TESTIMONY OF

Carole House[1]

BEFORE THE

United States House Financial Services Committee

Hearing on Navigating the Digital Payments Ecosystem: Examining a Federal Framework for Payment Stablecoins and Consequences of a U.S. Central Bank Digital Currency

March 11, 2025

Thank you Chairman Hill, Ranking Member Waters, and distinguished members of the Committee, for holding this hearing and the honor of the invitation to testify on the digital payments ecosystem. I applaud your leadership in convening the Committee on this important issue and continuing the years-long efforts of this Committee across several Congresses to evaluate and build legislation for a stablecoin regulatory framework. I hope my testimony will be helpful in considering some of the most important aspects of frameworks needed to drive innovation in a secure, competitive, safe, and sound digital payments ecosystem that reinforces national security interests, defends consumers, and preserves personal liberty.

I have spent my career working at the intersection of national, economic, and technological security. I have had the honor of serving three tours in the White House, including recently departing from my second stint at the National Security Council leading various policy efforts on cybersecurity, emerging technology, and digital assets, to include the U.S. Counter-Ransomware Strategy and the previous Administration's Executive Order on Ensuring Responsible Development of Digital Assets.[2] I previously led digital asset policy initiatives at the U.S. anti-money laundering and countering financing of terrorism (AML/CFT) regulator, the Financial Crimes Enforcement Network (FinCEN) and have served on advisory boards for the U.S. Commodity Futures Trading Commission (CFTC), the Idaho Department of Finance, and the New York Department of Financial Services (NYDFS). Through my ongoing work as a Senior Fellow at the Atlantic Council GeoEconomics Center and previous work as a consultant and executive at a venture

[1] Nonresident Senior Fellow, Atlantic Council GeoEconomics Center; Senior Visiting Scholar, Georgetown University. *Previous Advisory Roles:* Chair, Commodity Futures Trading Commission (CFTC) Technology Advisory Committee; Member of the Emerging Technology Advisory Committee (ETAC) to the Idaho Department of Finance (IDOF); Member of the Virtual Currency Advisory Board (VCAB) to the New York Department of Financial Services (NYDFS); Advisory Board Member, Third Way U.S.-China Digital World Order Initiative; Advisory Board Member, Digital Dollar Project. *Previous Government Roles:* Special Advisor for Cyber and Critical Infrastructure & Director of Cybersecurity and Secure Digital Innovation, White House National Security Council; Senior Strategic Policy Officer for Cyber and Emerging Technology, U.S. Financial Crimes Enforcement Network; Presidential Management Fellow (PMF) and Policy Advisor, White House Office of Management and Budget and U.S. Senate Homeland Security and Governmental Affairs Committee; Captain, U.S. Army.

[2] *See* The White House, Executive Order 14067, Ensuring Responsible Development of Digital Assets, (March 9, 2022).

capital firm, I have advised companies, academia, and policymakers in support of strategy, policy, standards, and product development ranging across areas like cybersecurity, AML/CFT, digital assets, and artificial intelligence and machine learning. The views I share are my own and do not reflect the views of the Atlantic Council.

The most important message I can underscore to this Committee is the criticality of ensuring our regulatory frameworks create a foundation for providing trustworthy and affordable access to financial services for consumers while also reinforcing the centrality of the United States in the financial system and as the home for *responsible*, cutting-edge innovation in emerging technologies and payments. That includes the critical need for timely progress on a comprehensive stablecoin framework that supports these objectives, as well as driving broader experimentation and competitiveness in digital payments. Just as important, any framework demands more than just policy that is clear, strong, and comprehensive, but also that is *implemented* and enforced timely and scoped to shape the sector.

While timely progress is critical, these frameworks must be deliberate, thoughtful, and comprehensive of the real and present risks, as well as opportunities, that we have observed in the digital asset ecosystem and broader financial system. In the wake of serious national security threats like billion-dollar hacks by rogue nations[3], growing integration of cryptocurrency as a tool for transnational organized crime[4], market manipulation and fraud that can threaten system integrity and stability, as well as pressure from adversarial nations seeking to develop and leverage alternative payment systems to weaken and circumvent the dollar[5], it is clear that strong safeguards, including for U.S. competitiveness, are needed. This framework also demands we ensure policy and enforcement approaches both domestically and internationally create a level playing field for U.S. firms – often the most compliant firms in the world – to be able to compete fairly. Otherwise, the foundation we build these systems on risk faltering, with the potential to not only reap significant harms but also prevent us from harnessing the greatest positive potential that is possible from a secure and innovative digital payments ecosystem.

[3] *See* Federal Bureau of Investigation (FBI), Public Service Announcement, I-022625-PSA, "North Korea Responsible for $1.5 Billion Bybit Hack," (February 26, 2025).

[4] *See* TRM Labs, "Understanding the Use of Cryptocurrencies by Cartels," (January 22, 2025); *and* Douglas Farah and Marianne Richardson, Georgetown University Journal of International Affairs, "The Growing Use of Cryptocurrency by Transnational Organized Crime Groups in Latin America," (March 20, 2023).

[5] *See* Hippolyte Fofack, Atlantic Council, "Piece by Piece, the BRICS Really Are Building a Multipolar World," (August 23, 2023).

Background: Exigency for Competition, Security, and Liberty

Stablecoin Features, Uses, Benefits, and Risks

Stablecoins, a class of cryptoassets that maintain a stable value in relation to another asset, most predominantly fiat currencies, hold potential to help drive needed innovations in our digital payments ecosystem. Stablecoins with proper protections can help improve efficiency in delivery of financial products and services, promoting greater transparency for monitoring of various risks in financial services, enhancing resiliency within the financial system, dismantling barriers to financial access and inclusion, and promoting innovation and competition that can strengthen U.S. markets and leadership.[6] With the current stablecoin market cap sitting at over $227 billion, use cases are growing across areas like dollar settlement for financial services firms[7], cross-border remittances, relief efforts like to Ukrainian refugees[8], and even for inflation hedges in places like Venezuela.[9] However, stablecoins are largely still used as settlement in trading activity on cryptocurrency platforms[10] – wide adoption in exchange for goods and services is not yet a reality, though it's possible that a clear regulatory framework to enable greater trust and accountability may facilitate higher adoption.

Most of the core features for any cryptocurrencies apply to stablecoins – including their ability to transfer significant value *peer-to-peer* (i.e., from user to user without the need for a typical custodial role of a third-party financial intermediary), *pseudonymously, immutably* (or irreversibly), with *global reach*, with *increased speed and cost efficiencies* – though we must note that these are all features that are attractive to both licit and illicit actors.[11] Challenges in mitigating risks in cryptocurrency are especially driven by by lagging AML/CFT compliance as well as broader prudential standards across the sector internationally[12], reinforced by the *absence or reduction of financial institution intermediaries and central points of control* in more highly decentralized cryptocurrency systems that can *obscure clear lines of responsibility and accountability* within cryptocurrency ecosystems. While stablecoins are used across more decentralized

[6] *See* CFTC TAC Subcommittee on Digital Assets and Blockchain Technology, Report, "Decentralized Finance," (January 2024); *and* Bank of International Settlements (BIS) Committee on Payments and Market Infrastructures, "Considerations for the Use of Stablecoin Arrangements in Cross-Border Payments," (October 2023).

[7] *For example, see* MoneyGram, "MoneyGram and Stellar Announce Cash to Crypto/Crypto to Cash Partnership with Zero-Fees for the First 12 Months," (June 15, 2022).

[8] *See* Ian Hall, Global Government Fintech, "UN Pilots Blockchain and USDC Stablecoin for Disbursements in Ukraine," (December 29, 2022).

[9] *See* Prashant Jha, "Venezuela Turns to Crypto to Battle Inflation and Instability," (December 31, 2024).

[10] *See Anneke Kosse, Marc Glowka, Ilaria Mattei and Tara Rice* BIS, Paper No. 141, "Will the Real Stablecoin Please Stand Up?" (November 2023).

[11] *See* Carole House, testimony before the House Financial Services Committee Subcommittee on Digital Assets, Financial Technology, and Inclusion, "Hearing on Crypto Crime in Context Part II: Examining Approaches to Combat Illicit Activity," (February 2024).

[12] *See* Financial Action Task Force (FATF), "Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers" (June 27, 2023).

networks, in most cases stablecoins generally at least central administrators and issuers that can ease establishing lines of responsibility.

Where there is an absence of clear responsible parties, compounded by the immutability or unchangeability of cryptocurrency ledgers, it can be extremely challenging to provide mechanisms for victim recourse as well as timely adaptation to take measures to stop movement of illicit funds or patch security vulnerabilities in networks and smart contracts.[13] However, in contrast to SWIFT, FedWIRE, and cash movements that do not publish transactions to public ledgers, on-chain stablecoin transactions include a lot of *public transparency* that can be beneficial to market surveillance and crypto investigations. Though ultimately the benefits presented by this transparency can be difficult to leverage with earlier-mentioned challenges with compliance, acceptance of accountability, and expertise across both public and private stakeholders.

Risks that can be presented by stablecoins without proper controls in place generally reflect the same kinds of risks that can exist in traditional finance (or "tradfi"). For example, fraud, market manipulations, and conflicts of interest across stablecoin leaders or public officials can present risks to investors and consumers. Pump-and-dump schemes and front-running capabilities enabled through maximal extractable value (MEV) schemes can endanger market integrity, and complex interconnections, concentration risks, and hardwired procyclicality in stablecoin or any other decentralized finance ("defi") systems can present risks to financial system stability. Failures like that of Synapse Financial Technologies[14] and of stablecoin Terra[15] underscored the consequences of insufficient oversight of regtech and stablecoin platforms, and the devastating consequences to consumers without access or ability to recover some or all of their funds.

The risks to national security on getting the stablecoin framework wrong – either by being too lax on controls or by overly restricting companies and driving innovation offshore – are also important to evaluate. If stablecoins present the greatest potential for at-scale adoption for cross-border payments in cryptocurrency, then national security concerns of losing sanctions and AML/CFT tool efficacy can present in several ways: either from failing to drive U.S. stablecoin competitiveness compared to other national currency-denominated stablecoins or payment systems; or risks that could present from stablecoins and other defi diminishing reliance or need for U.S. correspondent banking relationships in foreign exchange (FX) transactions or other cross-border funds flows. *(See Appendix A for a more detailed walkthrough of pros and cons for risk mitigation presented by specific features of cryptocurrencies like stablecoins)*

[13] *See* CFTC TAC Subcommittee on Digital Assets and Blockchain Technology, Report, "Decentralized Finance," (January 2024).
[14] *See* David Krause, Marquette University, "The Fall of Synapse Financial Technologies: Lessons and Implications for the Fintech Industry," (July 29, 2024)
[15] *See* Russell Wong, Federal Reserve Bank of Richmond, "Why Stablecoins Fail: An Economist's Post-Mortem of Terra," (July 2022).

The Need for a Framework

The United States does not yet have a comprehensive framework for regulation of stablecoins. Instead, existing authorities are fragmented at the Federal level largely only via AML/CFT regulation and then across certain states like New York[16] that cover stablecoins. In the absence of leveraging existing bank and trust charter authorities; using Dodd-Frank payment, clearing, and settlement activity designation authorities[17]; setting up a Federal payments charter[18]; or taking any other action to create a framework, the United States lags behind many other jurisdictions like the European Union, Singapore, Japan, and the United Arab Emirates that have established requirements and most importantly clear pathways to registration and supervision for stablecoins operating within their jurisdictions.[19]

The United States must prioritize establishing a stablecoin framework during this Congress. Similar in many functions and operations to more traditional financial assets, stablecoins and associated deposit and payments activities are things that we understand how to regulate and protect.[20] This framework is achievable, able to build on years of bipartisan efforts working across the aisle to construct a truly comprehensive approach. With Congress and the Administration positioned to prioritize this legislation, we are at a critical juncture to get a law passed in 2025.

We need strong prudential and consumer protection regulations to ensure that stablecoins are truly "stable," allowing any user to trust in its value and avoid losses from the issuer's default or illiquidity.[21] In this way, a clear regulatory framework that fosters trust can actually help set conditions that could help drive broader adoption and competition. We also need to have strong AML/CFT protections in place for stablecoin ecosystems. These different regimes do not operate in siloes, but instead mutually reinforce each other and address vulnerabilities that are being exploited by illicit actors targeting the cryptocurrency sector. For example, in the case of Democratic People's Republic of Korea (DPRK) hacks of cryptocurrency platforms, like the recent $1.5 billion Bybit hack, are exploiting both cybersecurity weaknesses and vulnerabilities as well as AML/CFT deficiencies in their crypto heists and subsequent laundering activities.[22] In

[1616] *See* NYDFS, "Superintendent Adrienne A. Harris Announces New DFS Regulatory Guidance on the Issuance of U.S. Dollar-Backed Stablecoins," (Jun 8, 2022).
[17] *See* Pub. L. 111–203, title VIII, § 802.
[18] *See* Ballard Spahr podcast, interview with Dan Awrey, "Should Congress Create a New Federal Charter for Non-Bank Payments Companies?" (November 14, 2024)
[19] *See* Atlantic Council, Cryptocurrency Regulation Tracker.
[20] *See* Austin Campbell, testimony before House Financial Services Committee Subcommittee on Digital Assets, Financial Technology, and Inclusion, "Hearing on Understanding Stablecoins' Role in Payments and the Need for Legislation," (April 19, 2023).
[21] *See* Howell Jackson, Tim Massad, Dan Awrey, Hutchkins Center on Fiscal & Monetary Policy at Brookings, "How We Can Regulate Stablecoins Now – Without Congressional Action," (August 2022).
[22] *See* Ledger Insights, "Bybit Crypto Hack: SAFE Wallet Reveals How It Happened," (March 7, 2025).

crypto heists, stablecoins have been targets[23] as well as laundering tools exploited by hackers.[24] Only through a comprehensive framework can we ensure that measures across the spectrum of areas like cybersecurity and AML/CFT are holistically addressed in these important ecosystems.

Though also important to note, especially in light of recent changes in enforcement posture – beyond just creating the policy framework, the government and industry must work to apply and *enforce* the framework. A policy that isn't enforced or implemented does nothing to benefit consumers nor U.S. firms with stronger compliance programs that have been operating at higher costs and less competitive advantages than many foreign-operating firms.

Proposed Stablecoin Legislation – Ensuring Sufficient Protections

There has been a great amount of attention paid to stablecoin legislation in recent years with various stablecoin bills introduced, including the McHenry-Waters bill[25] and Lummis-Gillibrand Payment Stablecoin Act[26] developed last Congress, as well as the STABLE Act[27] and GENIUS Act[28] introduced so far this Congress.

I am very glad to see the level of support within Congress for elevating stablecoin legislation to a priority this year, something I spoke to as essential in my testimony to the Subcommittee on Digital Assets, Financial Technology, and Inclusion last year.[29] I'm also pleased to see many elements included in the STABLE Act referenced for this hearing that I support, such as high-quality reserves on at least a 1:1 basis, envisioned roles for both state and Federal regulators, and restrictions on rehypothecating reserve assets as well as stablecoin issuer activities. However, the STABLE Act appears to walk back a lot of the hard work done for years across the aisle to develop the negotiated text between then-Chair McHenry and Ranking Member Waters in 2024. It's unclear why some of those critical protections, especially the prudential framework and clear AML/CFT and sanctions applicability to U.S. dollar-denominated stablecoin activity, are absent in the STABLE Act and the GENIUS Act or if the associated risks are otherwise being addressed.

[23] *See* Yohan Yun, Cointelegraph, "Infini Loses $50M in Exploit, Developer Deception Suspected," (February 24, 2025).
[24] *See* Ben Foldy, Wall Street Journal, "From Hamas to North Korean Nukes, Cryptocurrency Tether Keeps Showing Up," (October 27, 2023).
[25] *See* McHenry-Waters Bill, H.R. ___, 118th Congress (2024).
[26] *See* Lummis-Gillibrand Payment Stablecoin Act, S. 4155, 118th Congress (2024).
[27] *See* STABLE Act of 2025, H.R. ___, 119th Congress (2025).
[28] *See* GENIUS Act of 2025, S. ___, 119th Congress (2025).
[29] *See* Carole House, testimony before the House Financial Services Committee Subcommittee on Digital Assets, Financial Technology, and Inclusion, "Hearing on Crypto Crime in Context Part II: Examining Approaches to Combat Illicit Activity," (February 2024).

Here I outline some areas for the Committee's consideration in hopes that the legislation for stablecoins issued this year can be truly comprehensive[30]:

- *Ensuring Federal Line-of-Sight for Supervision on Issues of Systemic Importance:* The STABLE Act, in some ways similar to the existing banking regime, provides for both Federal and state authorities to charter stablecoin issuers. However, the STABLE Act does not include any coordination between the Federal and state regulators. Rather, the current draft permits a system where a trillion-dollar nonbank stablecoin issuer, engaging in globally-reaching payments activity that would typically place an institution under the oversight of Federal authorities, without any sufficient line of sight by the Federal Reserve of activities and risks that rise to systemic importance. Unclearly defined "exigent" circumstances, especially in the way of *Loper-Bright*, as the only context for certain additional regulatory authorities severely restrict a regulators' ability to monitor for and intervene to mitigate risks for assets that operate 24/7 around the world and with no concerns for borders.

  I agree with many others who have testified before you all that state authorities provide an important chartering and oversight capability, including agility and expertise that can help scale appropriate supervision. State regulators with strong prudential, AML/CFT, and consumer protection frameworks are critical partners on the front lines of regulating the cryptocurrency industry, and I'm sympathetic to the desire to preserve the states' regulatory authorities. Though, it stands to reason that when these issuers are operating systems, especially large platforms, that are administering a substitute for the *U.S. dollar* in international payments, some Federal regulator – like the Federal Reserve Board, with its responsibility for monetary policy and financial stability, or the Office of the Comptroller of the Currency (OCC) with its chartering and supervision authority – should have the ability to monitor for their critical risks and have a say in the standards that stablecoin issuers needs to meet, at a minimum when they are of a large enough size. The STABLE Act, as it currently stands, raises serious questions around the ability of Federal authorities to have visibility of and ability to respond timely to moments of financial crisis and address systemic risks that may arise.

- *Scope of Risk Coverage and Enforcement Regime:* The STABLE Act references risks to mitigate around operational and cybersecurity risks, but otherwise is severely lacking in reference to credit risk, market risk, concentration risk, and even limitations on additional management of capital and liquidity risk beyond the 1:1 reserve collateralization requirement. There is no clear articulation of

[30] *See also* a thorough outline of many similar issues – Tim Massad, testimony to the House Financial Services Committee Subcommittee on Digital Assets, Financial Technology, and Artificial Intelligence, "Hearing on The Golden Age of Digital Assets: Charting a Path Forward," (February 11, 2025). Note that many of the issues I outline were addressed in the previously negotiated McHenry-Waters bill.

responsibility for rules or implementation of requirements under privacy regimes like Gramm-Leach-Bliley Act or the AML/CFT framework of the Bank Secrecy Act (e.g., if Treasury/FinCEN would have sole AML/CFT rulemaking authority for payment stablecoin issuers or if they would be issued jointly). Additionally, the enforcement framework is unclear, with no references to specific penalties or enforcement provisions, including no clarity on extraterritorial operations of U.S. dollar-denominated stablecoins.

- *Affiliate Controls and Application of Bank Holding Company Act and Bank Services Company Act:* The STABLE Act does not address affiliate relationships and restrictions for nonbank payment stablecoin issuers to preserve separation of activities like banking and commerce. In this new bill, it is unclear to what extent controls like from the Bank Holding Company Act as well as authorities for oversight and delegation of functions as delineated under the Bank Services Company Act apply to payment stablecoin issuers.

- *AML/CFT and Sanctions:* While the STABLE Act and GENIUS Act delineate that payment stablecoin issuers are financial institutions under the Bank Secrecy Act, it is not clear (especially to the degree needed in the wake of Loper-Bright) to what degree rulemaking can cover different parts of stablecoin ecosystems and which agency would be responsible for the rulemaking and oversight. Stablecoins have been exploited by illicit actors ranging from cartels to sanctions evaders to terrorism financiers, especially leveraging the absence of sufficient compliance across international operations and defi platforms. The U.S. Treasury has underscored the benefit for Congress to clarify that any U.S.-dollar denominated stablecoin must comply with U.S. sanctions policy, including extraterritorial applicability, and also make clear the expectation to maintain and assert freeze and recovery capability for illicit proceeds across the stablecoin. We should not find it acceptable for a USD stablecoin to be leveraged in transactions to designated actors and jurisdictions that present threats to U.S. national security.

  While unlikely in this round of legislation, Congress should start solidifying its views and drafting legislation to expand the regulatory perimeter to help mitigate risks across more decentralized applications of the assets. Expanding such a perimeter would generally involve considering what other entities would be of greatest utility to cover due to visibility and control of the assets, and ensuring that a risk-based approach properly scopes the obligations and does so in full understanding of what is technologically and operationally possible. While there are many differing views on how to approach defi controls, it is encouraging to see that within the defi community there are actors who are trying to implement responsible innovative fixes, even if they are not yet successful, as we saw recently in the unsuccessful attempt by several THORChain developers to try to stop DPRK money laundering on their platform.[31] (Congress should consider this illustrative table – see Appendix B – built by the CFTC's Technology Advisory Committee to demonstrate the different kinds of controls that can be implemented throughout the cryptocurrency technology stack, showing that compliance is possible.)

- *Bankruptcy and Resolution Measures:* Bankruptcy protections are one of the last lines of defense for fostering consumer trust in a product – building comfort for the customer that they will be able to get access to or redeem their assets held by the platform or issuer at any time on demand. The U.S. Bankruptcy code, if applied to stablecoins in the wake of a failure, could be disastrous for token holders who would be treated equivalently to all other unsecured creditors. The McHenry-Waters bill outlined a potential alternative resolution process to help expedite recovery of assets for token holders that could work across Federal and state levels and provide critical recourse for consumers.

- *Fed Master Accounts and Broader Payments Framework:* There is no reference in the STABLE Act or GENIUS Act to the authority of the Federal Reserve to grant access for stablecoin issuers to a master account, something that likely will continue to be sought especially as stablecoins get more regulated and attain higher assurance of their safety and soundness. With this legislation aiming to serve as the comprehensive construct of guardrails and authorities to enable innovation and protect payments, it should include provisions like this to ensure the capability exists with the Federal Reserve for any issuer it deems to be appropriate to grant access.

  More broadly, stablecoin legislation would optimally be pursued as part of a holistic approach to regulation and supervision of all payments platforms, which are growing enough in complexity and adoption. Many of the risks for stablecoins are similar to those for broader payments, and given the desire to ensure critical protections for consumers regardless of the denomination of their asset or which app they happen to be using, Congress should keep an eye toward how to evolve regulatory frameworks to capture any of these activities regardless on if it is blockchain-based or not.

Again, I applaud the Committee's work on this issue and the continued leadership on these issues by key leaders like Chair Hill and Ranking Member Waster. I encourage the Committee to consider working from the previously negotiated McHenry-Waters bill, which includes bipartisan-vetted provisions that address many of the outstanding issues for the desired comprehensive stablecoin framework. I hope that my views on key missing elements will be helpful to the Committee in its thoughtful efforts to build out and

[31] *See* Aaron S., Bitdegree, "THORChain Dev Walks Away after Attempt to Stop Illicit Funds Fails," (February 28, 2025).

implement a competitive, comprehensive stablecoin framework that addresses risks while promoting responsible innovation.

Proposed CBDC Legislation – Privacy as Paramount in Retail CBDC

The new proposed CBDC Anti-Surveillance State Act bans CBDC experimentation. Innovations in digital payments and across digital forms of both public and private money can also take many forms – whether wholesale or retail CBDCs, stablecoins, tokenized deposits, digital payment applications, etc. – each of which carry a spectrum of diverse implementations and associated risks. Ultimately, it is likely that a mix of modernizations of public and privately-administered rails, such as with the current financial system, will be needed to achieve a future of vision like global instantaneous reach and accessibility of the dollar.[32]

This legislation is pointed specifically at addressing concerns around privacy specific to CBDCs, which is a greater point of concern around retail CBDC implementations rather than wholesale payments that aren't associated with specific consumers and related sensitive personal data. The bill proposes to address the privacy concerns by banning even experimentation to even assess if there are technological and governance implementations that could achieve desired privacy outcomes, whether in the U.S. or even just for templates that partner nations could implement. The bill also does not address privacy issues presented by private cryptocurrencies, such as privacy concerns exacerbated by public unobscured records of financial transactions and challenged cybersecurity practices across the sector.

An apparent improvement on this bill from earlier versions appears to be amending the prohibition to only retail CBDCs. Concerns around privacy for a retail CBDC are understandable and very important[33], especially in the United States given sentiments of Americans around making information available to the government and even challenges that have existed in trying to adopt digital identity infrastructure.[34] Many feel that given such concerns in the United States, focus on wholesale CBDCs as an initial area for innovation in cross-border settlement could be ripe for nearer-term exploration.

The kinds of building blocks that could enable privacy preservation and security in technologies like CBDCs – innovative technologies like digital identity infrastructure and privacy enhancing technologies like homomorphic encryption, multi-party computation, and zero-knowledge proofs – are also building blocks that can enable privacy and security in private cryptocurrency implementations as well. Even if specific development of a U.S.

[3232] *For example, see* SIFMA, "Regulated Settlement Network Proof-of-Concept," (December 2024).
[33] *See* Josh Lipsky and Ananya Kumar, "Don't Let the US Become the Country to Ban CBDCs," (May 21, 2024).
[34] *See* Ash Johnson, Information Technology and Innovation Foundation (ITIF), "The Path to Digital Identity in the United States," (September 23, 2024).

retail CBDC is not likely, broader research and development and experimentation across the more nascent and underlying technologies and components can be helpful to identify mechanisms to achieve desired objectives across a variety of future forms of public and private money innovations.

This bill could further exacerbate a growing gap for the United States in digital payments innovation, as over 100 countries representing 98% of global GDP[35] continue to explore CBDCs and conduct cross-border pilots.[36] The United States remains the only member of the G20 to not be in advanced stages of CBDC exploration.[37] CBDC experimentation is at the heart of significant research and development across the international community trying to shape what the future of the financial system looks like, experimentation that without a major U.S. leadership presence is in some ways both a symptom and a driver towards interest of potential rails less reliant on the dollar, and something in which we cannot idly forsake leadership.

In the interests of safeguarding capabilities for experimentation and ensuring that the United States remains at the forefront of digital payments innovation, I outline here some areas for consideration for this proposed anti-CBDC legislation:

- *Narrowing the Prohibition to Retail CBDCs:* Recent updates to the proposed CBDC Anti-Surveillance State Act appears to narrow the prohibition of research and development, testing, or issuance to retail CBDCs only with the addition of the feature "widely available to the general public" into the definition of CBDC. If that is the intent, this avoids several significant challenges presented by the previous House-passed[38] version of the bill, as well as that referenced in the recent Executive Order prohibition, that even the Congressional Budget Office (CBO) noted[39] included such broad definitions that it was unclear if they could be interpreted to ban existing digital forms of central bank reserves and impact the ability to conduct monetary policy. However, if this bill is aimed at prohibiting wholesale digital payments innovation, or other forms of digital payments innovations like tiered or intermediated innovations like in certain implementations of stablecoins or tokenized deposits, additional concerns would remain related to stifling the ability to modernize the U.S. financial system.

- *Legal Necessity Unclear:* The necessity of this legislation to prohibit any experimentation and research and development in CBDCs appears unnecessary if the ultimately concern is to ensure against the issuance of a retail CBDC without

[35] *See* Atlantic Council, CBDC Tracker.
[36] *See* Bank of International Settlements, "BIS Innovation Hub Work on Central Bank Digital Currency."
[37] *See* Atlantic Council, CBDC Tracker.
[38] *See* House Committee on Financial Services, "House Passes CBDC Anti-Surveillance State Act" (May 23, 2024).
[39] *See* Congressional Budget Office, "H.R. 5403, CBDC Anti-Surveillance State Act," (May 7, 2024).

Congressional approval. The Federal Reserve already published its own analysis[40] highlighting that the Federal Reserve Act does not authorize direct Federal Reserve accounts for individuals. Both the Fed and Treasury have also voiced that they would only move forward with issuance of a CBDC with clear support from both Congress and executive branches. With Congressional approval already assessed as a precondition to issuance of at least retail CBDCs, and supported as necessary by the lead executive authorities, this prohibition appears unnecessary to achieve the policy outcome when Congress could just withhold authorization. If the refocus of this updated proposed legislation is only prohibiting retail CBDCs, research and development as well as operations to optimize and conduct of digital wholesale payments and settlement activities by central banks would hopefully not affected by this legislation as the Congressional Budget Office assessed could have been impacted by previously proposed versions.[41]

- *Adjusting Framing – The U.S. Government Fully Supports Privacy in Any Democratic CBDC:* This bill's title and corresponding messaging unfortunately present an inaccurate picture that CBDCs must inherently intimate an authoritarian "surveillance state." CBDCs do not have to mean "Big Brother" just as cryptocurrencies do not have to mean anarchy. The implications for privacy are vastly different for wholesale versus retail CBDCs. Just as with privately-administered cryptocurrencies, inherent features like privacy and discoverability are completely dependent upon the specific design of the systems.[42] The Federal Reserve[43], the U.S. Treasury[44], and prior Administrations have been extremely consistent in messaging, including alongside the G7[45], that "rigorous standards of privacy" and accountability for that privacy are critical for any retail CBDC implementation. The CBDC discussion warrants nuance, just as the cryptocurrency discussion does.

- *Refocusing on Impactful Privacy Measures:* Rather than this legislation barring pilots and experimentation of implementations and building blocks to preserve privacy for some future possible CBDCs likely at least a decade away (research that could also help provide building blocks for other digital assets like stablecoins), Congressional action could instead pivot to focus on long-existing challenges

[40] *See* Federal Research, Research and Analysis, "Money and Payments: The U.S. Dollar in the Age of Digital Transformation," (January 2022).
[4141] *See* Congressional Budget Office, "H.R. 5403, CBDC Anti-Surveillance State Act," (May 7, 2024).
[42] *See* Sandra Waliczek, "Privacy Concerns around CBDCs – Are They Justified?" (November 7, 2023).
[43] *See* Federal Research, Research and Analysis, "Money and Payments: The U.S. Dollar in the Age of Digital Transformation," (January 2022).
[44] *See* U.S. Department of the Treasury, "The Future of Money and Payments: Report Pursuant to Section 4(b) of Executive Order 14067" (September 2022).
[45] *See* G7, "Public Policy Principles for Retail Central Bank Digital Currencies," (2021).

presented by the absence of comprehensive consumer data privacy legislation.[46] Especially given the low likelihood and far-off reality of cross-U.S. Government and public interest in a U.S. retail CBDC (which the Federal Reserve,[47] U.S. Treasury, and potentially Congress [ref. section 5] have all agreed would require Congressional approval to issue if there ever were such an interest), Congressional focus on privacy legislation would be a more impactful area for focus.

- *Needed Clarity on the Protections Meant for Private Stablecoins:* It is unclear exactly what protections are being offered under section 4, which defends from prohibition only "any dollar-denominated currency that is open, permissionless, and private, and fully preserves the privacy protections of United States coins and physical currency." This is oddly framed and could place significant prohibitions on industry cryptocurrency implementations, if this intimates that there are intended to be restrictions here placed on certain industry cryptocurrency implementation, such as private stablecoins that aim to get a master account with the Federal Reserve. It is unclear if this intimates that permissioned stablecoin implementations may be barred from direct or indirect relationship with the Fed. It is also unclear what fully preserved privacy protections means in this context, given that the privacy features of cash (e.g., can move value without a third party, is not posted to any ledgers) do not exactly equate to the privacy features of any existent cryptocurrency (e.g., value movements generally require certain types of third parties – even if unregulated intermediaries – such as miners and validators, and transactions post on public ledgers). It would be important to clarify which privacy features of cash they desire, or what the specific balance of discoverability versus obfuscation is desired in the cryptocurrency system, as part of broader clarity on what this section is intended to achieve.

In closing, I'd like to again underscore my gratitude for the honor of the opportunity to speak with you all today. It is critical that the United States make timely progress on establishing and implementing a comprehensive stablecoin regulatory framework that leverages years of effort on defining critical holistic protections that also reinforce the central role in the financial system and as a leader in technological innovation.

Thank you.

[46] *See* Thorin Klosowski, "The State of Consumer Privacy Laws in the US (And Why It Matters)," (September 6, 2021).

[47] *See* Federal Research, Research and Analysis, "Money and Payments: The U.S. Dollar in the Age of Digital Transformation," (January 2022).

Appendix A: Risks and Mitigations Presented by Key Features of Cryptocurrency

Cryptocurrency systems vary significantly in design and implementation, and their specific features carry potential positives and well as negatives for combating exploitation and illicit finance. Many of these features exist on a spectrum and do not exist as a complete extreme one way or the other, and require thoughtful evaluation to assess potential risk.

Figure 1. Potential Pros and Cons for Addressing Risks Presented by Key Features of Cryptocurrency, including Stablecoins[48]

Feature Description	Potential Pro	Potential Con
Decentralization – The extent to which the system has no single point of failure, does not rely on a single source of information, and is not governed by a central authority that is capable of altering or censoring this information. Generally will manifest across *functional* dimensions (e.g., access, development, governance, balance sheet, operational) and technological dimensions (e.g., open source software, smart contracts, etc.) of decentralization.	With greater decentralization, a system may exhibit greater operational resilience against manipulation by illicit actors like cybercriminals aiming to take over a network. A more decentralized system can also mitigate "too-big-to-fail" concentration risks and potentially enable greater competition in the marketplace.	With the removal or reduction of key intermediaries in high-risk, high-value activity, decentralization can challenge the ability to identify clear lines of responsibility and accountability for when things go wrong or to implement fixes to security vulnerabilities or recover stolen or illicit funds.[49] Fewer intermediaries can also reduce points for detection, implementation of controls, and interdiction of illicit activity.
Speed and Cost Efficiencies – The ability to transfer funds and financial assets quickly and with lower costs, generally driven through optimizing aspects like automation, network capacity,	Licit actors and consumers benefit from an alternative to existing systems like slow and	Efficiencies in cost and speed can also increase for illicit actors, enabling their ability to scale frauds and money laundering at lower cost

[48] This table is adapted from the table at the end of my previous testimony – Carole House, testimony before the House Financial Services Committee Subcommittee on Digital Assets, Financial Technology, and Inclusion, "Hearing on Crypto Crime in Context Part II: Examining Approaches to Combat Illicit Activity," (February 2024). . These illustrative summaries leverage descriptions from the CFTC TAC report on DeFi. *See* CFTC TAC Subcommittee on Digital Assets and Blockchain Technology, Report, "Decentralized Finance," (January 2024)

[49] *See* Osato Avan-Nomayo and Aislinn Kelly, The Block, "Circle Freezes USDC Funds in Tornado Cash's US Treasury-Sanctioned Wallets" (August 8, 2022).

and reducing or consolidating intermediaries.	costly cross-border remittances.[50]	and friction. The scalability in speed and reach enabled with crypto, reinforced by hardwired procyclicality of software- and algorithm-enabled activity, can expand the impact and speed of negative consequences until they can be mitigated.
Openness and Global Reach – The extent to which a system permits participants into the ecosystem and movement of assets anywhere in the world. "Permissionless" systems generally implement no restrictions to those who can access the system, while permissioned systems implement some type of control on ecosystem participation.	Can lower barriers to financial access for the 1.7 billion people around the world who are unbanked[51], and (if the system is sufficiently regulated and appropriately transparent) could improve achievement of financial inclusion objectives, as well as enhance the ability to detect illicit activity within an observable ecosystem. Wider adoption of U.S. cryptocurrency projects and stablecoins could also expand the reach of the U.S. dollar, including application of U.S. national security tools like sanctions and AML/CFT visibility.	With unrestricted openness can enable access for illicit actors like rogue states who are otherwise restricted from the global financial system. Level of tech savvy also presents remaining barriers to entry and broader adoption. With inadequacies in consumer protection and regulation, open systems could enable "predatory inclusion."[52]

[50] *See* The World Bank, "Remittance Prices Worldwide Quarterly: An Analysis of Trends in Costs of Remittance Services" (March 2023).

[51] *See* The World Bank, "The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19" (June 2022).

[52] *See* Tressie McMillan Cottom, "Where Platform Capitalism and Racial Capitalism Meet: The Sociology of Race and Racism in the Digital Society", 6:4 Sociology of Race and Ethnicity 441 (October 2020).

Transparency – Includes the nature and amount of information (such as critical information needed to understand risks like for counterparties, sanctions, screening, etc.) that is available, whether publicly or some means of disclosure, to ecosystem participants. Public, unobscured blockchains generally have a lot of information about the existence, amount, provenance, and destination of transactions that is visible to the public.	The high level of transparency of most cryptocurrency ledgers enables detection, monitoring, and establishment of trust and validation of accuracy of transaction information. To the extent needed information is available and consumable by counterparties and authorities, this can permit an unprecedented level of real-time market surveillance and even investigation of cryptocurrency illicit finance, often more efficiently than traditional investigations.[53]	Much of the raw data available cannot be effectively used by investigators due to issues of capacity, resources, or insufficient RegTech. The transparency of public ledgers is insufficient without additional AML/CFT measures, as they only include information that is "on-chain," not "off-chain" transaction and identity information. Transparency also presents significant privacy concerns, and is also not inevitable. Obscuring methods through use of anonymity-enhanced cryptocurrencies, mixers, and other privacy enhancing technologies (PETs) are already used, and likely to be integrated at greater scale.
Pseudonymity and Anonymity – The ability to conduct transactions without one's identity being known or discoverable.	Licit users can engage in more private financial activity without needing to disclose sensitive personal information that could be a target for illicit actors. This privacy and obfuscation can also be beneficial for those seeking to	This pseudonymity, without compensating AML/CFT controls like KYC measures and some form of discoverable identity elsewhere in the ecosystem, denies critical information for investigators and for

[53] *See* Ari Redbord, written testimony to the U.S. House Committee on Financial Services Subcommittee on National Security, International Development, and Monetary Policy, Hearing on Under the Radar: Alternative Payment Systems and National Security Impacts of their Growth (September 20, 2022).

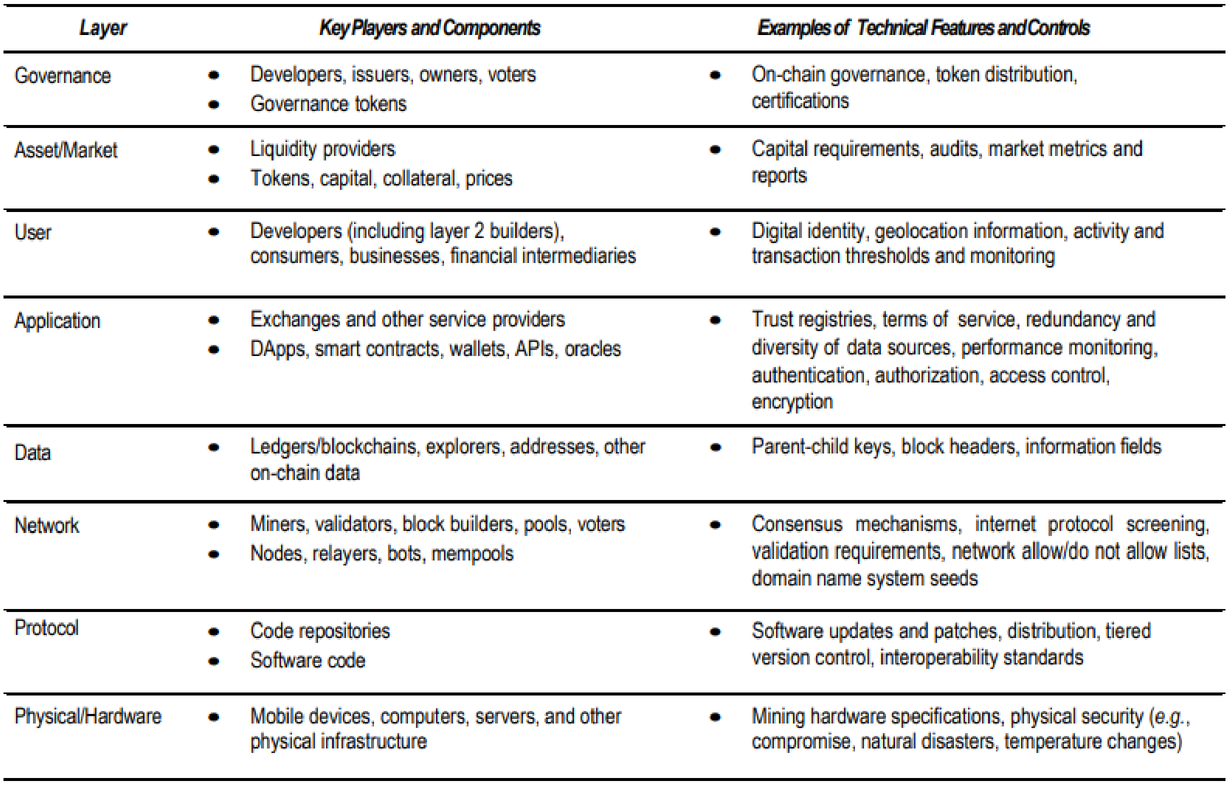
	avoid detection and discrimination by corrupt or authoritarian regimes.	counterparties to understand the nature of the risk of their counterparty. Even with transparency of funds flows and wallet information, absence of information about users significantly limits recourse for victims and holding accountable illicit actors.
Immutability and Censorship Resistance – The inability of network participants to change a system's ledgers, protocols, transactions, or other features.	Assets can be used to provide financial support to populations under repressive regimes via means the regime cannot interdict and deny access to.[54] Could promote greater auditability and resilience to manipulation by illicit actors in the financial system.	With increased immutability brings increased challenges to censor illicit actors and activities on a network. It also is more difficult to implement desired changes to a system, such as to patch a software vulnerability or recover assets stolen due to a security weakness.

[54] *See* Circle, blog, "Circle Partners with Bolivarian Republic of Venezuela and Airtm to Deliver Aid to Venezuelans Using USDC" (November 20, 2020).

Appendix B: Compliance across the DeFi Tech Stack

Policymakers may need to assess what reshaping AML/CFT and other illicit finance obligations should look like elsewhere in the "DeFi technology stack." At each "layer" of DeFi ecosystems, there are different options for players or components to focus obligations on and potential features or controls that could help meet regulatory objectives.

Figure 2. *Potential Mechanisms to Support Security and Compliance throughout the DeFi Tech Stack*[55]



Layer	*Key Players and Components*	*Examples of Technical Features and Controls*
Governance	• Developers, issuers, owners, voters • Governance tokens	• On-chain governance, token distribution, certifications
Asset/Market	• Liquidity providers • Tokens, capital, collateral, prices	• Capital requirements, audits, market metrics and reports
User	• Developers (including layer 2 builders), consumers, businesses, financial intermediaries	• Digital identity, geolocation information, activity and transaction thresholds and monitoring
Application	• Exchanges and other service providers • DApps, smart contracts, wallets, APIs, oracles	• Trust registries, terms of service, redundancy and diversity of data sources, performance monitoring, authentication, authorization, access control, encryption
Data	• Ledgers/blockchains, explorers, addresses, other on-chain data	• Parent-child keys, block headers, information fields
Network	• Miners, validators, block builders, pools, voters • Nodes, relayers, bots, mempools	• Consensus mechanisms, internet protocol screening, validation requirements, network allow/do not allow lists, domain name system seeds
Protocol	• Code repositories • Software code	• Software updates and patches, distribution, tiered version control, interoperability standards
Physical/Hardware	• Mobile devices, computers, servers, and other physical infrastructure	• Mining hardware specifications, physical security (*e.g.*, compromise, natural disasters, temperature changes)

[55] Table with illustrative examples of compliance as possible, taken from CFTC TAC DeFi Report.