Written Testimony of:

Ari Redbord
Head of Legal and Government Affairs
TRM Labs

Before 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

Introduction

Thank you Chairwoman Waters, Ranking Member McHenry, Subcommittee Chairman Himes, Ranking Member Barr, and Members of the Committee for holding this hearing and inviting me to participate. It is a true honor to be here today. I am humbled by the critical role this institution plays in protecting our democracy.

My name is Ari Redbord. I am head of legal and government affairs at TRM Labs, a blockchain intelligence company.

At TRM, we deliver a dynamic picture of blockchain-based activity in order to mitigate financial crime risk within the emerging digital asset economy. We do that by combining public data from 25 blockchains and from over a million different digital assets with advanced analytics and proprietary threat intelligence.

Cryptocurrency businesses, financial institutions, and law enforcement and regulatory agencies worldwide leverage our data and software solutions to measure, monitor, and investigate financial crime that involves digital assets and cryptocurrencies – from money laundering and ransomware attacks to hacks and terrorist financing.

I have spent my career working to protect the financial system from illicit actors – first for over a decade as a federal prosecutor in the U.S. Attorney's Office for the District of Columbia, and then at the U.S. Department of the Treasury as the Senior Advisor to the Under Secretary for

Terrorism and Financial Intelligence. There, I worked with teams from OFAC, FinCEN, and across the interagency to safeguard the financial system from illicit use by terrorist financiers, weapons of mass destruction proliferators, drug kingpins, and other rogue actors.

During my time at the Treasury Department, every morning I walked past an oil painting of Alexander Hamilton hanging outside of the Secretary's office. That painting reminded me of what we were there to protect: a complex financial system filled with both challenges and opportunities. Today, our financial system faces new and emerging challenges, but it is also filled with tremendous opportunities.

In this testimony, I hope to assist this Subcommittee in its consideration of several important issues that lie at the core of the global financial system. These issues include (1) **the U.S. dollar's role as the world reserve currency** amidst the creation of new forms of value transfer such as blockchain technology; (2) the ability of U.S. and allied governments, now and in the future, **to use economic sanctions as an effective coercive measure**; and, (3) **the ability of global regulators, law enforcement, and national security officials to track financial crime** and other illicit activity.

How the U.S. dollar, as the world's primary reserve currency, supports the efficacy of U.S. sanctions

The U.S. dollar has been the world's primary reserve currency since World War II. As a reserve currency, it is widely used by countries, multinational businesses, and financial institutions as a medium of exchange, store of value, and unit of account to power the global economy.

- As a medium of exchange, the dollar is used to invoice and settle roughly half of world trade[1] and accounts for 42 percent of global payments.[2]
- As a store of value, the dollar represents about 60 percent of allocated foreign exchange reserves held by central banks worldwide.[3]
- As a unit of account, about half of all international loans and global debt securities are denominated in dollars.[4]

High global demand for dollars provides multiple benefits to the United States, including lower interest rates, lower exchange rate risk, and higher purchasing power for the U.S. government, businesses, and consumers.

[1] https://crsreports.congress.gov/product/pdf/IF/IF11707
[2] https://www.swift.com/file/67001/download
[3] https://data.imf.org/?sk=E6A5F467-C14B-4AA8-9F6D-5A09EC4E62A4
[4] https://crsreports.congress.gov/product/pdf/IF/IF11707

The strength of the U.S. dollar also increases global use of the U.S. financial system, since access to the U.S. financial system is generally needed to settle transactions denominated in dollars, even when both parties are located outside the U.S.

The centrality of the dollar in global commerce, combined with the coupling of the dollar and the U.S. financial system, makes access to the U.S. financial system a near-necessity for businesses and governments worldwide.

The centrality of the U.S. financial system in the global economy provides two benefits to the U.S.:

1. The U.S. can limit access to the U.S. financial system through sanctions. This gives the United States a powerful economic coercive tool to achieve economic, national security, human rights, or technological objectives.

2. The U.S. can leverage its unique position within the global financial system to combat crime through financial intelligence and law enforcement investigations.

How certain alternative payment systems may impact the primacy of the U.S. dollar, the efficacy of U.S. sanctions, and the ability for the U.S. to monitor financial crime

History teaches us that absolute dollar primacy will likely not last forever and the key is therefore thoughtful risk management.[5]

We are in the midst of a financial technology revolution. From cryptocurrencies and stablecoins to app-powered transactions and domestic payments systems, it is easier than ever to create alternative payments mechanisms that avoid the U.S. dollar altogether or minimize its importance.

Both adversaries and allies alike are exploring alternative payment systems that may intentionally or inadvertently circumvent the U.S. financial system.

China and Russia are currently working to diversify their currency reserves and expand their bilateral trade in non-dollar currencies. China has long chafed at the sanctioning power of the United States, and is developing both centralized domestic payments systems – from private

[5]https://seekingalpha.com/article/2447275-world-reserve-currencies-what-happened-during-previous-periods-of-transition “There have been 5 other major reserve currencies over the past 500 years."

payments apps, like WeChat Pay and Alipay, to China's central bank digital currency (CBDC) the e-CNY – and a cross-border interbank payment system that could, once adopted, enable China to trade with Russia, India, and other global trading partners without having to use the dollar.[6]

In response to sanctions against Russia for its initial invasion of Ukraine in 2014, the Kremlin developed a SWIFT alternative called the System for Transfer of Financial Messages (SPFS),[7] the MIR domestic payments system[8], and, just this month, the Bank of Russia and the country's Ministry of Finance, under stress of international sanctions, announced plans to allow for the use of cryptocurrencies in cross-border trade.[9] Similarly, last month Iran made its first official import order – worth $10 million, according to reports – using cryptocurrency, in a move intended to evade U.S. sanctions.[10]

We are not just talking about adversaries. Allies in Europe[11] and the United Kingdom have called for an international currency to "dampen the domineering influence of the U.S. dollar on global trade."[12] Likewise, we have seen examples of private-sector led financial innovations (like M-PESA) that were not designed to circumvent the U.S. financial system, but nonetheless have that effect, and have attracted tens of millions of users around the globe.[13]

Although we have seen movement toward these alternative payment mechanisms, none has emerged as a true threat to the U.S. dollar. The e-CNY is in its early stages, and it remains to be seen whether or not it is adopted beyond China's borders. SWIFT still remains the dominant messaging service for cross-border payments.[14] However, if we are, in fact, moving slowly toward a multi-polar currency world, how can we ensure that new payment rails are consistent with democratic values? How do we, as President Biden set forth in the March 9, 2022 Executive Order on Ensuring Responsible Develop
ment of Digital Assets (executive order), prioritize principles of privacy, security, and "the ability to exercise human rights,"[15] in this new financial system?

---

[6] https://www.brookings.edu/wp-content/uploads/2022/05/es_20220607_dollar_transcript.pdf
[7] https://www.bbc.com/news/business-60521822
[8] https://www.reuters.com/business/finance/russia-vows-continue-mir-card-expansion-after-new-us-sanctions-2022-09-16/
[9] https://cointelegraph.com/news/russia-aims-to-set-rules-for-crypto-cross-border-payments-by-year-s-end
[10] https://www.reuters.com/business/finance/iran-makes-first-import-order-using-cryptocurrency-tasnim-2022-08-09/
[11] https://www.reuters.com/article/us-eu-juncker-euro/eus-juncker-wants-bigger-global-role-for-euro-idUSKCN1LS0BK
[12] https://www.theguardian.com/business/2019/aug/23/mark-carney-dollar-dominant-replaced-digital-currency
[13] https://www.worldbank.org/en/news/feature/2018/10/03/what-kenya-s-mobile-money-success-could-mean-for-the-arab-world
[14] https://www.reuters.com/business/finance/eu-excludes-seven-russian-banks-swift-official-journal-2022-03-02/
[15] https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-respons

As non-democratic regimes attempt to build alternative payment rails through centralized government brute force, there is an alternative: enable the free market to innovate faster on solutions that incorporate democratic principles. One place this is happening today is with open blockchain technology.

We are already seeing blockchain technology lead to more competitive markets, grow the economy, and advance national security. For instance, financial services, such as stablecoins, built on common protocols enable consumers to send money from Company A to Company B in the same frictionless way you can send an email from Gmail to Hotmail. This reduces lock-in, leads to more competitive markets, and gives consumers lower prices and greater choice.

How stablecoins can strengthen the U.S. dollar

The vast majority of stablecoins operated by the private sector are backed 1:1 by national currencies. Tens of billions of dollars' worth of stablecoins are in circulation and, according to TRM Labs, as of September 2022, 99% of fiat-backed stablecoin value is tied to the U.S. dollar.[16]

The fact remains that entrepreneurs highly value the integrity, stability, and safety of U.S. financial institutions. One can imagine a world in which entrepreneurs create financial services products using a U.S. dollar-backed stablecoin even where those products otherwise have little to do with the United States. However, that world will not come to fruition by default; through effective and targeted regulations that support stablecoin issuers, the U.S. can promote the worldwide distribution of the dollar, including to many places that otherwise would have little nexus to the U.S. financial system.

How the technical properties of blockchain enable more effective and efficient detection and investigation of fraud and financial crime

The native properties of public blockchains — data that is Transparent, Traceable, Public, Permanent, Private, and Programmable — can enable financial integrity professionals, law enforcement, regulators, supervisors, and other government agency officials to more readily identify risks and more effectively and efficiently detect and investigate financial crime.

ible-development-of-digital-assets

[16] TRM analysis

Transparent

Information about illicit funds moving through the financial sector currently resides on thousands of private corporate servers located in the U.S. and overseas. To combat financial crime, governments rely on financial institutions having adequate internal systems and data to report instances of fraud, money laundering, terrorist financing, and financial crime to regulators and law enforcement via Suspicious Activity Reports (SARs) or ad hoc notifications.

The nature of public blockchains as open and distributed ledgers means that each transaction is verified and logged in a shared, immutable record, along with the timestamp of the transaction and the blockchain addresses involved. This data from the public blockchain is transparent, enabling the financial industry and government agencies to monitor trends in financial crime, market abuse, and financial stability in real-time and conduct more effective sectoral risk assessments.

The transparency of blockchain-based transactions provides visibility into illicit transaction volume that would otherwise be unattainable safely. For instance, the U.S. Department of Justice's press release on the disruption of the darknet market Hydra Market asserts that the market received approximately $5.2 billion in cryptocurrency for the purchase of illicit goods and services, such as illegal drugs, stolen financial information, fraudulent identification documents, and money laundering services.[17]

Traceable

For anti-money laundering compliance specialists and auditors working in traditional finance, cumbersome manual investigation is required to verify Source of Wealth and Source of Funds for a single customer, often requiring collecting information from independent sources such as company registries, banks, accountants, and lawyers. For government investigators, it may take can take months or even years to follow the trail of a sophisticated criminal, oftentimes requiring subpoenas across multiple service providers in various jurisdictions, necessitating law enforcement to go through the cumbersome Mutual Legal Assistance Treaty (MLAT) process to seek foreign law enforcement assistance to obtain evidence.

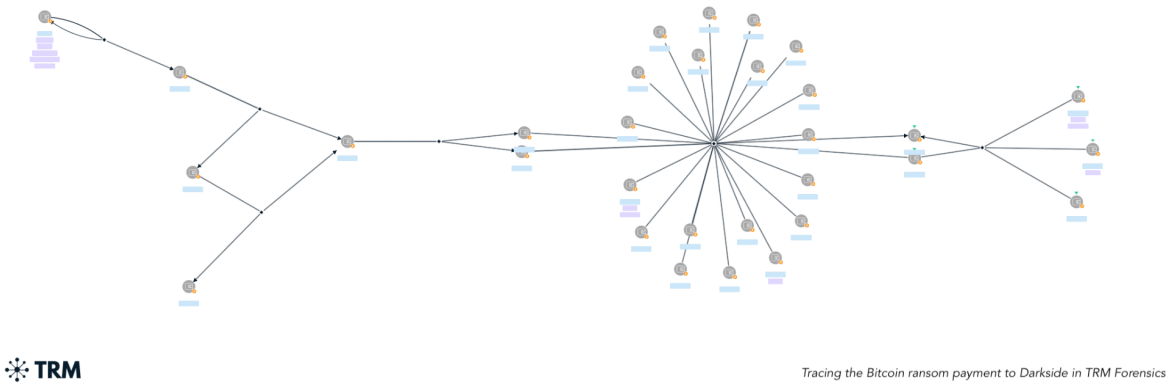
Because blockchains provide an immutable audit trail of every transaction, understanding the ultimate source and destination of funds, particularly across jurisdictions, is substantially easier, faster, and more reliable compared to tracing funds through traditional financing mechanisms. Blockchain intelligence software can transform the alphanumeric characters on the blockchain to

[17] https://www.justice.gov/usao-ndca/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace)

a visual representation of the flow of funds, allowing compliance specialists and law enforcement to "follow the money" around the world in real-time, accelerating investigation time.

The traceability of blockchain transactions also enables more advanced capabilities to detect suspicious activity. In traditional finance, compliance departments typically only view transactions to which they are a direct counterparty in order to measure risk. The consequence is that Transaction Monitoring rules are limited to behavioral patterns such as transaction type, amount, or velocity. With blockchain transactions, virtual asset exchanges can detect an incoming deposit of proceeds from a ransomware attack, even if the funds moved through multiple 'hops' or transactions before being deposited.

In the May 7, 2021, ransomware attack on Colonial Pipeline – an attack that shut down operations of the 5,500-mile pipeline that delivers 45% of the gasoline and jet fuel supplied to the U.S.'s east coast, causing gas lines closings and even school closings – law enforcement used blockchain intelligence to track, trace, and investigate the movement of the Bitcoin ransom payment.[18] Through the use of the blockchain and excellent police work, law enforcement was ultimately able to identify the destination of funds and seize the majority of the ransom payment. That recovery was possible because cryptocurrency was the medium of payment.[19]



Tracing the Bitcoin ransom payment to Darkside in TRM Forensics

[18] https://www.trmlabs.com/post/darkside-ransomware-report
[19] https://www.nytimes.com/2021/06/09/technology/bitcoin-untraceable-pipeline-ransomware.html

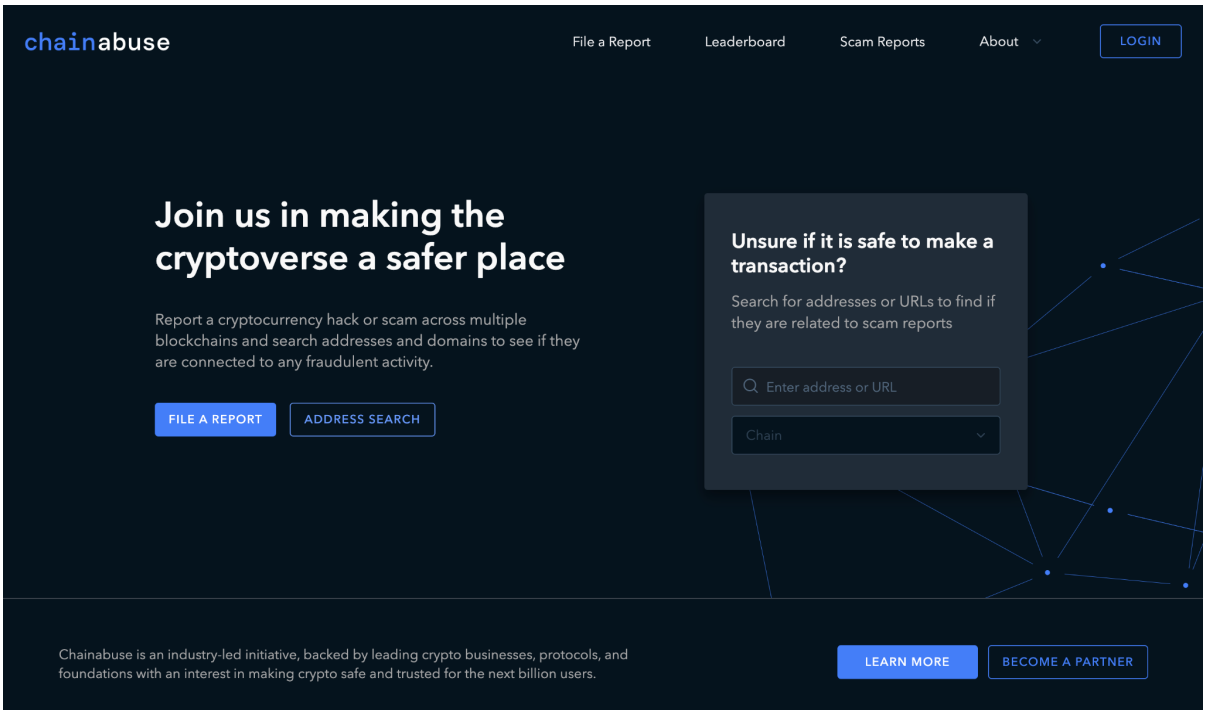
Public

Unlike transaction and customer data held by companies or financial institutions, public blockchains are distributed and not managed by a central authority. Thus, anyone — including law enforcement officials and regulators — can access, identify, and trace blockchain transactions without a SAR, subpoena, search warrant, MLAT, or on-site examination because that information is free and publicly accessible, independent of a third-party. In court, prosecutors are then able to present the blockchain as an objective "eyewitness" on a single transaction rather than rely on a witness, such as a law enforcement investigator.

Public blockchains enable law enforcement to link multiple victims together through on-chain transactional information, leading to more impactful investigations and disruptions. For instance, in the Frosties NFT fraud, a million-dollar scheme to defraud purchasers of NFTs advertised as "Frosties," investigators were able to see exactly the number of NFTs in question, determine the potential loss, and attempt to contact additional victims simply by observing public transactions on blockchains.[20]

[20] https://www.justice.gov/usao-sdny/pr/two-defendants-charged-non-fungible-token-nft-fraud-and-money-laundering-scheme-0

The public nature of blockchains enables greater information-sharing between consumers, enabling them to protect themselves from scams, hacks, and fraud. Through crypto fraud-reporting tools like Chainabuse.com, members of the public can increase visibility of notable schemes and limit further victims.[21]



Permanent

Storing transaction records for long periods of time is costly, cumbersome, and may be prohibited under local law. Consequently, records are often missing, creating hurdles for financial crime investigations. In contrast, transactions are permanently recorded on the blockchain, which allows institutions, auditors, and government investigators greater ability to "follow the money," even if the transaction is several years old.

In 2016, the virtual currency exchange Bitfinex was hacked and 120,000 BTC was stolen. In early 2022, two individuals were arrested for their alleged laundering of the stolen proceeds then valued at over $4.5 billion.[22] In the public statement of facts filed with the court for their arrest, blockchain transactions from 2017 appear to have played a large role in ultimately identifying the alleged launderers despite a years-long money laundering campaign.[23] Other cases such as

[21] https://www.chainabuse.com/
[22] https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency
[23] Id.

the Silk Road and Alphabay takedowns were successfully prosecuted because of breadcrumbs on the blockchain that happened months or years before the investigation.

Private

As more and more consumers, businesses, and governments transact on blockchains, it becomes even more important to enable financial privacy on blockchains, in order to protect consumer privacy, prevent corporate and nation-state espionage, reduce the risk of data breaches, and protect national security.

It bears emphasizing that privacy and blockchains are not incompatible. In many ways, blockchain-based technologies – by minimizing the need to store personal data in one centralized repository, by empowering individuals to assert control over who accesses their data, and by allowing individuals to determine for what purposes their data will be used – are *more* privacy-protective than the status quo.

Meanwhile, within the industry, Privacy-Enhancing Technologies (PETs) like zero-knowledge proofs are being deployed at the protocol, middleware, and application layers to advance data protection and privacy goals. PETs can be used to make information on blockchains private, such as transaction details or data on blockchain-based computer programs. Notably, PETs can be configured to make information selectively visible depending on certain conditions and policies, such as whether the requester is authorized to view the data.

Programmable

Blockchain provides a new opportunity to increase access to the financial system by reducing the cost of providing financial services. One example is compliance where blockchain allows for the integration of automated KYC/AML controls at the protocol, smart contract, and application layer.

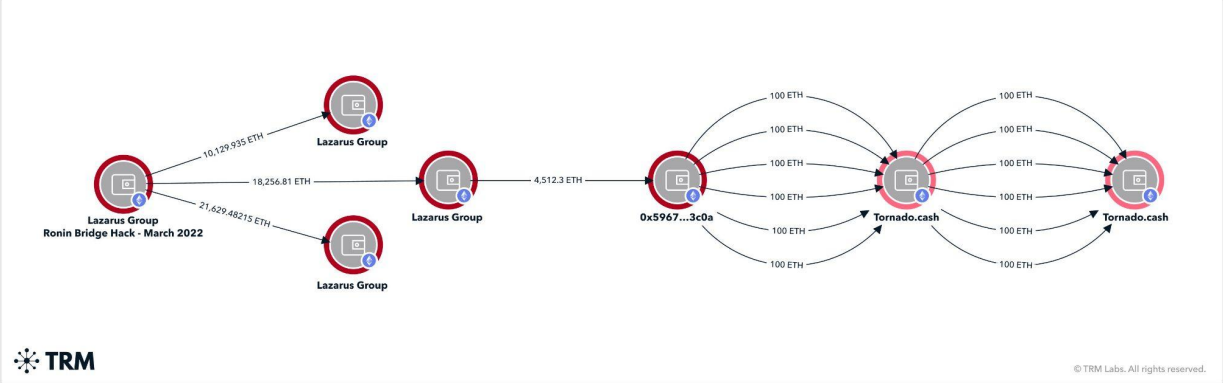
Blockchain-based “digital passports” could allow individuals and entities to store proof of KYC verification directly on the blockchain, a “win-win” for all parties—customers, institutions, and government—involved in transactions. Customers would seamlessly access financial services and minimize the distribution of sensitive personal information to new financial intermediaries. Developers could program automated approvals or denials directly into smart contracts and protocols to prevent sanctioned or other high-risk addresses from interacting with their services.

How the U.S.-based digital asset industry strengthens the efficacy of U.S. sanctions.

In a blockchain-based economy, sanctions are still a powerful tool and can be used as both a punitive measure and as a deterrent. For example, we have seen the U.S. Treasury's Office of Foreign Assets Control (OFAC) take a series of punitive actions related to Lazarus Group as North Korea – in the wake of crippling sanctions and global isolation – continues to attack cryptocurrency businesses at unprecedented speed and scale.[24] [25]

On March 23, 2022, North Korea's Lazarus Group struck the Ronin bridge, a service that allows users to move funds from one blockchain to another, stealing over $600 million in cryptocurrency that could potentially be used for weapons proliferation and other destabilizing activity.[26]

What followed was OFAC using blockchain intelligence to trace the stolen funds, sanctioning both the blockchain addresses to which the funds moved, and the mixing services that North Korean cybercriminals utilized to launder over a billion dollars of cryptocurrency – including centralized bitcoin mixer blender.io and decentralized Ethereum mixer Tornado Cash.[27] [28] These rapid sanctions designations were only possible because of the transparent nature of public blockchains. According to TRM analysis, total monthly deposits into Tornado Cash decreased by 68% in the month after it was sanctioned.[29]



[24] https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/BlockchainAnalysisEES.pdf?mtime=20220216090240&focal=none
[25] https://www.trmlabs.com/post/us-authorities-tie-north-koreas-lazarus-group-to-ronin-bridge-hack-through-ofac-sanctions
[26] https://www.fbi.gov/news/press-releases/press-releases/fbi-statement-on-attribution-of-malicious-cyber-activity-posed-by-the-democratic-peoples-republic-of-korea
[27] https://www.trmlabs.com/post/north-koreas-lazarus-group-moves-funds-through-tornado-cash
[28] https://www.trmlabs.com/post/u-s-treasury-sanctions-widely-used-crypto-mixer-tornado-cash
[29] TRM analysis

The strength of U.S. sanctions comes not from the primacy of the dollar alone, but also from the fact that the U.S. is the home to innovative companies and people who are transacting in a global economy. The key to effective U.S. sanctions is to ensure that the businesses that are leading in this new digital asset economy are in the U.S. and serve U.S. customers. Just as the most significant companies of the Internet age were born in the United States, so too can this new economy be incubated in the United States and other democracies. It is critical for economic competitiveness, but also national security.

In last week's framework, the Biden Administration wrote, "U.S. companies lead the world in innovation. Digital asset firms are no exception. As of 2022, the United States is home to roughly half of the world's 100 most valuable financial technology companies, many of which trade in digital asset services. The U.S. government has long played a critical role in priming responsible private-sector innovation. It sponsors cutting-edge research, helps firms compete globally, assists them with compliance, and works with them to mitigate harmful side-effects of technological advancement."[30] We must continue to foster responsible innovation and ensure that regulation provides essential guardrails to stem financial crime and protect consumers but, at the same time, remain technology neutral and foster innovation.[31]

The White House last week called for "U.S. leadership in the global financial system and economic competitiveness; financial inclusion; and responsible innovation."[32] This should be a clarion call to a race to create and serve businesses in this new economy. At the end of the day markets choose the reserve currency, not governments.

Recommendations

1. **Support the growth of dollar-backed stablecoins** operated by regulated U.S. entities by establishing rules that ensure the stability, security and interoperability of regulated stablecoins.
2. **Deepen U.S law enforcement training and operational capacity on blockchain-related investigations** at both the local and federal levels, and expand capacity-building efforts with foreign law enforcement partners.
3. For the United States to remain the world's leader in digital asset innovation, **responsible actors need clear, concise, and timely guidance on sanctions implementation**. Congress should require executive branch agencies to provide that guidance upon request, and to act on license applications within a specified period of time.

[30] 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/
[31] Id.
[32] Id.

Conclusion

Today there are new and emerging challenges to our financial system, but there are also tremendous opportunities. Every morning when I walked by that painting of Alexander Hamilton I reflected on a quote from Lin Manuel Miranda's musical: "What is a legacy? It's planting seeds in a garden you never get to see." This is our legacy, our opportunity to plant the seeds to ensure that democratic principles grow with an evolving financial system.