols assist communities in U.S. persistent poverty counties to overcome traditional barriers to accessing capital?

CBDC Research Priorities. Research conducted into the progress of other countries' CBDCs—namely China's—has illustrated the United States' lack of progress in this area, relatively speaking, but has also yielded useful insights into which areas to prioritize when conducting research for the creation of a CBDC. Further insights into research priorities when attempting to create a CBDC were gleaned during MITRE's involvement in the OpenCBDC project (Project Hamilton), conducted by MIT's Media Lab in conjunction with the Federal Reserve Bank of Boston:

1. Privacy/Auditability: How can users be given fine-grained privacy over their transactions, while at the same time providing the visibility needed for the financial system and law enforcement? Users want a digital currency with the anonymity of cash.
2. Policy and Architecture: How would a CBDC fit into existing systems? Who would operate it (e.g., federal reserve, local banks, treasury)? What are the implications for other payment providers (e.g., Visa, Mastercard, Paypal)?

[11] Treasury Strategic Plan 2022-2026. 2022. U.S. Department of Treasury, https://home.treasury.gov/system/files/266/TreasuryStrategicPlan-FY2022-2026.pdf.

3. Scalability: If the entire U.S. population was using such as system, could it handle the load, even at extremes such as the holiday shopping season?
4. Key Management (for the average person): How can approaches to private key recovery be simplified for the average person? What recovery/insurance system might be introduced for loss or remediation of theft?

Additional research questions specific to a U.S. CBDC are included in Appendix B.

5. *Opportunities to advance responsible innovation in the broader digital assets ecosystem*: Information about opportunities for the United States to advance responsible innovation in the broader digital assets ecosystem, in areas that are adjacent to R&D.

Maintaining and Increasing Participation in U.S. and International Bodies that Influence Standards for Digital Assets. The United States should participate in working groups across the full spectrum of digital assets to learn, leverage, and influence research within the ecosystem. The realization that the U.S. may likely not be in the international driver's seat on this topic further underscores this need. For example, the Federal Reserve Board of Governors and the Federal Reserve Bank of New York are members of the Bank for International Settlements (BIS) Committee on Payments and Market Infrastructures, an international standards setter that promotes, monitors, and makes recommendations about the safety and efficiency of payment, clearing, settlement, and related arrangements. This type of participation should provide significant knowledge and technical expertise into the design of a potential U.S. CBDC. Participation in the BIS's Innovation Hub—particularly new projects like Pyxtrial, which aims to develop a platform to monitor stablecoin's balance sheets—should offer important technical understandings for both stablecoin and CBDC projects. As security and reliability will be perhaps the most important elements of a potential U.S. CDBC architecture, the Office of Science and Technology (OSTP) should leverage research currently being undertaken by NIST, including MITRE participation in efforts to utilize blockchain technology to improve the security and traceability of microelectronics and industrial control software. Finally, influence in projects in which the U.S. is not a core member, such as the BIS's mCBDC initiative, will be critical for integrating democratic norms and interoperability with a potential U.S. CBDC.

Convening International Partners to Advance an Inclusive Vision to Strengthen Democratic Values Pertaining to the Use of Digital Assets. The United States should organize and lead a coordinated international effort—involving officials both from likeminded, democratic governments and from private sector entities—to counter Chinese efforts to advance authoritarian digital asset-related standards[12] with a coordinated *non*-authoritarian approach that promotes decentralized values. These efforts should build on the recent directives issued to U.S. agencies to "leverage U.S. positions in international organizations to message U.S. values related

[12] See, for example, J. Zheng and M. Chen. Web3 in China: Will It Happen, and What Form Will It Take?. 2022. Technode, https://technode.com/2022/08/25/web3-in-china-will-it-happen-and-what-form-will-it-take/. Last accessed February 27, 2023.

to digital assets," as detailed in the White House Framework for Responsible Development of Digital Assets.[13]

Advancing Accessibility Standards that Reduce Burden of Technology Adoption. The interfaces currently available to access the digital assets ecosystem require individuals to have a high level of technical sophistication and fail to meet basic Section 508 accessibility standards. This failure is due in part to the lack of adoption of user-centered design principles and a counterproductive focus on providing solutions primarily for a tech-savvy, early-adopter market segment—which limits the potential for rapid and widespread uptake and use case development. Standards bodies should set minimum requirements for accessibility to help mitigate the potential for a widening digital divide.

6. *Other information that should inform the R&D Agenda:*

Given the wide breadth of digital assets research needs that span multiple technological, social, policy, and financial and economic dimensions, an important first step is the development of an organizing framework to map research interdependencies, ambiguities, tradeoffs, and overlaps against a unifying set of use cases to help sequence and prioritize a productive research portfolio. This ensures that a foundational set of knowledge is retained in a coordinated manner, and is particularly essential when multi-disciplinary, multi-stakeholder teams are involved. This framework can serve to inform potential research solicitation and prioritization of investments and provide transparency to leadership teams that are accountable to deliver on Executive Order directives.

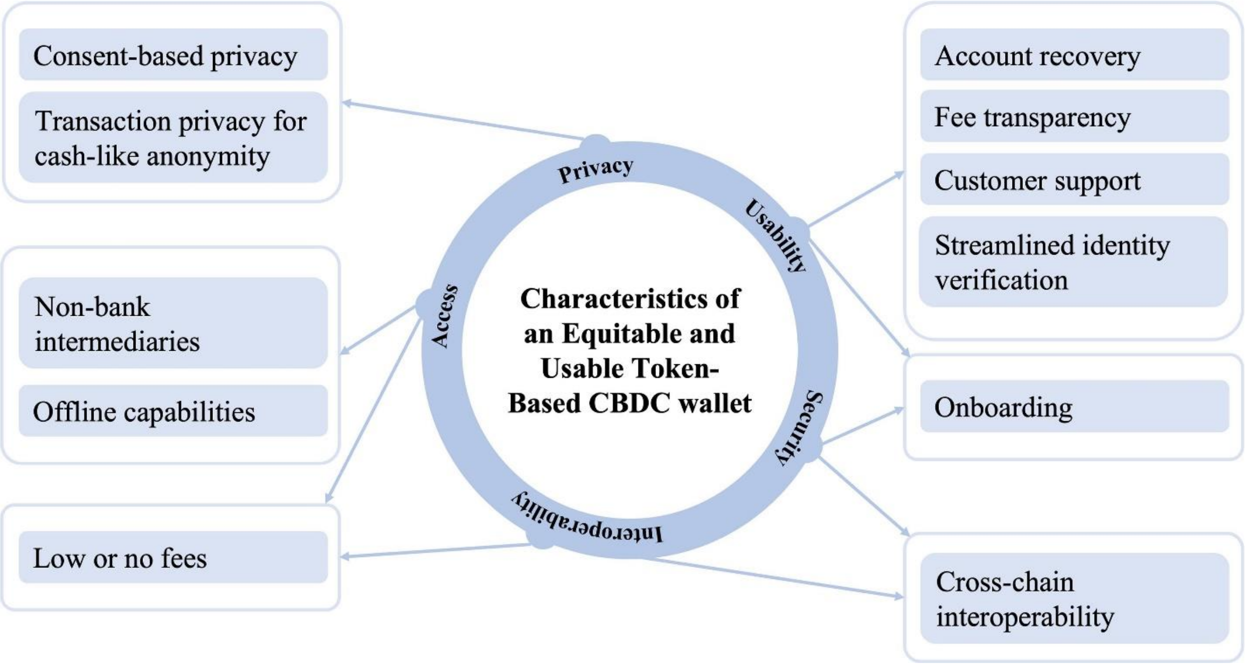
Furthermore, OSTP's charge to drive the national R&D agenda on digital assets will require convening a diverse set of stakeholders from across government, industry, and academia to identify pockets of digital assets expertise and to collaborate, where appropriate, on those technological advancements and innovations. In cases where there are uniquely specialized areas of expertise in industry or where there are overlapping mission objectives with government, it may be beneficial to investigate the potential for creating public-private partnerships to advance research on certain topics and/or to leverage or expand existing investments being made in digital assets research across government. Having a "big picture" view of the research needs and mapping that to the various entities with which the government may seek to collaborate based on their expertise on those needs will be a critical early step to support a national research strategy.

When the research agenda is fully formed and mature for execution, significant additional efforts will be required to manage and sustain the overall portfolio. It will be critical to establish an overall approach for synthesizing and integrating the outcomes from the various research projects to ensure the government is fully leveraging the value from those investments. Additionally, to support the large-scale technical research projects that will be needed, it may also be necessary to design a national strategy for investments in the labs and computing environments that will be critical to support that experimentation.

[13] FACT SHEET: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets. 2022. Executive Office of the President, https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/. Last accessed March 1, 2023.

Appendix A. Pre-Publication Information from Designing Digital Currency Wallets for Broad Adoption

MITRE identified 11 key user-centric issues to achieve an equitable and usable token-based CBDC wallet.[14]



UX area	Issues	Opportunities	Potential solutions
Low or no fees (access; interoperability)	• Lack of funds is the primary barrier to financial inclusion • High minimum balance requirements for accounts are a barrier to those who lack funds	• Cryptocurrencies can be transferred internationally in real time with little to no fees	Develop a CBDC with little to no fees and consider the cost of access (e.g., mobile devices, internet fees).
Non-bank intermediaries (access)	• Identity-based accounts require an intermediary	• Token-based accounts may not require an intermediary	For a CBDC, promote innovation in a two-tiered payment system by including new, non-bank intermediaries (e.g., intermediaries that offer payment services but do not handle customer funds). If people can access it only through a traditional

[14] B. Scollan, and E. Darling. Designing Digital Currency Wallets for Broad Adoption. 2023. Journal of Payments Strategy & Systems, 17(1), forthcoming.

UX area	Issues	Opportunities	Potential solutions
			bank, it will not be appealing to the unbanked.
Offline capabilities (access)	• Reliable internet access can be a barrier to financial inclusion	• Innovations in offline payments in other countries like India • Innovative methods for feature phone payments and banking in India • SMS-based crypto wallets used with stablecoins in Rwanda, Kenya, and Uganda	A CBDC should offer offline capabilities and access options on multiple device types (including hardware card and paper). Further research on mobile payments innovations in offline, feature phone, and SMS can be used to inform CBDC policy and design.
Customer support (usability)	• Non-custodial wallets have no customer support	• Customer support best practices of some custodial wallets and mobile payment wallets	A CBDC should provide customer support.
Fee transparency (usability)	• There is confusion around gas fees and transaction speed for crypto wallets	• UI design best practices from other domains (e.g., e-commerce user interface techniques that provide the user with transparent payment options based on delivery speed)	Wallets that interact with a CBDC should provide clarity and predictability regarding any fees, limits placed on spending amounts, number of transactions a person can make, etc.
Streamlined identity verification (usability)	• KYC/AML processes are cumbersome	• Simplify KYC/AML processes through user research and regulatory changes	A CBDC should offer tiered access that allows for a simplified KYC process. Further usability research on KYC/AML should be conducted, targeting populations that are unbanked or lack access to government IDs.
Account recovery (usability)	• Users must safeguard the seed phrase for non-custodial crypto wallets	• Help citizens keep their money safe and secure	A CBDC should make clear the importance and best practices of safeguarding one's funds. There should be a safe and secure way for users to recover their accounts if they have a lost password or lost device.

UX area	Issues	Opportunities	Potential solutions
Onboarding (usability; security)	• Potentially increased exposure to phishing that targets wallets • Crypto wallets have a steep learning curve	• Help citizens feel their money is safe and secure	CBDC wallets should provide clear onboarding materials to help novices enter the space. Wallets that interact with a CBDC should adhere to a higher security standard to inspire trust in the security of the issuer, intermediaries, the underlying technology, and the level of fraud protection offered.
Cross-chain interoperability (security; interoperability)	• Most of the money stolen by hackers in 2022 targeted cross-chain bridges, which are used to facilitate the transfer of funds between blockchains	• Achieve interoperability goals while preserving security	A CBDC should increase interoperability while improving security through broad adoption of standard protocols or use of an interlinked approach.
Transaction privacy for cash-like anonymity (privacy)	• Cryptocurrency transactions are not private: the sending address, receiving address, transaction amount, and date and time are all recorded on a public ledger that anyone can view	• Explore ZKPs • Determine the right balance between privacy and oversight	Use privacy by design methods. Learn from pilot implementations that leverage ZKPs (e.g., MIT Digital Currency Initiative's zkLedger).
Consent-based privacy (privacy)	• Users have concerns about data privacy (from peers and from the government) for financial transactions being exposed to third parties through a national digital ID	• Decentralised Identifiers (DIDs) enable a verifiable, decentralised digital identity that allows a user to create an identification token that contains their personal information and prove their identity without needing a central authority such as a bank or credit card company to create and manage the identity	Conduct further research into the use of DIDs to increase CBDC privacy. Consider data sharing with appropriate safeguards such as separating transaction and personal data. A token-based CBDC wallet must clearly communicate what information the government can see and why it needs to see it. Allow users to maintain a sense of authority and control of their personal data.

Appendix B. CBDC-Specific Research Questions

Additional CBDC-specific research questions aligned to the format published in the OSTP September 2022 report, "Technical Evaluation for a US Central Bank Digital Currency System."

Design Element	Focus Areas	Research Questions	Design Choices
Participants	Transport Layer	What approaches can be used to handle proxy authorizations? What implications exist for wholesale vs. retail implementations?	Less Intermediated vs. More Intermediated
	Interoperability	What data and data interchange standards are required for interoperability with third-party systems? What standards can help advance the accessibility challenges of different types of wallets for different user demographics?	Less vs. More Technical Interoperability with Other Payment Systems Human Coordination vs. Technical Interoperability
Governance	Permissioning	Is the system permissioned (and if so, how) or permissionless? What tradeoffs must be addressed if there is a permissionless substrate with a permissioned app layer?	Permissioned vs. Permissionless vs. Hybrid
	Identity Privacy	Which aspects of identity are kept private/confidential, from whom, under what circumstances, and how? How important is privacy to U.S. consumers, and does the perception of a lack of privacy threaten adoption of a CBDC?	Known to Central Bank vs. Intermediary vs. No One
	Remediation	Is there an end user layer that delays transaction finalization and a settlement layer that is immutable vs. a monolithic single layer?	On-Ledger vs. Off-Ledger Multi-Layer vs. Monolithic
Security	Cryptography	How can proofs-of-compliance be engineered that allow for law enforcement insights for legitimate transactions while masking transaction-level data?	Public-Key Cryptography (PKC) vs. PKC with Zero-Knowledge Proofs vs. Other
	Secure Interfaces	What security standards are required to mitigate cyberattacks at CBDC access points? Which key management options and wallet designs would work best for different types of users? How can new tactics, techniques, and procedure threats be mitigated?	Opensource vs. Proprietary Standards

Design Element	Focus Areas	Research Questions	Design Choices
Transactions	Transaction Privacy	How do privacy protections impact other requirements, such as processing speed, system/network security, scalability, and/or maintenance costs?	More Private vs. More Observable Transactions vs. Layering
	Transaction Programmability	Should atomic transaction bundling be supported?	Supported vs. Not Supported Atomic vs. Not Atomic
Data	Ledger History	Can decentralized data stores be used to provide transaction data security and privacy for end users?	None vs. Centralized vs. Distributed
Adjustments	Fungibility	Can the CBDC system support non-fungible units? What use case is envisioned, and how is it balanced with privacy—i.e., if all units have non-fungible properties, then are all units potentially traceable?	Fungible vs. Non-Fungible Units
System Stability	Core Stability	Which architectural features help reduce the failover time of the core processing application?	Speed vs. Robustness
	Market Stability	Could a U.S. CBDC create new vectors for economic contagion? Which leading indicators could provide an early warning of systemic risk? What "circuit breakers" could help contain external and internal economic shocks?	Private Risk Management vs. Federal Backstops
	Sociotechnical Stability	How does a CBDC solution compare competitively with alternative payment systems for trust and security? What are the implications for a CBDC-issued centrally vs. a digital dollar issued by multiple vendors? How can computational analysis be applied to systems composed of and secured by self-directed agents? What sociotechnical factors drive instability?	Centralized Stability vs. Tokenomic Stability Systems of Agents vs. Systems of Bits